Country Case Studies Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation

Samantha Bradshaw, Ualan Campbell-Smith, Amelie Henle, Antonella Perini, Sivanne Shalev, Hannah Bailey & Philip N. Howard.

Methodology Notes

These are the background case notes complied for Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation. For details on the methods behind this content analysis please see the methodology section of the report. This document contains data from over 1300 sources organized by country. The sources include high quality news articles, academic papers, white papers, and a range of other grey literature. As an annotated bibliography, the country cases here make use of significant passages from these secondary sources, and every effort has been made to preserve full citation details for future researchers. The full list of references can be found in our public Zotero folder.

Table of Contents

Angola

Introduction

Angola is not considered a free country by the Freedom House organisation (Freedom House, 2019a). was gained in 1975, the party Popular Movement for the Liberation of Angola (MPLA) has been in power. José Eduardo dos Santos was president for 38 years until João Lourenço took over after his election victory in August 2017. While the election went quite peacefully and was well organised according to the African Union election overseers, pro-government media, deficiencies in voter registration and the fact that the MPLA used government resources for their campaign gave them an unfair advantage. Oppositional parties called the election fraudulent, but the High Court of Angola dismissed the claims and instead accused them of providing fraudulent evidence themselves (Freedom House, 2019a).

The internet is one of the less tightly controlled forms of media available in Angola (Freedom House, 2019b), however access within the country is one of the lowest in the world with a penetration rate of only 21% in December 2019 (Internet World Stats, 2020). Concerning social media, in early 2020 Facebook is by far the most prevalent (82% of social media use), followed by Instagram and Pinterest (roughly 5% each) (GlobalStats, 2020). The main reason for these low rates is likely the cost of internet and mobile phone subscriptions, which are much higher compared to neighbouring countries (Freedom House, 2019b). For these reasons, conventional media sources such as print newspapers or the radio are the main resource for information in Angola.

An Overview of Cyber Troop Activity in Angola

Organizational Form

The Angolan government owns most of the media in the country and most influential outlets in Angola which are based outside of the country are usually privately owned by MPLA members and work as mouthpieces for the party. Additionally, the MPLA and its members are involved with owning service providers (TV, Radio and increasingly internet providers) and prevent any media criticism from reaching Angolan citizens (Freedom House, 2019).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Angola

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
	Evidence found	Evidence found	Evidence found		

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Given that most outlets and service providers are owned by the government or party members, the MPLA has a significant degree of control over what news gets broadcasted. Recently, the party appears to be going through something of a power-struggle, with some party members appearing displeased with President Lourenço as he is supporting the prosecution for corruption of family members and political servants of former President dos Santos (Freedom House, 2019a). How or if that has affected the party's general control over the media or their influence and disinformation campaigns remains unclear.

Activists and journalists critical of the Angolan government have been prosecuted regularly in the past, leading to a great deal of self-censorship (Freedom House, 2020). However, President Lourenço has replaced several heads of media outlets and urged them to serve the public interest rather than individual politicians. At the same time, Lourenço established the Angolan Regulatory Body for Social Communication (ERCA) in 2017, which is able to investigate journalists and producers of online content without judicial oversight and can ban websites that are not adhering to "good journalism". Moreover, a new penal code allows for jailing and fining individuals for acts such as spreading fake news, defamation, and "abuse of press freedom", which Freedom House (2019b) deems somewhat contrary to the president's pledge to increase media freedom in the country. Nevertheless, it appears that journalists are becoming more confident in highlighting cases of corruption and governmental misconduct through online platforms.

While the government does not seem to be actively censoring or blocking the internet, they do have the ability to do so at least partially through the state-owned Angola Telecom (BizCommunity, 2017). They are starting to pay more attention to the internet, as social media bots made up about 9% of online traffic during the 2017 election, a majority of which originated abroad (How Africa Tweets, 2018). Only journalists and media organisations had more influence on public opinion, while politicians themselves remain somewhat absent from online debates (Lea, 2018). Notably, there is fairly little information available regarding online bot activity, so their exact origins and intentions are not well known. Moreover, social media platforms such as Facebook's Messenger and WhatsApp are the most popular apps in Angola and Africa overall, making the tracking of information difficult (Dahir, 2018).

In May 2019 Facebook announced that it had taken down a set of 265 Facebook and Instagram pages that were producing "inauthentic behaviour" towards African countries, including Angola. From December 2012 onwards over US$800,000 was spent on political ads primarily paid for by Archimedes Group, a political consultancy firm based in Israel. These ads targeted specific elections to promote or attack local politicians, though most of the efforts appear to have targeted the latest Nigerian election. In Angola, the focus was on just a few, health related Facebook pages (Bright, 2019; DFRLab, 2019). It remains unclear who paid the Archimedes Group for this operation (Timberg & Romm, 2019). The incident, however, highlights once again that most cyber troop activity in Angola has little to no connection to Angolan political actors, even though they may be profiting from it. Still, many politicians and ministries have established Twitter accounts to inform citizens on latest government actions and provide advice. These activities have increased significantly during the COVID-19 crisis (Tyburski, 2020), but there is little evidence of disinformation or other forms of manipulation by official channels.

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Angola

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Bots, Fake Human	Pro-Government Support, Attack Opposition	Disinformation, Amplification	Facebook (Messenger) Twitter WhatsApp Instagram

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

At present, there seems to be very limited cyber troop capacity in the country. However, the Angolan government seems to be increasingly cooperating with China on surveillance and security: in December 2019 President Lourenço opened the Integrated Centre for Public Security financed by China and operated by forty-five employees who were trained in China (Macauhub, 2020). Additionally, in early 2019 it was announced that Angola and Rwanda had signed a deal to cooperate on security and public order in the interest of their citizens. This cooperation reportedly includes the sharing of technical advice and information of interest to law enforcement, though observers suggest that the development and execution of the project will take years (Agência Angola Press, 2019; Kuteesa, 2019). Whether these activities also reflect intentions by the Angolan government to establish or increase their cyber troop capabilities remains somewhat unclear, however, reports indicate that Angola is starting to increase their activities and capacity: the state has been planning to invest 11 million USD a year into cybersecurity, and opposition parties have accused the MPLA of targeted disinformation campaigns against them (Agência Angola Press, 2019; VOA, 2020).

Table 3: Cyber Troop Capacity in Angola

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
	11 million annually	Temporary	Decentralised	Low

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

References

Agência Angola Press. (2019a, February 27). Angola and Rwanda strengthen public security partnership—Politics—Angola Press—ANGOP. *Http://Www.Angop.Ao*. http://www.angop.ao/angola/en_us/noticias/politica/2019/1/9/Angola-and-Rwanda-strengthen-public-security-partnership,dcd58b0b-e01c-4f55-9a20-4ad5a8a27c27.html

Agência Angola Press. (2019b, July 26). State to spend USD 11 million / year on cyber security—Economy—Angola Press—ANGOP. *Http://Www.Angop.Ao*. http://www.angop.ao/angola/en_us/noticias/economia/2019/6/30/State-spend-USD-million-year-cyber-security,2283adbf-4b93-4344-96c3-e3cb3148c144.html

BizCommunity. (2017, August 22). Angola is emerging as a growing tech hub on the continent. *BizCommunity*. https://www.bizcommunity.com/Article/7/16/166368.html

Bright, J. (2019, May 20). Facebook's latest account purge exposes Africa's misinformation problem. *TechCrunch*. https://social.techcrunch.com/2019/05/20/facebook-account-purge-africa-fake-news/

Dahir, A. L. (2018, July 18). How social media bots became an influential force in Africa's elections. *Quartz Africa*. https://qz.com/africa/1330494/twitter-bots-in-kenya-lesotho-senegal-equatorial-guinea-elections/

DFRLab. (2019). *Inauthentic Israeli Facebook Assets Target the World*. Digital Forensics Lab. https://medium.com/dfrlab/inauthentic-israeli-facebook-assets-target-the-world-281ad7254264

Freedom House | Angola. (2019a). *Angola | Freedom House*. Freedom House. https://freedomhouse.org/country/angola/freedom-world/2019

Freedom House (2019b) *Freedom on the Net: Angola*. (2019). Freedom House. https://freedomhouse.org/country/angola/freedom-net/2019

GlobalStats. (2020, March). *Social Media Stats Angola*. StatCounter Global Stats. https://gs.statcounter.com/social-media-stats/all/angola

How Africa Tweets. (2018). *How Africa Tweets 2018*. https://portland-communications.com/publications/how-africa-tweets-2018/

Internet World Stats. (2020, March 26). *Africa Internet Users, 2020 Population and Facebook Statistics*. https://www.internetworldstats.com/stats1.htm

Kuteesa, H. (2019, February 28). Rwanda, Angola sign deal to bolster security, public order. *The New Times | Rwanda*. https://www.newtimes.co.rw/news/rwanda-angola-sign-deal-bolster-security-public-order

Lea, J. (2018). *The influencers behind Twitter in Africa*. Portland Communications. https://portland-communications.com/philanthropy/the-influencers-behind-twitter-in-africa/

Macauhub. (2020, January 6). *Chinese cooperation strengthens security in Angola and Cabo Verde* [Established in 2005, by the Government Information Bureau of the Macau Special Administrative Region (MSAR), Macauhub aims to promote the MSAR as a platform for developing ever-closer economic and trade ties between China and the Portuguese-speaking world.]. https://macauhub.com.mo/feature/pt-cooperacao-chinesa-reforca-seguranca-em-angola-e-cabo-verde/

Timberg, C., & Romm, T. (2019, May 16). Facebook shuts down Israel-based disinformation campaigns as election manipulation increasingly goes global. *Washington Post*. https://www.washingtonpost.com/technology/2019/05/16/facebook-shuts-down-israel-based-disinformation-campaigns-election-manipulation-increasingly-goes-global/

Tyburski, L. (2020, March 24). African leaders respond to coronavirus... On Twitter. *Atlantic Council*. https://atlanticcouncil.org/blogs/africasource/african-leaders-respond-to-coronavirus-on-twitter/

VOA. (2020, April 21). UNITA acusa MPLA de campanha de desinformação contra o seu líder. *VOA*. https://www.voaportugues.com/a/unita-acusa-mpla-de-campanha-de-desinformação-contra-o-seu-líder/5383941.html

Argentina

Introduction

According to Freedom House, Argentina has a good Internet freedom ranking when compared to other Latin American nations, with a score of 85 (Freedom House, 2020). Nonetheless, the country has reported organized social media attacks against at least 51 journalists in 2018 and 132 in 2017 (Shahbaz & Funk, 2019) – particularly targeting those who reported against the government (for example, outing corruption scandals), and who have been besieged with aggressive tweets (Shahbaz, 2018). Another report, issued by Reporters Without Borders (Reporters Without Borders, 2020), points to a significant drop in Argentina's press-freedom ranking from 52 to 57.

As a result of the increasing use of manipulation techniques online in political campaigns, in late 2018 Argentina's Electoral Council announced measures to tackle this phenomena in subsequent general elections. Measures included the auditing of digital electoral campaigns, including online manipulation techniques, and the publication of the official websites and social media accounts of candidates (El Pais, 2019; Shahbaz & Funk, 2019) Additionally, these measures included requirements on political parties and digital agencies to adhere to an ethical digital commitment and mitigate negative effects of manipulation techniques online (Cámara Nacional Electoral, 2019; Shahbaz & Funk, 2019).

An Overview of Cyber Troop Activity in Argentina.

Organizational Form

A UK Parliament report has found that Cambridge Analytica had a local partnership with the SCL group, and that it participated in an information campaign against Cristina Fernández de Kirchner. Alexander Nix, former Cambridge Analytica CEO, confirmed this involvement during a hearing at the UK Parliament (House of Commons: Digital, Culture, Media and & Sport Committee, 2019). Although that campaign was favorable to Mauricio Macri's candidacy and success during elections, Cambiemos has denied its involvement with Cambridge Analytica.

There is also evidence of social media experts and agencies working for political campaigns and using manipulation techniques. Gastón Douek, known locally as "the Lord of the Trolls", was responsible for the political campaigns of Martín Lousteau, Sergio Massa, Juan Schiaretti, Gabriela Michetti, and Omar Perotti (Alconada Mon, 2019b). Not only did he admit to having used automated and human trolls in Argentina, but also being involved in Mexican political campaigns in 2012 (Alconada Mon, 2019c). He worked for the intelligence service of Ecuador, negotiated with Cambridge Analytica (Alconada Mon, 2019b), and most recently was involved in trolling activities against players of the Barcelona Football Club (*«El señor de los trolls»: Un argentino, implicado en el escándalo que hace temblar a Barcelona*, 2020). Local newspaper La Nación identified other agencies engaged in the use of manipulation techniques online, such as Publiquest, Nicestream, Influencia2, and Becom1 (Alconada Mon, 2019b).

Additionally, during Macri's administration the opposition presented an 80-page report which claimed that Cambiemos financed an organized structure that harassed political opponents, disseminated disinformation, using both bots and human fake accounts (LPO, 2018). Although the report identified the paid public servants that were part of this group, Cambiemos denied its existence.

Filer and Fredheim (2016) gave evidence on the use of bots on Twitter during presidential campaigns in 2015 by the two most popular coalitions, Frente para la Victoria and Cambiemos. Two years later, the Electoral Council published a document where it audited the activities of online trolls during the legislative elections, giving evidence on the use of this tactic by several political parties (Cámara Nacional Electoral, s.f.). In 2019 pro-government and anti-government human and automated accounts amplified content and harassed opposition (Alconada Mon, 2019a).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Argentina

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
2012	Evidence found	Parties: Juntos por el Cambio and Frente de Todos (2019), Unidad Porteña, Unidad Ciudadana, and Cambiemos (2017), Cambiemos and Frente para la Victoria (2015) Politicians who used Gaston Douek's services: Martín Lousteau, Sergio Massa, Juan Schiaretti, Gabriela Michetti, and Omar Perotti	Cambridge Analytica, Publiquest, Nicestream, Influencia2, Becom1, Gaston Douek		

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

In 2018 Amnesty International released a report in which it analyzed tweets engaging with eleven journalists and activists who were attacked intensively on social media. Between October and November 2017, 354,000 tweets engaged with these accounts, and 53.2% of the attacks came from automated accounts (Amnesty International, 2018). The content of these messages discredited political parties and civil organizations, but often would be directed to public institutions, such as the national healthcare system or the judiciary. One campaign promoted the conspiracy theory that chemotherapy was the cause of death of cancer patients, and not cancer itself (Slipczuk, 2019).

In 2017, after the disappearance/death of the Argentine activist Santiago Maldonado, social media content was particularly polarized. Whilst the Twitter community associated with the opposition was led by politicians, the most active pro-government accounts were anonymous or fake accounts (Arugete & Calvo, s. f.).

Both pro-government and anti-government trolls were highly active during the general election campaign in 2019 and mainly used strategies of trolling and amplification in order to create pro-government and pro-party content (Alconada Mon, 2019a). Over the years a number of fake accounts have accumulated a considerable number of followers and these were crucial for amplification strategies (Arugete & Calvo, s. f.)

One of the main occurrences in 2019 was the mass posting of incoherent messages by fake accounts, which made visible the use of bots for amplification. The messages contained the hashtag #YoVotoMM, expressing support for Mauricio Macri, but they shared many common grammatical errors, incoherence, and phrases (Esteban, 2019).

Disinformation in Argentina has been reported on many platforms and strategies vary from 'pro-government' campaigns to discrediting the opposition. Experts report the use of 'para-addressee' strategies, where disinformation not only attacked a particular party ('counter-addressees'), but also intended to provide explanatory information to third parties, or 'para-addressees' (Aruguete, 2019).

Disinformation peaked in 2018 during the discussion on the legalization of abortion. Argentinian society was strongly polarized between political and civil society groups for and against the legalization of abortion. Fabricated stories reported a legal abortion (abortion was already permitted for pregnancies resulting from rape) where the fetus would have "agonized to death on a hospital tray during 10 hours" ("Falso En Las Redes," n.d.). Such disinformation led to the verbal and physical harassment of people involved in the case, including journalists and the judge who authorized the victim's abortion.

Strategies also included promoting a sense of national unity and resistance against a common enemy. One fabricated image made up a quote attributed to Winston Churchill: "If Argentina ever got organized it would rise and lead Latin America behind it". This story sought not only to instill nationalism, but also to stoke pre-existing historical tensions with the United Kingdom (Gardel, 2019).

Another distinct trend was the use of references to regional geopolitics in order to address political ideologies. Edited images portrayed former Brazilian president Luis Inacio Lula da Silva watching current president Jair Bolsonaro on TV from a penitentiary ("Falso En Las Redes," n.d.). Fake accounts of Nicolas Maduro were also created on Instagram and Facebook, with an edited image implying the accounts had been verified.

In 2019, the Reverso alliance between fact-checkers, media, and tech companies monitored and fact-checked widely disseminated and/or relevant content in social media and instant messaging apps. The most widespread disinformation on Facebook targeted politicians from the two main coalitions. An old speech of presidential candidate Alberto Fernández was manipulated with the intention to make it seem like he called Néstor Kirchner and Cristina Fernández de Kirchner "thieves". Fake information on how former President Nestor Kirchner died also spread massively. Other high-profile political and governmental figures were also targeted by disinformation campaigns. The first fake content to emerge during the electoral campaign was a manipulated video of Minister of Security Patricia Bullrich looking drunk, while content about a fake mansion supposedly belonging to María Eugenia Vidal, governor of Buenos Aires province, was among the top four most widely disseminated content. On Twitter disinformation about Alberto Fernández, Ofelia Fernández, as well as restrictions on the purchase of currency in other countries in the region were shared most widely. Disinformation shared via WhatsApp focused, among other things, on Macri's health and changes in the National Law on Education. («Los falsos más virales de la campaña que desmintió Reverso», 2019)

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Argentina

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Automation, Human, Fake and Real	Pro-government and pro-party, Attacks on opposition, Trolling, Distracting messages	Creation of disinformation, Mass reporting content, Data-driven strategies, Trolls, Amplification strategies	Twitter, Facebook, WhatsApp, Instagram

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

Legislative changes in 2017 included digital advertising as a form of regulated political advertisements; coincidentally or not, the government reduced its budget on advertising by 7%. The journalist Marco Bonelli estimated the investments at around 200 million pesos (El Pais, 2018).

Although there is not much evidence-based information on government or political parties' cyber troop capacities in Argentina, it is worth noting the existence of volunteer-led manipulation activities. In 2019, Ariel Garbarz and other Peronist, Socialist, Communist and Trotskyist activists coordinated anti-Macrist campaigns on Twitter (Gian, 2020a). On the opposing side, the Macrist volunteer cyber troops organisation *Banquemos* was founded in 2015 and is led by Ricardo Benedetti, a former public servant. In 2019 it gathered activists from the three political parties of the coalition Juntos por el Cambio. This group coordinated efforts to attack the opposition and call for rallies on Twitter, Facebook, and WhatsApp. They also propagated such narratives as "if the Kirchnerist come back, we'll be Venezuela". There are around fifteen people involved at the national level, but they also have district and city coordinators (Gian, 2020b).

Table 3: Cyber Troop Capacity in Argentina

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
-	-	Temporary	Decentralised	Low

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

References

Alconada Mon, H. (2019a, August). Guerra de trolls: La disputa electoral en las redes sociales. *La Nación*. https://www.lanacion.com.ar/politica/guerra-trolls-disputa-electoral-redes-sociales-nid2274363

Alconada Mon, H. (2019b, September). «El señor de los trolls»: Así funciona el mundo de las campañas sucias y las bases de datos irregulares. *La Nación*. https://www.lanacion.com.ar/politica/el-senor-de-los-trolls-asi-funciona-el-mundo-de-las-campanas-sucias-y-las-bases-de-datos-irregulares-nid2286145

Alconada Mon, H. (2019c, September). Gastón Douek: «No me adjudico ninguna fake news; ponemos sobre la mesa hechos reales». *La Nación*.

https://www.lanacion.com.ar/politica/gaston-douek-no-me-adjudico-ninguna-fake-news-ponemos-sobre-la-mesa-hechos-reales-nid2286146

Amnesty International (2018). *El debate público limitado. https://amnistia.org.ar/wp-content/uploads/delightful-downloads/2018/03/online-pre1.pdf*, 2018

Arugete, N., & Calvo, E. (s. f.). *El patrullaje anónimo*. Revista Anfibia. http://revistaanfibia.com/ensayo/el-patrullaje-anonimo/

Aruguete, N. (2019, January 7). Las agresiones en las redes sociales | Martín Becerra y Ernesto Calvo, investigadores de la violencia en entornos virtuales. *PAGINA12*. https://www.pagina12.com.ar/166754-las-agresiones-en-las-redes-sociales

Cámara Nacional Electoral. (2019). *Compromiso Ético Digital*. https://www.electoral.gob.ar/nuevo/paginas/pdf/CompromisoEticoDigital.pdf

Cámara Nacional Electoral. (s. f.). *Documento TROLLS. https://www.electoral.gob.ar/nuevo/paginas/pdf/DocumentoTROLLS.pdf*

El Pais. (2018, October 29). Trolls, bots y fake news en campaña | La Cámara Electoral pone el ojo en las redes sociales de cara a las próximas elecciones. *PAGINA12*. https://www.pagina12.com.ar/151844-trolls-bots-y-fake-news-en-campana

«El señor de los trolls»: Un argentino, implicado en el escándalo que hace temblar a Barcelona. (2020, February). https://www.lanacion.com.ar/deportes/futbol/barcelona-trolls-escandalo-messi-bartomeu-nid2335005

Esteban, P. (2019, August). El troll center no satisface a Mauricio | El hashtag “YovotoMM” fue tendencia, aunque terminó quedando en ridículo. *Página 12*. https://www.pagina12.com.ar/211268-el-troll-center-no-satisface-a-mauricio

Filer, T., & Fredheim, R. (2016). Sparking debate? Political deaths and Twitter discourses in Argentina and Russia. *Information, Communication & Society*, *19*(11), 1539-1555.

Gardel, L. (2019, January 24). *No, Winston Churchill no dijo: “No dejen que la Argentina se convierta en potencia, arrastrará tras ella a toda América Latina”*. Chequeado. https://chequeado.com/el-explicador/no-winston-churchill-no-dijo-no-dejen-que-la-argentina-se-convierta-en-potencia-arrastrara-tras-ella-a-toda-america-latina/

Gian, D. (2020a, January 21). Quién es el profesor de los «trolls» K. *Noticias*. https://noticias.perfil.com/noticias/politica/quien-es-el-profesor-de-los-trolls-k.phtml

Gian, D. (2020b, January 26). El blanqueo de los “trolls” M. *Noticias*. https://noticias.perfil.com/noticias/politica/el-blanqueo-de-los-trolls-m.phtml

Los falsos más virales de la campaña que desmintió Reverso. (2019, December 10). *Reverso*. https://reversoar.com/los-falsos-mas-virales-de-la-campana-que-desmintio-reverso/

LPO. (2018, October 3). *La oposición acorraló a Marcos Peña con denuncias sobre el uso de trolls*. La Política Online. https://www.lapoliticaonline.com/nota/115454-la-oposicion-acorralo-a-marcos-pena-con-denuncias-sobre-el-uso-de-trolls/

Reporters Without Borders. (2020). *Argentina: Endangered state media, police violence | Reporters without borders*. RSF. https://rsf.org/en/argentina

Shahbaz, A. (2018). *Freedom on the Net 2018: The Rise of Digital Authoritarianism*. Freedom House. https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism

Shahbaz, A., & Funk, A. (2019). *Argentina | Freedom House*. Freedom House. https://freedomhouse.org/country/argentina/freedom-net/2019

Slipczuk, M. (2019, January 2). #FalsoEnLasRedes: Las principales fotos, videos y noticias falsas que circularon por redes sociales en 2018 – Chequeado. *Chequeado*. https://chequeado.com/el-explicador/falsoenlasredes-las-principales-fotos-videos-y-noticias-falsas-que-circularon-por-redes-sociales-en-2018/amp/

AUSTRALIA

Introduction

Computational propaganda in Australia originates from domestic political organisations as well as foreign actors. Social media remains popular—with 95% of Australian Internet users on Facebook and 19% on Twitter. The Reuters Institute found that 73% of Australians enlist online sources in their news consumption, while 45% rely on social media (Fisher, 2019). In this context, two important events in the past year have highlighted the influence of computational propaganda in Australia. The federal election took place on 18 May 2019, and having been in government since 2013, The Liberal-National Coalition ('the Coalition') won the election under Prime Minister Scott Morrison. During the campaign, there was a proliferation of disinformation spread by multiple political parties. Likewise, the bushfire crisis in January 2020 saw a surge in trolls, bots and conspiracy theorists manipulating online debates. Analysis suggested that bot and troll accounts were involved in a 'disinformation campaign' about the crisis (Knaus, 2020). Dubbed Australia's 'black summer', this contributed to a heightened public awareness of the online manipulation of public opinion. Buzzfeed documented the spread of false and misleading theories about the bushfires, ranging from claims that the fires were started by environmentalists or Muslims, to images that misrepresented the scale of the fires (Wilson, 2020). This resulted in an increase in climate denialism on Facebook (Ryan & WIlson, 2020), as well as traditional media outlets peddling misinformation that fires are no worse than previous years (Cave, 2020).

An Overview of Cyber Troop Activity in Australia

Organizational Form

State Actors

Freedom House (2019) note that the Australian government does not manipulate online sources of information to advance its political interests. The government does act to counter foreign cyber troop activity. In response to online foreign influence attempts, in June 2018 the creation of the Electoral Integrity Assurance Task Force was announced, responsible for identifying and managing risks from cyber-attacks and electoral interference (Ziebel, 2018). The task force includes the Australian Electoral Commission (AEC), the Department of Home Affairs, the Australian Cyber Security Centre, and the Australian Security Intelligence Organisation. It investigated social media communications during the election and found eleven examples of illegal practice (Barbaschow, 2020).

Australia passed several bills in 2018 to protect domestic politics from foreign influence: the National Security Legislation Amendment Bill, the Foreign Influence Transparency Scheme Bill and the Telecommunication and Other Legislation Amendment Bill. In March 2019, Facebook suspended a network of accounts that purported to represent political communities in Australia, but originated from North Macedonia and Kosovo (Facebook Newsroom, 2019). As a precautionary measure, Facebook temporarily banned non-Australians from purchasing political advertisements in an attempt to combat foreign interference in the lead-up to the 2019 federal election (Westbrook, 2019). Following the election, the Electoral Integrity Assurance Taskforce did not identify foreign interference.

The Director-General of the Australian Signals Directorate (ASD), Mike Burgess, spoke at the Lowy Institute in March 2019 and detailed some of the ASD's offensive cyber capabilities. One such capability was the ASD's 'covert online operators'—indicating that "some activities involve ASD operators assuming false online identities to disrupt terrorist networks" giving the example of an operative who “typed in deliberately broken English and was so convincing, she was able to influence the man’s behaviour” (Burgess, 2019). In a military capacity, Australia has consolidated its cyber and information operations under the Information Warfare Division, formed in 2017 within the Department of Defence (Australian Government, 2020).

Political Parties

The 2016 federal election was dubbed the “Facebook election,” as political parties turned to social media to assist with campaigning (Wordsworth, 2016). Since then, social media have remained central to political parties’ campaign strategies. Freedom House (2019) noted that the 2019 election featured a “proliferation of online disinformation spread by domestic political parties”, and Facebook removed two instances of ‘coordinated inauthentic behaviour’ during the election (Murphy, 2019).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Australia

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
2016	Australian Signals Directorate	Labor Party, Liberal Party, United Australia Party, Bill Shorten, Scott Morrison, Tony Abbott			X

Source: Authors’ evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Disinformation

The 2019 federal election was “littered with false and exaggerated claims” which were propagated by fringe groups, anonymous pages, and major political parties (Knaus, 2019). The most contentious case of disinformation during the election was the rumour that the Labor Party would implement a ‘death tax’ (a 40% tax on inheritance). *The Guardian* reported that the rumour “appears to have begun on unsourced Facebook pages, spread to other users via direct messages and paid ads, before finally being amplified by Coalition politicians” (Knaus, 2019). The Labor Party notified Facebook of the rapid circulation of the false claim, including allegations that there was ‘orchestrated message forwarding’ on Facebook messenger (Murphy et al., 2019). Facebook was criticised for failing to remove the ‘death tax’ content, despite it being deemed false by the platform’s third-party fact checkers (Murphy, 2019).

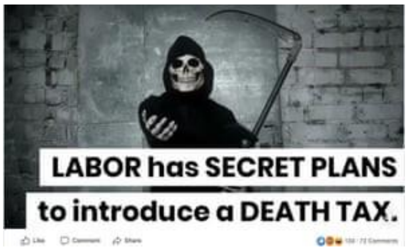


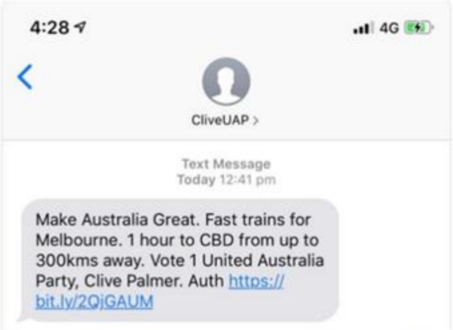
Figure 1: Labor’s ‘Death Tax’ disinformation on Facebook (Murphy, 2019)

Memes

Political memes are created and spread by digital marketing agencies, citizen groups and political parties. This can be particularly deceptive as memes fall outside of guidelines on political advertising. In fact, The New Daily reported that ‘weaponising memes’ was an “unexpected hallmark of the 2019 federal election” (Butler, 2020). Digital marketing agency Topham Guerin worked with the Liberal Party in that election, running a “24-hour meme machine” to disseminate “attention-grabbing, emotion-manipulating, behaviour-nudging messaging” (Workman & Hutcheon, 2019). Political meme pages were created in support of political parties, such as Innovative and Agile Memes (supporting The Coalition), The National Party of Memes (supporting Nationals), and ALP Spicy Meme Stash (supporting the Labor Party), leading to Buzzfeed to report on the use of “weaponised memes in Australia” (Esposito, 2018). The *Sydney Morning Herald* reported that a coalition of alt-right Facebook groups working with staff of the United Australia Party produced fake news, racist memes and messages against Labor and the Greens, which were liked and shared more than a million times during the campaign (Gladstone, 2019).

SMS Messages

A computational campaigning effort was undertaken by the United Australia Party during the Queensland election to the House of Representatives in January 2019. Financed with at least A$50 million (£27,232,500) from Clive Palmer, who also founded the party, SMS messages were sent to at least 5.4 million Australians (Figure 2). While many reactions were unfavourable — questioning where Palmer’s team got the numbers from—this activity was technically legal according to the Australian Communication and Media Authority who state on their website: “Australians can be contacted by phone, email, SMS in the lead up to election to seek views and influence your vote”. Palmer said that they would continue their campaigning effort including SMS messages and that there was no limit to the amount of money that would be spent (Mourad, 2019).

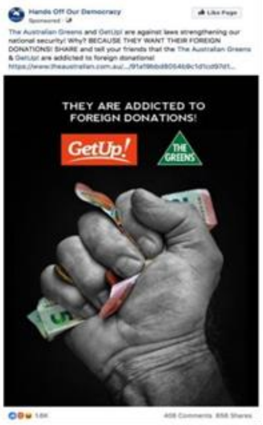


Make Australia Great. Fast trains for Melbourne. 1 hour to CBD from up to 300kms away. Vote 1 United Australia Party, Clive Palmer. Auth https://bit.ly/2QjGAUM

Figure 2: United Australia Party’s SMS Campaign (Mourad, 2019)

Political Advertisements

The Guardian found that Facebook ads from the party pages of Labor and the Coalition tended to be negative, often attacking the opposition party, whereas individual politicians’ pages had positive messaging (Evershed, 2019). Major parties used Facebook’s features of targeting ads at specific demographics, interests, and locations. Throughout the federal election campaign, the AEC received five hundred complaints about political advertising, of which ninety related to social media (Knaus & Karp, 2019). Although unauthorised paid electoral ads are in breach of the Commonwealth Electoral Act, anonymous, fringe groups paid to push political messaging on platforms such as Facebook. For example, *The Guardian* found an anonymous page ‘South Australian Conservative Support Page,’ which supported Liberal candidate Georgina Downer (Evershed, 2019). Similarly, ABC News reported on the page ‘Hands off our Democracy’ which contained no information about who was behind the group, despite using sponsored ads, to attack The Greens and activist group GetUp! (Figure 3). The AEC reported the page to Facebook, but it was deleted before action was taken (McGrath, 2019).



Hands Off Our Democracy
Sponsored

The Australian Greens and GetUp! are against laws strengthening our national security! Why? BECAUSE THEY WANT THEIR FOREIGN DONATIONS! SHARE and tell your friends that the The Australian Greens & GetUp! are addicted to foreign donations!
https://www.theaustralian.com.au/.../91af9bbd8054b8c1d1cd97d1...

Figure 3: ‘Hands off our Democracy’ (McGrath, 2019)

Conspiracy Theories

During the bushfire crisis in January 2020, disinformation and conspiracy theories spread about the cause of the fires. Conspiracy theories tended to focus on denying the impact of climate change and blaming The Greens. Disinformation spread across social media, entered major news outlets, was spread by government members of parliament, and was even picked up by American right-wing conspiracy theorists like Alex Jones (Knaus, 2020). Researchers discovered manipulative activity on Twitter around the #ArsonEmergency hashtag, which proposed the theory that arsonists were the cause of the bushfires, negating the role of climate change (Graham & Keller, 2020). There was evidence of misinformation and bot- and troll-like behaviour (Weber et al., 2020). *The Australian* falsely stated that 183 arsonists had been arrested since the start of the bushfire season, a figure which was picked up on social media by far-right figures. However, only twenty-four people had been charged with deliberately lighting bushfires (Macdonald, 2020). Dr Timothy Graham, from the Queensland University of Technology, found bot-like and troll-like accounts targeting the hashtags #arsonemergency, #bushfireaustralia and #australiafire (Stilgherrian, 2020).

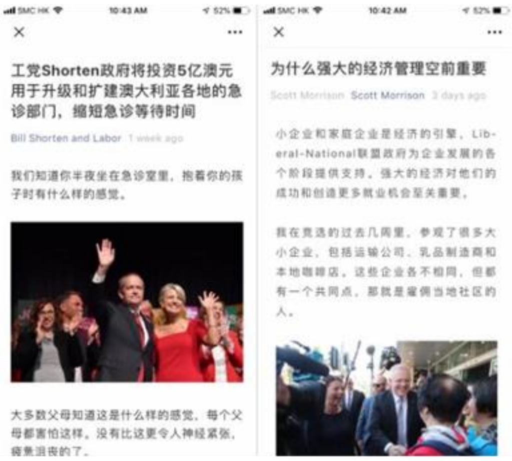
Trolling

ABC News reported that a Labor MP had reported “a relentless number of fake Facebook profiles commenting constantly” across Facebook pages and newspaper outlets. The fake accounts used comments to manipulate, misinform, attack MPs, and in some cases promote the Liberal Party (Gregory, 2019).

WeChat

Politicians from the Labor Party and the Liberal Party are active on WeChat to target the country’s ethnic Chinese population. With an estimated 3 million WeChat users in Australia, a survey found that 60% of Australian Mandarin speakers used the app as their main source of news and information (Hollingsworth, 2019). WeChat is an important platform for campaigning, credited as central to the Labor Party’s win in the marginal Melbourne seat of

Chisholm during the 2016 federal election. An account called ‘Bill Shorten and Labor’ made Chinese-language posts almost every day during the election season, and Prime Minister Scott Morrison also has a WeChat account that posts Chinese-language articles (Figure 4). Fabricated and misleading content is reported to circulate on WeChat groups. Labor has reportedly written to Tencent, WeChat’s parent company, over concerns of malicious and misleading content and fake news. For example, rumours spread about Labor’s promise to increase the number of refugees and claims that Labor would close power plants. *SBS News* reported that some anti-Labor material on WeChat could be traced to members of the Liberal Party (Elvin, 2019).



工党Shorten政府将投资5亿澳元用于升级和扩建澳大利亚各地的急诊部门，缩短急诊等待时间

Bill Shorten and Labor 1 week ago

我们知道你半夜坐在急诊室里，抱着你的孩子时有什么样的感觉。

大多数父母知道这是什么样的感觉，每个父母都害怕这样。没有比这更令人神经紧张，疲惫沮丧的了。

为什么强大的经济管理空前重要

Scott Morrison Scott Morrison 3 days ago

小企业和家庭企业是经济的引擎，Liberal-National联盟政府为企业发展的各个阶段提供支持。强大的经济对他们的成功和创造更多就业机会至关重要。

我在竞选的过去几周里，参观了很多大小企业，包括运输公司、乳品制造商和本地咖啡店。这些企业各不相同，但都有一个共同点，那就是雇佣当地社区的人。

Figure 4: Australian WeChat accounts (Hollingsworth, 2019)

Fake Accounts

The unexpectedly large Twitter following of Senator Kimberley Kitching was brought to the public’s attention in May 2018 after it was revealed that 27% of her followers were probably fake Russian accounts. It has since been revealed that she is not the only one with large Russian followings. However, she is adamant that her Russian following never exceeded 3%, even after she lost more than 4,500 followers in a Twitter culling of fake accounts in early November 2018. It remains unclear whether she instigated the fake following, or if this was done by a third party. Similarly, several prominent politicians with fake Twitter followers have lost a significant number of followers due to culls carried out by Twitter.

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Australia

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Bots, Fake Human	Pro-government messages, attacks on opposition, trolling	Disinformation, Facebook Ads, Amplifying Content	Facebook, Facebook Messenger, Twitter, WeChat

Source: Authors’ evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

The Australian government continues to invest in cybersecurity. The 2018/19 budget includes A$9 million (£4,893,363) to be allocated to the Department of Parliamentary Services over a four-year period to establish a cybersecurity operations network. Additionally, the Australian Cyber Security Centre has set up a 24/7 cyber newsroom in collaboration with the Crisis Coordination Centre to foster early warning and outreach efforts. The newsroom is supposed to capture all comments and opinions on cybersecurity issues while also engaging with citizens via Twitter, providing news updates on their website to "influence the narrative more broadly". The amount spent by political parties during the federal election campaign varies. It was reported that Clive Palmer's United Australia Party spent $60 million on election advertising, yet failed to win a single seat in parliament (Smee, 2019b).

Table 3: Cyber Troop Capacity in Australia

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
		Temporary (elections)	Decentralised	

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Russian Interference

After the 2016 federal election, the government admitted that they were unprepared for foreign interference on social media. Researchers Tom Sear and Mike Jensen (2019) have found a continuous cyber troop presence by groups associated with foreign countries, especially the Russian Internet Research Agency (IRA), finding evidence of the targeting of Australian citizens by the IRA as early as 2014. In evidence submitted to Parliament, Tom Sear found a correlation between Russian-generated social media activity and the downing of Malaysian Airlines Flight 17 (MH17), particularly interventions into Australian political social media (Sear, 2018b). Additionally, The National Media Research Council highlighted the work of Russian trolls and media outlets like Russia Today and Sputnik which disseminate misinformation.

Chinese Interference

The Australian government warned in 2017 of Chinese interference attempts (Westbrook, 2019). Researchers found in 2019 that Prime Minister Scott Morrison and the Coalition Government had been targeted by propaganda on WeChat that originated from accounts aligned with the Chinese Communist Party (Cannane et al., 2019). The International Cyber Policy Institute, part of the Australian Strategic Policy Institute (ASPI), warned that the 1.5 million monthly users of the Chinese platform WeChat in Australia could fall prey to misinformation and propaganda as the service is controlled by Beijing. To what extent this control encompasses content published outside of China is unclear, yet there is evidence that Mandarin-language content on WeChat in Australia and China differs (Jensen et al., 2018). The Electoral Integrity Assurance Task Force has worked with Western social media companies to ensure misinformation during elections is minimized, but it has been unable to talk to WeChat or its parent company, Tencent. On 18 February 2019 news broke that several Australian parties were hacked and, according to the prime minister, the attack originated from a "sophisticated foreign state actor", with suspicion focusing on China (Sear, 2018a). The ASPI has put China "on the top of their list" of suspects although Russia "would not be ruled out", according to Fergus Hanson, a cybersecurity expert at the Institute. In March 2019, the

Electoral Commissioner expressed his confidence that the attack did not affect the electoral integrity of the country.

Online Extremism

An Australian man murdered fifty-one people in an attack on two mosques in Christchurch, New Zealand, on 15 March 2019. The attack was livestreamed on Facebook, and the incident raised awareness of the online activities of extreme right-wing groups in Australia. Notably, some of these groups were involved in political campaigning during the federal election (Smee, 2019a). Alt-right Facebook groups campaigned in favour of the United Australia Party, disseminating "anti-Muslim messages, climate denial and conspiracy theories" that encouraged people to support anyone but Labor or the Greens (Gladstone, 2019). In the context of coronavirus, extremist groups have been peddling conspiracy theories on white supremacist forums to recruit new members. ABC News reported that the use of anti-China rhetoric had increased online since the start of the pandemic (Christodoulou, 2020).

References

Australian Government. (2020). Information Warfare Division: Joint Capabilities Group: Department of Defence. https://www.defence.gov.au/jcg/iwd.asp

Barbaschow, A. (2020). Countering foreign interference and social media misinformation in Australia. *ZDNet*. https://www.zdnet.com/article/countering-foreign-interference-and-social-media-misinformation-in-australia/

Burgess, M. (2019, March 27). *Director-General ASD speech to the Lowy Institute | ASD Australian Signals Directorate*. https://www.asd.gov.au/publications/speech-lowy-institute-speech

Butler, J. (2020, July 1). How to win an Australian election with one weapon: Memes. *The New Daily*. https://thenewdaily.com.au/news/2020/07/02/how-to-win-an-australian-election-with-one-weapon-memes/

Cannane, S., Hui, E., & Investigations, A. B. C. (2019, May 9). *'Head has been kicked hard by kangaroos': Chinese media mocks Australia and PM* [Text]. ABC News. https://www.abc.net.au/news/2019-05-09/pm-targeted-by-chinese-communist-party-related-wechat-accounts/11092238

Cave, D. (2020, January 8). How Rupert Murdoch Is Influencing Australia's Bushfire Debate. *The New York Times*. https://www.nytimes.com/2020/01/08/world/australia/fires-murdoch-disinformation.html

Christodoulou, M. (2020, June 11). *Extreme right-wing groups 'exploiting' COVID-19, Australian spy agency warns*. https://www.abc.net.au/news/2020-06-12/asio-briefing-warns-far-right-is-exploiting-coronavirus/12344472

Elvin, L. (2019, May 8). Labor calls on PM to rule out Liberal Party involvement in fake WeChat posts. *SBS News*. https://www.sbs.com.au/news/labor-calls-on-pm-to-rule-out-liberal-party-involvement-in-fake-wechat-posts

Esposito, B. (2018, March 26). Will Australia's Meme Wars Be Fun? *BuzzFeed*. https://www.buzzfeed.com/bradesposito/will-there-ever-be-an-australian-meme-war

Evershed, N. (2019, May 1). Lies, Trump enthusiasts and car parks: The Australian election campaign waged by Facebook ads | Australia news | The Guardian. *The Guardian*. https://www.theguardian.com/australia-news/datablog/2019/may/01/lies-trump-enthusiasts-and-car-parks-the-australian-election-campaign-waged-by-facebook-ads

Facebook Newsroom. (2019, March 26). Removing Coordinated Inauthentic Behavior from Iran, Russia, Macedonia and Kosovo. *Facebook Newsroom*. https://about.fb.com/news/2019/03/cib-iran-russia-macedonia-kosovo/

Fisher, C. (2019). *Digital News Report | Australia*. Reuters Institute. http://www.digitalnewsreport.org/survey/2019/australia-2019/

Freedom House. (2019). *Australia | Freedom on the Net*. Freedom House. https://freedomhouse.org/country/australia/freedom-net/2019

Gladstone, N. (2019, May 26). Alt-right Facebook memes pushed anti-Labor message. *Sydney Morning Herald*. https://todayspaper.smedia.com.au/smh/shared/ShowArticle.aspx?doc=SMH%2F2019%2F05%2F26&entity=Ar01000&sk=E0D8EC80&mode=text

Graham, T., & Keller, T. R. (2020, January 10). Bushfires, bots and arson claims: Australia flung in the global disinformation spotlight. *The Conversation*. http://theconversation.com/bushfires-bots-and-arson-claims-australia-flung-in-the-global-disinformation-spotlight-129556

Gregory, K. (2019, February 28). *Labor MP hits out against 'fake' Facebook profiles she says are attacking her* [Text]. ABC News. https://www.abc.net.au/news/2019-02-28/fake-facebook-profiles-allegedly-trying-influence-nsw-election/10857578

Hollingsworth, J. (2019, May 15). Australian politicians are using WeChat to target voters. But fake content could end up costing them. *CNN*. https://edition.cnn.com/2019/05/15/world/wechat-australian-election-intl/index.html

Jensen, M., Chen, T. C., & Sear, T. (2018, November 16). How digital media blur the border between Australia and China. *The Conversation*. http://theconversation.com/how-digital-media-blur-the-border-between-australia-and-china-101735

Knaus, C. (2019, May 20). False election claims spark push for truth in political advertising laws. *The Guardian*. http://www.theguardian.com/australia-news/2019/may/20/false-election-claims-spark-push-for-truth-in-political-advertising-laws

Knaus, C. (2020, January 11). Disinformation and lies are spreading faster than Australia's bushfires. *The Guardian*. https://www.theguardian.com/australia-news/2020/jan/12/disinformation-and-lies-are-spreading-faster-than-australias-bushfires

Knaus, C., & Karp, P. (2019, May 21). Australian Electoral Commission finds 87 cases of election ads breaching law. *The Guardian*. https://www.theguardian.com/australia-news/2019/may/22/australian-electoral-commission-finds-87-cases-of-election-ads-breaching-law

Macdonald, C. (2020, January 20). Australia's Bushfires Are the Worst Ever. So Is the Disinformation Campaign. *Vice*. https://www.vice.com/en_uk/article/v74dx3/conservatives-across-the-world-are-spreading-disinformation-about-wildfires

McGrath, P. (2019, February 26). Government contacts Facebook over mysterious political ads. *ABC News*. https://www.abc.net.au/news/2019-02-26/facebook-electoral-commission-emails-reveal-political-ad-concern/10834736

Mourad, S. (2019, January 17). Clive Palmer's campaign spams Australian voters with unsolicited SMS. *Mail Online*. https://www.dailymail.co.uk/news/article-6600995/Clive-Palmers-campaign-spams-millions-Australian-voters-unsolicited-political-SMS.html

Murphy, K. (2019, October 23). *Facebook removed 'coordinated inauthentic behaviour' during Australian election*. The Guardian. http://www.theguardian.com/australia-news/2019/oct/23/facebook-removed-coordinated-inauthentic-behaviour-during-australian-election

Murphy, K., Knaus, C., & Evershed, N. (2019, June 7). 'It felt like a big tide': How the death tax lie infected Australia's election campaign. *The Guardian*. https://www.theguardian.com/australia-news/2019/jun/08/it-felt-like-a-big-tide-how-the-death-tax-lie-infected-australias-election-campaign

Ryan, H., & WIlson, C. (2020, January 23). Facebook Won't Do Anything To Stop Climate Deniers Capitalising On Australia's Bushfire Crisis. *BuzzFeed*. https://www.buzzfeed.com/hannahryan/facebook-australia-bushfires-climate-change-deniers-facebook

Sear, T. (2018a, February 18). A state actor has targeted Australian political parties – but that shouldn't surprise us. *The Conversation*. http://theconversation.com/a-state-actor-has-targeted-australian-political-parties-but-that-shouldnt-surprise-us-111997

Sear, T. (2018b). *#MH17: Initial observations of RUssian influence operations relating to Australia* (Joint Standing Committee on Electoral Matters, Parliament of Australia). https://www.researchgate.net/publication/333917200_MH17_Initial_observations_of_Russian_influence_operations_relating_to_Australia_related_thereto_Submission_on_notice_Executive_Summary

Sear, T., & Jensen, M. (2019, April). Hashtag war. *Griffith Review*. https://www.griffithreview.com/articles/hashtag-war-russian-trolls-undermine-australian-democracy/

Smee, B. (2019a, May 3). 'Quite frightening': The far-right fringe of the election campaign is mobilising. *The Guardian*. http://www.theguardian.com/australia-news/2019/may/04/quite-frightening-the-far-right-fringe-of-the-election-campaign-is-mobilising

Smee, B. (2019b, May 18). Clive Palmer's $60m election ad blitz appears to have failed to win a single seat. *The Guardian*. http://www.theguardian.com/australia-news/2019/may/19/clive-palmers-60m-ad-blitz-appears-to-have-failed-to-win-a-single-seat

Stilgherrian. (2020). Twitter bots and trolls promote conspiracy theories about Australian bushfires. *ZDNet*. https://www.zdnet.com/article/twitter-bots-and-trolls-promote-conspiracy-theories-about-australian-bushfires/

Weber, D., Nasim, M., Falzon, L., & Mitchell, L. (2020). #ArsonEmergency and Australia's 'Black Summer': Polarisation and misinformation on social media. *2nd Multidisciplinary International Symposium on Disinformation in Open Online Media (MISDOOM 2020)*. https://arxiv.org/pdf/2004.00742.pdf

Westbrook, T. (2019, April 4). Facebook promises crackdown on fake news in Australia—Reuters. *Reuters*. https://www.reuters.com/article/us-australia-politics-facebook-idUSKCN1RG2RM

Wilson, C. (2020, January 22). Here's A Running List Of False And Misleading Information About Australia's Bushfires. *BuzzFeed*. https://www.buzzfeed.com/cameronwilson/unverified-false-information-list-australian-bushfires

Wordsworth, M. (2016, June 21). *Social media helps hopefuls win #ausvotes on a shoestring* [Text]. ABC News. https://www.abc.net.au/news/2016-06-21/social-media-and-the-election-campaign/7530208

Workman, M., & Hutcheon, S. (2019, November 7). *How the boomer meme-industrial complex helped shred Bill Shorten's campaign*. https://www.abc.net.au/news/2019-11-08/topham-guerins-boomer-meme-industrial-complex/11682116

Ziebel, W. (2018, June 9). Australia forms task force to guard elections from cyber attacks. *Reuters*. https://www.reuters.com/article/us-australia-security-elections-idUSKCN1J506D

Austria

Introduction

Austria has a comparatively long history of digital media manipulation, especially during election seasons when party competition becomes most intense. Austria's media landscape has become more and more partisan in recent years, leading to an abundance of information confusing citizens and increasingly polarizing the public(Koponen & Sanomat, 2018). Since the 2017 election a right-wing conservative coalition of the Austrian People's Party (ÖVP) and the right-wing Freedom Party of Austria (FPÖ) have governed Austria. Both parties engaged in underhanded campaigning strategies during the election, but it seems neither has faced any serious legal or public repercussions (Die Presse, 2019). Instead, both national and international papers are writing about the "phenomenon" of chancellor Sebastian Kurz who "brought the far-right into mainstream" (Fohringer, 2018).

Freedom House (2019) states that Austria's government has frequently been criticized for a lack of transparency, has weak party finance laws, is failing to adequately regulate lobbying, and is prevent parliament corruption. With regards of the FPÖ trying to gain control and power in Austria, the Freedom House Report also mentions that vice-chancellor and FPÖ chairman Heinz-Christian Strache said in 2017 that the Austrian Broadcast Corporation (ORF), which is partly controlled by the government, needed "optimization" of its objectives. How far Strache was willing to go to expand his own power in Austria, along with that of the FPÖ's, became clear during the so-called "Ibiza Affair" in May 2019 that involved a videotape of Strache asking for highly controversial electoral support from a woman who claimed to be connected to a Russian oligarch (Schuetze, 2019; Spiegel Politik, 2019). As a result of the affair, Strache had to give up all his political functions (Murphy, 2019; ORF at/Agenturen, 2019), and new federal elections were held in September 2019 (tagesschau.de, 2019), with Kurz being victorious once again (Dean & Kottasová, 2019), forming a coalition with the Green Party, which has been governing since early 2020 (der Standard, 2019).

An Overview of Cyber Troop Activity in Austria.

Organizational Form

In the past few years Austria's Social Democrats (SPÖ) experienced one of the biggest political scandals when it became public knowledge that they had hired an advisor by the name of Tal Silberstein who created content to attack oppositional parties and candidates (Kozlowska, 2017). However, activities like these have been going on for years, and the SPÖ is by no means the only party involved (Die Presse, 2019).

In 2017, at the time of the FPÖ's rise to power, Austria's media landscape was increasingly dominated by papers with close relations to the FPÖ such as unzensuiert.at and wochenblatt.at. These papers more or less publicly admit that they are not interest in independent journalism but want to support right-wing movements in Europe, especially parties such as the FPÖ or German AfD. Even so, the great reach of these outlets has nonetheless resulted in several politicians and citizens falling victim to online hate campaigns (Übermedien.de, 2018; Huffington Post, 2018; Winter, 2018). Again, the Ibiza Scandal shows that high-ranking politicians of the FPÖ clearly did not see any issues with these developments and have welcomed such shifts in the media landscape.

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Austria

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
		x	x		

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

During the presidential and federal elections in 2016 and 2017, negative comments about competing parties were disseminated through Facebook and Twitter without identifying their own affiliations. For example, the SPÖ's advisor at the time, Tal Silberstein, created two Facebook pages in October 2016 specifically to mock and undermine now chancellor Kurz's campaign. The SPÖ stopped working with Silberstein after he was accused of money laundering in his home country Israel (Kozlowska, 2017). While most Austrian parties have engaged in spreading narratives and information that attack rivals and support their own position, Chancellor Kurz has taken such actions outside of campaign times: Austrian newspaper Kontrast.at (2020) put together all instances in which Kurz has made false claims since his rise to power, and their list contains a total of twenty-eight instances where he was caught essentially lying.

Moreover, Kurz's ÖVP was embroiled in a major scandal relating back to underhanded campaigning techniques employed in 2017 when suspicions arose that they were sharing the personal data of political opponents and other private citizens with the Austrian Intelligence Services. Reports say that the information that was exchanged had been collected over years and may have significantly influenced the campaign strategy of the ÖVP (Pühringer, 2019). The Ibiza Affair also saw new tools and strategies being deployed to influence voters: in the tapes analysed and published by Spiegel and Süddeutsche Zeitung, the now ex-vice-chancellor and ex-chairman of the FPÖ (governing in coalition with the ÖVP) considered how controlling one of the biggest tabloid papers in Austria, Kronen Zeitung, could help control any political narratives and essentially build a media landscape similar to that in operation in Hungary, with outlets working as pro-government propaganda machines (Al-Serori et al., n.d.; Schuetze, 2019; Spiegel Politik, 2019).

Given the countries messy campaigning history and increasing amounts of trolling and hate speech online, demand to fight this development has grown over the past year. During a summit in April 2019, the ÖVP drafted a law dubbed the "digital anonymity ban" as it would require Austrians to provide a full name and address when signing up to platforms with more than 100,000 registered users and an annual revenue of over €500,000. Should they fail to do so they would risk receiving fines that could run into the millions according to reports by Der Standard (Al-Youssef, 2019). Critics have highlighted that the law would penalise the wrong platforms, as right-wing forums such as unzensuiert.at would not be affected or could simply move outside the country to avoid any penalty. Some observers pointed out that the ban could be a political move to undermine Der Standard, as the liberal newspaper functions as a lively political forum (Meaker, 2019). The law was supposed to come into effect in the beginning of 2020, however, the Ibiza Affair put a hold on that. Even though Kurz managed to win the federal elections in September 2019, as of now it remains to be seen whether it will be implemented.

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Austria

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Fake accounts to disguise own affiliation, human	Attacks on opposition, Support of own position/party, Driving divisions	Disinformation, Data-driven strategies,	Facebook… Far-right platforms (e.g. info-direkt.at)

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

Regarding capacity, Austria saw a true computational propaganda effort across the country and other German-speaking countries as several right-wing media outlets and social media channels campaigned against the ratification of the UN Migration Pact in 2018. Researchers have shown that organized right-wing activity online spiked during the time country leaders were heading to sign the deal and ultimately Austria was among the countries who did not sign. Whether the FPÖ was involved or supported this campaign is uncertain (Lëtzebuerg, 2019; Staijc, 2018). Most influence campaigns by state actors seem to remain temporary and focus on particular political events, such as elections, although the efforts of the FPÖ and particularly Strache could be hinting that they were aiming for a more permanent capacity.

Table 3: Cyber Troop Capacity in Austria

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
		Temporary	Decentralised	Medium

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

References

Al-Serori, L., Das Gupta, O., Münch, P., Obermaier, F., & Obermayer, B. (n.d.). Caught in the Trap. *Süddeutsche.De*. Retrieved March 12, 2020, from https://projekte.sueddeutsche.de/artikel/politik/caught-in-the-trap-e675751/

Al-Youssef, M. (2019, April 18). Government Seeks to Eliminate Internet Anonymity – With Severe Penalties. *DER STANDARD*. https://www.derstandard.at/story/2000101677286/government-seeks-to-eliminate-internet-anonymity-with-severe-penalties

Dean, S., & Kottasová, I. (2019, September 30). One of the world's youngest leaders returns in Austria after scandal brought his government down. *CNN*. https://www.cnn.com/2019/09/29/europe/austria-holds-snap-election-intl/index.html

der Standard. (2019, December 29). Regierung fast fix: In das Winterpalais fahren und als Türkis-Grüne zurückkommen. *DER STANDARD*. https://www.derstandard.at/story/2000112758075/regierung-fast-fix-in-das-winterpalais-fahren-und-als-tuerkis

Die Presse. (2019, January 28). Wie die SPÖ versucht, den Wahlkampf 2017 nicht zu wiederholen. *Die Presse*. https://diepresse.com/home/innenpolitik/5569748/Wie-die-SPOe-versucht-den-Wahlkampf-2017-nicht-zu-wiederholen

Die Volksempfänger. (2018, February 23). *Übermedien*. https://uebermedien.de/25597/die-volksempfaenger-wochenblick-und-unzensuriert/

Freedom House. (2019). *Austria | Freedom House*. https://freedomhouse.org/country/austria/freedom-world/2019

Helmut Fohringer. (2018, November 29). “Time” über Kurz: “Bringt extreme Rechte in den Mainstream.” *Die Presse*. https://diepresse.com/home/innenpolitik/5538547/Time-ueber-Kurz_Bringt-extreme-Rechte-in-den-Mainstream

Kontrast.at. (2020, February 13). Alle gesammelten Unwahrheiten von Sebastian Kurz im Faktencheck. *Kontrast.at*. https://kontrast.at/sebastian-kurz-ibiza-balkanroute-faktencheck/

Koponen, H. M., & Sanomat, H. (2018, January 24). In Austria, debate over ‘fake news’ lays bare societal polarisation. *International Press Institute*. https://ipi.media/in-austria-debate-over-fake-news-lays-bare-societal-polarisation/

Kozlowska, H. (2017, October 17). Austria’s march to the right got a boost from fake Facebook content. *Quartz*. https://qz.com/1103274/sebastian-kurz-win-what-role-did-facebook-play-in-austrias-election/

Lëtzebuerg, T. (2019, January 10). Forscher weisen nach, wie die Rechten ihren „Informationskrieg" gegen den UN-Migrationspakt führten. *Tageblatt.lu*. http://www.tageblatt.lu/headlines/forscher-weisen-nach-wie-die-rechten-ihren-informationskrieg-gegen-den-un-migrationspakt-fuehrten/

Meaker, M. (2019, September 28). Austria’s general election could spell the end of anonymity online. *Wired UK*. https://www.wired.co.uk/article/austria-online-anonymity-elections

Murphy, F. (2019, May 18). Austria’s far-right Vice Chancellor Strache steps down. *Reuters*. https://www.reuters.com/article/us-austria-politics-strache-resignation-idUSKCN1SO09F

ORF at/Agenturen. (2019, May 18). „Ibiza-Video“: Strache erklärt Rücktritt. *news.ORF.at*. https://orf.at/stories/3122849/

Pühringer, M. (2019, October 1). Hat die ÖVP den Geheimdienst für sich arbeiten lassen? *Kontrast.at*. https://kontrast.at/hat-die-oevp-den-geheimdienst-fuer-sich-arbeiten-lassen/

Rep. Steve King Goes Full White Nationalist In Interview With Austrian Site. (2018, October 19). HuffPost UK. https://www.huffpost.com/entry/iowa-rep-steve-king-austria-white-nationalist_n_5bca4851e4b0a8f17eec6001

Schuetze, C. F. (2019, May 18). Highlights From the Video That Brought Down Austria’s Vice Chancellor. *The New York Times*. https://www.nytimes.com/2019/05/18/world/europe/austria-video-strache.html

Spiegel Politik. (2019, May 17). War Österreichs Vizekanzler käuflich? *Der Spiegel*. https://www.spiegel.de/politik/ausland/heinz-christian-strache-geheim-videos-belasten-fpoe-chef-a-1268059.html

Staijc, O. (2018, July 11). Rechte Argumente für Österreichs Nein zum Migrationspakt. *DerStandard.At*. https://derstandard.at/2000090774730/Migrationspakt-Rechte-Argumente-fuer-Oesterreichs-Nein

tagesschau.de. (2019, May 18). Fall Strache: In Österreich gibt es Neuwahlen. *tagesschau.de*. https://www.tagesschau.de/eilmeldung/oesterreich-323.html

Winter, J. (2018, March 3). Wie FPÖ-nahe Medien politische Gegner an den Pranger stellen. *Profil.At*. https://www.profil.at/oesterreich/fpoe-medien-9267735

Azerbaijan

Introduction

Azerbaijan’s oil wealth has allowed its government to fund large international projects and rebuild its military in recent years. The government—led by Ilham Aliyev since 2003—has broad control over the media landscape. Indeed, the country is ranked 166th out of 180 in the World Press Freedom Index (Reporters Without Borders, 2020). While public assembly and access to traditional media are restricted, there has been an increasing use of social media as an alternative source for political information (International Election Observation Mission, 2020). The government has worked to block critical websites, hijack social media accounts, prosecute and intimidate journalists and activists, and use computational propaganda (Freedom of the Net—Azerbaijan, 2019) targeted against dissidents both in the country and abroad.

The Ministry of Transportation, Communications and High Technologies is entitled to block websites without a prior court decision (International Election Observation Mission, 2020). It has also been linked to the DDoS attacks on independent online media sites in 2017 (Megiddo, s. f.). Consequently, independent news platforms are using Facebook, Instagram, and YouTube to reach their audience, and many of the existing websites are managed from abroad (Geybulla, 2019b). Even so, content unfavourable to the government, such as evidence of police violence during protests in October 2019, have been taken down from Facebook with no further explanation (Geybulla, 2019b).

Slander is a criminal offense and is punished with three to five years of imprisonment. As a result, journalists and activists have been arrested for expressing anti-government viewpoints. Not only have exiled activists been blackmailed with hacked photos, audios, and emails (World Report 2020, 2019), but hackers also published personal information on the hijacked social media accounts (Geybulla, 2019b). Moreover, their relatives have been intimidated if they did not denounce them or convince them to stop their activities (World Report 2020, 2019).

As evidenced by a report by Qurium, an attacker using the subnet 85.132.24.7X and linked to the Azerbaijani Ministry of Internal Affairs has been behind several surveillance operations since 2016 (Qurium Media Foundation, 2020b). For example, it was through this IP address that Orkhan Shabanov made initial contact with Hacking Team, DDoS attacks against critical media were conducted[1], non-neutral Wikipedia articles about the police and the Nagorno-Karabakh War were edited, and mass phishing targeting political activists and journalists was deployed (Qurium Media Foundation, 2020a, 2020b). Ali Karimli, leader of the opposition party Popular Front “reported internet outage at his apartment in Baku” and that “all of his communications/messenger applications have been either hacked or being used by a third party” (Azerbaijan Internet Watch, 2020c).

Complementing the above-mentioned efforts, the government has also deployed social media manipulation. These computational propaganda efforts often focus on political events such as protests, rallies and elections (Geybulla & Muntezir, 2018), as well as suppressing opposition through the use of trolls and dissemination of disinformation, both domestically and internationally (e.g. in Armenia).

An Overview of Cyber Troop Activity in Azerbaijan.

Organizational Form

Early reports of social media manipulation in Azerbaijan first emerged in 2011 and focused on IRELI ("Forward") Youth (also called Ireli youth union or IRELI Youth Group) (AZ News Staff, 2011). IRELI Youth was formed in 2005, only a few months after a similar youth group called Nashi emerged in Russia (Durna Safarova, 2018). It is affiliated with the government and was established in order to "take active part in information war".

More recently, IRELI's profile has declined, in part due to controversies surrounding its leader's ties to the Fethullah Gülen movement, a controversial group denounced by the current Turkish government (Durna Safarova, 2018). Instead, the strategy seems to have evolved to concentrate on the creation and maintenance of large Facebook groups which post predominantly positive messages about Azerbaijani history. It has been confirmed that these are funded by the government, although this is not publicly disclosed (Durna Safarova, 2018).

IRELI's decline since 2014 is also due to the departure of leading figures in the group (the organization's leader Elnur Aslanov and its secretary-general Rauf Mardiyev). Following this, various other youth organizations such as the youth branches of the ruling party (Yeni ('New') Azerbaijani Party) have taken over their efforts (Earle, 2017; Geybulla, 2016). Youth groups allow a degree of plausible deniability and their involvement is preferred because they are cheaper to employ and more adept at using social media (Earle, 2017). While some trolling efforts are coordinated by youth groups, it is also possible that some young people join in with the harassment independently (DeGeurin, 2018).

In February 2018 President Ilham Aliyev announced a snap presidential election to be held on 11 April, which resulted in Aliyev securing another seven-year term. Given the restrictions imposed upon traditional media outlets, social media is used by activists and the opposition to disseminate information and organize campaigns. In the lead-up to the election, pro-government trolls and commentators were exceedingly active online (Freedom House, 2018). Political trolls often used comments copied and pasted from presidential or government statements—these individuals are said to be ruling party members, civil servants, and other pro-government supporters (Geybulla & Muntezir, 2018). In February 2018, Deputy Prime Minister Ali Ahmadov told members of the party's youth branch to use social media effectively and make necessary "sacrifices" ahead of the election, with many seeing this as an invitation to attack the opposition (Freedom House, 2018). These attacks came from personal social media accounts, but also from fake accounts disguised with different names, with the authors of the report noting that, while Azerbaijan is far from being equipped with troll factories equivalent to those active in Russia, it is "catching up" (Geybulla & Muntezir, 2018).

It is also worth noting that there were several allegations surrounding the activities of Ali Hasanov, the president's former Assistant for Public and Political affairs, primarily response for the government's relationship with the media. It was alleged that Hasanov was linked to the actions of the government's internet trolls (Safarova, 2020). However, he was dismissed on November 2019.

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Azerbaijan

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
2011	Ministry of Internal Affairs and Ministry of Transportation, Communications and High Technologies, former president's Assistant for Public and Political Affairs	Youth branches of Yeni Azerbaijani Party		IRELI Youth Group	Evidence found

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

IRELI Youth cultivated websites and blogs dedicated to contentious historical events such as "the Karabakh problem" (AZ News Staff, 2011). They have also been known to post abusive comments on social media, with frequently individuals being targeted on Twitter and other social media platforms if they criticize the government. The use of bots has also been observed (Geybulla, 2016). Independent journalists and activists, such as the investigative journalist Khadija Ismayilova, are often the targets of intimidation campaigns based on illicitly obtained intimate images (Freedom House, 2018).

The tactics used by these trolls are unsophisticated. Their techniques include spreading rumours, creating cartoons or memes, harassment, and reporting accounts until they are suspended (DeGeurin, 2018). According to a 2019 report by the Index of Censorship, pro-government automated and human fake accounts trolled and commented on YouTube videos on channels critical to the government, such as OsmanqiziTV and MeydanTC (Djalilov, 2019).

As regards mass-reporting, it is a well-documented tactic and was used against opposition media outlet Abzas.net on 27 December 2018, as hundreds of trolls attacked their Facebook page and reported it for violating Facebook's 'community standards' (Geybulla, 2019a). Similarly, in December 2019 activist Shakir Zade's YouTube channel was taken in response to reports issued by Milli TV, Qanun TV, and AnTV (*Activist's YouTube channel down*, 2019). Previous to these attacks, in April 2017 the journalist Sevinc Osmanqizi wrote an open letter calling on Ali Hasanov to order "his trolls" to stop attacking her on Facebook and YouTube (Said, 2018). Arzu Geybulla, an Azerbaijani journalist, observed that some trolls are tasked with trolling specific activists or members of civil society (Meisenzahl, 2018).

Hacking to gain access to social media accounts takes place alongside cyber troopers' use of fake accounts, takedown requests, and blackmail (Geybulla & Kobaidze, 2019). This includes attempts to compromise social media accounts belonging to opponents off the government and other activists (Geybulla & Muntezir, 2018). For example, on 24 November 2018, Aziz Karimov – a journalist in Baku – had his Facebook account hacked, resulting in his removal as administrator from several Facebook pages, including Turan News Agency, Azerbaijan's only independent news agency. At the same time, administrators of other Facebook pages were also compromised. For example, Azadliq Radio and Azerbaijan Service for Radio Free Europe lost all their video content (2,000 videos, posts and photos) and 25,000 of its 500,000 followers (Geybulla & Kobaidze, 2019). On 29 January 2018, Meydan TV lost 100,000 subscribers to its various Facebook pages, and all content since 2012 was deleted (Said, 2018). Their website continues to be the subject of regular Distributed Denial of Service (DDoS) attacks.

Many attacks have been linked to important moments in domestic politics. On 19 January 2019, an opposition rally witnessed attendees being questioned by the police based on the geolocation data from their phones which had been used to determine that they had been present at the rally. As Article 39 of the Law on Communication requires mobile providers to give any government institutions this information upon request, many took to social media to blame mobile phone operators for disclosing the names and phone numbers of those customers at the rally. After a wave of protests, accounts and pages belonging to individual activists and organizations were hacked (including figures such as Gultekin Hajibeyli, Ali N Aliyev, Ruslan Izzetli—one of the founders of D18, among others), first on 21 October and then again on 9 November 2019. In some cases, such as that of Ali N Aliyev, intimate photos of fellow activists were posted using his hacked profile (Geybulla, 2019b). And most recently, Facebook groups of LGBT-related media and groups were targeted, and LGBT rights activists had their personal Facebook account and emails hacked after a "non-violent march organized to mark International Women's Day" (*Coordinated digital attacks against Feminist movement members and LGBT rights activists*, 2020).

Public figures have also been targeted. For instance, in January 2020, Facebook groups and pages belonging to the Musavat party were hacked whilst page admins were participating in a commemoration ceremony in honour of Mammad Amin Rasulzade, the founder of Azerbaijan Republic (Azerbaijan Internet Watch, 2020a). Also, in December 2019 there was a takedown of the Instagram profile of Ali Karimli, leader of the Popular Front party, by his impersonated fake account (Azerbaijan Internet Watch, 2019). His WhatsApp and Telegram accounts were also hacked, and since April 2020 he has no access to the internet (Azerbaijan Internet Watch, 2020c).

It is also worth noting that Azerbaijan's conflict with its neighbor Armenia and the breakaway territory of Nagorno-Karabakh has traditionally driven conflicts over information; for example, the Azerbaijani government has propagated online conspiracy theories regarding pogroms against Armenians (AZ News Staff, 2011; Kucera, 2018) and hacked accounts posted content in Armenian Facebook groups to call for protests against Armenian Prime Minister Nikol Pashinyan (*Artsakh official warns of Azerbaijani fake news in Armenian groups on Facebook*, 2020). Moreover, trolls frequently reference atrocities committed by Armenia or the Armenian conflict to "hijack and distort" conversations regarding Azerbaijan's human rights record (Geybulla, 2016). More recently, after the lockdown over the weekend of June 6 and 7 2020, during which riot police apprehended people violating the quarantine without an arrest warrant (*Baku Police Accused Of «Revenge Operation»*, 2020), trolls targeted people critical to the harsh measures by accusing them of being partial and asking them to also write about the protests in the United States following the murder of George Floyd.

The authorities are openly discussing methods to prevent users from relying on social media platforms for disseminating news, sharing stories and expressing concerns. Suggestions for doing so have included creating a national social network and closing access to other more popular social media platforms, in order to prevent people from slandering Azerbaijan. During the 2020 COVID-19 pandemic, MP Ganir Pashayeva suggested the creation of a social media monitoring unit to "identify, track, and punish those who shared 'false' information on social media" (Geybulla, 2020). Although it was not created, journalists, activists, and members of the opposition, among others, who criticized the government's response were subject to administrative detention for their social media posts (Azerbaijan Internet Watch, 2020b).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Azerbaijan

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Automation, human Fake, hacked, and real accounts	Pro-government, pro-party messages, Attacks on opposition, Driving division/polarization, Suppressing speech	Creation of disinformation, Mass Reporting Content, Trolls, Amplifying content	Twitter, YouTube, Instagram

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

There is no detailed information about the organizational capacity and resources of cyber troops in Azerbaijan. However, as Geybulla (2016) states, volunteer work with IRELI was viewed as an entrance route for roles in public administration.

Activities are persistent but, according to Muntezir, the troll network deployed by Azerbaijan is ineffective and unprofessional. Social media accounts are visibly fake, with no pictures or history, and content is directly retrieved from Ilham Aliyev's speeches. He also mentions that there is evidence that trolls are asked to compile reports with content and screenshots of their comments. Orders about requested attacks are given via WhatsApp groups (Djalilov, 2019) and other platforms.

Table 3: Cyber Troop Capacity in Azerbaijan

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
-	-	Permanent	Reporting requirements, organization via WhatsApp and other platforms.	Medium

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

References

Activist's YouTube channel down. (2019, December 5). [Azerbaijan Internet Watch]. https://www.az-netwatch.org/news/activists-youtube-channel-down/

Artsakh official warns of Azerbaijani fake news in Armenian groups on Facebook. (2020, January 10). https://www.panorama.am/en/news/2020/01/10/Artsakh-official-Azerbaijani-fake-news/2220801

AZ News Staff. (2011, June 8). *News.Az—Ireli youth union focusing on IT*. https://news.az/articles/society/38037

Azerbaijan Internet Watch. (2019, December 1). *Political leader's Instagram page down* [Azerbaijan Internet Watch]. https://www.az-netwatch.org/news/political-leaders-instagram-page-down/

Azerbaijan Internet Watch. (2020a, February 3). *Opposition party social media accounts hacked*. Azerbaijan Internet Watch. https://www.az-netwatch.org/news/opposition-party-social-media-accounts-hacked/

Azerbaijan Internet Watch. (2020b, March 25). *Social media users questioned over coronavirus posts [Last update June 26]*. Azerbaijan Internet Watch. https://www.az-netwatch.org/news/social-media-users-questioned-over-coronavirus-posts/

Azerbaijan Internet Watch. (2020c, May 13). *Opposition leader's mobile and internet cut off ahead of live interview [updated]* [Azerbaijan Internet Watch]. https://www.az-netwatch.org/news/opposition-leaders-mobile-and-internet-cut-off-ahead-of-live-interview/

Azerbaijan Internet Watch. (2020d, May 15). *News agency website DDoSed [updated]* [Azerbaijan Internet Watch]. https://www.az-netwatch.org/news/news-agency-website-ddosed-updated/

Baku Police Accused Of «Revenge Operation». (2020, June 8). RadioFreeEurope/RadioLiberty. https://www.rferl.org/a/azerbaijan-rights-activist-accuses-baku-police-of-conducting-revenge-operation-/30659714.html

Coordinated digital attacks against Feminist movement members and LGBT rights activists. (2020, March 16). Azerbaijan Internet Watch. https://www.az-netwatch.org/news/coordinated-digital-attacks-against-feminist-movement-members-and-lgbt-rights-activists/

DeGeurin, M. (2018, October 22). *'How They Hit You Is Through Your Family": How Troll Farms Silence Democracy*. New York Mag. http://nymag.com/developing/2018/10/azerbaijan-trolls-q-a-katy-pearce.html

Djalilov, I. (2019, July 31). Trolls and insults: Azerbaijan's exiled media increasingly under fire. *Index on Censorship*. https://www.indexoncensorship.org/2019/07/trolls-and-insults-azerbaijans-exiled-media-increasingly-under-fire/

Durna Safarova. (2018, February 28). *Azerbaijani Government Taps Social Media to Woo Youth*. https://eurasianet.org/s/azerbaijani-government-taps-social-media-to-woo-youth

Earle, S. (2017, October 14). How social media is being used by governments to settle scores and silence critics. *Newsweek*. https://www.newsweek.com/trolls-bots-and-fake-news-dark-and-mysterious-world-social-media-manipulation-682155

Freedom House. (2018, November 1). *Freedom on the Net 2019—Azerbaijan*. https://freedomhouse.org/report/freedom-net/2018/azerbaijan

Freedom of the Net—Azerbaijan. (2019). Freedom House. https://freedomhouse.org/country/azerbaijan/freedom-net/2019

Geybulla, A. (2016, November 22). *In the crosshairs of Azerbaijan's patriotic trolls*. openDemocracy. https://www.opendemocracy.net/en/odr/azerbaijan-patriotic-trolls/

Geybulla, A. (2019a, January 15). In Azerbaijan, big brother is watching you everywhere: Offline, online, on mobile devices and social media apps. *The Foreign Policy Centre*. https://fpc.org.uk/in-azerbaijan-big-brother-is-watching-you-everywhere-offline-online-on-mobile-devices-and-social-media-apps/

Geybulla, A. (2019b, December 16). How does Facebook explain the disappearance of police violence videos in Azerbaijan? *openDemocracy*. https://www.opendemocracy.net/en/odr/how-does-facebook-explain-disappearance-police-violence-videos-azerbaijan/

Geybulla, A. (2020, June 25). Azerbaijan's COVID-19 response: Anything but adequate. *OC Media*. https://oc-media.org/opinions/azerbaijans-covid-19-response-anything-but-adequate/

Geybulla, A., & Grigoryeva, T. (2018, February 15). *What's behind Azerbaijan's snap elections*. Osservatorio Balcani e Caucaso. https://www.balcanicaucaso.org/eng/Areas/Azerbaijan/What-s-behind-Azerbaijan-s-snap-elections-186093

Geybulla, A., & Kobaidze, N. (2019, February 21). Surveillance and Internet Disruption in Baku. *Coda Story*. https://codastory.com/authoritarian-tech/surveillance-and-internet-disruption-in-baku/

Geybulla, A., & Muntezir, H. (2018, February 2). *Azerbaijan's authoritarianism goes digital*. openDemocracy. https://www.opendemocracy.net/en/odr/azerbaijans-authoritarianism-goes-digital/

International Election Observation Mission. (2020). *Republic of Azerbaijan, Early Parliamentary Elections, 9 February 2020. Statement of Preliminary Findings and Conclusions*. https://www.osce.org/odihr/elections/azerbaijan/445759?download=true

Kucera, J. (2018, February 22). *Baku Embraces Conspiracy Theory Blaming Armenians for Own Pogrom*. https://eurasianet.org/s/azerbaijan-officially-embraces-conspiracy-theory-blaming-armenians-for-own-pogrom

Marczak, B., Guarnieri, C., Marquis-Boire, M., & Scott-Railton, J. (2014, February 17). *Mapping Hacking Team's "Untraceable" Spyware*. The Citizen Lab. https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/

Megiddo, T. (forthcoming). Online activism, digital domination, and the rule of trolls: Mapping and theorizing technological oppression by governments. *Columbia Journal of Transnational Law*, *58*, 42.

Meisenzahl, M. (2018, July 2). *Paid trolls and online harassment: how a journalist confronts Azerbaijani censorship*. https://medium.com/berkman-klein-center/paid-trolls-and-online-harassment-how-a-journalist-confronts-azerbaijani-censorship-848c2f0072c7

Qurium Media Foundation. (2020a, January 15). *Fishing phishers in Azerbaijan* [Qurium Media Foundation]. https://www.qurium.org/alerts/azerbaijan/fishing-phishers-in-azerbaijan/

Qurium Media Foundation. (2020b, February 17). *Get to know "man", the person behind the phishing attacks in Azerbaijan* [Qurium Media Foundation]. https://www.qurium.org/alerts/azerbaijan/finding-man-the-phisher-of-journalists-in-azerbaijan/

Reporters Without Borders. (2020, February 14). *Azerbaijan: Journalists harassed, arrested, beaten while covering election protests*. IFEX. https://ifex.org/azerbaijan-journalists-harassed-arrested-beaten-while-covering-election-protests/

Safarova, D. (2020, January 17). Azerbaijan's notorious ideologue suffers precipitous fall. *Eurasianet*. https://eurasianet.org/azerbaijans-notorious-ideologue-suffers-precipitous-fall

Said, G. (2018, April 9). Freedom of speech is guaranteed Aliyev says as Azerbaijan blocks news websites. *Committee to Protect Journalists*. https://cpj.org/blog/2018/04/freedom-of-speech-is-guaranteed-aliyev-says-as-aze.php

World Report 2020: Rights Trends in Azerbaijan. (2019, December 10). Human Rights Watch. https://www.hrw.org/world-report/2020/country-chapters/azerbaijan

BAHRAIN

Introduction

Computational propaganda in the Kingdom of Bahrain takes place in an environment of political repression. Government and pro-government trolls are known to manipulate the online information ecosystem (Freedom House, 2019). The height of activity is reported to have occurred in the wake of the 2011 Arab Spring, with limited coverage in recent years. In February 2011 Bahrain witnessed thousands of pro-democracy activists taking to the streets to demand political and social reform. The demonstrations were repressed violently, and this repression has been maintained with the criminalization of online criticism of the ruling family and sustained social media aggression (Dooley, 2015). The CIVICUS Monitor (2020) rating of human rights violations reports that Bahrain is ranked as closed.

Bahrain's legal framework bans criticism of the royal family and imposes strict limits on content. In 2014 the King of Bahrain ratified a law imposing a prison sentence of up to seven years on anyone who insults him publicly (Elwazer, 2014). For example, in August 2017 a man was sentenced to six years in prison for retweeting an insult to the king (Freedom House, 2018). Article 70 of the Media Regulation Law penalizes content that is deemed 'fake news' or critical of public figures (Gulf Centre for Human Rights, 2018), and thus any site that is critical of the government is vulnerable to being blocked by the Telecommunications Regulatory Authority (Freedom House, 2018). The Gulf Centre for Human Rights (2018) reports that the prime concern of the Bahraini Cybercrime Directorate is content on social media. Nabeel Rajab, then-President of the Bahrain Center for Human Rights, was sentenced to two years in prison for 'broadcasting fake news' and for tweets alleging torture in Bahraini prisons (BBC, 2017). Likewise, women's rights defender Ghada Jamsheer was imprisoned in June 2016 for four cases of defamation related to her tweets; she was fined 10,000 dinars (US$26,500) and given a one year suspended sentence (Gulf Centre for Human Rights, 2016).

An Overview of Cyber Troop Activity in Bahrain

Organizational Form

Multiple organizations are tasked with monitoring and manipulating social media. In November 2013, a Cyber Safety Directorate at the Ministry of State for Telecommunication Affairs was launched to monitor websites and social media networks (Freedom House, 2018). The Ministry of the Interior stated in July 2018 that, in the interest of safety, security, and order, the General Directorate of Anti-corruption and Economic & Electronic Security should monitor "social media accounts that violate the law and harm civil peace and the social fabric" (Ministry of Interior, 2018). Human rights defender Maryam Al Khawaja has claimed that people from the Ministry of the Interior have set up fake accounts to target her with abuse by alleging she works for Iran, is a traitor, an extremist, and a liar (Dooley, 2015). Opposition activists received threatening messages from an Instagram account which claimed to belong to Truki Al-Majed, a lieutenant in the Interior Ministry. The account demanded activists shut down their social media accounts within 24 hours (Bahrain Mirror, 2018). Some activists believe that the troll community targeting human rights defenders is made up of activists loyal to the government; organized based on language skills and assigned specific activists or NGO researchers to target (Dooley, 2011).

Western public relations firms are reported to play a role in reputation management and surveillance. According to watchdog Bahrain Watch, the government has hired eighteen PR firms for promotional campaigns since February 2011, spending at least US$32 million in contracts (Al-Fardan, 2012). Two Washington-based firms, Qorvis Communications and Sanitas International, were reportedly hired by Bahrain to communicate with Western media and place opinion pieces in major media outlets (Goodman, 2011). The Huffington Post reported that Qorvis Communications, Potomac Square Group, and Bell Pottinger had all been hired to improve the Bahraini government's reputation at home and abroad (Halvorssen, 2011). Qorvis Communications was also discovered to have puppet accounts on Wikipedia, used to alter articles that did not portray their clients in a favourable light, including articles related to Bahrain (Morris, 2013). PR firms utilized bloggers posing as journalists on pro-government blogs, such as Bahrain Views and Bahrain Independent, as well as faking social media accounts and partisan op-eds (Nyst & Monaco, 2018). Olton, a UK-based intelligence and PR firm, allegedly received a US$250,000 contract from the Bahrain Economic Development Board in 2011 to "develop an electronic system to track international media" (Bahrain Watch, 2020). The Index on Censorship reports that Olton possessed software that was able to identify 'ringleaders' through social media, which it notes is particularly concerning as dozens of protesting students were dismissed from university based on evidence that was gathered through their Facebook profiles (Index on Censorship, 2012).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Bahrain

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
2011	Ministry of the Interior, Ministry of the Interior Cyber Crime Unit		Qorvis Communications, Olton (Multiple PR firms – explicit role in COMPROP unknown)		Evidence Found

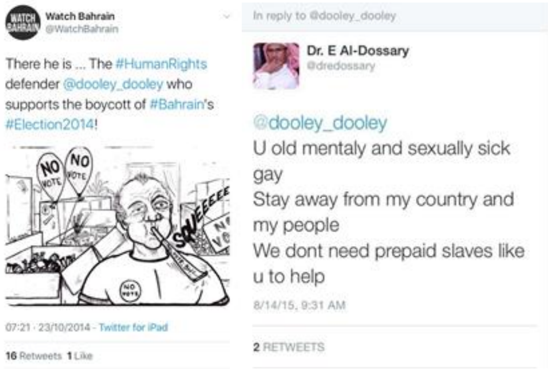
Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Trolling

Trolls in Bahrain have been found to spread disinformation, distort perceptions of the opposition, exacerbate conflicts and discredit valid information (Freedom House, 2019). Notably, journalists and activists are frequently "targeted with vitriolic state-sponsored trolling campaigns" (Nyst & Monaco, 2018). Nabeel Rajab, former President of the Bahrain Center for Human Rights, has been the recipient of "regular troll attacks on Twitter" which he believes are from government accounts (Dooley, 2011). This 'army of trolls' has allegedly been active since at least 2011, when hundreds of accounts emerged following the February protests. Al Jazeera reporter Gregg Carlstrom tweeted that "Bahrain has by far the hardest-working Twitter trolls of any country I've reported on". There are thousands of anonymous accounts with few followers and profile photos signifying support for the regime, such as a photo of the royal family (Owen Jones, 2013). Most recently, Freedom House (2019) reported that Twitter accounts impersonating users in prison were active in August 2018 and interacted with opposition supporters.

Brian Dooley, a human rights activist, has been the subject of continuous troll attacks for his work on Bahrain. Attacks are highly personalized, as illustrated in Figure 1, which includes homophobic harassment from an account supposedly run by Dr Ebrahim Al-Dossary, an adviser to Bahrain's prime minister, and a series of cartoons criticizing Dooley.



Watch Bahrain
@WatchBahrain

There he is ... The #HumanRights defender @dooley_dooley who supports the boycott of #Bahrain's #Election2014!

07:21 · 23/10/2014 · Twitter for iPad

16 Retweets 1 Like

In reply to @dooley_dooley

Dr. E Al-Dossary
@dredossary

@dooley_dooley
U old mentaly and sexually sick gay
Stay away from my country and my people
We dont need prepaid slaves like u to help

8/14/15, 9:31 AM

2 RETWEETS

Figure 1: Personalized online attacks (Source: Twitter, provided by Brian Dooley)

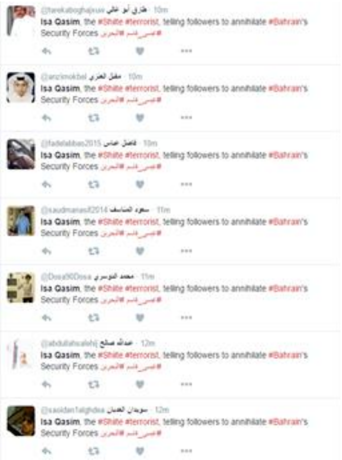
Doxing

Revealing an individual's identity and personal details online, known as 'doxing', is a common tactic for harassing journalists, protestors, and activists in Bahrain. One of the most infamous accounts, 'Hareghum' (@7areghum, created February 2011) disclosed information such as photos of people at anti-government rallies, their addresses, employment information, and contact details. The account was used to report and find information about suspected 'traitors' (Owen Jones, 2013). It allegedly advertised a Ministry of the Interior hotline where individuals could report protesters engaging in anti-government activity directly to the government (Nyst & Monaco, 2018). Pro-regime supporters have even used Twitter to report suspected 'traitors' to the Ministry of the Interior's official Twitter account (@moi_bahrain).

Sectarianism

Automated bots have been found to stoke sectarian tensions. In June 2016, Marc Owen Jones, a researcher of platform manipulation, found that trolls defended the decision to revoke the nationality of the Shiite cleric Isa Qasim ('de-nationalization' is a common tactic in Bahrain), with 50% of tweets in the subsequent period featuring #Bahrain coming from bots (Freedom House, 2018). Owen Jones (2016) identified 5,000 sectarian tweets related to this hashtag, originating from 1,800 bot accounts—later suspended by Twitter. Most accounts identified were created between February and July 2014 and condemned the 'terrorist' acts by the Shi'a opposition in Iran, using derogatory sectarian terms such as 'rawafid' (meaning 'rejectionists' of the true Islamic faith). A sample of this automated sectarian activity can be seen in Figure 2.

The Bahrain Center for Human Rights (2011) noted that hundreds of accounts on social networks, particularly Twitter, misrepresented the peaceful protests in February 2011 by calling them sectarian and broadcasting misattributed violent videos. The accounts appear to have originated from the Ministry of the Interior, and a report published by former chancellor of the minister's council Dr Salah Al-Bander had previously documented that the government was funding groups to incite sectarian divisions online.



@tarekaboghajous طارق أبو غالي · 10m
Isa Qasim, the #Shiite #terrorist, telling followers to annihilate #Bahrain's Security Forces #عيسى_قاسم #البحرين

@anzimokbel مقبل العنزي · 10m
Isa Qasim, the #Shiite #terrorist, telling followers to annihilate #Bahrain's Security Forces #عيسى_قاسم #البحرين

@fadelabbas2015 فاضل عباس · 10m
Isa Qasim, the #Shiite #terrorist, telling followers to annihilate #Bahrain's Security Forces #عيسى_قاسم #البحرين

@saudmanasif2014 سعود المناسف · 11m
Isa Qasim, the #Shiite #terrorist, telling followers to annihilate #Bahrain's Security Forces #عيسى_قاسم #البحرين

@Dosa90Dosa محمد الدوسري · 11m
Isa Qasim, the #Shiite #terrorist, telling followers to annihilate #Bahrain's Security Forces #عيسى_قاسم #البحرين

@abdullahsalehj عبدالله صالح · 12m
Isa Qasim, the #Shiite #terrorist, telling followers to annihilate #Bahrain's Security Forces #عيسى_قاسم #البحرين

@swidan1alghdea سويدان العضل · 12m
Isa Qasim, the #Shiite #terrorist, telling followers to annihilate #Bahrain's Security Forces #عيسى_قاسم #البحرين

Figure 2: Automated Sectarianism (Owen Jones, 2016)

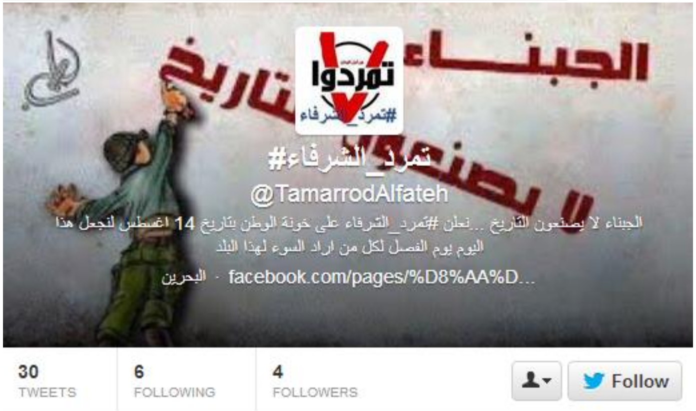
Harassment

Critics of the regime, including bloggers, activists, and journalists, continue to face harassment and prosecution. Some bloggers have been killed, such as Zakariya Rashi Hassan Al Asheri who was tortured to death in prison in 2011, leading others to self-censor and become less critical of the regime online (Owen Jones, 2013). Bahrain Watch (2013a) found that some activists and online critics were being arrested as a result of malicious links—sent from fake Twitter and Facebook accounts that impersonated well-known figures—which when clicked revealed the user's Internet Protocol (IP) addresses. It is claimed that the Ministry of the Interior's Cyber Crime Unit was orchestrating these attacks and Bahrain Watch identified more than 120 cases where a government account targeted a Twitter account with the IP-spying link using a public Twitter mention. In the year prior to the report (2012–13), at least eleven people had been imprisoned and charged with insulting the King on Twitter (Bahrain Watch, 2013a).

Research by Bahrain Watch (2013b) found connections between the Bahraini government and accounts on Twitter and Facebook which advocated for violence against both the government and protestors. Bahrain Watch found evidence that was "suggestive of a Government connection" and found 'extremist' accounts that explicitly advocated violence. For example, @TamarrodAlfateh was an account on Facebook and Twitter that encouraged Bahrainis to "revolt against the terrorists" on 14 August 2013, the same day that the opposition had planned to hold mass protests. Bahrain Watch linked this account to the government through IP addresses. It is important to note that this account had very limited reach, with only four followers (Figure 3).

Online harassment is used in combination with physical attacks and intimidation. Blogger Hassan Al-Sharqi was summoned by the National Security Agency in May 2017, and reportedly insulted, beaten and ordered by staff to cease his online activities (Gulf Centre for Human Rights, 2018).

Figure 3: Fake Twitter account (Bahrain Watch, 2013b)



#تمرد_الشرفاء

@TamarrodAlfateh

الجبناء لا يصنعون التاريخ ...نعلن #تمرد_الشرفاء على خونة الوطن بتاريخ 14 اغسطس لتجعل هذا اليوم يوم الفصل لكل من اراد السوء لهذا البلد

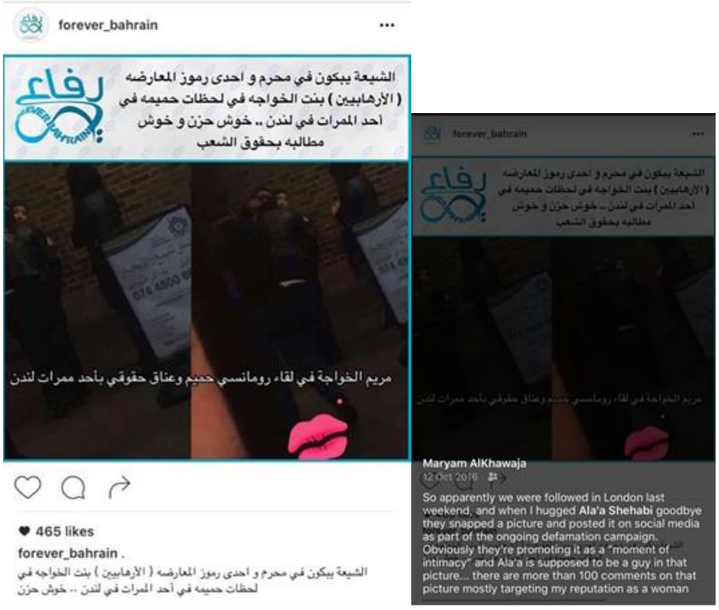
البحرين · facebook.com/pages/%D8%AA%D...

30 TWEETS | 6 FOLLOWING | 4 FOLLOWERS | Follow

Gendered Harassment and Trolling

No law in Bahrain prohibits discrimination on the grounds of sex, gender identity or sexual orientation (Human Rights Watch, 2019). In this environment of political repression, online gender-based harassment and trolling targeting women with violent and sexual attacks is prolific. Human rights activist Maryam Al-Khawaja has been subjected to harassment including violent rape and death threats, and has also been the target of countless defamation campaigns using fake photos (Nyst & Monaco, 2018). Al-Khawaja has been subjected to gendered and sectarian trolling (Figure 4), such as being called a 'Fatat Motaa'—which has become a common sexual slur used to target Shiite women. Such occurrences are not infrequent, with human rights activist Ebtisam al-Saegh also being threatened on Twitter with rape, and threats that videos of her torture and sexual assault during her 2017 detention would be released online if she did not end her online activism (Freedom House, 2019). Freedom House (2019) reported that a woman arrested in May 2019 for insulting the King over social media was subject to severe abuse during detention, which ultimately caused her to suffer a breakdown and need to be transferred to a psychiatric hospital.

Figure 4: Forever Bahrain account targeting Women Human Rights Defenders (Source: Facebook, 2016, provided by Maryam Al-Khawaja)



forever_bahrain

الشيعة يبكون في محرم و احدى رموز المعارضه (الأرهابيين) بنت الخواجه في لحظات حميمه في أحد الممرات في لندن .. خوش حزن و خوش مطالبه بحقوق الشعب

مريم الخواجة في لقاء رومانسي حميم وعناق حقوقي بأحد ممرات لندن

465 likes

forever_bahrain . الشيعة يبكون في محرم و احدى رموز المعارضه (الأرهابيين) بنت الخواجه في لحظات حميمه في أحد الممرات في لندن .. خوش حزن

Maryam AlKhawaja
12 Oct 2016

So apparently we were followed in London last weekend, and when I hugged **Ala'a Shehabi** goodbye they snapped a picture and posted it on social media as part of the ongoing defamation campaign. Obviously they're promoting it as a "moment of intimacy" and Ala'a is supposed to be a guy in that picture... there are more than 100 comments on that picture mostly targeting my reputation as a woman

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Bahrain

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Automated, Human, Fake	Progovernment messages, attacks on opposition, polarisation (sectarianism), trolling ad harassment	Creation of disinformation, trolls	Twitter, Facebook

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

Cyber troop activity in Bahrain is limited, but computational propaganda has increased following the upheaval caused by the Arab Spring in 2011. This coincided with Western PR firms being employed to manage Bahrain's image domestically and abroad, with the hiring of eighteen firms for promotional campaigns since February 2011, spending at least US$32 million in contracts (Al-Fardan, 2012). However, the extent to which these firms were involved in computational propaganda is unknown. Nonetheless, it was also revealed in 2016 that a Canadian company, Netsweeper, was paid US$1,175,000 for supplying the Bahraini government with a "national website filtering solution" (Pearson, 2016).

Table 3: Cyber Troop Capacity in Bahrain

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
	At least US$1,175,000	Temporary	Centralised	Medium

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Bahrain has reportedly been the target of foreign manipulation campaigns. The Ministry of Interior alleged that prior to parliamentary elections in November 2018, 40,000 SMS messages were sent that informed citizens that they had been removed from the electoral register. The government denied sending the messages but alleged that while some were sent in Bahrain, they also came from Iran. The Ministry of Interior also claimed that social media accounts calling for a boycott of the elections were run by users in Iran, Iraq, and Lebanon (Freedom House, 2019).

References

Al-Fardan, R. (2012, August 23). *Bahrain government hires 18 western companies to improve image after unrest*. Bahrain Watch. https://bahrainwatch.org/blog/2012/08/23/bahrain-government-hires-18-western-companies-to-improve-image-after-unrest/

Bahrain Center for Human Rights. (2011, May 22). Bahrain: After destruction of the actual protesting site at 'the Pearl', the government shifts to eliminate virtual protests. Bahrain Center for Human Rights. http://bahrainrights.org/en/node/4101

Bahrain Mirror. (2018, June 6). *Bahrain: Opposition Activists Receive Threatening Messages from Instagram Account*. Bahrain Mirror. http://bahrainmirror.com/en/en/news/47497.html

Bahrain Watch. (2013a, May 15). *The IP Spy Files: How Bahrain's Government Silences Anonymous Online Dissent*. Bahrain Watch. https://bahrainwatch.org/ipspy/viewreport.php

Bahrain Watch. (2013b, August 5). *Is Bahrain's Government running extremist accounts?* Bahrain Watch. https://bahrainwatch.org/blog/2013/08/05/is-bahrains-government-running-extremist-accounts/

Bahrain Watch. (2020). *Olton | PR Watch*. Bahrain Watch. https://bahrainwatch.org/pr/olton.php

BBC. (2017, July 10). Bahrain activist jailed for 'fake news'. *BBC News*. https://www.bbc.com/news/world-middle-east-40558063

CIVICUS. (2020). *CIVICUS Bahrain—Tracking conditions for citizen action*. https://monitor.civicus.org/country/bahrain/

Dooley, B. (2011, November 17). 'Troll' Attacks on #Bahrain Tweets Show Depth of Government Attempts to Silence Dissent. *HuffPost*. https://www.huffpost.com/entry/troll-attacks-on-bahrain_b_1099642

Dooley, B. (2015, September 25). No Stamp Required: All Too Easy for #Bahrain Twitter Trolls. *HuffPost*. https://www.huffpost.com/entry/no-stamp-required-all-too_b_8195486

Elwazer, S. (2014, February 6). New law: Insult Bahrain's king, get thrown in jail. *CNN*. https://edition.cnn.com/2014/02/06/world/meast/barhain-new-law/

Freedom House. (2018). *Bahrain | Freedom on the Net*. Freedom House. https://freedomhouse.org/country/bahrain/freedom-net/2018

Freedom House. (2019). *Bahrain | Freedom on the Net*. Freedom House. https://freedomhouse.org/country/bahrain/freedom-net/2019

Goodman, J. D. (2011, October 11). 'Twitter Trolls' Haunt Discussions of Bahrain Online [The New York Times]. *The Lede*. https://thelede.blogs.nytimes.com/2011/10/11/twitter-trolls-haunt-discussions-of-bahrain-online/

Gulf Centre for Human Rights. (2016, December 12). Bahrain: Human rights defender Ghada Jamsheer freed from prison, allowed to work off remainder of her sentence. https://www.gc4hr.org/news/view/1448

Gulf Centre for Human Rights. (2018). *Mapping Cybercrime Laws and Violations of Digital Rights in the Gulf and Neighbouring Countries*. Gulf Center for Human Rights. https://www.gc4hr.org/report/view/78

Halvorssen, T. (2011, May 19). PR Mercenaries, Their Dictator Masters, and the Human Rights Stain. *HuffPost*. https://www.huffpost.com/entry/pr-mercenaries-their-dict_b_863716

Human Rights Watch. (2019, January 17). *World Report 2019: Rights Trends in Bahrain*. Human Rights Watch. https://www.hrw.org/world-report/2019/country-chapters/bahrain

Index on Censorship. (2012, February 14). Bahrain's PR machine threatens free speech. *Index on Censorship*. https://www.indexoncensorship.org/2012/02/bahrains-pr-machine-threatens-free-speech/

Ministry of Interior, B. (2018, July 21). *MOI warns against anti-Bahrain social media activities*. https://www.policemc.gov.bh/en/news/ministry/83376/

Morris, K. (2013, March 8). *PR firm accused of editing Wikipedia for government clients*. The Daily Dot. https://www.dailydot.com/news/qorvis-lauer-wikipedia-paid-editing-scandal/

Nyst, C., & Monaco, N. (2018). *State-Sponsored Trolling*. https://www.iftf.org/fileadmin/user_upload/images/DigIntel/IFTF_State_sponsored_trolling_report.pdf

Owen Jones, M. (2013). Social media, surveillance and social control in the Bahrain Uprising. *Westminster Papers in Communication and Culture, 9*(2), 68–93.

Owen Jones, M. (2016, June 21). The Automation of Sectarianism: Are Twitter Bots Spreading Sectarianism in the Gulf? *Marc Owen Jones*. https://marcowenjones.wordpress.com/2016/06/21/the-automation-of-sectarianism/

Pearson, J. (2016, January 8). Canadian Company Netsweeper to Censor Bahrain's Internet for $1.2M. *Vice*. https://www.vice.com/en_us/article/yp3d8j/canadian-company-netsweeper-to-censor-bahrains-internet-for-12m

BELARUS

By Aliaksandr Herasimenka
Oxford Internet Institute, University of Oxford

Introduction

Belarus is one of the most stable authoritarian regimes with an extremely restricted media system. The regime emerged around 1995-96 and since then, it has operated an increasingly controlled network of legacy media that manipulate public opinion. This network relies on underlying tactics of disinformation rooted in old-school media manipulation used during the Soviet times, aimed at defaming political opponents of the regime and spreading misinformation (*Disinformation Resilience in Central and Eastern Europe*, 2018). National television remains a state monopoly, state institutions own major newspapers and the state regulates FM waves. The government uses these state-controlled media, along with selective financial support for content producers, restrictive laws and intimidation of users, to introduce manipulation into the online landscape (Freedom House, 2019).

However, the online landscape remains mostly free from government control and manipulation. There are several reasons for this. First, Belarus' government largely does not censor online content. Second, media that are independent from the state dominate online space when it comes to news originating from Belarus. However, as more people have started using social media actively and the scale of anti-government protest mobilization has grown recently, the regime has begun to invest more resources into social media manipulation. In this context, it makes sense to distinguish between media controlled by the state ("state-controlled") and "independent media" outlets. Russia is a major player in the Belarusian media market. Russian propagandists enjoy considerable influence on the Belarusian population, making Belarus very susceptible to Kremlin-backed propaganda (Freedom House, 2019).

An Overview of Cyber Troop Activity in Belarus

Organizational Form

There are four types of major actors that are involved in social media manipulation in Belarus. They are the state, the media, private individuals, and pro-Russian groups. First, the government seemed to be a key source of domestic online misinformation and disinformation in Belarus in recent years. It uses state news outlets, troll armies and the police to spread misinformation online. The Belarusian government controls more than six hundred news outlets (Freedom House, 2019). Examples of such outlets are the newspaper SB: Belarus Today that is owned by the administration of Alyaksandr Lukashenka, president since 1994, as well as three key state-owned television companies Belarus 1, ONT and CTV. Second, many misinformation narratives and disinformation stories originate from state-controlled media. In 2020, "every state outlet showed evidence of propaganda and manipulation," an independent media monitoring report suggests (Bykovskyy, 2020).

Third, several troll groups that are linked to the state operate in Belarus. The media link a key troll farm to a pro-state youth union known as the Belarusian Republican Youth Union (BRSM). The farm was set up by the union in 2011 following a series of Arab Spring-inspired protests. The union created it to oppose "dirt and lies" on social media (Herasimenka, 2013). The idea and aims are reminiscent of the 50-cent Army of human propagandists set up by the Chinese government. Within a year of the BRSM announcement, job adverts appeared that promised $10 per text that should be shared on "pro-opposition forums" (Viasna Human Rights Center, 2012). The aim of the job was to show "support for the ruling regime." Later the same year, an opposition candidate who ran in the 2012 parliamentary election faced a trolling campaign aimed at discrediting his candidacy on social media (Human Rights Defenders for Free Elections, 2012). By 2013, the BRSM created at least 430 pages and groups on VK, the most popular social media platform in Belarus that time. These groups and pages had an audience of at least 105,882 users (Herasimenka, 2013). In 2015 independent media confirmed the existence of the BRSM troll army based on evidence of coordinated activities (NN.by, 2015).

Fourth, members of the police force use fake accounts to harass activists and discredit them. One of the first uses of fake accounts to defame political opponents and trick journalists was reported back in 2012 (Human Rights Defenders for Free Elections, 2012). Since 2017, the police have been engaging in misinformation activity to target most radical political activists such as anarchist organizations. Specifically, anarchist activists accused the police forces of polluting social media platforms with fake accounts to monitor their activities and, in some cases, to harass them. Anarchist groups reported at least fifty-four accounts and pages on Facebook, Telegram and VK that were used for this purpose (*The Republican List of Rubbish Materials*, 2020). Some of these accounts published pictures and other private information obtained by the police during raids that targeted anarchists and other radical activists. This strategy targeted high-profile activists within the community and spread disinformation about them (Viasna Human Rights Center, 2019).

There are also signs of non-political misinformation that circulates in Belarus. For instance, during the COVID-19 pandemic, 171 social media accounts that originated in Belarus shared at least 229 posts that contained misinformation about the influence of 5G technology on the spread of the virus (Baltic Internet Policy Initiative, 2020). Most of this information originated on the Russia-owned social media platform VK.

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Belarus

Initial Report	Government Agencies	State-controlled media	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
2011	The police	Belarus 1, ONT, CTV, NTV-Belarus, SB			Troll farms: the BSRM	Evidence Found

Source: Authors' evaluations based on data collected.

Strategies, Tools, and Techniques

The prime sources of manipulative content on social media in Belarus are human-operated accounts. They cover social media platforms, websites, and messaging apps. There is little evidence of automated online programs in use.

Social media disinformation in Belarus often originates from the accounts of state-controlled outlets and groups. State-controlled media harass political opposition and minority voices and deceive the public into believing this disinformation. Up to 77.27% of news content broadcasted by three leading state-controlled television channels—Belarus 1, ONT, CTV—in November 2019 contained signs of propaganda and manipulation (Media IQ, 2020). This content mostly covered domestic politics such as the parliamentary election. These state-controlled outlets also try to present Belarus as the only stable country in the region, while framing its political system as the only credible one. Common narratives that mention foreign countries include presenting the EU institutions as “weak” and promising an imminent collapse of the West (Chulitskaya, 2019). Many of those narratives align with storylines propagated by local junk news outlets that are linked to Russia, such as vitbich.org and mogilew.by (Chulitskaya, 2019).

Trolling tactics rely on human users who spread pro-government information in the comment sections of leading independent media. Over the past decade, trolls praising the regime and denouncing the opposition have increased their operation significantly (Freedom House, 2019). Their purpose is to mobilize public opinion and to criticize any type of regime opponents. Several popular independent outlets claim that they have become victims of troll farms. According to the editors of leading news outlets that include Nasha Niva and Tut.by, these farms target comment sections on their websites to attack pro-democracy activists and regime opponents and to promote pro-government narratives (NN.by, 2015, 2020). There are also some signs of troll farms operating on social media platforms. However, it does not appear that they function as the major source of misinformation on social media. The platforms most impacted by disinformation are Facebook, OK, Telegram, VK and YouTube.

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Belarus

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Human	Pro-government messages, messages attacking foreign states, attacks on the opposition, the government, polarization strategies, trolling and harassment	Telegram channels, fake VK and Facebook accounts, YouTube channels, memes, misinformation websites	Telegram, YouTube, VK, Facebook, Twitter

Source: Authors’ evaluations based on data collected.

Organizational Capacity and Resources

The propaganda efforts appear to be both centrally coordinated and decentralized. Central coordination takes place through the government structures such as the office of the president, who controls all key figures in the police and state media. Certain groups of trolls operate in a more decentralized manner. However, their origins and affiliations are uncertain. There is scarce information available about the resource spent to support manipulation efforts. State-controlled media outlets are present in all regions of Belarus and require significant resources. As all of them share manipulative political content, we may safely assume that a portion of their 2020 state budget funding of $73 million (an increase compared to 2019) will be directed at propaganda (Law of the Republic of Belarus ‘On republican budget for 2020’, 2019).

Table 3: Cyber Troop Capacity in Belarus

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
>100	73 million to be spent to support state-controlled media in 2020	State backed media, troll groups and Russian-backed channels operate on a constant basis.	Somewhat centralized	Belarus troops: Low. Russian troops in Belarus: high

Source: Authors’ evaluations based on data collected.

A key foreign player in the Belarusian disinformation market is Russia. Belarus might be one of the most vulnerable countries to the influence of the Russian state propaganda. More than 40% of the population considered the Russian state-controlled television channels their main sources of information (Laputska & Papko, 2017). Two-thirds of all the content that is being broadcasted in Belarus originates from Russia (Laputska & Papko, 2017). Chulitskaya (2020) identified 64 actors—mostly junk news websites—that disseminated pro-Russian narratives online. These actors operated 149 social media groups, pages, profiles, and websites. A Warsaw-Based research center EAST identified at least 40 news outlets that are based in Belarus and focus on local agenda but are openly or covertly supported by Russia. Outlets such as vitbich.org, sozh.info and grodnodaily.net have a probable link to Russia through its embassy and other connections (Yeliseyeu, 2019). Sputnik Belarus, a branch of a vast news network Sputnik that is controlled by the Russian government, is one of the most visited online news sources that focus on Belarus (Yeliseyeu, 2020). The key narrative that Sputnik Belarus broadcasted in 2019 included "Belarusians as part of the Russian nation," "the west aggressiveness towards Belarus" and "neighbouring countries that joined the EU are degrading" (Yeliseyeu, 2020). The Russian news aggregators Yandex and Mail.ru also play a significant agenda-setting role for more than 30% of Belarusian internet users (SimilarWeb Website Ranking, 2020). However, the level of activity of Russian disinformation in Belarus is cyclical and depends on the relationship between Moscow and Minsk. Over recent years, Russian propaganda expanded significantly during periods of political discord between the two governments. During these periods, Russian-controlled websites and Telegram accounts carried out vitriolic campaigns against both state and non-state actors in Belarus (Freedom House, 2019).

Following the post-election protests in August 2020, the Belarus government invited a team of technicians, journalists and leaders from RT, a Russian television channel that was frequently found to spread misinformation, to substitute for local state television workers who resigned in protest (Cornaz, 2020).

Response

To respond to the growing amount of disinformation online, non-state actors have attempted to build fact-checking infrastructure, increase the reach of verified information and debunk junk news. Government actors are mostly concerned with information that originates in Russia. Recently, the Belarusian state has been increasingly conscious of the threat posed by information interference from Russia in domestic political debates. A crucial mechanism used by the Belarusian government to respond to this foreign state-backed misinformation is its own media network. The narrative of Russian state attempts to influence the situation in Belarus is dominant in Belarusian state media (Bykovskyy, 2020). To this end, the government has adopted a new Information Security Concept in March 2019 that is based around the goals of "information sovereignty." The Concept prioritizes state control of the information space. The most recent Freedom House (2019) report suggests that "the concept likely entails a greater response to Russia's increasingly aggressive disinformation and propaganda targeting the Lukashenka administration". As one expert put it, the concept "is aimed at ensuring the information security of the authorities" not the people" (Belarus Security Blog, 2019).

References

Baltic Internet Policy Initiative. (2020, June 23). Distribution of fake information about the link between COVID-19 and 5G in Belarus, May-June 2020 [Rasprostraneniye feykovoy informatsii pro svyaz' COVID-19 i 5G v Belarusi, may-iyun' 2020]. *Information Policy*. http://www.infopolicy.biz/?p=13919

Belarus Security Blog. (2019, April 4). The information security concept of Belarus. *Belarus Security Blog*. https://bsblog.info/the-information-security-concept-of-belarus/

Bykovskyy, P. (2020). Russian media increased the number of articles about Belarus by a third in May. Report on pro-Kremlin narratives in Belarusian media [Rossiyskiye SMI na tret' uvelichili kolichestvo materialov o Belarusi v maye. Otchot o prokremlevskikh narrativakh v belarusskikh media] (The Media IQ monitoring). Media IQ. https://mediaiq.by/article/rossiyskie-smi-udvoili-kolichestvo-materialov-o-belarusi-v-mae-otchet-o-prokremlevskih

Chulitskaya, T. (2019). Malign narratives, explanatory articles and examples.

Chulitskaya, T. (2020). Stage IV. Dataset of Pro-Russian sources.

Cornaz, I. (2020, September 3). *Combat entre information et propagande en Biélorussie* [InfoSport]. Rts.Ch. https://www.rts.ch/info/monde/11576351-combat-entre-information-et-propagande-en-bielorussie.html

Damarad, V., & Yeliseyeu, A. (Eds.). (2018). *Disinformation Resilience in Central and Eastern Europe*. http://prismua.org/en/dri-cee/

Freedom House. (2019). *Freedom on the Net 2019: Belarus*. Freedom House. https://freedomhouse.org/country/belarus/freedom-net/2019

Herasimenka, A. (2013, 00, 29.01). In VK, BRSM multiplies. Protest groups are frozen [U vkontakte pamnažajecca BRSM, pratestnyja supolki zamierli]. Generation.bY. http://generation.by/news5903.html

Human Rights Defenders for Free Elections. (2012, August 6). *Black PR used against BPF candidate in Pinsk*. Spring96.Org. http://spring96.org/en/news/55437

Laputska, V., & Papko, A. (2017). *Belarus' Vulnerabilities and Resilience to Foreign-Backed Disinformation Warfare*. https://east-center.org/information-security-belarus-challenges/

Media IQ. (2020). *Quarterly report: September – December 2019* (The Media IQ monitoring). https://mediaiq.by/article/quarterly-report-september-december-2019

Law of the Republic of Belarus 'On republican budget for 2020', no. 269–3 (2019). http://minfin.gov.by/upload/bp/act/zakon_161219_269z.pdf

NN.by. (2015, September 23). Instructions for trolls come from the BRSM - SCREENSHOTS [Instruktsii trollyam postupayut iz BRSM — SKRINSHOTY]. Nasha Niva. https://m.nn.by/ru/articles/156818/

NN.by. (2020, June 6). 'Nasha Niva' Webstite experiences troll invasion from the BRSM [Na sayte «Nashey Nivy» nashestviye trolley iz BRSM]. Nasha Niva. https://nn.by/?c=ar&i=253092&lang=ru

SimilarWeb Website Ranking. (2020). *Top Websites in Belarus*. SimilarWeb. https://www.similarweb.com/top-websites/belarus/

The republican list of rubbish materials. (2020). The Ministry of Anarchism of the Republic of Belarus. https://docs.google.com/document/d/1pSjs8cybAIN507Zbi8kZUN5j4uHxN5KI5O50zE6X36g/edit?fbclid=IwAR1OY38vlSWo-sSfcqXvzMnO-3CpFiZzd9Ch-by9XhVXxdrVE2D6xUidplY&usp=embed_facebook

Viasna Human Rights Center. (2012, May 11). *Who hires internet-trolls?* Spring96.Org. http://spring96.org/en/news/52412

Viasna Human Rights Center. (2019, March 22). *Picks of the week*. Viasna Human Rights Center. http://spring96.org/en/news/92407

Yeliseyeu, A. (2019). Fundamental Shifts in Anti-Belarusian Disinformation and Propaganda: Analysis of Quantitative and Qualitative Changes. EAST (Eurasian States in Transition).

Yeliseyeu, A. (2020). *Sputnik Belarus's Propaganda and Disinformation: Narratives, Methods, and Trends*. East Center. https://east-center.org/sputnik-belarus-propaganda-and-disinformation-narratives-methods-and-trends/

Bolivia

Introduction

On 20 October 2019, Bolivia held general elections. The results, which anticipated the renewal of the already thirteen years of Evo Morales' government, were followed by nineteen days of violent mass protests, prompted by allegations of electoral fraud. On 10 November, the Organization of American States (OAS) published a preliminary report where it stated there were signs of fraud and that a new election should be held. Although Evo Morales accepted a new round of elections, the opposition and the military and police demanded his resignation. He stepped down a day later. Subsequently, Jeanine Áñez, second Vice president in the Senate, proclaimed herself as interim president. Although the elections were scheduled for 3 May 2020, they were postponed to 6 September due to COVID-19.

Since Jeanine Áñez took office, concerns about incidents of violence and repression, as well as threats to freedom of expression have become increasingly prevalent. The Inter-American Commission on Human Rights (also known as the Comisión Interamericana de Derechos Humanos (CIDH)) released a preliminary report in which it stated that during the October and November protests there were at least fifty journalists who were assaulted by the military and the police (Organization of American States, 2019).

With COVID-19 spreading across the country, in March 2020 the government announced that it would identify people who were spreading online disinformation regarding the pandemic («Bolivia anuncia "ciberpatrullajes" contra la desinformación sobre el COVID-19», 2020). In May the president signed the Executive Decree 4231 aimed at punishing "people who spread fake news about Covid-19", but after criticisms over threats to freedom of expression the government annulled the decision (BBC Monitoring, 2020b). Nevertheless, at least sixty-seven people accused of spreading disinformation were arrested during the pandemic. Although cyberpatrolling is not regulated and enforced in Bolivia, this technique was used to identify them («Preocupación por 67 detenciones en aplicación de decretos presidenciales que criminalizaban con prisión por "desinformación" en Bolivia», 2020). In response, the Inter-American Commission on Human Rights, along with other international and local organizations, such as Internet Bolivia, not only called for clarifications of their status, but also began investigations into the matter. Additionally, another person was arrested on charges of being a so-called "digital warrior" and committing the crime of "sedition" (Farfán, 2020).

An Overview of Cyber Troop Activity in Bolivia.

Organizational Form

In 2016 the Bolivian government – under Morales' presidency – created the National Direction of Networks within the Ministry of Communication. The aim was not only to have a greater online presence, but also to identify fake accounts and news (Zegada Claure, 2019). According to Zegada Claure (2019), the Direction created Facebook profiles to support the government and later trained young people to present a positive image of the government in social media discussions and favour Morales during the 2019 elections («Analysis: Fires, fake news and "digital warriors" roil Bolivia election race», 2019; Díaz Arnau, 2020a)

In addition to this, there is evidence that the government hired the Mexican agency Neurona, which "specialises in fake news and smear campaigns" (BBC Monitoring, 2020a). The agency and the ex-minister of Communications are being investigated for irregularity in the direct assignment of eight contracts between 2017 and 2018 worth 12.4 million bolivianos (around 1.8 million dollars). Neurona stated it worked on social media and communication strategies, among other things, for Morales' campaigns (León, 2019). Similarly, the government paid 549,840 bolivianos (almost 80,000 dollars) to the agency Espora for the design of a digital strategy and the analysis of social media use and influencers in Bolivia (Página Siete, 2019), although there is no further evidence about the nature of the work undertaken.

The political party Unidad Democrata is also suspected of using the services IDEIA Big Data, a company which uses the techniques of psychological profiling. An analysis of the pitch desk of the company shows that "several sentences in the slides are exact transcriptions of a presentation of Cambridge Analytica chief executive" (Goldhill, 2019). The company also claims "to have worked" with the Unidad Democrata in Bolivia (Goldhill, 2019).

Whilst the presence of coordinated online activities propelled by Morales' government has not been extensively examined, researchers and journalists have recently observed an extraordinary wave of new Twitter accounts in late 2019 that supported the interim government. Also, on December 10, 2019 the Inter-American Commission on Human Rights published preliminary findings (Organization of American States, 2019) in which it identified that these accounts supported Luis Fernando Camacho and Jeanine Áñez, president of the Civic Committee of Santa Cruz and interim President, respectively (Gallagher, 2019). In spite of the ideological connection, there is no evidence to link the incident to Camacho or Áñez.

It is also worth noting that a US Army veteran called Luis Suarez actively participated in automating his own account in order to amplify content favouring the opposition (Díaz Arnau, 2020b). In fact, his account was among those most active in the online campaign in favour of Morales' removal. According to Julián Macías Tovar, social media coordinator for the Spanish party Podemos, who examined a set of accounts during the November and December crisis, stated that the automation was done via the use of "a custom app named tfb-suarez" (Gallagher, 2019).

Most recently, the interim government has accused the former government of attacking the Twitter account of the Ministry of Justice and posting a list of people in Bolivia with COVID-19. However, forensic analysis by the Ministry pointed towards the account @SoyUnCocodriloS, which had the credentials of the official account and is associated with José Daniel Llorenti (Europa Press, 2020). Llorenti is the nephew of the former Permanent Representative to the United Nations and Ambassador of Bolivia to the United Nations and a founding member of the "Generación Evo" movement. He has also an arrest warrant related to his involvement with Morales' Digital Warriors strategy (Ibid.).

Finally, it is worth noting that there have also been references to foreign activities targeting Bolivia during the election campaigns and the associated political turmoil of late 2019. In October 2019, Facebook removed thirty-six accounts, six pages, four groups, and ten Instagram accounts originating in Iran that focused on Bolivia, among other Latin American countries (Gleicher, 2019).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Bolivia

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
2016	National Direction of Networks within the Ministry of Communication (during Morales' presidency)		IDEIA, Neurona		Luis Suarez

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Under Morales' government, its cybertroopers focused their social media activities on identifying information and accounts that were critical to the government and countering their narratives, as well as trolling the opposition («Analysis: Fires, fake news and "digital warriors" roil Bolivia election race», 2019; Díaz Arnau, 2020a). However, there is not enough analysis of their activities and strategies.

With the crisis triggered by the accusations of irregularities in the 2019 general elections in 2019, several journalists, academics, and activists examined and reported on the use of social media manipulation techniques intended to support the interim government. Evidence of trolling campaigns, the mass creation of new accounts for amplification, copypasta messages, and disinformation have been seen in the last months of 2019. Campaigns were not only targeted to local audiences but to foreign audiences as well.

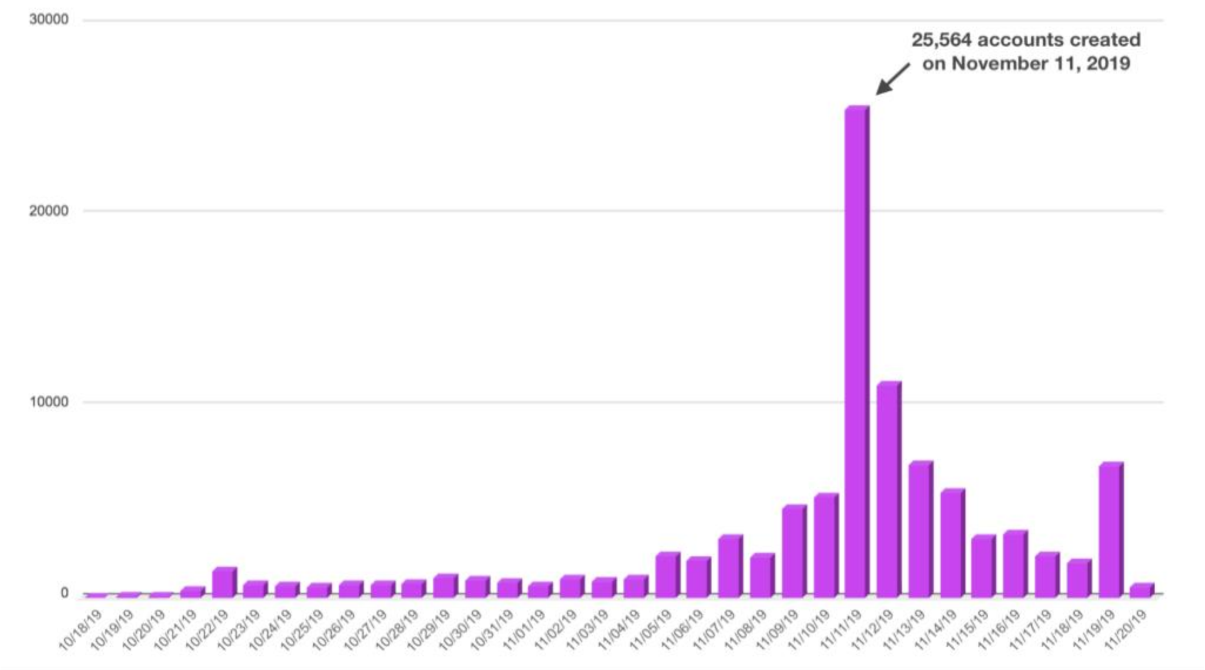
The Inter-American Commission on Human Rights reported the existence of a campaign aimed at harassing former officials of Evo Morales' government and activists of the Movement for Socialism party (MAS) during the weeks of protests in 2019. Many of them were physically harmed, with their homes looted or burnt down. Additionally, and in some cases prior to the physical riots, their home addresses, telephone numbers, and other personal data were disseminated through WhatsApp, Facebook, and other platforms. Independent and community journalists were also targeted, and information about the hotels where foreign journalists were staying at was also disseminated and many of them had to leave the country due to the lack of security guarantees (Organization of American States, 2019).

Julián Marcías Tovar also identified at least 68,000 newly created accounts, activated between 18 October and 20 November, that supported the campaign against Morales— some of which were already active before his resignation—and more than 25,000 were created on 11 December (Graph 1). They promoted and amplified a campaign in favour of the interim government, spreading the appearance of a broad acceptance of the interim government (Gallagher, 2019).

Additionally, according to researcher Rodrigo Quiroga, 23,900 new accounts created between 11 and 12 November 2019 followed Camacho, who increased his followers from 2,000 to more than 135,000; similarly, Áñez increased her followers base from 8,000 to 168,000 (del Castillo, 2019). Some of these accounts also followed members of Morales' MAS. However, their tweets and interactions supported the interim government (del Castillo, 2019).

The campaign was also focused on installing hashtags, such as #BoliviaLibreyDemocratica, #NoHayGolpeEnBolivia, #EvoEsFraude, and #BoliviaUnida (Organization of American States, 2019). According to Julián Macías Tovar, these accounts were created within a one month time frame, with a peak on 11 November. Although it cannot be confirmed that all these accounts were fake, the researcher Luciano Galup has observed that the username of at least 30,529 of the accounts following Camacho were composed using eight numerical digits, such as alejand00816798 (Gallagher, 2019).

Graph 1. New Bolivian Twitter accounts created between October 18 and November 20, 2019



Source: Gallagher, 2019

It is worth noting that, according to The Verge, 4,320 fake accounts were part of a campaign mostly targeted internationally to establish and perpetuate the narrative that a coup d'état had not occurred. The first identified message that would then be replicated in English and Spanish was "Friends from everywhere, in Bolivia there was no coup". Although it is possible that the original message on Facebook was genuinely written by a student critical of Morales, "the sentiment was co-opted and amplified by what experts say is a network of automated Twitter accounts" (Schiffer, 2019). However, there is no evidence of who was behind these operations.

In addition to this, an analysis by DFRLab of Twitter activity during the 2019 crisis found copypasta messages disseminated by at least 1,435 bot accounts that countered the coup narrative. Among these messages, DFRLab identified the above-mentioned "friends from everywhere, in Bolivia there was no coup.", along with other messages that were almost identical and contained the phrases **"**I denounce to the world…" and "Evo incumplió El Art. 168 de la CPE" ("Evo violated Article 168 of the Constitution") (DFRLab, 2019). Some of these messages were posted as images in an attempt to look "as if they were coming from disparate sources" (DFRLab, 2019).

Disinformation was already a problem in Bolivia and it has intensified with recent crises in the country, such as the fires in the Chiquitania region occurring since mid-2019, as well as the incidents in October and November 2019 and later immediately after the interim government took office. Examples of this include messages that highlighted the role of CIA in making #BoliviaNoHayGolpe a trending topic in the state of Virginia, where the agency has its headquarters, and the dissemination of a fake photo in which Evo Morales and Chapo Guzman were photoshopped into an image with Pablo Escobar (Gallagher, 2019).

During this period, as has been previously mentioned, Luis Suarez used an algorithm to amplify content and hashtags, such as #pitita and #NoFueGolpe. He retweeted content 3,000 times a day over a period of ten days (Díaz Arnau, 2020a). In an interview, he states that Morales' cybertroopers not only disseminated disinformation but also mass reported against citizens critical to the government, taking advantage of the newly created accounts with few followers that posted that there was no coup in Bolivia. As a result, he designed an algorithm to identify those accounts and amplify their tweets. (Díaz Arnau, 2020b)

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Bolivia

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Automated bots, Humans	Pro-government, pro-party Attacks on opposition Distracting messages Driving polarisation, Suppressing speech	Disinformation, Data driven strategies, Trolls, Amplification strategies	Twitter, WhatsApp, Facebook

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

There are no details about how cyber troops in Bolivia are organized nor the resources allocated for their activities.

Table 3: Cyber Troop Capacity in Bolivia

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
		Temporary	Somewhat centralised	Medium

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

References

Analysis: Fires, fake news and «digital warriors» roil Bolivia election race. (2019, October 17). *BBC Monitoring*. https://monitoring.bbc.co.uk/product/c2016061

BBC Monitoring. (2020a, May 8). Bolivia, Peru media highlights 6 May 2019. *BBC Monitoring*. https://monitoring.bbc.co.uk/product/c200supf

BBC Monitoring. (2020b, May 14). Bolivia, Peru media highlights 13 May 2020. *BBC Monitoring*. https://monitoring.bbc.co.uk/product/c201plnh

Bolivia anuncia «ciberpatrullajes» contra la desinformación sobre el COVID-19. (2020, March 18). *La Vanguardia*. https://www.lavanguardia.com/politica/20200318/474252441598/bolivia-anuncia-ciberpatrullajes-contra-la-desinformacion-sobre-el-covid-19.html

del Castillo, C. (2019, November 21). Una campaña coordinada con miles de nuevas cuentas de Twitter y bulos contra Morales lava la imagen internacional del golpe en Bolivia. *El Diario*. https://www.eldiario.es/tecnologia/operacion-expulsar-Morales-Bolivia-Twitter_0_965203787.html

DFRLab. (2019, November 26). Amid the crisis in Bolivia, a Twitter flood of coup denial, bot accusations, and memes. *Medium*. https://medium.com/dfrlab/amid-the-crisis-in-bolivia-a-twitter-flood-of-coup-denial-bot-accusations-and-memes-1490b7222c3

Díaz Arnau, O. (2020a, January 12). Cibertropas. *Correo del Sur*. https://correodelsur.com/ecos/20200112_cibertropas.html

Díaz Arnau, O. (2020b, January 12). *"Nunca formé parte del Comando Cibernético del Ejército de EEUU*. https://correodelsur.com/ecos/20200112_nunca-forme-parte-del-comando-cibernetico-del-ejercito-de-eeuu.html?fbclid=IwAR2c97hU4G_wGzfymvHehKK4IKNhkqas1sIZhpQcS0bmrqEa4MaDX_zCV5w

Europa Press. (2020, April 14). El Gobierno de Bolivia acusa a personas vinculadas a Morales de atacar el Twitter de Justicia para dar «fake news». *Europa Press*. https://www.europapress.es/internacional/noticia-gobierno-bolivia-acusa-personas-vinculadas-morales-atacar-twitter-justicia-dar-fake-news-20200414125118.html

Farfán, W. (2020, April 30). Presentan a un 'guerrero digital' que implica a diputado del MAS y éste rechaza la acusación. *La Razón*. https://www.la-razon.com/nacional/2020/04/30/presentan-a-un-guerrero-digital-que-implica-a-diputado-del-mas-y-este-rechaza-la-acusacion

Gallagher, E. (2019, December 31). Information operations in Bolivia. *Medium*. https://medium.com/@erin_gallagher/information-operations-in-bolivia-bc277ef56e73

Gleicher, N. (2019, October 21). Removing More Coordinated Inauthentic Behavior From Iran and Russia. *About Facebook*. https://about.fb.com/news/2019/10/removing-more-coordinated-inauthentic-behavior-from-iran-and-russia/

Goldhill, O. (2019, August 14). *A «big data» firm sells Cambridge Analytica's methods to global politicians, documents show*. Quartz. https://qz.com/1666776/data-firm-ideia-uses-cambridge-analytica-methods-to-target-voters/

León, Y. (2019, December 26). Neurona Consulting, investigada por millonarios contratos con el Gobierno de Evo, borra su sitio web. *Los Tiempos*. https://www.lostiempos.com/actualidad/pais/20191226/neurona-consulting-investigada-millonarios-contratos-gobierno-evo-borra-su

Organization of American States. (2019, December 10). *CIDH presenta sus observaciones preliminares tras su visita a Bolivia, y urge una investigación internacional para las graves violaciones de derechos humanos ocurridas en el marco del proceso electoral desde octubre de 2019* [Text]. https://www.oas.org/es/cidh/prensa/comunicados/2019/321.asp

Página Siete. (2019, April 21). El Gobierno pagó Bs 549.840 a Espora, otra firma mexicana, por 2 consultorías—Diario Pagina Siete. *Página Siete*. https://www.paginasiete.bo/nacional/2019/4/21/el-gobierno-pago-bs-549840-espora-otra-firma-mexicana-por-consultorias-215714.html

Preocupación por 67 detenciones en aplicación de decretos presidenciales que criminalizaban con prisión por "desinformación" en Bolivia. (2020, May 20). *Observacom*.

https://www.observacom.org/preocupacion-por-67-detenciones-en-aplicacion-de-decretos-presidenciales-que-criminalizaban-con-prision-por-desinformacion-en-bolivia/

Schiffer, Z. (2019, November 18). *Bot campaign on Twitter fuels confusion about Bolivian unrest*. The Verge. https://www.theverge.com/2019/11/18/20970888/bot-campaign-twitter-facebook-bolivia-uprising-coup-confusion

Zegada Claure, M. T. (2019). El escenario boliviano en 2018: Estabilidad económica e incertidumbre institucional. *Revista de ciencia política (Santiago), 39*(2), 147-164. https://doi.org/10.4067/S0718-090X2019000200147

BOSNIA AND HERZEGOVINA (BiH)

Introduction

Bosnia and Herzegovina (henceforth: BiH) is a partly free decentralized parliamentary republic characterized by a fragmented constitutional regime and partisan gridlock among nationalist Bosniak, Serb and Croat communities. The country is split into two entities Serb-majority Republika Srpska and the Federation of BiH, whose residents are mainly Bosniak and Croats (Freedom House, 2020). Sensationalist and clickbait content, oftentimes fabricated and completely fake, is frequently shared on social media to incite hostility between the different nationalities and Serbia. For instance, in December 2017, one story by the title "After Bakir defended Bosnia today in front of Vučić and Čović: See what the minister of Serbia has said..." covered fabricated hostilities and confrontations between the Serbian Minister of Defense Aleksander Vulin and Bakir Izetbegović, the BiH politician and member of the tripartite Presidency (CIK Media, 2017). Additionally, much of the national news media landscape is hyper-partisan in nature, and journalists who try to work independently often face political pressure, harassment, and other threats (Freedom House, 2020). At the same time there is no legislation or other non-governmental initiatives to regulate online content, which makes any or all information spread online, particularly on social media, somewhat unreliable (Cvjetićanin et al., 2019).

In response to the COVID-19 pandemic the Bosnian administration has started imposing new limitations on freedom of speech in order to limit the spread of fake news and conspiracies about the virus. There are concerns over these new restrictions as they appear to be abused in order to target opposition representatives and citizens critical of pandemic-related measures (Kovačević, 2020). Additionally, restrictions vary between entities and districts, making the situation somewhat unclear and confusing for citizens (Kovačevic, 2020; RFE/RL, 2020). Additionally, Balkan Insights collected a total of 163 cases of digital rights being breached during the virus pandemic across several countries in Eastern Europe, including BiH (Ristic, 2020).

An Overview of Cyber Troop Activity in Bosnia and Herzegovina

Organizational Form

The stopfake.org website, an initiative to monitor and report fake news in the Ukraine and surrounding countries, reports that most disinformation in BiH is disseminated through local media; however, foreign media, notably the Serbian edition of Sputnik, Sputnik Srbija, is increasingly active in spreading disinformation through local language radio broadcasts and social media which predominantly disseminates anti-West rhetoric (EU vs Disinfo, 2020).
According to an EU-backed report by the citizens' association Zašto Ne? (Why Not?), foreign influence is most strongly exerted through connections with BiH-based media outlets, which use each other as sources and redistributors of disinformation, forming a disinformation hub used by local and possibly foreign actors to influence public opinion. The hub contains twenty-nine media outlets in total, fifteen of which are located in Serbia and fourteen in BiH (twelve of the latter in Republika Srpska) (Cvjetićanin et al., 2019). According to local journalists the media outlet Television of Republika Srpska (RTRS) as well as the News Agency of Republika Srpska (SRNA) are the main two sources of misinformation in the entity of Republika Srpska (European Western Balkans, 2019).

Disinformation stems from two major categories of actors: 'opportunistic disinformers' operating mostly through anonymous websites and social media accounts with financial gain as the primary motive; and political and state actors who spread disinformation via public and commercial media outlets to mobilize support for their political agendas. Anonymous websites account for two thirds of disinformation monitored by Zašto Ne?, spawned by an industrious ecosystem of content production and dissemination on social media. The authors state, “The congruence of media disinformation and specific political interests raises concerns over targeted disinformation campaigns in the online sphere, some related to foreign actors and sources” (Cvjetićanin et al., 2019).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Bosnia and Herzegovina

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
	National News Agencies			x	x

Source: Authors’ evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

According to the Zašto Ne? researchers, more than 60% of online disinformation in BiH is political in nature, focussing on the US administration and the EU, whose ‘value system’ is often portrayed as undesirable for local cultures. Clickbait, fake news, disinformation, and conspiracy theories are the most common forms of biased reports. Most activities seem focused on sharing and further disseminating fake news (Cvjetićanin et al., 2019). Sputnik Srbija has been particularly active in sharing narratives attacking the West, particularly the EU, since 2015 over six hundred articles have been shared, ranging from stories on the EU failing during the refugee crisis to driving divisions between Balkan countries by depicting the Western Balkans as a “battlefield” of the EU (EU vs Disinfo, 2020). Analyses reported on by Zašto Ne? researchers also show that Sputnik Srbija tends to have a positive bias towards the Alliance of Independent Social Democrats (SNSD), a Serbian nationalist and extremist party involved in governing both entities of BiH (Cvjetićanin et al., 2019).

A majority of the targets of biased reporting in BiH are political parties, politicians, and institutions. Moreover, about 60% of them are local. For the most part it appears that political actors affiliated with the SNSD are presented in a positive light, while those in opposition with SNSD are portrayed negatively (Cvjetićanin et al., 2019). Much of the activity within the country seems comparably rudimentary, with disinformation being shared through news outlets while there is no evidence of more sophisticated automated or data-driven strategies, though no evidence does not mean such activities are not happening.

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Bosnia and Herzegovina

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Human	Support Attack Opposition Driving Divisions	Disinformation Amplifying Content	

Source: Authors’ evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

Information on cyber troop activity within Bosnia and Herzegovina is scarce. Given the fragmented state of the country and its government, most domestic disinformation activity focuses on conflicts between different political forces. Many of the narratives are disseminated from outlets controlled by forces outside of the country. For those located inside, there exists little to no evidence to tie them to any one particular actor or party, although the perspectives they share give hint as to whom they sympathize with. Still, sympathizing alone is not enough to claim that particular outlets are working directly for a specific party.

The sharing and production of fake stories seems quite consistent, though it cannot be said with certainty that they are run by national state actors. Considering the general disorganization of the state, its cyber troop capacity and coordination is thus quite limited.

Table 3: Cyber Troop Capacity in Bosnia and Herzegovina

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
		Temporary	Liminal	

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

References

CIK Media. (2017, December 6). UZBUNA U BiH| Nakon što je Bakir danas branio Bosnu prev Vučiće i Čovićem: Pogledajte šta je Ministar odbrene Srbije poručio…. *CIK Media*. https://cik-media.com/uzbuna-u-bih-nakon-sto-je-bakir-danas-branio-bosnu-prev-vucice-i-covicem-pogledajte-sta-je-ministar-odbrene-srbije-porucio/

Cvjetićanin, T., Zulejhić, E., Brkan, D., & Livančić-Milić, B. (2019). *Disinformation in the online sphere: The case of BiH* (p. 100). Zašto Ne? https://zastone.ba/app/uploads/2019/05/Disinformation_in_the_online_sphere_The_case_of_BiH_ENG.pdf

EU vs Disinfo. (2020, May 27). Sputnik Srbija narratives fuel East-West division in Western Balkans, NATO Stratcom Report finds. *StopFake*. https://www.stopfake.org/en/sputnik-srbija-narratives-fuel-east-west-division-in-western-balkans-nato-stratcom-report-finds/

European Western Balkans. (2019, December 5). Disinformation and fake news widespread in the Western Balkans. *European Western Balkans*. https://europeanwesternbalkans.com/2019/12/05/disinformation-and-fake-news-widespread-in-the-western-balkans/

Freedom House. (2020) *Freedom House | Bosnia and Herzegovina*. Freedom House. https://freedomhouse.org/country/bosnia-and-herzegovina/freedom-world/2020

Kovacevic, D. (2020, March 19). Bosnia's Republika Srpska Imposes Fines for Coronavirus 'Fake News.' *Balkan Insight*. https://balkaninsight.com/2020/03/19/bosnias-republika-srpska-imposes-fines-for-coronavirus-fake-news/

Kovačević, L. (2020, March 24). ŠIRENJE ISTINE ILI PANIKE: Korona virus kao alibi za policijsku represiju. *Zurnal.Info*.

RFE/RL. (2020, March 24). OSCE Concerned About Measures Against "Fake News" In Bosnia. *Radio Free Europe/Radioi Liberty*. https://www.rferl.org/a/osce-concerned-about-measures-against-fake-news-in-bosnia/30507012.html

Ristic, M. (2020, June 3). Insults, Leaks and Fraud: Digital Violations Thrive amid Pandemic. *Balkan Insight*. https://balkaninsight.com/2020/06/03/insults-leaks-and-fraud-digital-violations-thrive-amid-pandemic/

Brazil

Introduction

Organised social media manipulation strategies for political campaigning emerged in Brazil as early as 2010. These early efforts included the use of fake accounts to disseminate content in support of Dilma Rousseff propaganda, as well as misinformation about opposition candidate José Serra via blogs and Orkut, Brazil's main social media channel at the time (Gragnani, 2018a). In her second presidential election in 2014 it played a major role in the campaigns of Rousseff and Aecio Neves, as well as in later regional elections, and it became crucial in the campaign that ultimately led to her impeachment (Arnaudo, 2017). The use of computational propaganda has increased year-on-year.

Prior to the 2018 general elections, Brazilian authorities were aware of and responsive to the threat of online disinformation, and even introduced standard practices to prevent these strategies from contaminating campaigns. In 2017, the Superior Electoral Court (TSE), the body responsible for running the elections in Brazil, passed electoral reforms that explicitly prohibited fake accounts, automation, and disinformation for campaign purposes (Resolução N° 23.551/2017, n.d.).

However, freedom of expression continues to be undermined in Brazil, with attacks on opposition parties and the deployment of disinformation and hate speech, which has become "more explicit every day" (Santana, 2020). Journalists who are critical of the government, such as Patricia Campos Mello, Constança Rezende, and Glenn Greenwald, are not only being targeted by Bolsonaro's supporters, but also by serving politicians who openly encourage attacks and hate speech, particularly against minorities. For instance, in one of his YouTube addresses Jair Bolsonaro attacked Bianca Santana, a black journalist and activist exposed the links between Bolsonaro's family and the paramilitary group behind the killing of councilwoman Marielle Franco in 2018 (Santana, 2020).

It is also worth noting that in late June 2020, the Senate passed a law holding online platforms with more than two million users to regulate themselves to stop the creation and spread of disinformation and defamatory content. Moreover, the bill bans mass messaging and asks instant messaging apps to "store message chains forwarded over a thousand times for 15 days, so that the source of the content that goes viral can be identifies if legally required" (Mari, 2020). It also addresses the disclosure of spending, targeted audiences, and identification of the responsible entity for political campaign ads if legally required to do so (Mari, 2020).

An Overview of Cyber Troop Activity in Brazil

Organizational Form

During the October 2018 presidential elections, Movimento Brasil Livre (MBL) a political party running for the first time, shared false information on their portals (Maleronka & Declercq, 2018). Bolsonaro's campaign also employed bulk messaging and coordinated influence campaigns, often using disinformation, among other strategies to attack the opposition. There is significant evidence that both Flávio and Eduardo Bolsonaro were actively involved in their father's campaign, with their phone numbers having been linked to the administration of at least nine and eleven pro-Bolsonaro WhatsApp groups, respectively. Additional collaborators acted as content curators, shared disinformation, and monitored groups (Nemer, 2020), in some cases being paid for these activities (Nemer, 2019). Some of these groups remain active at the time of writing. Other supporters formed part of a virtual militia called the Virtual Activist Movement (MAV), which operated by infiltrating WhatsApp groups and disseminating disinformation (Nemer, 2019). Evidence surfaced from the 2018 campaigns that private companies— both foreign and domestic—were contracted for mass messaging services, including the Brazilian internet marketing company Yacows (Ricard & Medeiros, 2020). AM4 Company worked for Bolsonaro’s campaign to send bulk messages to 1,500 WhatsApp groups and “revert negative episodes in favour of Bolsonaro’s campaign” (Evangelista & Bruno, 2019). Other companies, including credit agencies such as Serasa Experian, sold databases for targeted advertisement, and even leaked databases from phone companies were used by parties to target users over WhatsApp. At least four companies—Yacows, Quickmovile, SMS Market, and Croc Services—were involved in digital advertising for political parties. In addition Steve Bannon, who was vice president at Cambridge Analytica and friend of the Bolsonaro family, collaborated with the campaign (Ricard & Medeiros, 2020).

However, these activities were not the limit of private companies’ involvement in the campaign. Even though the private financing of political campaigns is prohibited in Brazil, Bolsonaro’s campaign was nonetheless largely financed by the private sector (Ricard & Medeiros, 2020). For example the businessman Paulo Maurinho was one of the people who financed the militia organized within pro-Bolsonaro WhatsApp groups to coordinate propaganda (Nemer, 2019).

As Jair Bolsonaro has assumed the presidency, he has repeatedly used his social media accounts to disseminate propaganda, attack journalists, and even to divert public debate. Although the government has denied its existence, several accounts from whistle-blowers indicate there is a team of people within the offices of the President, coordinated by Eduardo and Carlos Bolsonaro and tasked with overseeing the creation and dissemination of disinformation and hate speech (Caccia Bava, 2020). Members of this group include not only bloggers, but also lawmakers and figures from the business community (Santana, 2020). This structure has been referred to as Gabinete do Ódio (in English, Cabinet of Hate) and is currently under stigation through a formal Comissão Parlamentar Mista de Inquérito (CPMI).

Furthermore, according to Facebook, the pro-Bolsonaro page Bolsofeios, which targets opposition figures and disseminates hate speech was created with an IP address located in the Chamber of Deputies. Additional evidence on the telephone number and email registered on the admin of the page point towards Eduardo Guimarãe, the parliamentary secretary of deputy Eduardo Bolsonaro (PSL-SP) (Redação A Tarde, 2020).

Other individuals also play critical roles in the development and dissemination of governmental propaganda. According to Nember (2019), Taíse de Almeida Feijó, a former employee at AM4 Company, was hired as an adviser to the Office of the Secretary General of the Presidency. Social media influencer Jouberth Souza, journalist Oswaldo Eustáquio, and blogger Allan dos Santos have also been identified as acting to spread disinformation favourable to Bolsonaro. They also own websites as well as accounts that amplify government’s propaganda (DFRLab, 2020).

In July 2020, Facebook removed Instagram and Facebook accounts, pages, and groups based in Brazil that were involved in coordinated inauthentic activities targeting domestic audiences. According to the company, they "found links to individuals associated with the Social Liberal Party and some of the employees of the offices of Anderson Moraes, Alana Passos, Eduardo Bolsonaro, Flavio Bolsonaro, and Jair Bolsonaro" (Gleicher, 2020).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Brazil

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
2010	Evidence found	Evidence found (Eg. Social Liberal Party, Eduardo Bolsonaro, Flávio Bolsonaro, Taíse de Almeida Feijó, Eduardo Guimarãe)	Evidence found (Eg. AM4 Company, Havan, Yacows, Steve Bannon)		Paid supporters Virtual Activist Movement (MAV) Businessmen (Eg. Paulo Maurinho) Social media, bloggers, journalists, and influencers (Jouberth Souza, Allan dos Santos, Oswaldo Eustáquilo)

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Whilst computational propaganda has been in use in Brazil since 2010, it was particularly evident in the 2018 elections, and "fake news" became a major concern. Authorities were handling sanctions quickly, and the Superior Electoral Court (Tribunal Superior Eleitoral, TSE) subpoenaed Facebook to remove over 196 pages that contained false information, including the page of Movimento Brasil Livre, a major force in the impeachment of Rousseff and Bolsonaro's rise (Maleronka & Declercq, 2018).

Brazil has shown quite an innovative spirit towards political propaganda and the 2018 election was marked by a few incidents illustrating this characteristic. First, the concept of politicians as social media celebrities and influencers is not a novel phenomenon in Brazil. In fact, the current President Jair Bolsonaro started doing live-broadcasts and putting videos on YouTube as early as 2016. Interestingly, this approach took on a different direction when certain politicians became carriers of disinformation themselves. Congresswoman Joice Hasselmann spread false information accusing the Rousseff's Workers' Party of having ties with the Hezbollah (Joao Filho & Felizardo, 2018). She also alleged that one of the mainstream media companies had a contract worth up to 600 million reais (approximately £130 million) to support the Workers' Party.

In the weeks leading up to the first round of elections, which took place on 3 October 2018, Brazilians complained about the large volume of disinformation circulating on social media. However, research by the Oxford Internet Institute has shown that traffic on Twitter was particularly low (Machado et al., n.d.). Multiple reports released in the period between the first and second rounds of voting, along with findings from investigative journalists, showed that the bulk of Brazilian disinformation was being disseminated through WhatsApp. Over 120 million Brazilians use the platform regularly, making it an effective way of reaching the entire population (Paulo Higa, 2018). As research has shown, the total volume of disinformation spread over WhatsApp was at least eleven times greater than the total dissemination of junk news on Twitter, and clustered networks of WhatsApp groups were used to disseminate disinformation to thousands of users (Machado et al., 2019).

Further research also showed that the Brazilian public was consuming disinformation not only in the form of news articles, but also via audio-visual content, such as memes, false audio testimonies and even edited videos. One piece of research analysed the top fifty images being disseminated on 347 WhatsApp groups, with a staggering total of 107,256 images being shared (Chico Marés e Clara Becker, 2018). Only four of the analysed images were in fact genuine. YouTube and Facebook links were being shared to disseminate false and inflammatory content over WhatsApp, as closed platforms became vehicles for content that went viral on open ones. As investigative journalist Patricia Mello later revealed, Brazilian firms had contracts with advertising agencies in the United States to promote digital advertising in Brazil (Campos Mello, 2018). Further research revealed that data brokerage was being used to promote targeted ads in the campaign (Bruna Martins dos Santos & Joana Varon, 2018). Mass messaging services were also used by several candidates. For instance, AM4 Company worked for Bolsonaro's campaign by spreading content to around 1,500 WhatsApp groups, including some material created by the agency (Evangelista & Bruno, 2019). They used targeted content, which was sent according to how members of groups were identified as supporters, detractors, or neutral to the campaign.

Disinformation also played a major role outside the campaign, including during the 2018 truckers' strike, which paralyzed truck transportation throughout the country and caused billions of dollars' worth of damages to the economy. Another tragic case was a rumour that alleged that former councilwoman Marielle Franco was the wife of one of Rio de Janeiro's drug lords. This rumour was released two hours after her murder in March 2018 (Gragnani, 2018b). This disinformation was released mostly over WhatsApp, and the company has reacted to pressure from authorities and civil society to reduce the virality of inflammatory content on their messaging system. Nonetheless, some Twitter profiles linked to Bolsonaro invited users to new platforms such as Gab and Telegram, where there is less content moderation or possibility of dialogue between the platform holders and authorities (DFRLab, 2018). As examined by DFRLab (2018), Brazil became one of the main sources of users on the platform. In 2018, content about Bolsonaro represented "a significant proportion" and the most influential accounts were linked to the Brazilian far-right.

Despite peaking during the 2018 Brazilian elections, disinformation strategies did not die out after the campaign. Some of the WhatsApp groups coordinated by Flávio and Eduardo Bolsonaro continue to operate, and have become more radical (Nemer, 2020) As disagreement emerged, so did new groups. According to Nemer (2019), these groups can currently be categorized as either, government propaganda (the most extreme supporters), insurgency (prior supporters who are now part of the opposition), or social supremacy (aligned with the far-right speech). WhatsApp has been widely used for political propaganda. In fact, between October 2018 and September 2019, WhatsApp banned at least 1.5 million Brazilian users because of automation, disinformation, and hate behaviour (Militão & Rebello, 2019).

Joice Hasselmann, who was a prior ally of Bolsonaro, has denounced that "a group of presidential staff routinely spreads fake news and defames the opposition across social networks as part of their day job" (Mari, 2019). She has also said that the so-called Cabinet of Hate uses sentiment analyses to make decisions on their strategies and takes advantage of the 1.4 million and 468,000 bots that amplify Jair and Eduardo Bolsonaro's tweets, respectively (Mari, 2019).

Several incidents manifest the coordinated activities of pro-Bolsonaro accounts. Online defamation campaigns besieged journalist Patrícia Campos Mello, after she published details on how private companies were providing illegal services to the political campaigns in 2018 (Nemer, 2020). Another journalist, Glenn Greenwald, was similarly targeted after publishing a story about the links of members of the government to corruption and conspiratorial behaviour by the prosecutors and judges behind Lula's prosecution (DFRLab, 2019). Most recently, such attacks have been made against Luiz Henrique Mandetta, former Minister of Health who was fired on 16 April 2020 (DFRLab, 2020). Many others have been targeted in similar ways. These campaigns are boosted by amplification techniques (DFRLab, 2019) and false information (DFRLab, 2020), and they make use of automated accounts (DFRLab, 2019) and multiple forms of media, such as hyper-partisan websites, Facebook groups, Twitter accounts, and WhatsApp groups (DFRLab, 2020). In general, they are also promoted by members of the government, including Jair Bolsonaro himself.

During the first year of Bolsonaro's government, violence against the press increase by 54% (Santana, 2020). According to Reporters Without Borders (2020), since 2020, there is a more performative strategy of attacks designed to discredit journalists and the media, with the president encouraging supporters to attack them publicly. Between January and March 2020, Jair Bolsonaro attacked at least thirty-two journalists, while his son Eduardo has made at least thirty such attacks in March alone. Female journalists receive the most attacks. In fact, out of the twenty gendered attacks in January and February, sixteen were made by state officials. Moreover, judicial harassment and calls for boycotts, such as calls for advertisers to prioritize pro-government media- are becoming more common (Reporters Without Borders, 2020).

Most recently, Bolsonaro has been criticized for putting the population at risk by generating and spreading disinformation on the Coronavirus. For instance, he "distorted a speech by a WHO director", proclaimed that people should use the unproven anti-malarial drug hydroxychloroquine, and attacked scientists (João Filho, 2020). As a result, Twitter, Facebook, and Instagram deleted some of his content online, such as videos of his tour in a commercial area with no respect for social distancing, and the promotion of hydroxychloroquine, one of the first major world leaders to be corrected in such a way (Reporters Without Borders, 2020). Within the first months of the coronavirus spreading, both he and government members disseminated "over one hundred examples of false information" (Ricard & Medeiros, 2020). Additionally, the network of Instagram and Facebook accounts, groups, and pages taken down by Facebook on July 2020 and linked to the Social Liberal Party not only posted about the pandemic but also published hate speech content and criticisms of the opposition, including journalists (Gleicher, 2020).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Brazil

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Bots and Human Real and Fake	Pro-government, pro-party, Attacks on opposition, Distracting messages, Driving polarization, Suppressing speech	Disinformation, Data-driven strategies, Trolls, Amplifying content	WhatsApp, Facebook, Twitter, Instagram

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

During the 2018 election campaigns, Bolsonaro spent at least twelve million reais (around US$3 million) on a contract with the company Havan to send massive messages via WhatsApp (Campos Mello, 2018). According to Campos Mello (2018), sending out WhatsApp messages cost from 0.08 to 0.12 reais for using databases owned by the campaigning party and up to 0.40 reais for databases that belong to an advertising company.

The WhatsApp groups that were coordinated by Flávio and Eduardo Bolsonaro were organized in a pyramid-like structure. Some members had specific roles, such as admin, moderator, and distributor (Nemer, 2020) and received between R$400 and R$1000 per week (Nemer, 2019). Although there is evidence of their continued operations, there is no further evidence yet on a rewards scheme.

Finally, it has been suggested that Bolsonaro's administration has deployed an office dedicated to spreading disinformation and promoting hate campaigns (Caccia Bava, 2020). The Gabinete do Ódio is said to have a coordinated structure inside the Planalto Palace. According to deputy Joice Hasselmann, for every campaign set to amplify Bolsonaro's messages, the Office spends around 20,000 reais ($4,800) of public cash (Mari, 2019). The use of state sponsored resources and organization to finance, direct, and deploy these operations has the potential to greatly increase their effect on political discourse and societal polarization, as demonstrated in the review above.

Table 3: Cyber Troop Capacity in Brazil

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
	Bolsonaro's 2018 election campaign: Bulk messaging on WhatsApp: US$ 3 million contract WhatsApp groups: distributors: ~R$ 400/week admins: ~R$ 600/week content creators: up to R$1,000/week	Permanent and Temporary	Somewhat Centralised	Medium

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

References

Arnaudo, D. (2017). Computational Propaganda in Brazil: Social Bots During Elections. *Computational Propaganda Project Working Paper Series*, *2017*(8). http://comprop.oii.ox.ac.uk/2017/06/19/computational-propaganda-in-brazil-social-bots-during-elections/

Bruna Martins dos Santos, & Joana Varon. (2018). *Data and Politics—Brazilian Country Report*. Coding Rights. https://ourdataourselves.tacticaltech.org/media/ttc-data-and-politics-brazil.pdf

Caccia Bava, S. (2020, April 29). As milícias digitais do capitão—Le Monde Diplomatique. *Le Monde Diplomatique*. https://diplomatique.org.br/as-milicias-digitais-do-capitao/

Campos Mello, P. (2018, October 18). *Empresários bancam campanha contra o PT pelo WhatsApp*. Folha de S.Paulo. https://www1.folha.uol.com.br/poder/2018/10/empresarios-bancam-campanha-contra-o-pt-pelo-whatsapp.shtml

Chico Marés e Clara Becker. (2018, October 17). [Agência Lupa] O (in)acreditável mundo do WhatsApp. *Agência Lupa*. https://piaui.folha.uol.com.br/lupa/2018/10/17/whatsapp-lupa-usp-ufmg-imagens/

DFRLab. (2018, September 24). *#ElectionWatch: Migration to Gab in Brazil – DFRLab – Medium*. https://medium.com/dfrlab/electionwatch-migration-to-gab-in-brazil-67a1212c4c76

DFRLab. (2019, July 3). *Real Users Inadvertently Boost Bot Campaign Against Glenn Greenwald in Brazil*. Medium. https://medium.com/dfrlab/real-users-inadvertently-boost-bot-campaign-against-glenn-greenwald-in-brazil-fcbcf0e9ef57

DFRLab. (2020, April 21). How Bolsonaro's disinfo machine targeted Brazil's pro-quarantine health minister. *Medium*. https://medium.com/dfrlab/how-bolsonaros-disinfo-machine-targeted-brazil-s-pro-quarantine-health-minister-95e0cbe6d146

Evangelista, R., & Bruno, F. (2019). WhatsApp and political instability in Brazil: Targeted messages and political radicalisation. *Internet Policy Review*, *8*(4). https://policyreview.info/articles/analysis/whatsapp-and-political-instability-brazil-targeted-messages-and-political

Filho, João. (2020, April 12). Coronavírus: Mentiras fabricadas pelo 'gabinete do ódio' ditam ações do presidente no combate à pandemia. *The Intercept*. https://theintercept.com/2020/04/12/gabinete-odio-coronavirus-bolsonaro/

Filho, Joao, & Felizardo, N. (2018, October 27). *Joice Hasselmann deu a largada para as maiores mentiras da eleição*. https://theintercept.com/2018/10/26/joice-hasselmann-mentiras/

Gleicher, N. (2020, July 8). Removing Coordinated Inauthentic Behavior. Retrieved July 18th 2020 from https://about.fb.com/news/2020/07/removing-political-coordinated-inauthentic-behavior/.

Gragnani, J. (2018a, March 21). *Fake profiles boosted Brazilian ex-president Dilma*. https://www.bbc.com/news/blogs-trending-43371212

Gragnani, J. (2018b, April 20). *Pesquisa inédita identifica grupos de família como principal vetor de notícias falsas no WhatsApp*. https://www.bbc.com/portuguese/brasil-43797257

Machado, C., Kira, B., Hirsh, G., Marchal, N., Kollanyi, B., Howard, P., Lederer, T., & Barash, V. (n.d.). *News and Political Information Consumption in Brazil: Mapping the 2018 Brazilian Presidential Election on Twitter*. The Computational Propaganda Project. Retrieved 12 May 2019, from https://comprop.oii.ox.ac.uk/research/brazil2018/

Machado, C., Kira, B., Narayanan, V., Kollanyi, B., & Howard, P. (2019). A Study of Misinformation in WhatsApp Groups with a Focus on the Brazilian Presidential Elections. *Companion Proceedings of The 2019 World Wide Web Conference*, 1013–1019. https://doi.org/10.1145/3308560.3316738

Maleronka, A., & Declercq, M. (2018, July 25). Rede de páginas de fake news do MBL é derrubada pelo Facebook. *Vice*. https://www.vice.com/pt_br/article/gy355w/rede-de-paginas-de-fake-news-do-mbl-e-derrubada-pelo-facebook

Mari, A. (2020, July 1). *Brazilian Senate passes fake news bill*. ZDNet. https://www.zdnet.com/article/brazilian-senate-passes-fake-news-bill/

Mari, A. (2019, December 9). *Fake news probe in Brazil exposes 'Office of Hate' within government*. ZDNet. https://www.zdnet.com/article/fake-news-probe-in-brazil-exposes-office-of-hate-within-government/

Militão, E., & Rebello, A. (2019, September 30). WhatsApp bane ao menos 1,5 mi de contas no Brasil por robôs e fake news. *UOL*. https://noticias.uol.com.br/politica/ultimas-noticias/2019/09/30/whatsapp-fake-news-robos-envio-em-massa-eleicoes-2018-contas-banidas.htm

Nemer, D. (2019, August 24). Grupos pró-Bolsonaro no WhatsApp não se desmobilizaram com a vitória. Pelo contrário, estão mais radicais. *The Intercept*. https://theintercept.com/2019/08/23/grupos-pro-bolsonaro-whatsapp-estao-mais-radicais/

Nemer, D. (2020, February 14). Eduardo e Flávio Bolsonaro são criadores de WhatsApp de mentiras. *The Intercept*. https://theintercept.com/2020/02/14/eduardo-flavio-bolsonaro-criadores-whatsapp-mentiras-jornalista/

Paulo Higa. (2018, July 19). *Facebook tem mais usuários que WhatsApp no Brasil e chega a dois terços da população – Negócios*. Tecnoblog. https://tecnoblog.net/252119/facebook-127-milhoes-usuarios-brasil/

Redação A Tarde. (2020, March 4). Dados enviados pelo Facebook ligam Eduardo Bolsonaro à contas falsas. *Portal A TARDE*. http://www.atarde.com.br/politica/noticias/2121456-dados-enviados-pelo-facebook-ligam-eduardo-bolsonaro-a-contas-falsas

Reporters Without Borders. (2020, April 16). *Brazil quarterly analysis. President Bolsonaro's systematic attempts to reduce the media to silence | RSF*. Reporters Without Borders. https://rsf.org/en/news/brazil-quarterly-analysis-president-bolsonaros-systematic-attempts-reduce-media-silence

Ricard, J., & Medeiros, J. (2020). Using Misinformation as a political weapon: COVID-19 and Bolsonaro in Brazil. *Harvard Kennedy School Misinformation Review*, *1*(COVID-19 and Misinformation). https://doi.org/10.37016/mr-2020-013

Resolução nº 23.551/2017. Retrieved 26 May 2019, from http://www.tse.jus.br/legislacao-tse/res/2017/RES235512017.html

Santana, B. (2020, June 22). Jair Bolsonaro accused me of spreading 'fake news'. I know why he targeted me | Bianca Santana. *The Guardian*. http://www.theguardian.com/commentisfree/2020/jun/22/jair-bolsonaro-fake-news-accusation-marielle-franco

Cambodia

Introduction

The Cambodian People's Party (CPP) has been ruling Cambodia for over thirty years. Over the years, media freedom has declined, and the government has taken actions towards tightening restrictions and enabling pro-government outlets to dominate the local media landscape.

In May 2018, the major media outlet Phnom Penh Post was sold to a Malaysian investor known to have links to Prime Minister Hun Sen (Wiseman, 2019). That same year, in the run-up to the elections, media outlets, including the Cambodia Daily was forced to shut down, Voice of Democracy's and Voice of America's news and education programs were banned on FM radio stations, and Radio Free Asia's office in Phnom Penh was forced to close (Freedom House, 2019; Wiseman, 2019), and activists and citizens in general were harassed and intimidated for their posts on social media, leading to high levels of self-censorship (Freedom House, 2019).

In late 2019, the director-general of the General Department of Information and Broadcasting announced the intention to revoke licenses of media outlets considered to be spreading disinformation and to block media outlets "not officially registered with the Ministry of Information, or not using the country's .kh Internet domain" (Wiseman, 2019).

Most recently, in the context of COVID-19 pandemic, the government has been actively monitoring social media to identify people who post content related to what they label as "false rhetoric" (Turton, 2020). At the beginning of the pandemic, the Information Ministry accused forty-seven Facebook accounts and pages of purposefully spreading misinformation about the COVID-19, and as of April 2020 (Human Rights Watch, 2020b), at least thirty people had been arrested on charges of promoting "fake news" (Human Rights Watch, 2020a).

An Overview of Cyber Troop Activity in Cambodia

Organizational Form

There is evidence of bots and fake accounts being used by politicians to boost their popularity on social media. Prime Minister Hun Sen has been accused of artificially boosting his popularity, by hiring foreigners to create fake accounts and increase the number of fans of his page (BBC News, 2016). Launched in 2015, Hun Sen's Facebook page had almost nine million followers in 2017 and was ranked by global public relations firm Burson-Marsteller as the eighth most popular of any world leader (Paviour, 2017).

In March 2016, local outlet the Phnom Penh Post reported that the majority of Hun Sen's recent likes came from foreign accounts. The single biggest groups of likes came from Indian accounts (255,692), with significant numbers also from the Philippines (98,256), Myanmar (46,368), Indonesia (46,368) and several others, according to the Post (Nass & Turton, 2016). It is suspected that these followers are not real. According to the report, companies running offshore 'click farms' might be behind them, in which low-paid workers create fake accounts to help bolster likes, followers and views on their clients' social media profiles (Nass & Turton, 2016). Lawyers for the opposition leader Sam Rainsy asked Facebook for information about the account of Hun Sen, including as spending on advertisements and the purchase of likes. However, (as of May 2019) the filed case is still under examination (Freedom House, 2019) and its result might define Facebook's role in the region.

Cambodian citizens have frequently been targeted by authorities over political speech on Facebook critical of the ruling party (Dara & Baliga, 2018). In 2014 the Council of Ministers' Press and Quick Reaction Unit created a task force known as the Cyber War Team, which monitors, collects and diffuses information on social media platforms to "protect the government's stance and prestige" (Blomberg & Naren, 2014). In a ministerial order signed on 28 May 2018, three ministries agreed to work with telecoms firms "to prevent the spread of information that can cause social chaos and threaten national security." (Vicheika, 2018).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Cambodia

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
	Ministry of Information, Cyber War Team at the Press and Quick Reaction Unit	Evidence found			Evidence found

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

In Cambodia, as reported in many other Southeast Asia countries, many journalists, academics, and political figures appeared to have gained hundreds of new Twitter followers at the beginning of 2018. Prominent Twitter users in Thailand, Vietnam, Myanmar, Taiwan, Hong Kong and Sri Lanka noticed the same phenomenon—a surge in followers from anonymous, recently created accounts, adopting local sounding names but barely engaging on the platform (The Straits Times Staff, 2018). In each country, the accounts use regionally authentic names, languages and profile photos to follow local influencers (Ruiz & Saksornchai, 2018).

The accounts were created in March 2018 and have since followed hundreds of Twitter users, but most have not tweeted or accrued any followers themselves (O'Byrne, 2018). Hundreds of the accounts with Cambodian names have followed a variety of Cambodia-based Twitter users, including the Ministry of Education, the Quick Press Reaction Unit, Australian Ambassador to Cambodia Angela Corcoran, the CNRP's Deputy Director-general of Public Affairs Kem Monovithya, and dozens of reporters at Cambodia-based news outlets (O'Byrne, 2018). For example, Maya Gilliss-Chapman, a Cambodian tech entrepreneur, said her Twitter account @MayaGC was being swamped by a daily deluge of follows from new users. She says she acquired over 1,000 new followers since the beginning of March (The Straits Times, 2018). Danielle Keeton-Olsen, an American journalist in Cambodia, said her Twitter followers surged from about 700 to over 1,700 in April 2018 (Ruiz & Saksornchai, 2018). Some affected users have speculated that one or more state actors might be behind the new accounts (Reed, 2018).

The proliferation of false information is a problem in Cambodia, as it is for other countries in the region. The government and the opposition often accuse each other of spreading false information, including leaked conversations about corrupt business dealings and politicians' infidelity (Hutt, 2017). Prime Minister Hun Sen regularly accuses critical media outlets of spreading "fake news" (Lema & Wongcha-um, 2018). The term "fake news," however, is routinely manipulated by politicians in order to stifle criticism against them (Dara & Baliga, 2018).

In November 2019, Sam Rainsy, the main opposition party leader, planned to return from self-exile. This triggered a disinformation campaign co-ordinated by the Press and Quick Reaction Unit which was mainly oriented towards mischaracterizing his statements and intimidating the opposition through fake "forced confession videos from his supporters" (Nachemson, 2019).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Cambodia

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Bots, Fake Human	Support, Attacks on opposition	Disinformation, amplifying content	Twitter, Facebook

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

Freedom House (2017) also reported allegations of paid content manipulation made in late 2016 "involving an online activist and social media celebrity, Thy Sovantha", who is claimed to have been offered US$1 million from representatives of the prime minister to lead campaigns against acting CNRP President Kem Sokha (Sokhean and Meyn, 2016).

Table 3: Cyber Troop Capacity in Cambodia

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
		Permanent	Decentralised	Medium

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

References

BBC News. (2016, March 18). Hun Sen denies buying Facebook likes. *BBC News*. https://www.bbc.co.uk/news/world-asia-35839701

Blomberg, M., & Naren, K. (2014, April 20). *'Cyber War Team' to Monitor Web—The Cambodia Daily*. https://english.cambodiadaily.com/news/cyber-war-team-to-monitor-web-72677/

Dara, M., & Baliga, A. (2018, April 6). Hun Sen 'mulling fake news bill'. *Phnom Penh Post*. https://www.phnompenhpost.com/national/hun-sen-mulling-fake-news-bill

Freedom House. (2019). *Freedom of the Net | Cambodia*. Freedom House. https://freedomhouse.org/country/cambodia/freedom-net/2019

Human Rights Watch. (2020a, April 29). *Cambodia: Covid-19 Spurs Bogus 'Fake News' Arrests*. (2020a, April 29). https://www.hrw.org/news/2020/04/29/cambodia-covid-19-spurs-bogus-fake-news-arrests

Human Rights Watch. (2020b, April 10). *Cambodia: Reporter Jailed for Quoting Hun Sen on COVID-19*. (2020b, April 10). https://www.hrw.org/news/2020/04/10/cambodia-reporter-jailed-quoting-hun-sen-covid-19

Hutt, D. (2017, May 9). *Fake news, real danger in Southeast Asia*. http://www.atimes.com/article/fake-news-real-danger-southeast-asia/

Lema, K., & Wongcha-um, P. (2018, January 22). 'Fake news' crutch used by SE Asian leaders to control media,... *Reuters*. https://www.reuters.com/article/us-asia-mediafakenews-analysis/fake-news-crutch-used-by-se-asian-leaders-to-control-media-critics-charge-idUSKBN1FB0F8

Nachemson, A. (2019, November 5). *Cambodia launches online disinfo campaign to repress opposition groups*. Coda Story. https://www.codastory.com/disinformation/cambodia-disinfo-opposition/

Nass, D., & Turton, S. (2016, March 9). Only 20 per cent of PM’s recent Facebook ‘likes’ from Cambodia. *The Phnom Penh Post*. https://www.phnompenhpost.com/national/only-20-cent-pms-recent-facebook-likes-cambodia

O’Byrne, B. (2018, April 2). Twitter bots begin following Southeast Asian opinion-makers. *Phnom Penh Post*. https://www.phnompenhpost.com/business/twitter-bots-begin-following-southeast-asian-opinion-makers

Paviour, B. (2017, October 31). What a Facebook experiment did to news in Cambodia. *BBC News*. https://www.bbc.co.uk/news/world-asia-41801071

Reed, J. (2018, April 18). South-east Asia sprouts fake followers for prominent Twitter users. *Financial Times*. https://www.ft.com/content/e59dba5a-421d-11e8-803a-295c97e6fd0b

Ruiz, T., & Saksornchai, J. (2018, April 20). Someone’s Building a Twitter Bot Army in Thailand. *Khaosod English*. http://www.khaosodenglish.com/featured/2018/04/20/someones-building-a-twitter-bot-army-in-thailand/

Sokhean, B., & Meyn, C. (2016, December 11). *Threats, Guns Enter Crusade Against Kem Sokha*. The Cambodia Daily. https://english.cambodiadaily.com/editors-choice/threats-guns-enter-crusade-kem-sokha-121837/

The Straits Times Staff. (2018, April 22). Surge in anonymous Asia Twitter accounts sparks bot fears. *The Straits Times*. https://www.straitstimes.com/asia/se-asia/surge-in-anonymous-asia-twitter-accounts-sparks-bot-fears

Turton, S. (2020, March 24). *Cambodia locks up critics over ‘fake’ coronavirus news: Rights group*. Nikkei Asian Review. https://asia.nikkei.com/Politics/Cambodia-locks-up-critics-over-fake-coronavirus-news-rights-group

Vicheika, K. (2018, June 6). Cambodia Forms Task Force to Monitor ‘Fake News’ on Social Media. *VOA Cambodia*. https://www.voacambodia.com/a/cambodia-forms-task-force-to-monitor-fake-news-on-social-media/4425534.html

Wiseman, J. (2019, October 1). Cambodia ‘fake news’ laws tighten noose on press freedom. *International Press Institute*. https://ipi.media/cambodia-fake-news-laws-tighten-noose-on-press-freedom/

China

Introduction

The disinformation landscape in China is particularly complex. A wide range of state, state-sponsored, and volunteer actors actively use computational propaganda as a tool for censorship and control. The Chinese government has been involved in multiple disinformation campaigns with international reach, typically to either improve its public image, or to achieve blunt political goals, such as to influence election results in foreign countries. In the past year alone, there have been at least three notable cases of such activity: the pro-democracy protests in Hong Kong, where the government launched extensive disinformation campaigns in order to undermine the legitimacy of the protesters (Borak 2019); the 2020 elections in Taiwan, during which the government attempted to sway the public opinion towards the pro-Chinese candidate (Kurlantzick 2019); and more recently, the outbreak of the global COVID-19 pandemic, in which the government has attempted to clear itself of responsibility, often by spreading disinformation about the pandemic's origin, or depicting China as a saviour-nation (Kao and Li 2020).

An internal EU report on COVID-19 related disinformation, released on April 20, found the Chinese government to be highly involved in the spread of disinformation regarding the virus. The report identified use of both overt and covert tactics, utilizing high levels of coordination between official representatives and departments of the Chinese government and system at large. It also found manipulative Chinese involvement in multiple countries unrelated to COVID-19, indicating a somewhat global strategy and reach. While places like the U.S. and Taiwan were obvious targets for these activities, the report also found pro-China disinformation to appear in less obvious places, like Iran, Italy, and Serbia. Moreover, government propaganda has significantly increased its Arabic content. The report also acknowledged the existence of a "trilateral convergence" of anti-western disinformation narratives between Iran, China, and Russia in regards to the handling and spread of the coronavirus (and how these countries are doing much better than those in the West) (European External Action Service 2020).

An Overview of Cyber Troop Activity in China

Organizational Form

In 2019, the Chinese government launched an extensive disinformation campaign against the democracy protestors in Hong Kong by utilizing Facebook, Twitter and YouTube, platforms that are blocked in China, to spread disinformation, sow discord, and undermine the legitimacy of the activists (Stewart 2019). In June 2020 Twitter took down 23,750 core accounts that have been connected to the Chinese government. They also found around 150,000 accounts designed to boost and amplify content from these core accounts. This network was involved in a range of manipulative and coordinated activities. The accounts tweeted mostly in Chinese and spread geopolitical narratives in favour of the Chinese Communist Party, while also spreading misleading narratives about the political dynamics in Hong Kong (Twitter 2020). Furthermore, Facebook identified seven pages, three groups and five accounts involved in "coordinated inauthentic behaviour" related to the protests**.** YouTube also removed 210 channels that were actively spreading disinformation about the protest (Ibid).

Taiwan has also been a key target for disinformation campaigns coming from mainland China. Despite its relative size, Taiwan is thought to be the country facing the single largest amount of disinformation from outside governments. In December 2019, weeks before their elections, Taiwanese media reported that Facebook removed 118 fan pages, fifty-one accounts, and ninety-nine groups aimed at targeting the island (Magnier 2020).

In general, analysts say that Beijing’s global cyber campaigns tend to focus primarily on Taiwan, Hong Kong, and India’s Tibetan enclave. This is in contrast with Moscow’s more global strategy that is arguably not afraid to go after the inner workings of other global countries. According to Magnier (2020), it seems that China has decided to take on a more globally responsible image, believing this image will serve it better than the Russian “chaos” approach, while still growing its influence within the bounds of its current system and region. Despite this, recent events regarding COVID-19 have provided evidence for the existence of a more global and active state media messaging strategy that “demonstrates disinformation tactics more familiar to coordinated and persistent Russian state sponsored disinformation” (European External Action Service 2020).

Computational propaganda and the manipulation of online content is often used alongside traditional forms of censorship and information control. As early as 2009, news outlets reported that the Chinese Communist Party had raised a "50-Cent Army" of astro-turfers who are rumoured to be paid RMB 0.50 ($0.70) for each patriotic pro-Chinese comment they posted on blogs and social media sites. Despite this rumour, in a study conducted by King et al. (2017) they find that almost all 50c workers in their sample were actually government employees. In the study they argue that most of the posts are about cheerleading the government and promoting positive discussion of valence issues. This is consistent with their theory that the “strategic objective of the regime is to distract and redirect public attention from discussions or events with collective action potential” (Ibid). In terms of activity levels, the study estimates that the “army” writes approximately 448 million 50c posts a year.

In addition to government actors involved in the manipulation of social media, there is evidence to suggest that private companies also operate in China, typically serving the interests of commercial businesses. Since May 2018, more than two hundred people in China have been arrested, and thousands of others confronted by police for taking part in illegal online groups called "wǎngluò shuǐjūn," or Network Navy ("network water army"). Network navies are considered loose organizations of thousands of people recruited through various sites similar to Mechanical Turk, who offer services to companies looking to boost their online presence through “grassroots” marketing and campaigns. According to Chinese government officials these groups have engaged in various illegal activities such as creating spam, fraudulent news sites, and social media trolling in order to shape public opinion. (Gallagher, 2018).

Last year, ProPublica obtained a copy of a contract won by OneSight Technology, a Beijing-based online marketing company, to boost the following of China News Service, the second largest state-owned news agency in the country. They also uncovered a group of coordinated accounts linked to OneSight, indicating the company’s involvement in social media manipulation campaigns regarding Hong Kong and the spread of COVID-19. On the agency’s client list one can find prominent companies like Alibaba and Huawei, but also government media outlets directly run by the government’s propaganda department, like China Daily and CGTN (Kao and Li 2020).

Another private actor operating in China is the American-based company Devumi, which sells Twitter followers and retweets to celebrities, businesses and anyone who wants to appear more popular or exert influence online. Most of the Twitter accounts managed by Devumi resemble real people, and some are even associated with a kind of large-scale social identity theft. At least 55,000 of the accounts use the names, profile pictures, hometowns, and other personal details of real Twitter users, including minors (Confessore et al., 2018). According to The New York Times, an editor at China's state-run news agency, Xinhua, paid Devumi for hundreds of thousands of followers and retweets on Twitter. Even though the Chinese government has blocked Twitter in the country, it is widely used for propaganda abroad (Ibid).

Citizens and youth groups also contribute to computational propaganda campaigns in China. One notable example is the nationalist volunteer social media army known as "little pink", or xiao fenhong, a name derived from the colour of a popular online forum used by nationalists. These young nationalist volunteers usually spread positive messages about China, but also coordinate "mass bombings" of public figures' social media platforms, flooding targets with intimidating posts and shutting down online debate. Their targets are varied, from Taiwan's pro-independence president, to international airlines accused of mistreating Chinese customers (Yang, 2017).

Many members of the "little pink" army belong to the "Emperor's Board", an online forum followed by 29 million people, where "crusades" are coordinated. China's troll army also organises via private groups on Facebook. The most popular of these has 40,000 members, who must express their support for the party before joining. According to the Financial Times, the Communist party provides support for the little pinks, arming them with memes produced by state agencies as well as private studios (Ibid).

In 2014, leaked documents detailed how the Chinese government employed influencers to post pro-government messages on the internet, as part of a broader effort to "guide public opinion" (Sonnad, 2014). Among the leaked documents were instructions, their posting quotas, and summaries of their activity. The emails revealed hundreds of thousands of messages sent through Chinese microblogging and social media services like Sina Weibo, Tencent video, and various internet forums, including working links to the actual posts (Ibid).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in China

Initial Report	Government Agencies	Private Contractors	Civil Society Organizations	Citizens & Influencers
	Chinese embassy in Rome, Chinese Foreign Ministry State owned China Radio International in Italy Cyberspace Administration of China (CAC) The China News Service	Beijing based company OneSight Technology, American-based company Devumi	Nationalist volunteer social media army, known as "little pink", or xiao fenhong	Influencers

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Hong Kong protests: Strategies being used by Beijing's cyber units in relation to the pro-democracy protests in Hong Kong are focused around two main strategies: promoting specific narratives, and attacking dissidents. Content promoted by China-backed manipulators typically attempt to discredit the legitimacy of protesters and promote a positive image of the Chinese government. Some messages have promoted conspiratorial narratives blaming the west for sowing unrest in Hong Kong (Borat, 2019). Accounts found by Twitter and Facebook that were used to promote these messages were hacked, automated, and fake accounts (Kao and Li, 2020).

A typical strategy that has been used for attacking dissidents is “doxing”, which refers to the publishing of private information belonging to a particular individual with the intent of provoking harassment or physical harm. In November 2019, Hong Kong’s Privacy Commissioner for Personal data has reported approximately 2,000 cases of doxing since the protests began. Some of the websites that store these lists of dissident information are based on mainland-Chinese or Russian servers and use so-called bulletproof anonymous hosting. Bulletproof hosting is a service provided by web hosting firms that allows their customers to upload materials that are usually not allowed to be distributed by many regular service providers. By doing so, bulletproof hosts usually allow content providers to bypass the terms of service regulating Internet content in a specific country. These sites have been promoted by groups that are linked to the Chinese Communist Party, which is believed to be responsible for over two hundred cases of doxing (Chan & Blundy, 2019).

Taiwan Elections: A recent study by the V-Dem Institute at the University of Gothenburg in Sweden has found Taiwan to be the country most exposed to foreign false news dissemination. So-called content mills have been disseminating fake news around the country, specifically messages against incumbent president Tsai Ing-Wen who has been a main advocate for disengagement from China. These stories include one that accused her of lying about her Doctorate degree (Kuo & Yang, 2019).

Besides spreading fake news, these media manipulators have been introducing other novel ways in which they can manipulate opinions, argues Jarvis Chiu, senior manager for the Institute of Information Industry in Taiwan. These include armies of trolls that leave comments in strategic places and by such try to shift the focus of the debate. Moreover, fake accounts have been used to share pro-Beijing messages and amplify specific content, while “subliminal attacks” have included repeatedly searching for a candidate’s name in order to influence search algorithms. These attacks have not been directly linked to Chinese state actors, however, some links have been found, including one Chinese defector, Wang Liqiang, who revealed that he was instructed to interfere in Taiwan’s midterm elections in 2018, as well as the presidential elections held in race in January 2020 (Kuo & Yang, 2019).

COVID-19: Italy’s recent battle with the COVID-19 pandemic has received tremendous attention from Chinese disinformation campaigns. With the outbreak of the pandemic in Italy, China has enhanced its dissemination of carefully picked bits of information and narratives depicting it as an ally and saviour of the Italian people. In addition to artificial amplification techniques, such as hashtag manipulation by coordinated bots, it has also partaken in the creation of fake info-graphs and videos. These messages were then widely shared by official accounts tied to the Chinese Government, such as the Chinese embassy, official state media, and other official representatives (DFRLab, 2020).

For example, according to the DFRLab (2020), China's medical aid to Italy was combined with a "carefully designed propaganda strategy pushed through official channels", such as the Chinese Embassy account, who tweeted in support of Italy's struggle. One of the main hashtags tweeted by the embassy's account, #ForzaCinaItalia ("go China and Italy"), reached an abnormally large online crowd. Research later found that over 45% of the accounts that shared the hashtag in the twelve days since it was posted by the embassy were automated accounts. In another case, on 10 March, two days before China sent its medical aid package to Italy, a Facebook page named "Grazie Cina" ("Thanks China") appeared and quickly amassed thousands of followers while exclusively sharing content that was either pro-China or depicting the EU as Italy's main aggravator. For example, one post mentioned that China was "the only serious and responsible interlocutor [for Italy] to tackle this crisis," and condemned Germany and other EU countries for "stealing 800,000 masks" and other medical supplies bound for Italy. Much of the content shared by this page originated from government-affiliated and state media social media accounts, and nearly 40% of accounts who shared the hashtag #GrazieCina were found to be bots (DFRLab, 2020).

In another incident during the pandemic, multiple videos began appearing on social media sites, all depicting Italians playing the Chinese national anthem out of their windows, in praise of its government's assistance to Italy. The videos were widely shared by accounts officially linked to the Chinese government, including the China Global Television Network, the spokesperson of China's foreign ministry, and "Learn Chinese", which has about 3 million followers. However, approximately one week later, research done by Italian fact checkers discovered that all the videos were shot in the same location. Furthermore, all videos used the same audio track, suggesting a coordinated editing campaign based on a singular case rather than a popular movement (DFRLab, 2020).

Like Italy, the US has also not been immune to COVID-based disinformation. In the outset of the pandemic in the US, panic spread in various parts of the country as some Americans received text messages stating the government would soon impose a nationwide lockdown. It was later revealed that these messages were amplified by Chinese agents. The messages were so widespread that the White House's National Security Council had to issue an announcement via Twitter that the messages were fake (Wong et al., 2020). Another case targeting the US occurred on 12 March, one day after the World Health Organization (WHO) declared COVID-19 a global pandemic. The spokesman of the Chinese Foreign Ministry tweeted an article claiming the virus originated and spread in the US, and not China. The tweet received tens of thousands of retweets and likes, with the participation of several diplomatic accounts, and was later reinforced by more false articles repeating the conspiracy (Wallace, 2020).

The Telegraph has found that the Chinese state has also been successfully circumventing social media political ads rules and buying advertisements that praised China's success in handling the COVID-19 crisis. According to the Telegraph "the ads are part of a worldwide propaganda campaign, coordinated across Facebook, Instagram, Twitter and traditional media, attempting to depict China as a global leader in the fight against Covid-19 and drown out accusations that it made the crisis worse by trying to cover up its own breakout" (Dodds & Cook, 2020).

Economic: Beyond spreading disinformation regarding the COVID-19 pandemic, the Chinese government has been also been found trying to push pro-China messages concentrating on economic issues. After President Trump imposed tariffs on China in early 2018, Chinese media outlets received government funds for paid advertising in English on Twitter and Facebook. The goal of these advertisement was to convey the Chinese position on trade and economics to the American people. As such, outlets like China Daily, CGTN, and Global Times (owned by the official newspaper of the Chinese Communist Party) began promoting info-graphs and videos justifying China's position and its willingness to make a deal with Trump (DFRLab, 2019).

The success of these campaigns cannot be measured, however, opinion polls in Ukraine and Slovakia have shown that China is perceived as more helpful during the current pandemic than the EU. Moreover, a poll in Italy has shown that Italians consider China a better international partner than the United States (European External Action Service, 2020).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in China

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Automated, Fake Human	Global influence Enhancing China's image globally during Covid-19 Messages attempting to discredit the legitimacy of protesters in Hong Kong, Pro Chinese government messages, pro-China content in regards to handling of COVID -19 50 cent army promotes mostly positive and distracting messages. Attacking dissidents in Hong Kong Interference in Taiwan elections	Hashtag manipulation, Creation of fake info-graphs and videos, Amplifying content through the use of bots, Spreading fake news regarding Covid-19, Hong Kong Protesters, and Taiwanese politicians Doxxing Political ads abroad	Twitter, Facebook, WeChat, Weibo

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

The scope of government-led activity in the Hong Kong protests is hard to assess, however, data collected from accounts that were deleted by platforms may be revealing. Research found that in at least one large coordinated network, there were over nine hundred "core" accounts, originating from mainland China, that shared content attempting to undermine the Hong Kong protesters' legitimacy. These accounts were significantly amplified by some two hundred thousand automated accounts, engaging with the messages being disseminated (PA Media, 2019).

The amount spent by the government on partnerships with private contracting companies and individuals is unclear, though fragments of evidence have recently surfaced. For example, the contract between state-owned China News Service and private contracting company OneSight, made to increase the company’s Twitter following, was for a sum of approximately $175,000 (Kao and Li, 2020). Some of these companies often approach established influencers with relatively large followings and offer them money in exchange for posting content. Compensation for individual influencers varies according to the size of their following, and potentially, also their geography. Evidence shows that some users were offered between $60 to $360 per post for sharing a photo or video. One Chinese-Australian artist with a Twitter following of seventy thousand was offered $240 to post a fifteen-second clip showing the Chinese government defeated the pandemic (Ibid).

Other evidence suggests that the Chinese government has launched a new project with a contract worth $1 million to operate and help grow its overseas social media accounts (Quartz Staff, 2019). The Cyberspace Administration of China asked that the team be comprised of at least six people who could “tell China’s stories with multiple angles, express China’s voice, and get overseas audience recognition and support for Xi Jinping thought.” This is thought to be part of a wider approach to China’s public diplomacy to “tell China’s story well” mentioned in a speech by president Xi Jinping in 2013. This wider strategy is focused on using China’s own communication channels to promote official Chinese views and opinions and to strengthen China’s international influence (Huang & Wang, 2019).

The contract between the China News Service and the winning bidder OneSight asked for more specific goals, including increasing Twitter followers by 580,000 within six months, and that at least 8% of these followers need to come from North America, Australia, and New Zealand. China’s Ministry of Foreign Affairs put out a similar project for 3.38 million yuan ($480,000) on 21June 2019, five days after two million Hong Kong protestors called for full withdrawal of the extradition bill and for an inquiry into allegations of police brutality. The newspaper Global Times was found to win the contract (Ibid).

Analysts at the US-based cybersecurity firm FireEye have alleged that the Chinese government divides the focus of its various cyber units based on their skill level. Thus, those focused on Hong Kong and Taiwan, places of specific and immediate interest for China, are the highest skilled operatives. Operatives considered to be “more persistent than skilled” worked in units that focused on Southeast Asia and other regions, which are relatively less crucial for Chinese interests (Magnier, 2020). China’s 50-cent army reportedly numbers between 500,000 and 2 million (King et al., 2017).

Table 3: Cyber Troop Capacity in China

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
Around six employees for the CAC project to boost China social media presence abroad. At least 500,000 members of the “50-cent army”.	175,000$ to increase Government news agency “China News Service” Twitter followers. Between 60-360$ paid to influencers per post, “50-cent army” paid workers receive 0.70 $ per post $ 1 million contract to boost China social media presence and influence abroad	900 core accounts working on the Hong Kong protests and over 200,000 automated accounts, Information from 2009 estimated around 500,000 workers in the “50-cent army” that produce around 488,000000 posts a year.	Permanent	High

	$ 180,000 contract between The China News Service and OneSight to boost its Twitter followers at home and abroad. $ 480,000 contract between China's Ministry of Foreign Affairs and the winning bidder Global Times newspaper.			

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Other

In contrast to information operations abroad, China employs an extensive censorship regime domestically. The Chinese government often uses the term "fake news" to delegitimise criticism of the state. The discourse of 'fake news' is used to crack down on dissident voices or discredit opinions that confront the government. According to the Wall Street Journal, "while it didn't explicitly spell out what it meant by 'fake news'," the government has been cracking down on the dissemination of rumours or thinly sourced reports that it says contribute to social instability". According to the People's Daily, nine government departments are involved in the crackdown on such activity (The Wall Street Journal, 2014).

References

Borak, M. 2019. Bots or people? Pro-China disinformation campaigns make it hard to tell. *Abascus.* https://www.abacusnews.com/digital-life/bots-or-people-pro-china-disinformation-campaigns-make-it- hard-tell/article/3023864

Chan, E., & Blundy, R. 2019. 'Bulletproof' China-backed doxxing site attacks Hong Kong's democracy activists. *Hong Kong Free Press.* https://hongkongfp.com/2019/11/01/bulletproof-china-backed-doxxing-site- attacks-hong-kongs-democracy-activists/

Confessore, N., Dance, G. J. X., Harris, R., & Hansen M. 2018. The Follower Factory. *The New York Times.* https://www.nytimes.com/interactive/2018/01/27/technology/social-media-bots.html.

DFRLab. 2019. Made in China: Economic Influence Operations. *Medium*. https://medium.com/dfrlab/made-in- china-economic-influence-operations-733fb07bdc87

DFRLab. 2020. China exploits Italian coronavirus outbreak to expand its influence. *Medium.* https://medium.com/dfrlab/china-exploits-italian-coronavirus-outbreak-to-expand-its-influence- 967a6998fea3

Doctorow, C. 2016. China's online astroturf is mostly produced by government workers as "extra duty". *Boing Boing.* https://boingboing.net/2016/06/13/chinas-online-astroturf-is-m.html.

Dodds, L., & Cook, J. 2020. China Exploits Facebook delays over advertising rules to spread coronavirus propaganda. The Telegraph. https://www.telegraph.co.uk/technology/2020/04/26/china-exploits- facebook-delays-advertising-rules-spread-coronavirus/

European External Action Service. 2020. Disinformation on COVID-19: Information environment assessment. *European External Action Service.*

https://www.documentcloud.org/documents/6877118-INTERNAL- Coronavirus-3rd-Information-Environment.html

Gallagher, S. 2018. China launches salvo against "network navy" of trolls who spread fake news. *Ars Techinca.* https://arstechnica.com/tech-policy/2018/02/china-launches-salvo-against-network-navy-of-trolls-who- spread-fake-news/.

Huang, Z. A., & Wang, R. 2019. Building a Network to "Tell China Stories Well": Chinese Diplomatic Communication Strategies on Twitter. *International Journal of Communication.*

Kao, J., & Li, M. S. 2020. How China Built a Twitter Propaganda Machine then let it Loose on Coronavirus. *ProPublica.* https://www.propublica.org/article/how-china-built-a-twitter-propaganda-machine-then- let-it-loose-on-coronavirus

King, G., Pan, J., & Roberts, M. E. 2017. How the Chinese Government Fabricates Social Media Posts for

Strategic Distraction, Not Engaged Argument. *American Political Science Review.* 111(3), pp. 484-501.

Kuo, L., & Yang, L. 2019. Taiwan's citizens battle pro-China fake news campaigns as election nears. *The Guardian*. https://www.theguardian.com/world/2019/dec/30/taiwan-presidential-election-referendum-on-ties- with-china#maincontent.

Kurlantzick, J. 2019. How China is Interfering in Taiwan's Election. *Council on Foreign Relations.* https://www.cfr.org/in-brief/how-china-interfering-taiwans-election

Magnier, M. 2020. West studies Beijing's disinformation campaign in Taiwan looking for clues into its cyber playbook. *South China Morning Post.* https://www.scmp.com/news/china/article/3045648/west- studies-beijings-disinformation-campaign-taiwan-looking-clues-its

PA Media. 2019. 200,000 Chinese Twitter bots silenced over Hong Kong protests. *Silicon Republic.* https://www.siliconrepublic.com/companies/hong-kong-protests-china-twitter

Quartz Staff. 2019. China's propaganda machine is spending over $1 million to buy influence on foreign social media. *Quartz.* https://qz.com/1691785/chinas-paying-to-build-its-influence-on-foreign-social-media/

Sonnad, N. 2014. Hacked emails reveal China's elaborate and absurd internet propaganda machine. *Quartz.* https://qz.com/311832/hacked-emails-reveal-chinas-elaborate-and-absurd-internet-propaganda- machine/.

Stewart, E. 2019. How China used Facebook, Twitter, and YouTube to spread disinformation about the Hong Kong protests. *Vox.* https://www.vox.com/recode/2019/8/20/20813660/china-facebook-twitter-hong- kong-protests-social-media.

The Wall Street Journal. 2014. China's Big Problem With 'Fake News'. *The Wall Street Journal.* https://blogs.wsj.com/chinarealtime/2014/03/28/china-targets-fake-news/.

Twitter Safety. 2020. Disclosing networks of state-linked information operations we've removed. *Twitter Blog.* https://blog.twitter.com/en_us/topics/company/2020/information-operations-june-2020.html.

Wallace, D. 2020. China promoting US lockdown protests, spreading coronavirus misinformation online: report. *Fox News.* https://www.foxnews.com/world/china-coronavirus-misinformation-american-russia-trolls.

Wertime, D. 2016. Meet the Chinese Trolls Pumping Out 488 Million Fake Social Media Posts. *Foreign Policy.* https://foreignpolicy.com/2016/05/19/meet-the-chinese-internet-trolls-pumping-488-million-posts- harvard-stanford-ucsd-research/

Wong, E., Rosenberg, M., & Barnes, J. E. 2020. Chinese Agents Helped Spread Messages That Sowed Virus Panic in U.S., Officials Say. The New York Times. https://www.nytimes.com/2020/04/22/us/politics/coronavirus-china-disinformation.html.

Yang, Y. 2017. China's Communist party raises army of nationalist trolls. *Financial Times.* https://www.ft.com/content/9ef9f592-e2bd-11e7-97e2-916d4fbac0da.

Colombia

Introduction

Colombia scored 67 in Freedom House's 2019 Freedom on the Net report and is considered a partly free country. Despite this, there are increasing concerns about the growing occurrence of non-transparent surveillance systems, political violence, and self-censorship.

Disinformation strategies are not a new concern in Colombia. Since 2016, when a referendum was held regarding the proposed peace deal between the government and the Revolutionary Armed Forces of Colombia (FARC), disinformation was already in circulation on WhatsApp (Pablo Medina Uribe, 2018). In the same year, a hacker named Andrés Sepúlveda was arrested for illegally accessing government information (Watts, 2019). He confessed to multiple crimes, including hacking and promoting disinformation campaigns in Colombia, as well as many other Latin American countries.

During the 2018 presidential campaign social media played a significant role as a platform for propaganda (Freedom House, 2019) and was again used to spread disinformation and destabilize civil society during the protests of November 2019 (Jakes, 2020). Additionally, there is evidence of the use of data-driven strategies during the last local elections (Ángel, 2019).

Computational propaganda is not deployed constantly in Colombia, rather it increases during elections and other polemicized situations. Despite a modest use of bots (Cortés, 2019), it has been demonstrated that politicians and other high profiles were the most significant actors in originating and amplifying disinformation (Argüello, s. f.; Freedom House, 2019).

An Overview of Cyber Troop Activity in Colombia

Organizational Form

Some academics attribute the narrow victory of 0.2% for the 'No' vote during the 2016 Peace referendum to disinformation, since polls had predicted 'Yes' votes to win by a large margin (Argüello, s. f.). The referendum was aimed to ratify the final peace deal between the government and the FARC guerrillas. The then-president Juan Manuel Santos amended the peace treaty with the FARC and it was approved by Congress. However, there is no further evidence on the organizational form of any disinformation campaign related to these events.

In addition to this, in 2016 the hacker Andrés Sepúlveda reported that he illegally accessed confidential documents, trolled, and even coordinated over 30,000 fake accounts on Twitter to promote disinformation. He has also said that he had been hired by government parties to promote smear campaigns against the opposition and to generate discontent (Watts, 2019).

During the 2018 presidential campaigns computational propaganda techniques were used in favour of the different candidates, though there is not sufficient evidence to attribute any responsibility for such efforts. However, there is evidence that the advertising company Emotions Media Group promoted content production and digital impulsion on behalf of a party during the national elections, although the specific party concern has not been identified (Serrano, 2018).

As LaFM has reported, the following year the Spanish company Eliminalia, which officially purports to erase internet information and data, was found to be involved in the use of computational propaganda for five local campaigns, including that of a candidate for Mayor of

Medellín (Ángel, 2019). Investigative journalism revealed that the company had also been hired for political campaigns in Ecuador and the Dominican Republic.

In addition to the activities of private companies, there have also been reports of co-ordinated efforts within the government to orchestrate disinformation efforts. La Liga Contra el Silencio, a Columbian media alliance dedicated to investigative journalism, released a thorough report on a team comprised of public servants from different departments and other pro-government actors who have since September 2019 been coordinating propaganda actions on Twitter (La Liga Contra el Silencio, 2020).

Finally, it is worth noting that foreign actors also deployed their own computational propaganda resources in the region. A report by the US State Department concluded that during a one-month period in 2019, Russian-linked Twitter accounts operated in Ecuador, Peru, Bolivia, Colombia, and Chile—countries where mass protests and demonstrations were having place— posting similar messages "within 90 minutes of one another" (Jakes, 2020).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Colombia

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
2016	Evidence found	Evidence found	Emotions Media Group, Eliminalia		

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

During the 2018 elections, the spread of disinformation aroused the concerns of the authorities as well as competing parties. A Twitter user identified a network of websites that was used until early 2018 to disseminate political propaganda. This comprised a chain of different sites focussing on varying themes, including pets, cars, beauty, and other topics (Serrano, 2018). As the election approached, the websites introduced political agendas into their content production. For example, one article on a pet website promoted a candidate's stance on global warming. Similar propaganda articles were released throughout the entire network of websites. It transpired that the chain of sites was maintained by an advertisement company called Emotions Media Group, which had been hired to promote content production and digital impulsion on behalf of a given party. However, the party has not been identified.

As well as the dissemination of material intended to promote the interests of particular candidates and parties, computational propaganda techniques were also used to perpetuate online smear campaigns. While attacks on Iván Duque — candidate for Centro Democrático— were focused on his supposed close links to a corrupt elite, attacks on Gustavo Petro— candidate for Colombia Humana— presented the latter as an ally to Nicolás Maduro's regime and a terrorist (Argüello, s. f.; Espinel & Rodríguez, 2019).

The escalation of negative disinformation campaigns led the candidates to sign a "fake news non-aggression treaty" (Politica El Tiempo, 2018), where they agreed to act respectfully towards each other during campaigns and repudiate any malicious use of disinformation against their adversaries. Nonetheless, misinformation continued to abound on social media. In June

2018, before the second round of elections, new hoaxes circulated online. One hoax portrayed former adult actress Mia Khalifa as Gustavo Petro's illegitimate daughter, supposedly voting against her father. Another featured Petro sharing a hoax which portrayed another adult actor as the apparent winner of a quantum physics prize. While it is unclear if either hoax had political intentions, they obtained thousands of shares and followers—the Khalifa post registered 23,000 shares (Penarredonda, 2018). The spread of misinformation remains very high.

One trending disinformation strategy in Latin American countries is to cast doubt on the integrity of the electoral process. These conspiracy theories were repeated in Brazil, Mexico, and in Colombia, but in no case has there been any evidence of large-scale ballot tampering. Though fake accounts imitating politicians and celebrities have been identified, it seems that the bulk of disinformation in Colombia has been disseminated organically (Argüello, s. f.). Many politicians have engaged with fake content and even shared websites that spread blatantly false and polarizing information, such as voces.com.co and oiganoticias.com.

As a result, there have been increasing efforts to introduce fact-checking and verification techniques. These have ranged from mainstream media alliances, such as Semana and El Tiempo, to specific sections in media outlets like Colombia Check, La Silla Vacía and El Poder de Elegir, some of which, for instance, focused on WhatsApp chains (Penarredonda, 2018). The volume of disinformation was far beyond what those bodies could handle and they were often flooded with requests from users.

On the other hand, amplification techniques of pro-government content have been detected in Twitter during 2019. As the Digital Forensic Research Lab (2019a) concluded, in three Twitter campaigns that took place between May and July that year, automated accounts were used to amplify content, although they were not of fundamental importance to the campaign.

Disinformation campaigns were also observed during the protests triggered by the national strike of 21 November 2019. On the one hand, xenophobic messages were spread across social media and WhatsApp, targeting Venezuelans who were accused taking advantage of the turmoil to loot, encouraging panic among the population (Digital Forensic Research Lab, 2019b). At the same time, the president Iván Duque was subject of a trolling campaign exposing details about his private life. Research by Diretoria de Analisis de Politicas Públicas of Fundação Getulio Vargas and Linterna Verde has shown that the incident revealed the use of anti-government cyborg accounts (Cortés, 2019).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Colombia

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Human, Bots, Real and fake accounts	Pro-government, pro-party messages, Driving division/polarization, Trolling and suppressing speech, Attacks on opposition	Disinformation, Amplification strategies, Data-driven strategies, Trolls	WhatsApp, Twitter, Facebook, YouTube

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

Computational propaganda techniques in Colombia have mostly been observed during election campaigns. However, there is also presence of both pro-government and anti-government cyber troops in moments of crisis, as a way to (re)shape debate (Digital Forensic Research Lab, 2019a).

In the case of a pro-government WhatsApp group that coordinated actions on Twitter in late 2019, the team was comprised of public servants working across different departments, such as a consul, the advisor for Innovation and Digital Transformation, Senators' advisors, as well as individuals affiliated to the Centro Democrático party, such as its Coordinator of Youth and previous candidates for local elections. They numbered at least eighty-eight in September 2019. Two people acted as administrators of the WhatsApp group and one as moderator. The moderator sent information about each campaign, such as suggested hashtags and content or immediate results. Moreover, there is evidence that before the creation of the WhatsApp group, members were invited to an event at a Hilton hotel about tools for social media impact (La Liga Contra el Silencio, 2020).

Table 3: Cyber Troop Capacity in Colombia

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
<= 88	-	Temporary	-	Low (2019)

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

References

Ángel, S. (2019, August 22). *¿Quiénes aparecen mencionados por empresa que estaría interfiriendo en elecciones locales?* La FM. https://www.lafm.com.co/politica/quienes-aparecen-mencionados-por-empresa-que-estaria-interfiriendo-en-elecciones-locales

Argüello, L. B., Donara Barojan, Roberta Braga, Jose Luis Peñarredonda, Maria Fernanda Pérez. (s. f.). *Disinformation in Democracies: Strengthening Digital Resilience in Latin America*. Atlantic Council. https://www.atlanticcouncil.org/publications/reports/disinformation-democracies-strengthening-digital-resilience-latin-america

Cortés, C. (2019, December 6). *Ataques como tendencias. La estrategia de los semi-bots*. La Silla Llena. https://lasillavacia.com/silla-llena/red-de-la-innovacion/ataques-como-tendencias-la-estrategia-de-los-semi-bots-71846

Digital Forensic Research Lab. (2019a, August 29). Bot-Like Accounts and Pro-Government Hashtags in Colombia. *Medium*. https://medium.com/dfrlab/bot-like-accounts-and-pro-government-hashtags-in-colombia-35609a5b62f1

Digital Forensic Research Lab. (2019b, December 16). Chaos and panic lead to misinformation after Colombia's national strike. *Medium*. https://medium.com/dfrlab/chaos-and-panic-lead-to-misinformation-after-colombias-national-strike-ff4ae1cd3de3

Espinel, O. A. P., & Rodríguez, L. M. R. (2019). Polarización y demonización en la campaña presidencial de Colombia de 2018: Análisis del comportamiento comunicacional en Twitter de Gustavo Petro e Iván Duque. *Revista Humanidades: Revista de la Escuela de Estudios Generales*, *9*(1 (January-June)), 14.

Freedom House. (2019). *Colombia | Freedom House*. Freedom House. https://freedomhouse.org/country/colombia/freedom-net/2019

Iriarte, R. (2017, August 15). *Colombia's path from revolution to WhatsApp*. https://mobilisationlab.org/colombia-path-revolution-whatsapp/

Jakes, L. (2020, January 19). As Protests in South America Surged, So Did Russian Trolls on Twitter, U.S. Finds. *The New York Times*. https://www.nytimes.com/2020/01/19/us/politics/south-america-russian-twitter.html

La Liga Contra el Silencio. (2020, February 6). *En las entrañas de una 'bodeguita' uribista*. La Liga Contra el Silencio. https://ligacontraelsilencio.com/2020/02/06/en-las-entranas-de-una-bodega-uribista//

Pablo Medina Uribe. (2018, Winter). *In Colombia, a WhatsApp Campaign against *Posverdad**. https://wilsonquarterly.com/quarterly/the-disinformation-age/in-colombia-a-whatsapp-campaign-against-posverdad/

Penarredonda, J. L. (2018, July 20). #ElectionWatch: Everyday Misinformation in Colombia. *DFRLab*. https://medium.com/dfrlab/electionwatch-misinformation-was-everyday-business-in-colombian-election-7b46ab536d9d

Politica El Tiempo. (2018, April 26). *Candidatos presidenciales firmaron pacto por la no violencia en elecciones 2018—Presidenciales—Elecciones Colombia 2018 -*. https://www.eltiempo.com/elecciones-colombia-2018/presidenciales/candidatos-presidenciales-firmaron-pacto-por-la-no-violencia-en-elecciones-2018-209888

Serrano, S. (2018, March 5). *La máquina de noticias engañosas que ayuda a Iván Duque*. ELESPECTADOR.COM. https://www.elespectador.com/elecciones-2018/noticias/politica/la-maquina-de-noticias-enganosas-que-ayuda-ivan-duque-articulo-742761

Watts, J. (2019, April 1). Hacker claims he helped Enrique Peña Nieto win Mexican presidential election. *The Guardian*. https://www.theguardian.com/world/2016/mar/31/mexico-presidential-election-enrique-pena-nieto-hacking

Worley, W. (2018, June 13). *Misinformation Is Shaping the Colombian Election*. Centre for International Governance Innovation. https://www.cigionline.org/articles/misinformation-shaping-colombian-election

Costa Rica

By Simone Bunse
LEAD University, Costa Rica and Georgetown University, USA

Introduction

Costa Rica is one of Latin America's most stable democracies. It has a multi-party political system, holds elections every 4 years, and its media is free and independent.

A small middle-income country with a population of 5 million people, it has a very high level of internet penetration (74% as of January 2020), with 73% of the population actively using social media (Kemp, 2020).

The use of social media for electoral campaign purposes first became visible in 2010. Yet, it was still in its infancy. Parties did not have broad user databases[2] and Facebook usership had just started growing (Global Stats, 2009). It was not until the 2014 election that presidential candidates and political parties integrated social media more prominently into their electoral communications. Nonetheless, most candidates lacked organized e-campaigning strategies (Cruz Romero, 2015). Out of the 5 main contending parties (National Liberation Party (PLN), Social Christian Union (PUSC), Citizen Action Party (PAC), Libertarian Movement (ML), and Broad Front (FA), only two (PLN and PAC) had online campaign strategies in 2014 (Cruz Romero, 2015).

PAC is a newer, largely urban-based party. Its social media userbase had grown organically, from a much younger politically active audience who were already active on social media. PLN, in turn, is a much older and traditional party. Its older and more conservative base was slow to adopt social media. Thus, the PLN had to grow and organize usership to position its agenda on social media somewhat artificially.[3] Their clumsy efforts were noted with disdain during the 2014 presidential debates, when the party tasked some of their members with commenting on social media platforms to support their candidate and criticize opponents.[4]

In 2016, Bloomberg journalists revealed that imprisoned Colombian hacker, Andrés Sepúlveda, had researched the opposition in Costa Rica in early 2013 (Robertson, Riley and Willis, 2016). PLN's presidential candidate, Johnny Araya, admitted having had contacts with Miami-based political strategist Juan José Rendon, for whom Sepúlveda claimed to work. However, Araya denied hiring his firm or any of his associates during the election campaign (Cambronero, 2016). As a result of these revelations, Costa Rica's far-left FA party, whose presidential candidate, José María Villalta, was leading the polls in December 2013 and eventually placed third, accused the PLN of cyber-espionage and asked the country's electoral tribunal TSE to open an investigation. The TSE did so in 2016 but it archived the case in 2018, citing a lack of evidence.[5] In this case it did not take sinister cyber troop activity to damage the credibility of Villalta.[6] Alarmed by the polls, Costa Rica's business community openly organized under the name "Costa Rican Alliance" ("Alianza Costa Rica") to campaign against Villalta. It distributed printed material to companies that portrayed his policies as a threat to the business community, to employment, and to Costa Rica's democracy (Agüero, 2014).

Yet, by 2018 social media had become both an important strategic platform "to launch attacks and spread false information" during the election of that year (OAS, 2018), but also to oppose reforms by the incoming government and polarize society. This report analyzes "cyber troop" activity in Costa Rica since 2018. Following Bradshaw and Howard's (2017; 2018) definition, "cyber troops" are "government or political party actors tasked with manipulating public opinion online". The case study here examines the organizational form, strategies, and tools at the disposal of cyber troops for spreading false information online, and seeks to analyze the capacity and resources invested in online manipulation. It argues that Costa Rican cyber troops are homegrown and homemade, and that various political parties, civil society organizations and individuals have been implicated in spreading disinformation deliberately during election campaigns, promoting anti-establishment populist, homophobic, and xenophobic discourses. However, it also argues that, thus far, cyber troops in Costa Rica have lacked the level of sophistication we have seen in Brazil, Mexico, or Colombia.

Facebook and Twitter have been the most prominent platforms for sharing disinformation. Human trolls are visible on both platforms, but the use of automated bots, cyborgs, hacked or stolen accounts, or the type of targeted advertising observed during the Cambridge Analytica scandal is still very limited.[7]

More recently, attempts by political actors to disinform have moved to the personal messaging system WhatsApp. This is alarming because it makes it much more difficult to uncover systematic political disinformation. Despite watchdogs created by the government and by private actors, as well as efforts by the TSE to stem systematic disinformation, the small size of the country, its high internet penetration and use of social media, combined with weak institutional cybersecurity systems, a low awareness of privacy risks, and widespread digital illiteracy create a fertile ground for the "professionalization" of cyber troop activity ahead of the 2022 elections.

An Overview of Cyber Troop Activity in Costa Rica

Organizational Form

Cyber troop activity in Costa Rica is largely of domestic origin. Various politicians and political parties have been implicated in cyber troop activity. During presidential election campaigns, political parties and their presidential candidates hire national or foreign private contractors, strategists and digital marketing agencies to manage their online campaign rhetoric. Cyber troop activity became particularly visible during the 2018 election campaign but continued in fierce opposition to the incoming government's fiscal and civil service reforms. Cyber troops have also involved civil society organizations and leaders. The analysis that follows provides key examples of how these different actors have tried to mislead Costa Rican citizens.

Political Parties and Their Presidential Candidates

The most visible attempts to manipulate public opinion using social media have been pursued by conservative politicians from parties which have not yet held executive power in Costa Rica: the far-right National Integration Party (PIN) and the religious-right parties called National Restauration Party (PRN) and New Republic (NR).

PIN's presidential candidate and former security minister Juan Diego Castro – an avid Facebook, Twitter and YouTube user – has been dubbed a "Trump in the Tropics" (Grosser, 2018) due to his populist discourse, media appearances, and social media attacks on the integrity of Costa Rica's electoral process.[8] The latter included sharing numerous messages, misleading photos and videos via Facebook and Twitter stating that he had pressed legal charges against the TSE, alleging that it was permitting electoral fraud (Madrigal, 2017). One of his widely shared false conspiracy theories involved a quid pro quo between the PLN and TSE's president Luis Antonio Sobrado, such that the PLN's presidential candidate, Antonio Alvarez Desantí, would win the election and allow his campaign to be financed by Honduran drug money, in exchange for a reform that would be passed by the PLN in parliament that would grant Sobrado a monthly luxury pension of over USD 17,000 (Chinchilla Cerdas and Oviedo, 2018). While pension reform was indeed underway in parliament, it did not contain such a provision.[9] Neither did the TSE receive any legal complaint about illegal campaign financing of the PLN, as claimed by Castro.[10]

The PRN and the NR represent Costa Rica's evangelical community but have also attracted conservative catholic voters. The PRN rose to prominence over its opposition to same-sex marriage, an issue that dominated the 2018 election campaign after the unfortunate, politicized timing of an opinion issued by the Interamerican Court of Human Rights in November 2017 and published in January 2018 (Interamerican Court of Human Rights, 2017). It stated that all rights extended to heterosexual couples should be extended to gay couples. This led to heightened aggression in the campaign rhetoric and a highly polarized political debate which "[eclipsed] all discussion of the parties' manifestos as a whole".[11]

The most prominent case of cyber troop activity linked to the PRN's presidential candidate Fabricio Alvarado, his campaign manager Juan Carlos Campos, and the private political consulting firm Opol Consultores, was the publication of six unrepresentative polls ahead of the runoff presidential election on Opol's media outlet elmundo.cr. Seeking to influence the second round of voting, the polls had been commissioned by the PRN campaign and positioned Fabricio Alvarado consistently between 10 and 15 points ahead (Cambronero, 2018). Alvarado and the PRN shared these polls widely on Facebook and sent audios and videos of the poll results to the Costa Rican press, giving the impression that these were independent polls by a non-partisan polling company.

The publication of a seventh poll was interrupted, as Opol complained about threats by PAC supporters who questioned the company's independence. A month after the election, Opol revealed the link between the misleading polls and Fabricio Alvarado to the TSE, because the PRN refused to pay an invoice of USD 31,200 for the polls. The case sparked a debate in the country about reforming its electoral laws to ensure transparency in relation to the origin and financing of polls.[12]

A second scandal linked to the PRN's electoral campaign involved the obtaining of access to 3.9 million mobile phones (44% of all active mobile lines in Costa Rica) for political propaganda purposes ahead of the run-off presidential election. As such, the party illegally obtained private data from 2.5 million voters (76% of all eligible voters in the country) (Arias Retana, 2019b). An investigation by Costa Rica's leading daily newspaper, *La Nación*, established that the PRN sent 6.4 million text messages between March 14 and 24 with 12 different campaign adds (Arias Retana, 2019b) depending on age, gender and voting location without the required legal consent by the recipients. The biggest activity was registered on the day of a televised presidential debate, when the PRN sent 2 million messages (Arias Retana, 2019b). According to records from the TSE, the USD 230,000 service was provided by ADD Integral Solution[13] who, in turn, subcontracted Tecnologías SMS del Este. The PRN paid another USD 35,000 to ADD Integral Solution for a voter market analysis (Arias Retana, 2019). While this incident involved campaign adds, all messages directed voters to Fabricio Alvarado's Facebook page which contained the questionable polls mentioned above. It also shows that both political parties and private companies have ignored existing legal requirements in their digital advertising efforts, with companies being prohibited from selling private data bases in Costa Rica.

Cyber troop activity in Costa Rica has been higher in election periods, and most false news during the 2018 campaign focused on corruption and religion (Hidalgo, 2019). However, it did not cease after the election. Cyber troop activity has continued to focus on polarizing public opinion on diversity and inclusion issues, has focused on boycotting government reforms, and has followed an anti-immigrant discourse.

One of the most investigated cases was a scandal directedly linked to the NR, a party that was founded by Fabricio Alvarado after breaking away from the NPR in October 2018. The NR (although not officially recognized as a party by Costa Rica's Parliament) currently has six representatives in the legislature. They include Jonathan Prendas, whose brother Francisco Prendas became the president of the party. The scandal concerned the false claim published on the webpage diariolacarta.com (owned by Francisco Prenda's communication firm OBS and founded in May 2019) that the government would raise VAT from 13% to 16% in July 2019 (Sequeira and Chinchilla Cerdas, 2019).

The two Prendas brothers and Fabricio Alvarado subsequently shared the link to the false claim via their social media platforms, from which it was passed on more than 1,100 times by their followers (Cerdas, Sequeira and Oviedo, 2019). Their claim was explosive, even though identified as false by Costa Rica's Treasury and the Government. It came at a time when the country was paralyzed by strikes relating to the implementation of the tax reforms that the Costa Rian Parliament had passed in December 2018 to help address a deep fiscal crisis. The case sparked a fierce parliamentary debate about the destabilizing effects of fake news in Costa Rica's democracy and the involvement of political parties in the spread of false news. Jonathan Prendas defended himself by accusing the government of attacking their nascent media organization and arguing that other political parties were doing the same.

Civil Society Organizations and Individuals

Civil society organizations as well as individual citizens joined the disinformation campaign surrounding the country's reform efforts. Albino Vargas, the Secretary General of Costa Rica's civil servant trade union (ANEP) also shared the false Diario la Carta news via Twitter to mobilize his base to strike against the government.[14] Vargas further rallied secondary students on false claims related, for example, to diversity and inclusion issues and dual education which were also spread via Facebook by the National Educators Association (ANDE).[15] The student leader who organized secondary students via Facebook to join the strikes and stage protests was a former intern of Jonathan Prendas (Cerdas, 2019). The strikes led to the closure of more than 100 secondary schools and forced out the education minister, Edgar Mora. Mora had to resign, inter alia, given the widespread false information that the government would replace separate bathrooms for girls and boys in schools with gender neutral common bathrooms, the creation of a "diversity day" which was claimed would advocate homosexual relationships between children, and over the false claim that the government's new dual education program would force students to work for companies without pay or health insurance. The incident shows how politicians and civil society organizations have used citizens' digital illiteracy to advance their political goals through the deliberate spread of disinformation. Alarmingly, a survey conducted by the University of Costa Rica concluded that two of every ten Costa Ricans admitted to sharing false news via social media or WhatsApp, even though they thought that the information was untrue (CIEP, 2019).

Another group of civil society actors that has frequently and deliberately spread false information to manipulate public opinion online is a group of xenophobic activists, with a network of six to eight different Facebook pages[16] that publish similar information, roughly at the same time.[17] In August 2018, following an influx of Nicaraguan migrants, the group placed a series of untrue claims related to Nicaraguan immigrants on their social media sites within the same week (Artavia, 2018).[18] The images and messages also circulated via WhatsApp, triggering a violent anti-immigration manifestation at the Merced Park, a traditional meeting point of Nicaraguans in the Center of San José. Of the 400 protestors, 44 were arrested (Artavia and Solis, 2018 and Tico Times, 2018). This unprecedented aggression against Nicaraguans in Costa Rica led to a national televised presidential address calling for calm as well as a special session in parliament during which the executive explained how it was managing the situation with the Nicaraguan refugees. A legislative advisor to PRN deputy Carmen Chan subsequently used the incident to share videos and xenophobic audios of the manifestation on the legislator's Facebook page "Costa Rica Unida" ("United Costa Rica") and critique the government's immigration policy (Alfaro, 2018). Another politician exploited the incident to advocate for the withdrawal of the policy of extending Costa Rican citizenship to children born in Costa Rica to Nicaraguan parents.

Since the Merced Park incident, the number of both xenophobic and homophobic Facebook accounts have grown further in Costa Rica, with around 165,000 followers combined (Robles, 2019 and Loaiza, 2019).

Private Contractors

Political parties in Costa Rica have not only worked with polling agencies, but also with private firms whose services include developing trolls. Some of the known cases involve "Soluciones Digitales" and "OW Marketing Agency". The head of OW Marketing, Iván Barrantes, was President Guillermo Solis' digital campaign advisor when the PAC was elected to form government for the first time in 2014. He was paid around USD 190,000 (CRC 111 million) for his services[19] before continuing to work ad honorem for President Solis while maintaining his private clients. This caused an outcry and he resigned his post as special presidential advisor. Since then Barrantes has worked for various other parties in Guatemala and Costa Rica (including the PLN, ML and PRN) during national and municipal elections. A firm believer in "political marketing" (Murillo, 2015), his most recent emphasis seems to be opposition work.[20]

In sum, various political parties, trade unions and other civil society organizations as well as private actors have been implicated in spreading disinformation deliberately during and after elections following an anti-establishment populist discourse or homophobic and xenophobic lines. The growth of the religious right, represented by the PRN and its spin off NR as well as Juan Diego Castro, have visibly contributed to this phenomenon and to an ever more toxic public discourse.[21] Since 2014, private digital marketing companies or strategists have been hired during elections to "develop stories" and "place ideas" (Chinchilla Cerdas, 2018a). Table 1 summarizes the organizational form and prevalence of social media manipulation in Costa Rica.

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Costa Rica

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
2014		National Integration Party (PIN); National Restauration Party (PRN); New Republic (NR)	Opol Consultores (elmundo.cr); ADD Integral Solution; Tecnologías SMS del Este; Grupo Comunicaciones OBS; Soluciones Digitales; OW Marketing Agency	Evidence Found	Evidence Found

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Cyber troops in Costa Rica have relied on different tools and tactics to manipulate public discussions about politics online. As seen by the examples above, politicians or individuals associated with them have not been shy about publishing false claims or conspiracy theories on their own social media platforms, as part of their political communication strategies and to mobilize their supporter base. On other occasions they have used questionable private news outlets to give an impression of independence and credibility. The digital media sources, which have been publicly accused of lacking independence and which have frequently mixed real with fabricated news, have included, but are not limited to, Diario La Carta, Noti Costa Rica, Noti Goico, Noticias Pococí, El Mundo Costa Rica, El Cantor Político, Guana Noticias, and El Guardián. Political activists or individuals have also disseminated false news that have pretended to be from the BBC or the local press via personal Facebook accounts, anonymous Facebook groups and WhatsApp. Sometimes the mainstream media picks up such news or politicians piggyback on false information generated by civil society groups or individuals sharing it with their followers.[22]

Costa Rican legislators employ parliamentary advisors to manage their digital communications. Digital communications have included exaggeration or other forms of misleading imagery to support their agendas. For example, using pictures of automatic and semiautomatic rifles, Carolina Hidalgo, then President of Costa Rica's legislature from the PAC, tweeted misleading information in February 2019 about a motion adopted in the Legislative Assembly's Public Security Committee modifying proposed government reforms of the country's high caliber weapons regulation (Chinchilla, 2019). The image and tweet gave the impression that carrying automatic weapons would no longer be prohibited in Costa Rica after the adoption of the motion, a development that she opposed. However, the possession of automatic rifles remains prohibited. Protecting the status quo, the parliamentary committee instead rejected the incorporation of new legal prohibitions related to the possession of semiautomatic rifles which is allowed under current legislation (Mora, 2019).

Fake accounts and false followers have been detected on occasion, but most accounts are human rather than automated. One expert interviewed by the researcher said:

> "There are always humans behind the trolls, there is very little automation in Costa Rica. So far the problem is "handmade" and there is much room to systemize."[23]

Human trolls which are particularly active on Twitter in Costa Rica. Prominent strategies include defamation and harassment attempts, attacks on the government and the promotion of social unrest. As one interviewee put it, on Twitter a “war is raging between progressive groups and an army of religious trolls.”[24] Another interviewee argued:

> “The real division is not necessarily religion, but it has to do with human rights and social topics. Abortion is a prime example. Even if activist groups do not have a chance to get anywhere in terms of a change in policies, they use social media to feed and mobilize their hard core base to remind them what they are all about.”[25]

Trolls have also been active on Facebook. A well-known independent Costa Rican journalist, radio host and youtuber complained in February 2018 to his 55,000 followers about a troll intimidation attack by Fabricio Alvarado’s campaign after he posted an opinion piece supporting gay rights. The troll attack led to his account being frozen by Facebook for 24 hours.[26] Alvarado’s supporters, in turn, have accused the government of spying and attacking their social media networks. A former parliamentary advisor to legislator Harllan Hoepelman from the PRN (now PR) complained to Costa Rica’s Constitutional Court in February 2020 that, by the means of trolls, the government’s controversial former Presidential Data Analysis Unit (UPAD) reported and blocked his social media pages. Both political parties and the government deny supporting online trolls. The Prosecutor’s Office (“Ministerio Público”) is investigating, but thus far without any concrete results nor a formal accusation.

In sum, attacks on Twitter and Facebook in Costa Rica have lacked the level of sophistication seen elsewhere in the world. Thus far, the TSE has not detected active networks of Twitter bots that are deployed ahead of or during an election to shape or affect a candidate’s image.[27] One interviewee mentioned:

> “If there is any attempt of bots, they are done badly in Costa Rica. For example, in one instance 10 accounts sent the exact same text, so these are easily identified. But any such attempts are disjointed. Theoretically, bots could have much greater impact, but I am not sure this is true for small countries, such as Costa Rica. Here politics is local – so if lies are being spread, for example about immigrants, this travels wide and fast over WhatsApp without the use of bots.”[28]

Similarly, sophisticated “deepfakes”, in which a person in an existing image or video is replaced with someone else to manipulate content, have not yet been generated in Costa Rica for political propaganda purposes. Instead, political activists have usually used existing imagery from elsewhere, making it easy to identify as false. In April 2020, for example, a false picture of supposedly Nicaraguan migrants entering Costa Rica via Boca Tapada was shared widely via Facebook and WhatsApp. In reality, the photo showed a group of Central American migrants crossing the river Suchiate to get from Guatemala to Mexico on their way to the US. It had been published by the AFP a few months earlier. Numerous similar examples have been identified by *La Nación*.

Finally, the systematic use of social media influencers (paid or unpaid) by political parties or other political actors to amplify their messages, has not been an issue in Costa Rican elections to date.

Social Media Platforms

Facebook is by far the frontrunner of all social media platforms in Costa Rica for any cyber troop activity. Surveys since the 2014 election have showed that 70% of voters have used

Facebook for news and information (CIEP, 2014). As of May 2020, active Facebook usership was around 68%, compared to 18% for Pinterest and 10% for YouTube (Global Stats, 2020). Twitter and Instagram trail far behind with under 2% (Global Stats, 2020). Although the general public uses Facebook rather than Twitter, Costa Rican politicians and political activists do have Twitter accounts. One interviewee explained that political activists rely on Twitter to move their issues persistently into the spotlight, so that politicians perceive them not as a fringe debate but as a real social concern:

> "Despite low Twitter usage, repetition pays to affect politicians' perception of the public mood."[29]

More recently, attempts by political actors to disinform have moved to WhatsApp and include voice messages and memes.[30] WhatsApp is used by 83% of the population (Latinobarómetro, 2018). According to research by *La Nación*, 76% of the false news items detected during the 2018 election were distributed via Facebook, 10% appeared in Facebook and WhatsApp, 8% was only shared via WhatsApp, and 6% were on Twitter (Hidalgo, 2019). By July 2019, more than half of all false news identified by *La Nación* circulated via WhatsApp (Arias Retana, 2019c).

To slow the dissemination of false information, WhatsApp has responded with numerous revisions to its mechanics and its terms of use. Until 2018, WhatsApp users had been able to forward a message to 250 groups at once. Given the rapid spread of fake news in personal communications, this was subsequently reduced to 20. In 2019, WhatsApp tightened these limits further, initially to 5 and in April 2020, the company announced that users who receive a frequently forwarded message would only be able to share it to one chat at a time (Hern, 2020). The effect of such policies in Costa Rica remains to be seen. One interviewee mentioned:

> "WhatsApp is a private messaging system, not social media. It is private and hidden. Hence, the WhatsApp fake news phenomenon is a threat that can only be stemmed with greater digital literacy."[31]

Table 2 summarizes the observed strategies, tools and techniques of social media manipulation in Costa Rica.

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Costa Rica

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Human	Polarization strategies including attacks on government reforms, immigration, diversity and inclusion, and religious values/human rights/social issues, Trolling and Harassment, Defamation attempts/accusations of corruption	Facebook pages, disinfo/misinfo websites, including news websites linked to political parties, memes, misleading photos or images from elsewhere	Facebook, WhatsApp, Twitter

Organizational Capacity and Resources

Cyber troop capacity in Costa Rica is low compared to other countries in Latin America. Activities by politicians or their political operatives are still mostly uncoordinated and rely on human accounts and human trolls. Given that the country does not have an army and lacks experience with the type of military intelligence operations seen in other Latin American countries, its current low level of sophistication is unsurprising.

During election periods political parties have small teams working on their digital communications which reduce in size after the elections have finished. As one interviewee said:

> "There is little money for such [cyber troop] campaigns in between elections, they spring up more systematically during election campaigns."[32]

Public data on the amount of resources spent on digital marketing, data mining and cyber troop capacity is almost non-existent. This has been, in part, due to the fact that neither digital marketing agencies nor researchers hired privately during election campaigns need to register with the TSE. Only companies which conduct polls intended to be published during elections and the media which accept money for political advertising need to register by a certain deadline with the TSE. But digital marketing agencies are currently outside of the legislation operating under "a veil of opacity", as one interviewee lamented.[33] In addition, while the TSE looks into spending on marketing, costs to develop trolls, for example, are hidden in the category of digital marketing. Hence, it is difficult to isolate resources spent on political propaganda by cyber troops.

The scandals outlined above reveal some of the resources spent on developing manipulated content or actors which have been involved in the past. They include the USD 31,200 the PRN owed to Opol for the unrepresentative polls, USD 230,000 paid for digital advertising, and USD 35,000 for a voter market analysis to ADD Integral solutions. But the amounts paid on any trolling activity by companies, such as Soluciones Digitales or OW Marketing Agency are unknown.

According to Iván Barrantes, communication strategy fees amount to USD 50,000 per month in Costa Rica (Cambronero, 2014). Of the USD 190,000 he was paid during the 2014 election, almost USD 130,000 (CRC 75 million) was a bonus for winning (Chinchilla Cerdas, 2014; and Cambronero, 2014). Such amounts pale into insignificance compared to the USD 600,000 budget Andrés Sepúlveda had at his disposal for cyber troop activities during Mexican President Pena Nieto's election campaign (Robertson, Riley and Willis, 2016). Table 3 captures cyber troop capacity in Costa Rica.

Table 3: Cyber Troop Capacity in Costa Rica

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
Small	USD 31,200 for unrepresentative polls by Opol; USD 230,000 digital advertising paid to ADD Integral Solution; USD 35,000 to ADD Integral	Mostly Around Election Periods, with some continuity afterwards	Low	Low

	Solution for a voter market analysis; Contracts with Soluciones Digitales, OW Marketing Agency, OBS for unknown amounts.			

Government and Private Responses

Various public and private projects have been undertaken to stem the spread of online disinformation in Costa Rica. These include initiatives by the TSE to protect the integrity of the electoral process, as well as fact-checking projects by the government, the UCR, the digital daily CrHoy.com, and *La Nación*. Each is briefly described below.

TSE initiatives

The TSE has opted to fight disinformation campaigns through education and communication (rather than pursuing a punitive approach). Its strategy rests on three main pillars: a) enhanced digital literacy; b) improved communication; and c) prompt reaction to disinformation campaigns.[34]

The digital literacy program is run by TSE's Institute of the Formation and Study of Democracy (IFED).[35] Since 2019 the program has involved collaboration with Facebook and Twitter. The program started as a pilot project ahead of the 2020 municipal elections to evaluate and improve responses to disinformation before the 2022 general elections. Facebook facilitated the content of workshops in digital literacy and trained TSE officials as instructors. Given the TSE's concern about the spread of false news and to further strengthen the module developed by Facebook, TSE collaborated with the UCR's fact checking initiative "Double Check" (see below) who provided an additional training session on detecting fake news in Costa Rica to TSE officials. A diverse population of 750-760 people received training in digital literacy across the country as a result.[36] Some workshops were conducted with a target audience, including local politicians, municipal leaders, and political youth leaders. Others were open to the public. In a similar agreement, Twitter gave three different seminars to community managers, political parties, and the media on how to identify disinformation and propaganda.

The second pillar of the TSE's strategy has consisted in improving communication by sharing interviews and videos debunking common electoral myths, and explaining electoral processes to journalists, especially municipal elections. The program involved working with directors of major news outlets and opinion formers. According to one interviewee:

> "The goal was to prevent false news from going viral. Developing a relationship and open communication channel with the media was important to ensure that when dubious material is discovered, they doubt it, ask critical questions, and call the TSE to verify before contributing to false news going viral. This way the TSE wanted to save itself a lot of problems."[37]

The third pillar of the TSE's response to disinformation campaigns has involved the implementation of prompt reactions by including in its agreement an open channel with Facebook that contained provisions to take down content which could threaten the integrity of the 2020 municipal electoral process. To achieve this, the electoral judges would be compelled at a first stage to issue a resolution providing evidence to justify their decision. Once justified, the TSE would subsequently be permitted to call a number at Facebook to request that content be taken down.[38] The provision would only be used in extreme situations, for instance when public order or the fundamental right to vote were threatened by fake news or organized social media manipulation. This was not the case during the 2020 municipal elections. Hence, the mechanism has not been used to date. Facebook further agreed to share details with the TSE about the amounts spent on electoral campaign advertising and by whom. Yet, in practice this is only possible if the advertisement is labeled as electoral campaign advertising. One interviewee admitted that:

> "It is unlikely that any sinister activity or deliberate false information campaign will be labeled as electoral campaign advertising, nor is it likely to be paid for by a political party directly."[39]

Facebook offered three additional products to Costa Rica's TSE ahead of the municipal elections. On election day voters upon opening their Facebook page: a) were alerted that the election is taking place, b) automatically got a link to the TSE informing them where they could vote; and c) could share that they voted to incentivize participation. The idea for the 2022 general election is to have in place a similar agreement with Facebook.[40]

A fourth pillar of the TSE's strategy did not come to fruition. The TSE had hoped to create a fact-checking alliance between all main news outlets at a national level with the help of Facebook. The idea was that each news company would assign two of their journalists to an overarching fact-checking team during the election process and would publish the unit's findings in all participating news outlets. The unit would keep ownership of editorial process while enjoying the symbolic support of the TSE. Facebook was subsequently to notify their users of the false news. This initiative failed to take off, given the rivalry between existing individual efforts at fact-checking. These individual efforts include "the Government Clarifies" (Gobierno Aclara) program, the UCR's "Doble Check" (DobleCheck) program, Crhoy.com's initiative "Don't fall for it" ("No Caiga"), as well as the "Don't be Fooled" ("NoComaCuento") project by *La Nación*. Each of them is further explained below.

PAC Government Initiatives

The website "The Government Clarifies", launched on July 31, 2019, was the government's direct response to the incorrect claim that VAT would be raised by 3%. The platform is managed by the Communication Ministry and focuses mainly on anonymous content circulating on social media rather than information produced by the media. The public can follow "Gobierno Aclara" via the website, Facebook, Twitter as well as WhatsApp (Zuñiga, 2019). Of the 18 items identified as false and published by the government (see Table 4) which were circulating on social media or via WhatsApp between 31 July 2019 and 7 June 2020, six had to do with the welfare state, falsely claiming Costa Rican citizens would lose some of their current social benefits (in one occasion to immigrants), three had to do with the corona crisis or natural disasters, two were related to fiscal reforms and the country's liquidity, another two were false govt. endorsements of bitcoin, and a few others concerned false news about the president, related to the first lady, government salaries, the education ministry and transport regulations. 15 out of 18 were false news items that were negative about the government.

Table 4: Summary of anonymous False News on Social Media Identified by the Costa Rican Government (July 2019 - 7 June 2020)

Topic	No. of Items	Type
Welfare State/Social Service Provision	6	negative
Corona Virus	3	negative
Fiscal Reform and Govt. Liquidity	2	negative
Bitcoin	2	positive endorsement
First Lady	1	positive endorsement
Ministry of Education/Education Policy	1	negative
Public Sector Salaries	1	negative
Transport regulation	1	negative
President	1	negative
Total	18	

Source: Author's summary based on archive available at https://aclaraciones.presidencia.go.cr/ .

Private Initiatives

"Double Check" started in October 2018 to contrast news and detect false, misleading statements or half-truths in Costa Rica's political discourse as well as the media. It is financed by the UCR's Office of Dissemination and Information and has been supported by the University Radio and Television (Channel 15), as well as the university newspaper *Semanario Universidad*. Since February 2020, "Costa Rica Noticias", the main public television news program features weekly contributions from "Double Check". The initiative received the 2019 National Journalism Prize Pío Víquez awarded by Costa Rica's Ministry of Culture. Of the 128 items which circulated on social media and were identified as outright false by the editors (rather than misleading) between 1st October 2018 and 5th July 2020, 22 were lies related to the coronavirus, followed by 14 pieces of disinformation on government spending and public sector salaries. Another 14 items were anti-establishment propaganda. 11 items were fake news related to immigration and xenophobic content. Attacks on the government's health policies also featured 11 times. False information relating to taxes and the PAC's fiscal reform were identified 10 times. Another eight pieces related to the 2018 strikes and attacked on the Minister of Education and false news about his policies. Abortion featured seven times, as did false news related to the economy. 5 articles published by Doble Check within this timeframe referred to disinformation on the country's security situation or arms. Pro-government propaganda featured only twice, so did elections. Finally, seven fake news items covered various other topics. The source of at least 17 of these items were current legislators. These results are summarized in Table 5.

Table 5: Summary of Information shared on Social Media Identified as outright false by "Double Check" between 1 October 2018 and 5 July 2020

Topic	No. of Items	Type
Corona Virus	22	positive and negative
Government Spending and Public Sector Salaries	14	negative
Anti-Establishment/Anti-Government	14	negative

Immigration/Xenophobic content	11	negative
Public Health Policy	11	negative
Fiscal Reform and Taxes	10	negative
Strikes	8	negative
Ministry of Education/Education Policy	8	negative
Abortion	7	negative
Economy/Poverty/Debt	7	negative
Various other	7	positive and negative
Security/Arms/Crime	5	negative
First Lady/Pro-Government Propaganda	2	positive endorsement
Elections	2	negative
Total	128	

Source: Author's summary based on archive available at https://doblecheck.cr/. Only articles which were marked with an "X" as false were included, not items which were identified half-truths.

Similarly, the project "Don't Fall for it" started after the 2018 elections to counteract the impacts of false content that circulates on the Internet. It was developed by the influential news website crhoy.com, owned by the banker and former finance minister Leonel Baruch.

The only fact-checking initiative which monitored social media during the election was *La Nación's* "Don't be Fooled" project, which started in January 2018.[41] Readers were invited to submit stories to be verified by *La Nación* which subsequently published examples of false claims in its online edition (BBC Monitoring, 2018). Given the success of the project it continued after the election. During its first year of operation, the initiative debunked 209 items (Mora, 2019), of which 63 were circulating during the election (Hidalgo, 2019) and 51 were related to the fiscal reform (Arias Retana, 2019a). As such 54% of all false news items were related to two issues: the general election as well as the incoming government's fiscal reform attempts (Arias Retana, 2019a).

Conclusion

Social media in Costa Rica has become an important strategic political campaign tool. While there is no systematic "weaponization of social media" to engineer election results, numerous political parties, trade unions and individual citizens have discovered the potential of social media for political campaigning since the Cambridge Analytica scandal in the US.

The deliberate spread of disinformation during and after elections has become particularly visible since 2018, when religious parties significantly consolidated their presence within Costa Rica's political landscape. Both the PRN and the PR have frequently been linked to the spread of fake news, the publication of unrepresentative opinion polls, the recruitment of trolls, and harassment on Facebook and Twitter.

The production of political propaganda in Costa Rica is still predominantly a home-grown and human activity. Neither the TSE nor private initiatives have found any sophisticated attempts at automation, or the use of professionally manipulated imaging to mislead voters. Since the

2018 election, disinformation attempts have focused on local contentious social and political topics. Exploiting existing polarization, key themes include corruption, government reforms, immigration, as well as abortion and marriage equality.

While Facebook and Twitter remain the most prominent platforms to share disinformation, the use of WhatsApp has risen sharply. Increasing digital literacy in the country is hence crucial. Fact-checking has been an important response both by the government and private actors. So too have efforts by the TSE to stem the emergence of systematic disinformation. Nonetheless, observers fear that there will be a progressive professionalization of cyber troop activity in Costa Rica ahead of the 2022 elections, given the small size of the country, its high internet penetration and use of social media, its weak institutional cybersecurity systems, and a low awareness of privacy risks and digital literacy.

References

Agüero, M. (2014, January 15) "Grupo Alianza Costa Rica Pide Advertir a Empleados Sobre José Maria Villalta" (Available at: https://www.nacion.com/el-pais/politica/grupo-alianza-costa-rica-pide-advertir-a-empleados-sobre-jose-maria-villalta/CR22UO4CUNECTDLPDUYPTRFHTE/story/).

Alfaro, J. (2018, August 20) "Diputada de Restauración Nacional Acuerpa a Asesor que Respaldó Marcha Xenophóbica", Semanario Universidad. (Available at: https://semanariouniversidad.com/pais/diputada-de-restauracion-nacional-acuerpa-a-asesor-que-respaldo-marcha-xenofobica/).

Arias Retana, G. (2019a, January 15) "#NoComaCuento: Mayoría de Noticias Falsas Surgió con Elecciones y Reforma Fiscal, durante el 2018". *La Nación*. (Available at: https://www.nacion.com/no-coma-cuento/mayoria-de-noticias-falsas-surgio-con-elecciones/TUQMI7BUWFCFTANXHTZDTVBWVI/story/).

Arias Retana, G. (2019b, December 9) "Restauración Nacional Obtuvo Datos Privados de 2,5 Milliones de Cotantes sin Consentimiento". *La Nación*. (Available at: https://www.nacion.com/el-pais/politica/restauracion-obtuvo-sin-consentimiento-datos/SYADJQEIKRHLTNI76BUMZHJHLI/story/).

Arias Retana, G. (2019c, July 21) "Noticias Falsas en WhatsApp se Multiplicaron en el Primer Semestre del Año". (Available at: https://www.nacion.com/no-coma-cuento/noticias-falsas-en-whatsapp-se-multiplicaron-en-el/6N6P2UP7XNFJXGASUZWJDTJZM4/story/).

Arias Retana, G. and Hidalgo, A. (2019, June 21) "#NoComaCuento: Noticias Falsas en WhatsApp se Multiplicaron en el Primer Semestre del Año" (*La Nación*, 21.6.2019) (Available at: https://www.nacion.com/no-coma-cuento/noticias-falsas-en-whatsapp-se-multiplicaron-en-el/6N6P2UP7XNFJXGASUZWJDTJZM4/story/).

Arrieta, E. (2016, March 31) "Frente Amplio Pide a Fiscalia Investigar Incursión de Hack en Campaña 2014". (Available at: https://www.larepublica.net/noticia/frente_amplio_pide_a_fiscalia_investigar_incursion_de_hacker_en_campana_2014).

Artavia, S. (2018, August 18) "Ola de Noticias Falsas Antecedió Agresiones". *La Nación*. (Available at:https://www.nacion.com/el-pais/politica/ola-de-noticias-falsas-antecedio-agresiones/KAC4GDBPIBGSXG5RQ4GACQGTYA/story/).

Artavia, S. and Solís, G. (2018, August 18) "20 Detenidos por Agresiones Xenofóbicas en San José". *La Nación*. (Available at: https://www.nacion.com/el-pais/politica/20-detenidos-por-agresiones-xenofobicas-en-san/WKDKQGKT7RCV7K6ZKOMRFZPXOE/story/).

BBC Monitoring (2018, March 30) "'Don't be Fooled' – Busting Fake News in Costa Rica". (Available at: https://monitoring.bbc.co.uk/product/c1dp0mdj).

BBC News (2018, February 5) "Costa Rica Goes Into Run-Off as Evangelical Lead". (Available at: https://www.bbc.com/news/world-latin-america-42938510).

Bloomberg News (2016, May 12) "Colombian Election Hacker Moved From Protective Custody". (Available at: https://www.bloomberg.com/news/articles/2016-05-12/colombian-election-hacker-moved-from-protective-custody).

Bolaños, D. (2019, July 23) "Video de Sindicato Difunde Falsedades Sobre Educación Dual desde el 2016". *Double Check*. (Available at: https://doblecheck.cr/video-de-sindicato-difunde-falsedades-sobre-educacion-dual-desde-el-2016/).

Bradshaw, S. and Howard, P. N. (2017) "Troops, Trolls and Troublemakers: A Global Inventory of Social Media Manipulation". *COMPROP Working Paper Series.* (Available at: https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdf).

Bradshaw, S. and Howard, P. N. (2018) "Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation". *COMPROP Working Paper Series.* (Available at: http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/07/ct2018.pdf).

Cambronero, N. (2014, August 5) "Estratega de Luis Guillermo Solís recibió 75milliones en premios por ganar las elecciones" (*La Nación*, 5.8.2014) (Available at: https://www.nacion.com/el-pais/politica/estratega-de-luis-guillermo-solis-recibio-c-75-millones-en-premios-por-ganar-las-elecciones/EIELTHLXORAWXFNGGDGU4VZFEA/story/).

Cambronero, N. (2016, April 1) "Hacker Andrés Sepúlveda Informó a Bloomberg de que en Costa Rica Hizo un Trabajo Normal", *La Nación* (1.4.2016) (Available at: https://www.nacion.com/el-pais/politica/hacker-andres-sepulveda-informo-a-bloomberg-de-que-en-costa-rica-hizo-un-trabajo-normal/NTORSMNFR5AVNEYABH5A7QKQ2A/story/).

Cambronero, N. (2018, May 24) "Encuestas de Opol se hicieron por encargo de Restauración Nacional de cara a segunda ronda". *La Nación.* (Available at: https://www.nacion.com/el-pais/politica/encuestas-de-opol-se-hicieron-por-encargo-de/67BL2AJD2FGCPHG7CMMIPTCXFU/story/).

Cerdas, D. E. (2019, July 30) "Dirigente estudiantil 'bromea' con cobre de 'la mensualidad' a Albino Vargas por organizarle bloqueos". *La Nación.* (Available at: https://www.nacion.com/el-pais/educacion/dirigente-estudiantil-bromea-con-cobro-de-la/BHXF43XTORFPXLEIZBQMV5JA6Y/story/).

Chinchilla Cerdas, S. (2018a, February 23) "Fabricio Alvarado se Acerca a Estratega de Campaña de Luis Guillermo Solís y Antonio Alvarez". *La Nación*. (Available at: https://www.nacion.com/el-pais/politica/fabricio-alvarado-se-acerca-a-estratega-de-campana/DQW2JQCKMBDVXHGZMZEMYSKHLU/story/).

Chinchilla Cerdas, S. (2018b, November 2) "Tras la Pista de Una Página que Difunde Noticias Falsas en Costa Rica". *La Nación.*(Available at: https://www.nacion.com/el-pais/politica/tras-la-pista-de-una-pagina-que-difunde-noticias/OLNERNVJY5GY5IZARECMHWO5TM/story/).

Chinchilla Cerdas, S. (2019a, July 28) "Extrañas Alianzas Impulsan Protestas". *La Nación.* (Available at: https://www.nacion.com/el-pais/politica/extranas-alianzas-impulsan-protestas/YBMDGEQQ6BBGVGTCQ53VERRRDY/story/).

Chinchilla Cerdas, S. (2019b, October 2) "TSE se Alia con Facebook y Twitter Para Combatir Noticias Falsas de Cara a Elecciones Municipales". *La Nación.* (Available at:

https://www.nacion.com/el-pais/politica/tse-se-alia-con-facebook-y-twitter-para-combatir/CSION76QV5GHFDDUH7KNWPXHMQ/story/).

Chinchilla Cerdas, S. and Oviedo, E. (2018, January 5) "#NoComaCuento: Juan Diego Castro cuestrinonó al presidente del TSE con base en una premisa falsa". *La Nación*. (Available at: https://www.nacion.com/el-pais/politica/juan-diego-castro-cuestiono-al-presidente-del-tse/2N6V5M3WDZEAZFVGZYZBWPTW2M/story/).

Chinchilla Cerdas, S.; Sequeria, A. and Oviedo, E. (2019, July 31) "Página ligada a presidente de partido fabricista difunde noticia falsa sobre aumento del IVA". *La Nación*. (Available at: https://www.nacion.com/el-pais/politica/pagina-ligada-a-presidente-de-partido-fabricista/IAWX7HSMFJGCFF37D5ALQE5LQ4/story/).

Chinchilla, D. (2019, February 23) "Carolina Hidalgo Divulgó Información Imprecisa Sobre Rifles de Alto Calibre" (Doble Check, 2019, February 23) (Available at: https://doblecheck.cr/carolina-hidalgo-divulgo-informacion-imprecisa-sobre-rifles-de-alto-calibre/).

CIEP (2014) "Electoral opinion poll" (University of Costa Rica: San José. January 2014).

CIEP (2019) "Informe de Resultados de Estudio de Opinion Sociopolítica – Audiencias Noticiosas de Medios Digitales" (University of Costa Rica: San José. July 2019). (Available at: http://cicom.ucr.ac.cr/wp-content/uploads/2019/07/Informe-Audiencias-noticiosas-de-medios-digitales.pdf?fbclid=IwAR3FTLuEY9oDYd_4jdqgNysgsX0JiQFmx3Fz5Mgdb-zSHfOk1APYQ2dto_c).

Colburn, F. and Cruz, A. (2018) "Latin America's Shifting Politics: The Fading of Costa Rica's Old Parties" *Journal of Democracy*, Volume 29, Number 4, October 2018, pp. 43-53.

CrHoy.com (2018, August 18) "Videos: Fuera Alvarado Gritan Manifestantes en la Merced". (Available at: https://www.crhoy.com/nacionales/videos-fuera-alvarado-gritan-manifestantes-en-la-merced/).

Cruz Romero, R. (2015) "Social Networks and Politics: The Use of Facebook in the Costa Rican 2014 Presidential Election" *International Journal for e-Learning Security (IJeLS)*, Volume 5, Issue 2, September 2015.

Diario Extra (2020, August 5) "Utilizan Logo de Diario Extra para montar Noticias Falsas". (Available at: https://www.diarioextra.com/Noticia/detalle/409933/utilizan-logo-de-diario-extra-para-montar-noticias-falsas).

Doble Check Costa Rica (Available at: https://doblecheck.cr/).

El País (2016, April 1) "El Hacker Colombiano que Incomoda a Varios Goberinos de América Latina. (Available at: https://elpais.com/internacional/2016/04/01/america/1459533039_924819.html).

Gallagher, E. (2018, February 9) "Interview with Colombian Hacker Andrés Sepúlveda". (Available at: https://medium.com/@erin_gallagher/interview-with-colombian-hacker-andr%C3%A9s-sep%C3%BAlveda-f985fe860f7f).

Global Stats (2009) (Available at: https://gs.statcounter.com/social-media-stats/all/costa-rica/)

Gobierno Aclara (2018, July 31) "Ministerio de Comunicación Lanza Plataforma Digital Contra la Desinformación". (Available at: https://aclaraciones.presidencia.go.cr/ministerio-de-comunicacion-lanza-plataforma-digital-contra-la-desinformacion/).

Gobierno Aclara. (Available at: http://aclaraciones.presidencia.go.cr/).

Grosser, S. M. (2018, January 9) "A Trump in the Tropics? Why a Demagogue Became the Leading Contender in Costa Rica's Upcoming Election". *OXPOL*. (Available at:

https://blog.politics.ox.ac.uk/a-trump-in-the-tropics-why-a-demagogue-became-the-leading-contender-in-costa-ricas-and-what-this-means-for-the-upcoming-election/).

Hern, A. (2020, April 7) "WhatsApp to Impose new Limit on Forwarding to Fight Fake News" (The Guardian, 7.4.2020). (Available at: https://www.theguardian.com/technology/2020/apr/07/whatsapp-to-impose-new-limit-on-forwarding-to-fight-fake-news).

Hidalgo, A. (2019, May 4) "Cómo la desinformación se filtró en las elecciones de Brasil, México, El Salvador, Colombia y Costa Rica?". *La Nación*. (Available at: https://www.nacion.com/no-coma-cuento/como-la-desinformacion-se-filtro-en-las/2HOZ6CJV4JGVPFKHCARQCTGFQY/story/).

Interamerican Court of Human Rights (2017) "State Obligations Concerning Change of Name, Gender Identity, and Rights Derived from a Relationship Between Same-Sex Couples (Interpretation and Scope of Articles 1(1), 3, 7, 11(2), 13, 17, 18 and 24, in relation to Article 1, of the American Convention on Human Rights)", Advisory Opinion OC-24/17, Inter-Am. Ct. H.R. (ser. A) No. 24 (Nov. 24, 2017) (Available *at* http://www.corteidh.or.cr/docs/opiniones/seriea_24_eng.pdf).

Inter-American Development Bank (2020) "Reporte Ciberseguridad 2020 – Riesgos, Avances y el Camino a Seguir en América Latina y el Caribe". (Available at: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf).

Kemp, Simon (2020) Digital 2020: Costa Rica. (Available at: https://datareportal.com/reports/digital-2020-costa-rica#:~:text=There%20were%203.76%20million%20internet,at%2074%25%20in%20January%202020).

La Nación (2016, February 14) "Iván Barrantes: Del Triunfo con Luis Guillermo Solís, a la Debacle del Libertario". (Available at: https://www.nacion.com/el-pais/ivan-barrantes-del-triunfo-con-luis-guillermo-solis-a-la-debacle-del-libertario/CH4WHIUFS5BDVMFC7TOTFTNQNI/story/).

Latino Barómetro Database (various years) (Data available at: http://www.latinobarometro.org/latOnline.jsp).

Latinobarómetro (2018) Informe 2018.

Loaiza, V. (2019, October 22) "Página de Detenido por Explosiones Atacaba a Grupos LGBTI y Migrantes con Noticias Falsas". *La Nación*. (Available at: https://www.nacion.com/sucesos/crimenes/pagina-de-detenido-por-explosiones-atacaba-a/DASL6QUH5JEJRLI2OFXNNRAJOM/story/).

Madrigal, L. M. (2020, February 27) "Abogado Denuncia que la UPAD Espió y con Troles Bloquearon sus Redes Sociales". *Delfino*. (Available at: https://delfino.cr/2020/02/abogado-denuncia-que-la-upad-le-espio-y-con-troles-bloquearon-sus-redes-sociales).

Madrigal, R. Q. (2017, November 28) "Juan Diego Castro Presenta Denuncia Privada Sobre Fraude Electoral". *La Nación*. (Available at: https://www.nacion.com/el-pais/politica/juan-diego-castro-presenta-denuncia-privada-sobre/DBZDI3XXWNCABHUEPT6VYTVVWA/story/).

Mayorga, A. (2018, May 30) "Buenos Días De Debajo de la Mesa. *La Nación*. (Available at: https://www.nacion.com/opinion/columnistas/buenos-dias-de-abajo-de-la-mesa/E6D72LBB6RAL3JDABOUOMPGXY4/story/).

Mojica, Y. (2018, August 29) "San José's Little Nicaragua: La Merced Park After the Hate". *Tico Times*. (Available at: https://ticotimes.net/2018/08/29/san-joses-little-nicaragua-la-merced-park-after-the-hate).

Mora, J. A. (2019a, January 30) "Gustavo Arias, Fundador de Proyecto #NoComaCuento de '*La Nación*' recibe mención honorífica en Premio Nacional de Periodismo". *La Nación*. (Available at: https://www.nacion.com/viva/cultura/gustavo-arias-fundador-de-proyecto-nocomacuento/X7I7YEF5JBGAZJJ2EZ6KPLKZDY/story/).

Mora, J. A. (2019b, February 22) "Congreso Enciendo Nueva Polémica por Tendencia de Armas". *Delfino*. (Available at: https://delfino.cr/2019/02/congreso-enciende-nueva-polemica-por-tenencia-de-armas).

Mora, J. A. (2019c, December 9) "Restauración, el TSE y los polémicos mensajes de texto de 126 milliones". *Delfino*. (Available at https://delfino.cr/2019/12/restauracion-el-tse-y-los-126-millones-en-mensajes-de-texto-que-el-tribunal-se-niega-a-pagar).

Murillo, A. (2015, June 28) "Entrevista con Iván Barrantes, Exconsejero de Luís Guillermo Solis: 'Nadie sabe bien qué es el cambio poítico'". *La Nación*. (Available at: https://www.nacion.com/el-pais/politica/entrevista-con-ivan-barrantes-exconsejero-de-luis-guillermo-solis-nadie-sabe-bien-que-es-el-cambio-politico/ROTLIY2ZIFBPVOBDEPB27XY3BI/story/).

Organization of American States (2018a) "Electoral Observation Mission National Elections Costa Rica – Final Report". OAS: Washington DC.

Organization of American States (2018b, February 5) "OAS Electoral Observation Mission in Costa Rica says that the Costa Rican electoral system is robust". (Available at: http://www.oas.org/documents/eng/press/Informe-Preliminar-MOE-CR-2018-Eng.pdf).

Organization of American States Press Release (2014, February 3) "Preliminary Report of the Electoral Observation Mission of the OAS in Costa Rica" (Available at: https://www.oas.org/en/media_center/press_release.asp?sCodigo=E-032/14).

Robertson, J.; Riley, M. and Willis, A. (2016, March 31) "How to Hack an Election" (Available at: https://www.bloomberg.com/features/2016-how-to-hack-an-election/).

Robles, M. (2019, August 26) "#NoComaCuento: Páginas Xenofóbicas Crecen en Facebook a un Año" (*La Nación*, 26.8.2019) (Available at: https://www.nacion.com/no-coma-cuento/paginas-xenofobicas-crecen-en-facebook-a-un-ano/W3X2KQNTCNEZ5G4M4UXHWL33PY/story/).

Ruiz Valerio, J.F. (2017) "Los desafíos de la consolidación electoral: El caso del Tribunal Supremo de Elecciones" *Derecho Electoral*, Primer Semestre 2017, Número 23 (Available at: https://www.tse.go.cr/revista/art/23/ruiz_valerio.pdf).

Sequiera, A. and Chinchilla Cerdas, S. (2019, July 31) "Jonathan Prendas Defiende Noticia Falsa Sobre Alza del IVA en Sitio Web Ligado a él" (Available at: https://www.nacion.com/el-pais/politica/jonathan-prendas-defiende-noticia-falsa-sobre-alza/REH5KMKUOJC43HKI6HOFPUTVYE/story/).

Sonneland, H. K. (2018, January 18) "Explainer – Costa Rica's 2018 Election" (Americas Society/Council of the Americas: 2018 Election Guide). (Available at: https://www.as-coa.org/articles/explainer-costa-ricas-2018-elections).

The Dialogue (2018, January 6) "How Much is Fake News Influencing Latin Elections?. *Latin America Advisor*. (Available at: https://www.thedialogue.org/analysis/how-much-is-fake-news-influencing-latin-elections/).

The Tico Times (2018, August 19) "False Social Media Posts Preceded Anti-Immigrant Protest in Costa Rica". (Available at: https://ticotimes.net/2018/08/19/false-social-media-posts-preceded-anti-immigrant-protest-in-costa-rica).

Tribunal Supremo de Elecciones (2018) TSE DFPP-EE-RA-001/2018.

UCR Noticias (2017, December 20) "Castro y Álvarez consiguen empate técnico en última encuesta del año". (Available at: https://www.ucr.ac.cr/noticias/2017/12/20/castro-y-alvarez-consiguen-empate-tecnico-en-ultima-encuesta-del-ano.html).

Zúñiga, A. (2019, August 1) “Costa Rica Launches Platform Dedicated to Fighting Fake News”. *Tico Times*. (Available at: https://ticotimes.net/2019/08/01/costa-rica-launches-platform-dedicated-to-fighting-fake-news).

CROATIA

Introduction

Croatia is a free democracy, though it continues to suffer from corruption (Freedom House, 2019). The media is trying to adapt to digitalization and the country is home to a vibrant mix of online websites. Croatia suffers from disinformation shared via social media, particularly on Facebook, and on news websites. A negative trend towards restricting media freedom started in 2016 after a snap parliamentary election installed a new government of social conservatives, voting out the social democrats (Peruško, 2020). In early January of 2020 the country held presidential elections, which incumbent President Kolinda Grabar-Kitarović lost to her opponent Zoran Milanović. She blamed her defeat on fake news and sexism, claiming the media landscape is "complete chaos" (Gotev, 2020). The next parliamentary elections were held on 5th July 2020, and the ruling Croatian Democratic Union consolidated their power by winning 66 of the 151-seat parliament (Chadwick, 2020).

According to the 2020 Reuters Digital News Report, Croatia has an internet penetration rate of 92%, and citizens access their news online via computers (65%) and smartphones (78%). Social media networks are increasingly popular for receiving news, including Facebook (55%), YouTube (28%), WhatsApp (16%) and Viber (14%). However, Croatians have very little trust (29%) in the veracity of news on social media (Peruško, 2020), and disinformation is key to this lack of trust. According to a Eurobarometer survey in March 2018, 47% of Croatians encounter fake news every day and 29% encounter fake news at least once a week (Veljković, 2019). As part of the wider European action plan against disinformation, initiated by the European Commission, the government plans to create a national contact point and real-time alert system that will work with other EU member states to counter online disinformation (Veljković, 2019), however, plans to counter disinformation have been talked about for a long time without much results. Finally, Russian influence in Croatia remains an ongoing concern in the country (Karasik, 2019, 2020).

In relation to the COVID-19 pandemic, in the early spring the country's official statistics were promising but they started rising again over the summer. Prime Minister Andrej Plenković stated that in comparison to other countries, there was no great hardship in Croatia, though there are on-going concerns about the lack of tourism in the summer of 2020 that could seriously harm the Croatian economy (Dellanna, 2020). Nevertheless, a report by Balkan Insights revealed that Croatia had some of the most serious cases of digital rights abuse during the pandemic. A total of thirty-one cases were recorded from January to May, including an incident where a list of infected patients was shared through messaging apps, violating the patients' privacy rights (Ristic, 2020).

An Overview of Cyber Troop Activity Croatia

Organizational Form

The government has been criticized for trying to influence the media landscape by manipulating the distribution of EU social funds for the non-profit media sector. The new conservative government heavily cut the funding and has yet to deliver the media strategy that it has been promising (Peruško, 2020). Moreover, the Ministry of Economy, Entrepreneurship and Crafts approved a grant of 98,999 HRK (~$14,800) from the EU funds to the internet portal Dnevno.hr, which is known to be a leading producer of disinformation in Croatia (Vidov, 2019). Dnevno is a far-right news provider with web outlets in Croatia, Serbia, and Bosnia Herzegovina (Milat, 2019). Recently, another website known to spread disinformation and foster hatred towards minorities was found to have received about 1.3 Million HRK (~$202,000) from the ministry. Both websites applied for funds through the ESF Operational Programme for Effective Human Resources 2014-2020 (Ćimić, 2020; Mediji Zajednice - Potpora Socijalnom Uključivanju Putem Medija, Faza I., 2020). This move was particularly ironic considering that in early 2019, Croatia had officially joined the EU fight against fake news in the context of the 2019 EU parliamentary elections (Total Croatia News, 2019). In general, though, while media is highly polarized, they are free from direct political inference or manipulation (Freedom House, 2019), although a recent report has noted that Croatian legislation to protect media and journalists from political influence are highly ineffective and found political motivation in the appointments and dismissals of editorial staff (Bilic, 2020).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Croatia

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
	Evidence found – funding websites	Evidence found			

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

As one of the leading distributors of disinformation in Croatia, the internet portal Dnevno shares anything from conspiracies about German chancellor Merkel trying to steal Croatia's sovereignty to anti-EU, anti-refugee and Islamophobic narratives, generally promoting nationalism and hatred (Vidov, 2019). With their slogan of 'we write what others hide' the portal has spent the past years driving divisions amongst different ethno-nationalist groups. In 2017 a new management took over the site, vowing to take it to the center-right of the political spectrum and to 'write the truth'. However, especially in Croatia, the portal of Dnevno still works with conspiracies and clickbait headlines (Milat, 2019).

Meanwhile, many politicians are active on social media themselves and do not shy away from making contributions to ongoing issues. For example, in the spring of 2020 the Croatian fact-checker Faktograf received critique from politicians as well as private individuals, quickly degenerating into accusations of censorship, for teaming up with Facebook to weed out misinformation on the platform (Vladisavljevic, 2020b). With the upcoming parliamentary election less than a week away, campaigning is currently in full swing. Most parties have active and visible campaigns, and while partisan narratives, fake news and nationalist rhetoric are on the forefront (Vukobratovic, 2020), there is little to no reporting of any more sophisticated, data-driven campaigning techniques being employed. Rather, the recent Coronavirus pandemic seems to be dominating the elections (Vukobratovic, 2020).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Croatia

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Human	Support Attacking opposition Driving Divisions	Disinformation	Facebook

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

All in all, there is very little information available on any cyber troop activity in the country. As it appears, Croatia experiences the usual surge in activity during elections and other politically sensitive times, but no party or government agency appears to be running permanent cyber troops. For now, the government appears to influence opinions predominantly indirectly, by, for example, disrupting the media landscape through funding decisions.

Table 3: Cyber Troop Capacity in Croatia

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
		Temporary	Decentralised	Liminal

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

References

Bilic, P. (2020). Monitoring Media Pluralism in the Digital Era: Application of the Media Pluralism Monitor in the European Union, Albania and Turkey in the years 2018-2019 (p. 21). Centre for Media Pluralism and Media Freedom. https://cadmus.eui.eu/bitstream/handle/1814/67796/croatia_results_mpm_2020_cmpf.pdf?sequence=1&isAllowed=y

Chadwick, L. (2020, July 4). Croatia's ruling conservatives win parliamentary election. Euronews. https://www.euronews.com/2020/07/04/croatia-election-will-the-ruling-party-s-early-election-gamble-pay-off

Ćimić, I. (2020, August 6). Milijun kuna javnog novca dodijeljeno opskurnom ekstremističkom portalu. Index HR. https://www.index.hr/clanak.aspx?id=2203372

Dellanna, A. (2020, April 27). Coronavirus: "There's no hardship in Croatia", says Prime Minister Plenkovic | Euronews. Euronews. https://www.euronews.com/2020/04/25/coronavirus-there-s-no-hardship-in-croatia-says-prime-minister-plenkovic

Freedom House. (2019) Freedom House | Croatia. https://freedomhouse.org/country/croatia/freedom-world/2019

Gotev, G. (2020, January 13). Croatia president blames poll defeat on sexism, "fake news." Www.Euractiv.Com. https://www.euractiv.com/section/elections/news/croatia-president-blames-poll-defeat-on-sexism-fake-news/

Karasik, T. (2019, February 18). R. Jezic: The businessman behind the Croatian trial that could give Russia the keys to Europe | View. Euronews. https://www.euronews.com/2019/02/18/r-jezic-the-businessman-behind-the-croatian-trial-that-could-give-russia-the-keys-to-europ

Karasik, T. (2020, January 15). Is the new EU Presidency a Russian Trojan horse? Croatia's trial of the decade suggests it is | View. Euronews. https://www.euronews.com/2020/01/15/is-the-new-eu-presidency-a-russian-trojan-horse-croatia-s-trial-of-the-decade-suggests-it

Mamić, A. (2020, June 25). Croatian General Election Preview: Expert Analysis from Ankica Mamic. Total Croatia News. https://www.total-croatia-news.com/politics/44533-ankica-mamic

Mediji zajednice—Potpora socijalnom uključivanju putem medija, faza I. (2020). Europski Strukturni i Investicijski Fondovi. https://strukturnifondovi.hr/natjecaji/mediji-zajednice-potpora-socijalnom-ukljucivanju-putem-medija-faza-i/

Milat, A. (2019, February 1). Moment of Truth: Reality Bites for Notorious News Brand. Balkan Insight. https://balkaninsight.com/2019/02/01/moment-of-truth-reality-bites-for-notorious-news-brand-01-31-2019/

Peruško, Z. (2020). Digital News Report: Croatia (Digital News Report). Reuters Institute for the Study of Journalism. http://www.digitalnewsreport.org/survey/2020/croatia-2020/

Ristic, M. (2020, June 3). Insults, Leaks and Fraud: Digital Violations Thrive amid Pandemic. Balkan Insight. https://balkaninsight.com/2020/06/03/insults-leaks-and-fraud-digital-violations-thrive-amid-pandemic/

Total Croatia News. (2019, January 21). Croatian Government to Join EU Fight against Fake News. Total Croatia News. https://www.total-croatia-news.com/politics/33682-fake-news

Veljković, S. (2019, January 21). Vlada kreće u borbu protiv lažnih vijesti. Večernji List. https://www.vecernji.hr/vijesti/vlada-krece-u-borbu-protiv-laznih-vijesti-1295825

Vidov, P. (2019, November 5). Croatian Government uses European Funds to Support Spreading Disinformation. Faktograf.hr. https://faktograf.hr/2019/11/05/croatian-government-uses-european-funds-to-support-spreading-disinformation/

Vladisavljevic, A. (2020a, May 18). Croatian Parliament Dissolved Ahead of Summer Elections. Balkan Insight. https://balkaninsight.com/2020/05/18/croatian-parliament-dissolved-ahead-of-summer-elections/

Vladisavljevic, A. (2020b, May 27). Facebook-Partnered Croatian Fact-Checkers Face “Huge Amount of Hatred.” Balkan Insight. https://balkaninsight.com/2020/05/27/facebook-partnered-croatian-fact-checkers-face-huge-amount-of-hatred/

Vukobratovic, N. (2020, June 18). Croatian Election Campaign Haunted by Anti-Serb Rhetoric | Balkan Insight. Balkan Insight. https://balkaninsight.com/2020/06/18/croatian-election-campaign-haunted-by-anti-serb-rhetoric/

Cuba

Introduction

As a one-party communist state, Cuba has no political pluralism, suppresses dissent, and severely restricts freedom of the press, assembly, speech, and association. The government controls virtually all media outlets in Cuba and restricts access to outside information. The small number of independent media outlets that do operate in the country are deemed illegal and considered "enemy propaganda".

Access to the internet has historically been very limited and most citizens can still only access the government-controlled national intranet. Despite gradual improvements to the infrastructure, the service is still inaccessible or slow and unreliable for most Cubans, as well as continuously subjected to monitoring (Freedom House, 2019). It is also unaffordable to most citizens. Since 2008 home access was primarily available for an elite, but remained constrained for most Cubans, who bought "a scratch-off phone card and surfed on a cut-rate smartphone" from Wi-Fi public spots (Faiola, 2019). In December 2018 3G mobile telephone service was introduced. Nevertheless, it is still not affordable for the vast population, with the cheapest package costing $7 per month, while the median monthly income is $44 (Faiola, 2019). Most recent developments in 2019 include the legalization of the extension of public Wi-Fi hotspots to private homes and small businesses, a recognition of access that was already available through clandestine private networks (CPJ Central & South America Staff, 2019). However, it is forbidden to disseminate "information contrary to the social interest, morals, good manners, and integrity of people" on public networks and host websites "on servers located in a foreign country" (CPJ Central & South America Staff, 2019).

Dissent and criticism (both on- and offline) are suppressed and punished by the state. Cuba remains one of the most unconnected and repressive countries with regard to communication and information technologies. A recent study by the Open Observatory of Network Interference (OONI) found forty-one blocked sites on the island's internet, while foreign internet services remain virtually inaccessible (Xynou et al., 2017). Nevertheless, Cuba differs from other repressive regimes as its main strategy to keep citizens away from unwanted content is to make the required technology unavailable, rather than employing sophisticated blocking techniques. They do, however, have a fairly well-developed system to filter domestic SMS for messages containing words such as "democracy", "dictatorship", or "human rights".

Additionally, the Cuban government tries to control the online public narrative by launching copy-cat versions of global services such as Wikipedia, Facebook, WhatsApp, and Twitter. This way, citizens are only exposed to highly curated versions of each page: in 2010 the Cuban Wikipedia Ecured was launched, in 2013 a Cuban Facebook La Tendedera followed, in 2015 a blogging page known as Reflejos was launched, and in 2018 ToDus, the national version of WhatsApp. Most applications are specially developed for the national intranet by the Computer Science University (Freedom House, 2019), which has been identified as being involved in computational propaganda operations. At the same time, circumvention of government restrictions by independent digital media and citizens has also acquired new dimensions and scope.

An Overview of Cyber Troop Activity in Cuba.

Organizational Form

Computational propaganda techniques are used by the government to manipulate information and promote pro-government narratives and harass opposition figures (Freedom House, 2019). Students loyal to the Communist Party are allegedly being used as social media marketers, to amplify messages supporting the government and attacking opposition. A local news outlet has reported that students from the University of Information Science in Havana are responsible for spreading socialist propaganda on Twitter, during events they referred to as the "Twitazo" (Torres & Vela, 2018).

On the other hand, interference from foreign governments in domestic political debate has been recorded for some time. In 2014, news outlets reported that the US government had developed and implemented an app aimed at undermining the Cuban government. According to the news articles (Associated Press, 2014), the US Agency for International Development (USAID) launched the app ZunZuneo, a social network built on texts. "According to documents obtained by the Associated Press and multiple interviews with people involved in the project, the plan was to develop a bare-bones "Cuban Twitter," using cell-phone text messaging to evade Cuba's strict control of information and its stranglehold restrictions over the internet." Documents show that the US government planned to build a subscriber base through "non-controversial content" and then introduce political content aimed at inspiring Cubans to organize demonstrations against the regime. According to the Associated Press (2014), "at its peak, the project drew in more than 40,000 Cubans to share news and exchange opinions. But its subscribers were never aware it was created by the US government, or that American contractors were gathering their private data in the hope that it might be used for political purposes".

Additionally, reports (Iannelli, 2018; Norton, 2018) accuse the US Office of Cuba Broadcasting of using "native" and "non-branded" accounts on Facebook and YouTube to spread right-wing, pro-US, pro-capitalist propaganda in Cuba. A spokesperson of the Broadcasting Board of Governors said the project never took off, though this statement appears unverifiable at the moment.

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Cuba

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
2014	Evidence found				Evidence found

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Human rights activists have reported the use of technical tools to manipulate public debate. The Foundation for Human Rights in Cuba (FHRC) has denounced the growing use of digital tools of cyber warfare against political dissidents in Cuba. They reported situations in which their email and Facebook accounts were hacked and have reported more than 14,000 viral attacks on their websites (Foundation for Human Rights in Cuba, 2017). The objective, according to FHRC, is to generate or exacerbate conflicts among various organizations and to discredit them by resorting to the techniques of modern black propaganda: falsifying statements, editing video and audio tapes, and making photomontages that are then disseminated via the computers, phones, sites, emails, and Facebook hijacked accounts of the opposition activists that they want to discredit.

In addition, sites dedicated to "black propaganda" and psychological warfare have multiplied. These blogs, often operating under the facade of fictitious names, provide a platform for state security agents charged with spreading rumours, attacking the credibility of those who they find "uncomfortable", and sowing disinformation lines that justify the repressive operations of their institution (Foundation for Human Rights in Cuba, 2017). Meanwhile, evidence also indicates the use of bots and trolls by the Cuban government. Experts and activists have tracked dozens of automated social media accounts attempting to masquerade as humans, which are used to amplify certain hashtags and messages to influence what is trending. One strategy employed by them is the use of pictures of white, attractive public figures (Torres & Vela, 2018). According to the Cuban Democratic Directorate, pro-government bots on Twitter were active during the local elections in 2018 (Freedom House, 2019). Most recently, Twitter suspended several pro-government accounts arguing that it detected multiple accounts by one same user were artificially amplifying information. As has been stated, "while the top state-run media outlets have different profiles, they frequently publish similar if not identical articles" ('Twitter restores some blocked Cuban official accounts', 2019).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Cuba

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Human, Automation, Fake and Hacked	Pro-government, pro-party messages, Attacks on opposition, Suppressing speech	Disinformation, Trolls, Amplification strategies	Facebook, Twitter,

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

Cuban pro-government cyber troops are centrally operated by the University of Informatic Sciences (UCI), which is based on an isolated former Soviet military base and has its own tv channel and radio station. According to RadioViva 24 (Alemán de Las Casas, 2020) cyber troops are managed by Eddy Mc Donald Torres, who plans the design and implementation of attacks. They are constituted of UCI students, who only graduate if they comply with their assigned schedule of digital attacks and pro-government publications, but also by other citizens, who are recruited with the promised reward of a stable internet connection and food. Some of the attacks against opposition on Twitter were located not only at the UCI, but also at the University "Marta Abreu" of Las Villas and the Ministry of Communications (Pentón, 2019). Tasks assigned to students also include cyberattacks. Supporters of the Young Communist League (Unión de Jóvenes Comunistas - UJC) have also been trained to counter critics to the government on social media (ADN Cuba, 2019).

Table 3: Cyber Troop Capacity in Cuba

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
		Permanent	Operation centre at Universidad de las Ciencias Informáticas (UCI). Schedule of attacks and online responses.	Medium

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

References

ADN Cuba. (2019, September 19). La UJC lanza campaña para contrarrestar el efecto de las redes sociales entre los jóvenes cubanos. *ADN Cuba*. https://adncuba.com/noticias-de-cuba/actualidad/la-ujc-lanza-campana-para-contrarrestar-el-efecto-de-las-redes-sociales

Alemán de Las Casas, F. (2020, February 12). *La UCI y los ataques del régimen cubano a los opositores en las redes sociales* [Radio Viva 24]. https://radioviva24.com/2020/02/12/la-uci-y-los-ataques-del-regimen-cubano-los-opositores-en-las-redes-sociales/

Associated Press. (2014, April 3). US secretly created 'Cuban Twitter' to stir unrest and undermine government. *The Guardian*. https://www.theguardian.com/world/2014/apr/03/us-cuban-twitter-zunzuneo-stir-unrest

CPJ Central & South America Staff. (2019, September 12). *In new Cuban internet measures, journalists see a trap* [Committee to Protect Journalists]. https://cpj.org/blog/2019/09/cuban-internet-measures-journalists-trap.php

Faiola, A. (2019, July 8). How Facebook and Twitter triggered Cuba's biggest protests for years. *The Independent*. https://www.independent.co.uk/news/world/americas/cuba-protests-facebook-twitter-telegram-mobile-internet-prices-a8993611.html

Foundation for Human Rights in Cuba. (2017, June 20). Alejandro Castro Espín: Cuba's Cyberwar and Black Propaganda operations. *Foundation for Human Rights in Cuba*. http://www.fhrcuba.org/2017/06/alejandro-castro-espin-cubas-cyberwar-and-black-propaganda-operations/

Freedom House. (2019). *Cuba | Freedom House*. https://freedomhouse.org/country/cuba/freedom-net/2019

Iannelli, J. (2018, August 21). U.S. Planned Cuban Facebook Propaganda on Radio Marti, TV Marti. *Miami New Times*. https://www.miaminewtimes.com/news/us-planned-cuban-facebook-propaganda-on-radio-tv-marti-10625033

Norton, B. (2018, August 27). US Government Admits It's Making Fake Social Media Accounts to Spread Propaganda in Cuba. *The Real News Network*. https://therealnews.com/columns/us-government-admits-its-making-fake-social-media-accounts-to-spread-propaganda-in-cuba

Pentón, M. J. (2019, September 12). *Twitter suspende decenas de cuentas asociadas con el gobierno cubano y revela por qué lo hizo*. El Nuevo Herald. https://www.elnuevoherald.com/noticias/mundo/america-latina/cuba-es/article235020537.html

Torres, A., & Vela, H. (2018, March 8). Twitter accounts masquerading as Cubans spread socialist propaganda. *Local 10 News*. https://www.local10.com/news/cuba/miami-activists-allege-cuban-government-is-engaging-in-social-media-manipulation

Twitter restores some blocked Cuban official accounts. (2019, September 13). *Reuters*. https://www.reuters.com/article/us-cuba-twitter-idUSKCN1VY259

Xynou, M., Filastò, A., & Basso, S. (2017, August 28). *Measuring Internet Censorship in Cuba's ParkNets*. OONI. https://ooni.org/post/cuba-internet-censorship-2017/

CZECH REPUBLIC

Introduction

The Czech Republic is a free democracy with a competitive media ecosystem. However, hyper-partisan reporting and the complicated relations between media, private business and politicians are cause for concern. Additionally, the country has experienced a number of corruption scandals where businesses attempted to meddle with politics directly (Freedom House, 2019). Billionaire Andreij Babiš acts as the country's prime minister and leader of the Movement of Dissatisfied Citizens (ANO) party, whose media holdings are held in a trust controlled by a close associate. In 2017, a leak exposed Babiš' interference with the editorial policy of the daily newspaper MF Dnes. Allegedly, he had instructed the publication to publish of articles intended to damage his political rivals (Freedom House, 2018). Amid concerns about the political independence of traditional media, trust levels in news organizations are low at 33%, according to Reuters' 2019 Digital News Report (Štětka, 2019). Increasingly Czechs access news online, through computers and smartphones and, in particular on social media networks, including Facebook (45%), YouTube (23%) and Facebook Messenger (15%). Trust in news on social media networks is even lower at 16%, and trust in news found through online searches is also relatively low (29%).

An Overview of Cyber Troop Activity Czech Republic

Organizational Form

Politicians and parties engage intensively in campaigning against one another during elections and other politically sensitive events, though it appears that major disinformation operations and conspiracy attacks are supported by Russia. For example, President Miloš Zeman's re-election campaign in late 2017 (the election took place in January 2018) was accompanied by a smear campaign spreading rumours that main his opposition, Jiří Drahoš, had connections to the secret police during the Communist era of the country. Analysts believe these allegations were spread by Russia (Freedom House, 2019). During the 2019 European parliamentary elections the right-wing Freedom and Direct Democracy party (SPD) was the most heavily involved in producing disinformation and other manipulative content. Sympathetic websites and partisan news outlets openly shared the SPD's content, and the editor of one such website, Ivan David of Nová Republika (New Republic), even ran as the leader of the SPD ballot in the EU election (Syrovátka, 2019).

At present, there are more than one hundred websites spreading disinformation in the Czech Republic (konspiratori.sk, 2020), some of the major platforms include Parlamentní listy (in English Parliamentary Letters, however, it has nothing to do with the Czech Parliament which has distanced itself from the site); AC24; AE News (also known as Aeronet); Nová Republika (New Republic); První Zprávy (First News); and Sputnik CZ (the Czech branch of the Kremlin's international media outlet). The engagement numbers of these sites are in the millions: Parlamentní listy was found to have about 800,000 readers per month, and a total of about 8 million users in 2017 (Malcolm, 2020; Schultheis, 2017), while Sputnik CZ had over 2.5 million visitors in July 2018 alone (Klingová, 2018). Most of these outlets have found ways to engage Czech politicians as well. For example, Parlamentní offers politicians the ability to open accounts and reach out to readers through the platform. Paramentní has also received support from the Czech president, who has given about forty interviews to the outlet and has supplied them with exclusive information in the past (Malcolm, 2020).

Generally, there is a growing concern in the Czech Republic that the media landscape is turning more and more partisan, with various outlets leveraging their connections to politics and business, while political parties increasingly maintain websites and outlets solely devoted to their viewpoints by providing what they call 'alternative information', but which is actually fake or deliberate disinformation that distorts reality (Schultheis, 2017). It appears that these developments have affected the public's trust in media in general: 77% of respondents in a recent GLOBSEC (2020) polling stated they believe that their media is (rather) not free, while 36% thought that the government influences media, and 39% of Czechs believe oligarchs and strong financial groups influence the media in their country. Finally, Freedom House (2019) has raised concerns about the continued intimidation and harassment of journalists by public officials in their 2019 report on the country (Euractive & AFP, 2019).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Czech Republic

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
		x			x

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

The disinformation narratives spread throughout the Czech Republic via social media, particularly Facebook, and other websites tend to aim at polarizing the public, often misinterpreting statements or statistics to drive pro-Russian and anti-EU narratives (Brokes, 2020; Sybera, 2019; Syrovátka, 2019). Strikingly, disinformation did not increase too much during the 2019 EU parliamentary election, though the final week of the campaign saw some increase in news articles on the election, most of which presented an anti-EU viewpoint. For the most part, however, news media did not share their own stories during the campaign, but amplified messages of politicians, many of which contained disinformation (Syrovátka, 2019). EU elections are also not perceived as particularly important elections by the Czech public, which also explains why the election experienced less intense disinformation and influence campaigns compared to other domestic elections.

Next to this issue of fake news and disinformation, observers have reported on trolls, hackers and Twitterbots hired by Russia being active in Czech online spaces (Heijmans, 2017; Sybera, 2019). However, there were no reports available on such or other more sophisticated cyber troop techniques being employed by domestic political actors of the Czech Republic.

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Czech Republic

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Human	Support Attack opposition Driving Divisions Distracting	Disinformation Trolls	Facebook

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

At present it appears that influence or disinformation campaigns instigated by domestic political actors are only active to a significant degree during elections, or in connection with other specific, politically sensitive topics and events (Klingová, 2019), though some occasional claims are made outside of politically sensitive times as well. During elections, however, Czechs encounter a deluge of disinformation and fake news, much of which is assumed to be spread with support from Russia (Heijmans, 2017; Sybera, 2019). Such foreign influence operations, particularly by Russia, seem to have a much more permanent nature. Not surprisingly, Russia also maintains its own outlets such as Sputnik with local language coverage in the Czech Republic (Brokes, 2020).

Table 3: Cyber Troop Capacity in Czech Republic

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
		Temporary	Decentralised	

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

To counter these efforts, members of Czech civil society are increasingly organising themselves to form alliances against the spread of disinformation. Several consultancies have launched, which help cut off websites and suspect outlets from online ads, oftentimes depriving them of their main source of income (Brokes, 2020; Malcolm, 2020). In 2018 the Facebook page Czech Elves launched, which is a group of volunteers fighting internet trolls, primarily combatting foreign influencers in Czech cyberspace (most Russians) (Zamecnik, 2020). In light of the COVID-19 pandemic, some articles are suggesting that foreign influence originating from China could start appearing on Czech cyberspace, as China is attempting to minimize the damage the virus has done to their image (DigiComNet, 2020; Karásková & Šebok, 2020). Moreover, several Czech hospitals experienced cyberattacks that are believed to be the work of Russian hackers ("Russian Hackers May Be behind Cyber Attacks on Czech Hospitals, Says ESET," 2020).

References

Brokes, F. (2020, June 10). Czech civil society fights back against fake news | DW | 10.06.2020. *Deutsche Welle*. https://www.dw.com/en/czech-civil-society-fights-back-against-fake-news/a-53758412

DigiComNet. (2020, May 30). Chinese propaganda on COVID-19: Eldorado in the Czech Cyber-Space. *Medium*. https://medium.com/@DigiComNet/chinese-propaganda-on-covid-19-eldorado-in-the-czech-cyber-space-6a95c0c97fb1

Euractive, & AFP. (2019, June 17). Czechs alarmed as populist leaders take aim at public media. *Www.Euractiv.Com*. https://www.euractiv.com/section/elections/news/czechs-alarmed-as-populist-leaders-take-aim-at-public-media/

Freedom House (2018). *Freedom House | Czech Republic*. (Freedom House. https://freedomhouse.org/country/czech-republic/freedom-world/2018

Freedom House (2019). *Freedom House | Czech Republic*. Freedom House. https://freedomhouse.org/country/czech-republic/freedom-world/2019

GLOBSEC. (2020). *Voices of Central and Easthern Europe: Perceptions of democracy & governance in 10 EU countries* (pp. 1–57). GLOBSEC. https://www.globsec.org/wp-content/uploads/2020/06/Voices-of-Central-and-Eastern-Europe-read-version.pdf

Heijmans, P. (2017, June 17). Czechs prepare to fight disinformation onslaught as elections loom | DW | 17.06.2017. *Deutsche Welle*. https://www.dw.com/en/czechs-prepare-to-fight-disinformation-onslaught-as-elections-loom/a-39281431

Karásková, I., & Šebok, F. (2020, June 29). El Dorado in Czech Cyberspace—Transitions Online. *Transitions Regional Intelligence*. https://www.tol.org/client/article/28966-el-dorado-in-czech-cyberspace.html

Klingová, K. (2018, September 24). What Do We Know About Disinformation Websites in the Czech Republic and Slovakia? *GLOBSEC*. https://www.globsec.org/news/what-do-we-know-about-disinformation-websites-in-the-czech-republic-and-slovakia/

Klingová, K. (2019, January 30). 2018: The Disinfo Year in Review. *GLOBSEC*. https://www.globsec.org/publications/2018-the-disinfo-year-in-review/

konspiratori.sk. (2020). *Konspiratori.sk*. Konspiratori.Sk. https://www.konspiratori.sk/

Malcolm, W. (2020, January 31). Does Czech Republic Have a Fake News Problem? *Prague Business Journal*. https://praguebusinessjournal.com/does-czech-republic-have-a-fake-news-problem/

Russian hackers may be behind cyber attacks on Czech hospitals, says ESET. (2020, April 22). *Expats.Cz*. https://news.expats.cz/weekly-czech-news/russian-hackers-may-be-behind-cyber-attacks-on-czech-hospitals-says-eset/

Schultheis, E. (2017, October 21). The Czech Republic's Fake News Problem. *The Atlantic*. https://www.theatlantic.com/international/archive/2017/10/fake-news-in-the-czech-republic/543591/

Štětka, V. (2019). *Reuters Institute Digital News Report 2019—Czech Republic*. RISJ. http://www.digitalnewsreport.org/survey/2019/czech-republic-2019/

Sybera, A. (2019, September 9). Truth Missing in Action in Czech Information Wars. *Balkan Insight*. https://balkaninsight.com/2019/09/09/truth-missing-in-action-in-czech-information-wars/

Syrovátka, J. (2019, June 13). #EUelections2019: Disinformation's Role in the Czech Republic | StopFake. *StopFake*. https://www.stopfake.org/en/euelections2019-disinformation-s-role-in-the-czech-republic/

Zamecnik, A. (2020, May 19). An army of volunteer 'elves' fights disinfo in the Czech Republic. *Coda Story*. https://www.codastory.com/disinformation/volunteers-fight-disinfo-czech-republic/

Ecuador

Introduction

Before the elections in Ecuador in 2017, there was substantial evidence that former President Rafael Correa had established a series of troll farms in order to spread pro-government messages, discredit the opposition, and suppress political dissent and journalistic freedom. His government also controlled and blocked content “based on copyright infringement, specially targeted to political activists” (Rofrío et al., 2019). On one occasion, Correa used a speech to name and shame people who had written abusive comments about him on Twitter and Facebook, revealing three people's full names, ages, and addresses (BBC News, 2015). Beyond government-run troll-farms, the 2017 elections in Ecuador also demonstrated evidence of social media manipulation.

The general elections of 2017 represented an inflection point, for after ten years in office, Rafael Correa was not eligible for re-election (Rofrío et al., 2019). Following the inauguration of newly-elected President Lenin Moreno, according to Freedom House (2019) internet freedom has improved and there have been fewer instances of disinformation and of coordinated campaigns on social media. However, there is evidence of continuing operations by accounts related to the previous government, especially during significant events.

An Overview of Cyber Troop Activity in Ecuador.

Organizational Form

According to the civil society organization Fundameios, the spread of misinformation during Correa’s administration came from political actors representing both the government and opposition parties. Both sides were involved directly and indirectly in the design and dissemination of falsified, altered, and decontextualized content, in order to confuse the population (Fundamedios, 2017). The National Secretary of Intelligence also contracted private companies, such as Emerging MC de México SA de CV, Illuminati Lab, Ximah Digital SA, Eye Watch, and more, to pursue organized manipulation operations since 2014 («Secretaría Nacional de Inteligencia gastó $ 7,1 millones para desprestigiar a opositor Galo Lara», 2019; Tronchoni, 2020).

Gastón Douek and Carlos Ibañez Constantino created Emerging MC de México SA de CV in 2009, using the company to manage operations related to the government’s goal to perform surveillance on Galo Lara, the main opposition leader, with the aim of securing his extradition. They also have other brands, including Tantra Soft SA, Nicestream, Eye Watch, and Illuminati Lab. Illuminati Lab helped Correa’s presidential campaign in 2013 and managed the government relations with Ares Rights to take down unfavourable online content and made the government’s initial contact with Hacking Team. Eye Team, on the other hand, was used to hack web sites critical of Correa's administration, attacked Galo Lara, and collapse the web site Bananaleaks—containing leaks from Correa's administration—and created a copy with distorted content (Tronchoni, 2020).

In addition to this, Ximah Digital has been in liquidation since 6 August 2019 by order of the Superintendency of Companies. Javier Sarmiento Fierro and Juan Carlos Váscones are the two shareholders and, until Fernando Alvarado Espinel took over the Ministry of Communication, they received contracts from the government for work with Ximah Digital and other brands they owned. Ximah Digital was also known for working for Lenin Moreno (at an initial phase before he grew estranged from Correa, but there are no further details), and Cynthia Viteri (for her local election campaign for Mayor of Guayaquil). However, there is no further evidence of manipulation techniques in this campaign («Secretaría Nacional de Inteligencia gastó $ 7,1 millones para desprestigiar a opositor Galo Lara», 2019). It is also worth mentioning that a network of sixteen agencies was also associated with computational propaganda operations. Most of them shared the same official address as Ximah Digital SA, the long-time contractor. Ximah Digital initially acted as the country's exclusive Twitter sales channel, as it already had connections with the government and in 2014 it was revealed that well-known pro-government troll accounts were managed by its employees. Years later it moved towards more sophisticated operations (eg. AI), and now exports its services and "trains other digital agencies to be trolls" (Carpenter-Arévalo, 2019).

Correa’s government also used the website Somos+ to investigate and respond to social media users who criticized it. There have also been several reports of state-sponsored ‘troll farms’ in Ecuador. An investigation conducted by Fundación Mil Hojas in 2015 revealed that Correa had hired businesses to run “troll centers”—offices (Alpert, 2018). Catalina Botero, former Special Rapporteur for Freedom of Expression for the Inter-American Commission on Human Rights, has reported that investigations had tracked the IP addresses of such troll farms and linked them to computers in government offices (Freedom House, 2017a).

Moreover, it has been stated that high-ranking officials such as Fernando Alvarado, Secretary of Communication (Lara-Dillon, 2012), were involved in operations to harass journalists and critics. In November 2016, leaked documents related to publicist Kenneth Godwin revealed a proposal to use public funds to hire companies (Inteligencia Emocional and Kronopio) for the creation and expansion of political propaganda supporting the Ecuadorian government. These companies maintained a close relationship with Vinicio Alvarado Espinel, a high-ranking government official.

After the change of administration, the landscape of coordinated campaigns changed. However, even if minor, there is evidence of continuing operations by Correist accounts. In fact, the National Communications Secretariat denounced in early 2019 the phenomenon that fake social media accounts were using manipulation techniques to discredit Moreno and his government (Freedom House, 2019). This followed an earlier accusation in 2017 that institutional accounts, such as “Enlace Ciudadano”, were posting unauthorized content (Freedom House, 2019).

Finally, it is worth noting that in July 2020 Facebook removed accounts and pages on Instagram and Facebook, which originated in Canada and Ecuador and were targeting other countries in Latin America. The company linked these accounts to Canada-based Ecuadorian PR firm Estraterra and "political consultants and former government employees in Ecuador" (Gleicher, 2020).

Estraterra was created in July 2016 by Roberto Wohlgemuth (former advisor at the National Secretary of Public Administration), Pablo Yánez (former vice minister of Tourism), and María Augusta Enríquez (former advisor to the ministry of Production led by Vinicio Alvarado Espinel) (Tres exfuncionarios de Rafael Correa crearon Estraterra S.A., vetada ahora por Facebook, 2020, DFRLab, 2020). They were closer to Vinicio and Fernando Alvarado, who were central to the propaganda strategy during Correa’s electoral campaigns and administration. Giovanni López, Jr., former technical assistant for media and public relations for the vice presidency, was also one of the names identified as being behind the accounts removed by Facebook.

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Ecuador

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
2013	National Communications Secretariat and Ministry of Communication (between 2013 and 2017) No evidence since 2017.	Evidence found	Emerging MC de México SA de CV, Illuminati Lab, Ximah Digital SA, Eye Watch, Inteligencia Emociona, and Kronopio (between 2013 and 2017) Estraterra		

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

The businesses hired by the President Correa administration used fake accounts to voice support for Correa and attack his opponents (Alpert, 2018). Fernando Balda, a deputy from the opposition party Sociedade Patriótica, has also accused Correa's government of setting up a troll centre in order to harass journalists and critics of the government through false accounts on Twitter, Facebook, and YouTube. Such accusations were corroborated by Diario El Comercio, a newspaper established over one hundred years ago (Lara-Dillon, 2012). On the other hand, political opponents of former President Rafael Correa have also employed defamatory social media campaigns (Digital Guarimbas, 2017).

The leaked documents related to publicist Kenneth Godwin—and the political propaganda operations—revealed a budget for operating propaganda accounts on social media and a proposal to handle social media campaigns attacking opposition leaders like ex- Secretary for Communications Mónica Chuji, local press watchdog Fundamedios, the Inter-American Commission on Human Rights and its Special Rapporteur for Freedom of Expression Catalina Botero, among others (Ecuador Transparente, 2016).

Content takedowns were also used as a strategy to curb political discourse. A study by Fundamedios revealed that, between April and July 2016, approximately thirty Twitter accounts linked to anti-government users with high numbers of followers were suspended after receiving repeated complaints (Freedom House, 2017b).

In the lead-up to the 2017 presidential elections, Freedom House reported that social media accounts belonging to politicians, journalists and opposition activists were hacked and used to disseminate messages against the opposition's vice-presidential candidate Andrés Paez (Freedom House, 2017b; Puente, 2017). Disinformation was used as a campaign tool by both major parties to support their position as well as undermine the opposition. One prominent example, highlighted by Snopes (Alpert, 2018), described rumours about Correa's party tampering with votes via messages spread on the popular messaging platform, WhatsApp.

Whilst most social media accounts are fake and human-led, there is some evidence that bots were widely used during the 2017 general elections. As noted by Rofrío et al. (2019) in their analysis of tweets between January and April 2017, there is evidence that bot activities could be linked to most running candidates and political parties (Movimiento CREO & Movimiento SUMA, Movimiento Alianza País, Partido Social Cristiano, and Izquierda Democrática & Movimiento Unidad Popular & Movimiento de Unidad Plurinacional Pachakutik). Most of these accounts were recently created. However, it is worth noting that "almost 46% of all bots collected supported the official candidates, Lenin Moreno, and other candidates, such as Guillermo Lasso, received almost a tweet against for every tweet in favor" (Rofrío et al., 2019).

Additionally, Pavliuc (2020) studied the decade of the network of Twitter accounts associated with PAIS Alliance. While their disinformation operations were quiet between 2010 and 2016 and more active between 2016 and 2019, it was in 2018 when activity was boosted by recently created accounts that focused on both unique and popular hashtags. Moreover, in 2019 Twitter removed a network of 1,019 (mostly fake) PAIS Alliance political party-related accounts. They used amplification techniques—"hashtag manipulation and retweet spam"—to spread negative content about Moreno's administration (Twitter Safety, s. f.).

Most recently, disinformation and trolling campaigns to drive division and suppress speech during the COVID-19 crisis have also been linked to pro-Correa fake accounts. They mainly originated outside Ecuador—mostly in Mexico and Venezuela. Although there is no evidence connecting these accounts with specific individuals, these locations represent the two countries where the people closest to Correa, and responsible for the previously-identified "troll centres" during his presidency, had gone before the closure of State borders («Las noticias falsas, el virus particular de Ecuador que achacan a correístas», 2020). National intelligence sources attribute these actions to Correist-circles abroad.

The Facebook announcement of the removal of Ecuador-based Facebook and Instagram accounts and pages in July 2020 demonstrated the continuing practice of public opinion manipulation in social media. The operations were mostly aimed at amplifying content and showing support and/or criticism of certain topics or political actors. These accounts targeted Latin-American countries, mainly promoting left-wing candidates and criticizing specific leaders of the opposition (Gleicher, 2020; DFRLab, 2020). They were activated sporadically for specific civic events. After examining the creation dates and content of the pages, DFRLab (2020) found that "several of the network's assets operated almost exclusively during presidential campaigns in South America, including in Chile (2017), Ecuador (2017), Venezuela (2018), Argentina (2019), and Uruguay (2019)". In Ecuador they promoted content supportive of Lenin Moreno, who was candidate for Alianza País party, but after he took office, he distanced himself from Correa. Since then, the network posted attacks against Moreno (Ibid.). These Facebook and Instagram accounts and pages were related to off-platform websites (eg. shared same user account for Google Analytics and server), which shared similar content (Ibid.). They also used duplicate and fake accounts, using profile pictures created through artificial-intelligence and also pictures of celebrities.

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Ecuador

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Human, Automation, Fake, Hacked	Pro-party, Attack opposition, Distracting, Suppressing speech	Disinformation, Trolls, Amplification	Twitter, Facebook, YouTube, Instagram, Telegram, WhatsApp

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

According to documents leaked in 2016, Fernando Alvarado, Secretary of Communication, took U.S.$81,915.76 in commissions related to contracts made by Kenneth Godwin with the Presidency (Ecuador Transparente, 2016). Another document proposed the management of a 24/7 community manager and other security implementations for the monthly fee of U.S.$15,000, which included the creation of a troll centre to influence public opinion on social media by, among other tactics, attacking and harassing dissidents (Ecuador Transparente, 2016).

The government also spent U.S.$5.2 million between August 2012 and July 2013 on a contract with Illuminati Lab to develop a centre in which to use profiling and manipulation techniques. This was the company that had a major role during the 2013 general election. Additionally, the government spent U.S.$7.1 million on a surveillance campaign to extradite Galo Lara. Of that budget, U.S.$6.7 million were spent between 2013 and 2014 on Emerging MC de México SA de CV and U.S.$280.000 on Ximah Digital SA («Secretaría Nacional de Inteligencia gastó $ 7,1 millones para desprestigiar a opositor Galo Lara», 2019).

Table 3: Cyber Troop Capacity in Ecuador

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
	During Correa's administration, contracts with several firms, which ranged from U.S.$280.000 to U.S.$6.7 million.		Centralised	Currently minimal

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

References

Alpert, M. (2018, February 9). «Noise and Confusion»: Fake News in Ecuador. *Snopes.com*. https://www.snopes.com/news/2018/02/09/how-fake-news-has-factored-into-ecuadors-recent-votes/

BBC News. (2015, January 30). President Correa's troll warfare. *BBC News*. http://www.bbc.co.uk/news/blogs-trending-31057933

Carpenter-Arévalo, M. (2019, September 24). In Latin America, the business of trolling threatens Twitter's disruptive power. *TechCrunch*.

https://social.techcrunch.com/2019/09/24/in-latin-america-the-business-of-trolling-threatens-twitters-disruptive-power/

Ecuador Transparente. (2016). *The Godwin Papers*. Associated Whistleblowing Press. https://data.awp.is/ecuadortransparente/2016/11/16/42.html

Freedom House. (2017a). *Freedom on the Net 2017—Cuba*. Freedom House. https://freedomhouse.org/report/freedom-net/2017/cuba

Freedom House. (2017b). *Freedom on the Net 2017—Ecuador*. Freedom House. https://freedomhouse.org/report/freedom-net/2017/ecuador

Freedom House. (2019). *Ecuador | Freedom House*. https://freedomhouse.org/country/ecuador/freedom-net/2019

Fundamedios. (2017, July 25). Informe especial sobre Fake News; «información» que desinforma. *IFEX*. http://www.ifex.org/ecuador/2017/07/24/fake-news-informe/es/

Gleicher, N. (2020, July 8). Removing Coordinated Inauthentic Behavior. Retrieved July 18th 2020 from https://about.fb.com/news/2020/07/removing-political-coordinated-inauthentic-behavior/.

Lara-Dillon, M. (2012, March 1). Inédito: Gobierno de Ecuador habría montado un «troll center». *PulsoSocial*. https://pulsosocial.com/2012/03/01/inedito-gobierno-de-ecuador-habria-montado-un-troll-center/

Las noticias falsas, el virus particular de Ecuador que achacan a correístas. (2020, marzo 26). *EFE*. https://www.efe.com/efe/america/sociedad/las-noticias-falsas-el-virus-particular-de-ecuador-que-achacan-a-correistas/20000013-4206109

Pavliuc, A. (2020, January 26). Watch six decade-long disinformation operations unfold in six minutes [Medium]. *The Startup*. https://medium.com/swlh/watch-six-decade-long-disinformation-operations-unfold-in-six-minutes-5f69a7e75fb3

Puente, D. (2017, December 18). Ocho cuentas de Twitter habrían sido «hackeadas», según colectivo. *El Comercio*. http://www.elcomercio.com/actualidad/politica-cuentas-twitter-hackeadas-ecuador.html

Rofrío, D., Ruiz, A., Sosebee, E., Raza, Q., Bashir, A., Crandall, J., & Sandoval, R. (2019). Presidential Elections in Ecuador: Bot Presence in Twitter. *2019 Sixth International Conference on eDemocracy eGovernment (ICEDEG)*, 218-223. https://doi.org/10.1109/ICEDEG.2019.8734426

Secretaría Nacional de Inteligencia gastó $ 7,1 millones para desprestigiar a opositor Galo Lara. (2019, August 23). *El Universo*. https://www.eluniverso.com/noticias/2019/08/23/nota/7483197/senain-gasto-71-millones-desprestigiar-opositor-galo-lara

Tronchoni, N. (2020, February 21). I3 Ventures: Carlos Ibáñez, de 'hackear' para Correa en Ecuador a ayudar a Bartomeu | Deportes | EL PAÍS. *El País*. https://elpais.com/deportes/2020/02/21/actualidad/1582288987_436925.html

Twitter Safety. (s. f.). *Disclosing new data to our archive of information operations*. Retrieved March 31st 2020 from https://blog.twitter.com/en_us/topics/company/2019/info-ops-disclosure-data-september-2019.html

Egypt

Introduction

Over the past half-decade, the Egyptian government has increased its repressive hold over freedom of information on the Internet. It has extended existing policies of censorship and surveillance while displaying evidence of limited and relatively unsophisticated computational propaganda techniques (Freedom House, 2016). Thus, computational propaganda and cyber troop efforts in Egypt must be viewed in the context of existing Internet controls and censorship efforts. Egypt also plays a role in spreading or facilitating disinformation elsewhere in the region.

An Overview of Cyber Troop Activity in Egypt.

Organizational Form

Since assuming the presidency in June 2014, President Abdel Fattah el-Sisi has increasingly utilized social media and Internet controls (Freedom House, 2019). Internet freedom declined further since 2018 as a result of new legislation. In August 2018 President Sisi signed a new law called the media regulations law (Law No. 180) that forces media outlets to obtain a license from the Supreme Council for Media Regulation. According to the law a media outlet includes any website or social media account with at least five thousand subscribers. Individuals behind such outlets could be subject to account deletion, fines, and even imprisonment if they are found to be distributing information deemed to threaten national security, disturb the public peace, spread fake news, promote discrimination, violence, racism, hatred or intolerance (TIMEP, 2019). The consequence of the new legislation is that any social media accounts or blogs with more than five thousand followers will be treated as media outlets. This makes them liable for publishing 'false news,' which remains undefined and subject to interpretation by the newly formed SCMR. According to Mohamed Abdel-Haiz, a board member of the journalists' union in Egypt, the "vaguely defined national security violations, as well as vaguely defined political, social, or religious norms" allow for wide interpretation and threaten journalists' freedom (Daugherty, 2019).

In addition to the media regulations law, in August 2018, the president also signed the Law on Combating Cybercrimes (Law No. 175) which created a legal framework to block websites deemed a threat to national security or the economy, as well as criminalizing VPNs. Individuals who visit banned websites may be jailed for up to one year, and ISPs (Internet Service Providers) are required to hold browsing data and disclose it to security forces upon request (AFTE, 2018). These efforts have been further reinforced by the creation of the government's Media and Rumour Monitoring Unit, headed by Naaym Saad Zaghloul, and the creation of a hotline in March 2018 for citizens to report fake news (Magdy, 2018).

The government begun to block a large number of websites in 2017, when twenty-one websites were blocked in a single day on the grounds of "supporting terrorism and lies". Websites on this list included local and international news outlets such as Mada Masr and Al Jazeera (AFTE, 2018). According to the Association for Freedom of Thought and Expression (AFTE) at the end of the first quarter of 2019, 512 websites were reported blocked by the authorities (AFTE, 2019). Ahead of the April 2019 constitutional referendum, the monitoring group NetBlocks found that more than 34,000 websites were blocked in an alleged attempt to suppress opposition to the amendment (Freedom House, 2019). One of the websites that was blocked was Batel, a site launched to voice opposition to the proposed amendment and which asked Egyptians to declare the amendment void by signing their petition. After the first time website was blocked it continued to create new copies of the website, however, these were also all blocked within hours of their launch. By 22 April Batel claimed that it had received over 700,000 votes (Shea, 2019). Despite this clear connection between the blocking of Batel and the referendum, no relation was found between the other 34,000 blocked websites and the referendum. NetBlocks theorizes that when the Batel campaign created a series of different domain names hosted on the same IP address, the intelligence service decided to block the underlying IP, resulting in 34,000 other websites becoming inaccessible in the country (Ibid).

While supporters of President Sisi claim that the laws safeguard freedom of expression, opponents have pointed to the country's penchant for jailing journalists, activists, and political figures on "Fake news" charges, arguing that the law is being used as a media censorship tactic (Funke & Flamini 2019). For example, defendants in Case 441, commonly referred to as the Media Hub of the Muslim Brotherhood, were charged based on alleged associations with the Muslim Brotherhood. However, according to TIMEP (2018) "these claims are often unjustified and issued due to the defendants' critical remarks of the regime". Human rights' activist Amal Fathy, was sentenced to two years in prison on charges of "spreading false news", a result of posting a video on Facebook which criticized the government for the country's levels of sexual harassment (Michaelson, 2018). An Egyptian economist and author, Abdel-Khaleq Farouq, was arrested in October 2018 for his book titled *Is Egypt Really a Poor County?* for publishing 'fake news' that challenged President el-Sisi's economic policies. While the detention of journalists is not new, the Committee to Protect Journalists has described the influx of detentions as "fresh waves of repression", particularly under the new justification of 'false news' charges (Hendawi, 2018).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Egypt

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
	Supreme Council for the Administration of the Media, Media and Rumour Monitoring Unit	Abdel Fattah al-Sisi, Naaym Saad Zaghloul	New Waves, El Fagr		

Strategies, Tools, and Techniques

Disinformation: Cyber troops in Egypt use a variety of strategies, tools and tactics to spread disinformation and manipulate public discussions about politics online. Following the removal of President Morsi in 2013, there was a surge of disinformation on Facebook and Twitter as both opponents and supporters of the ousted president spread rumours, fabricated images, and created fake accounts. For example, the Facebook page of Egypt's Freedom and Justice Party (FJP), the political arm of the Muslim Brotherhood, posted old photos of children killed in Syria, blaming the Egyptian Army and claiming the photos were from Egyptian protests (Al Arabiya, 2013; BBC, 2013). The volume of disinformation has led to verification pages, such as 'Da Begad?' or 'Is This Real?' to fact-check by verifying posts, images, and videos (BBC, 2013).

Harassment and trolling: A Reporters Without Borders (2018) report on online harassment notes that many Egyptian journalists' social media accounts are increasingly being shut down by "the regime's online armies". For example, the Twitter account of BBC Cairo correspondent Waël Hussein was blocked, and fake accounts began to disseminate content under his name. Furthermore, in March 2018, the Facebook page of opposition TV network Watan and a Muslim Brotherhood affiliated page were removed – reported to be a result of government supporters reporting the pages to Facebook for violating their terms of service (Freedom House, 2018).

Egyptian authorities are said to have organized "troll armies" that deployed abusive language, threats, harassed people online, and bullied critics—particularly women (Warren, 2018). Aya Nader, who reports on human rights issues for Al-Monitor and Open Democracy, stated that she has to "think twice" before writing a story or conducting an interview, and has considered writing under an alias – "the online electronic armies or trolls have a great role in that, I have been named and shamed [for writing content that's critical of the government]" (Morgan, 2017).

Other trends that have been taking place are "follow and report" activities in which troll accounts target various users by reporting them for content. In an analysis done by Eskander (2019) he shows that during the month of October 2019 up to 150 accounts claimed to have been suspended across just one week. Eskander argues that there seems to be a number of systematic Twitter suspensions, such as Arabic content being marked as 'hateful conduct'. For example, when reposting an Arabic tweet that got suspended on Twitter in English, the tweet does not get suspended.

Amplification of propaganda: Fake accounts are often more popular than legitimate accounts—according to *The Arab Weekly*, Education Minister Mahmoud Abo el-Nasr's fake account had 80,000 followers compared to the 55,000 followers on his official page (The Arab Weekly 2018). Coordinated fake accounts appear to amplify both pro- and anti-regime political content. The BBC discovered that while posts by the official Twitter account of President Abdel Fattah al-Sisi attracted an average of 2,000 to 3,000 likes each, many of these accounts appeared suspicious. For example, their activities appeared only to promote pro-Sisi posts, suggesting coordinated activity to make posts more visible (BBC Monitoring, 2018). In June and July 2018, hashtags such as #El-Sisi_Zaemy_Waftakher (El-Sisi is my leader and I'm proud), as well as opposition hashtags such as #Erhal_Yasisi (Sisi, leave) were posted thousands of times. Both hashtags contained evidence of organic and inorganic activity, with accounts supporting 'Sisi_leave' coming from those that also tweet about Palestine and are in support of the Muslim Brotherhood (Kanishkkaran, 2018).

Coordinated inauthentic behaviour: During 2019 a number of global coordinated inauthentic networks stemming from Egypt surfaced. These networks mostly targeted audiences in the Middle East and North Africa, and were linked to marketing firms and newspapers based in Egypt. In one case, Facebook removed 333 accounts, 195 ages, 9 groups and 1194 Instagram accounts that were involved in foreign interference created by the Egyptian marketing firm New Waves. The network created fake accounts mostly posturing as females whose messages included the combination of uplifting and humorous content with political content in an attempt to gather a wide following before diving into regional politics. The assets targeted Middle Eastern countries such as Libya, Turkey, Yemen, Somalia, and Lebanon. According to the report, "the assets frequently posted about local news, politics, elections and topics including alleged support of terrorist groups by Qatar and Turkey, Iran's activity in Yemen, the conflict in Libya, successes of the Saudi-led coalition in Yemen, and independence for Somaliland" (DFRLab, 2019).

The Egyptian company, run by former military officer Amir Hussein, was also found to be involved in a covert operation to praise Sudan's military on social media days after Sudanese soldiers killed pro-democracy demonstrators in Khartoum in June. The New York Times revealed that the company paid new recruits $180 a month to write pro-military messages using fake accounts on various social media platforms. Although sufficient evidence to link the operation to the Egyptian government was not found, according to the New York Times, there were many hints that such a link existed (Walsh and Rashwan, 2019).

An additional influence operation attributed to actors within Egypt surfaced in April 2020 when Twitter announced the takedown of 2541 accounts and 7.9 million tweets. The accounts were found to be linked to the El Fagr newspaper. Previous takedowns on Facebook and Instagram in October 2019 were also found to be related to El Fagr. The accounts consisted of both fake accounts and bots who tweeted various news content, commercial content, as well as subversive political astroturfing content. To topics in this dataset are similar to topics in past Egypt-attributed takedowns that include negative content towards rivals such as Qatar and Iran and positive content towards the Egyptian government (DiResta et al., 2020).

COVID 19 and misinformation: The ongoing coronavirus pandemic has heavily influenced the global disinformation landscape. According to Washington Post "In some countries the virus has provided a pretext for governments to pass emergency legislation that is likely to curb freedoms long after the contagion has been extinguished". In the Middle East governments have detained and punished journalists who questioned the way the state has been dealing with the pandemic. In Egypt, the press credentials of Guardian's correspondent, Ruth Michaelson, were revoked by the Egyptian government after she reported on a study that questioned Egypt's official number of coronavirus cases (Loveluck et al., 2020). Beyond these threats against journalists, Egyptian authorities have used the vague charge of "spreading false news" and "terrorism" to arrest and detain a number of health workers who spoke out on various safety concerns regarding in safe working conditions, personal protective equipment, limited testing of health care workers, etc. Amnesty international (2020) has documented the cases of eight health care workers who were arbitrarily detained between March and June for their concerns posted on social media.

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Egypt

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Fake, real, bots, Impersonated accounts	Amplification of pro- and anti-regime political content, pro-Palestine and anti-Muslim Brotherhood hashtags, online harassment, Anti-Turkey, Qatar, Iran and Libya. Pro Saudi intervention in Yemen, pro-Somalia independence,	Disinformation, fabricated photos, troll armies, amplification of hashtags	Facebook, Twitter, Instagram

References

AFTE. 2019. First Quarterly Report on the Situation of Freedom of Expression in Egypt “January – March 2019”. *Association for Freedom of Thought and Expression.* https://afteegypt.org/en/afte_releases/2019/05/06/17457-afteegypt.html.

AFTE. 2018. The State of Internet Censorship in Egypt. *Association for Freedom of Thought and Expression*. https://afteegypt.org/en/digital_freedoms-2/2018/07/02/15445-afteegypt.html/2

Al Arabiya. 2013. Brotherhood posts old photos of Syrian children as victims of Egypt’s army. *Al Arabiya.*

Amnesty International. 2020. Egypt : Helath care workers forced to make impossible choice between death or jail. *Amnesty International.* https://www.amnesty.org/en/latest/news/2020/06/egypt-health-care-workers-forced-to-make-impossible-choice-between-death-or-jail/.

BBC News. 2013. Altered Images: Egypt's disinformation war. *BBC.*

BBC Monitoring. 2018. Online trolls and fake accounts poison Arab social media. *BBC.* https://www.bbc.com/news/technology-45372272.

Daugherty, O. 2019. Egypt clamps down on 'fake news' with heavy fines, strict regulations. *The Hill.* https://thehill.com/policy/international/434741-egypt-clamps-down-on-fake-news-with-heavy-fines-and-strict-regulations.

DFRLab. 2019. Facebook Disabled Assets Linked to Egypt and UAE-Based Firms. *Medium.* https://medium.com/dfrlab/facebook-disabled-assets-linked-to-egypt-and-uae-based-firms-a232d9effc32.

DiResta, R., & Kheradpir, T., & Miller, C. 2020. “The World is Swimming in a Sea of Rumors” :

Influence Operations Associated with El Fagr Newspaper (Egypt). *Stanford Internet Observatory*. https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/egypt_whitepaper.pdf.

Eskander, W. 2019. How Twitter is gagging Arabic users and acting as morality police. *Open Democracy*. https://www.opendemocracy.net/en/north-africa-west-asia/how-twitter-gagging-arabic-users-and-acting-morality-police/.

Freedom House. 2016. Freedom on the net. Egypt. https://freedomhouse.org/country/egypt/freedom-net/2016.

Freedom House. 2018. Freedom of the Net. Egypt. https://freedomhouse.org/country/egypt/freedom-net/2018.

Freedom House. 2019. Freedom on the net. Egypt. https://www.freedomonthenet.org/country/egypt/freedom-on-the-net/2019

Funke, D., & Flamini, D. 2018. A guide to anti-misinformation actions around the world. *Poynter*. https://www.poynter.org/ifcn/anti-misinformation-actions/#egypt.

Hendawi, H. 2018. Egypt arrests author, publisher over book on economy. A*P News.* https://apnews.com/de0495a5cef14799b12402b2f1802e50.

Kanishkkaran, K. 2018. Bots Are Dominating Political Debate in Egypt. *InfoTime.*

Loveluck, L., Dixon, R., & Taylor, A. 2020. Journalists threatened and detained as countries on multiple continents restrict coronavirus coverage. *The Washington Post.* https://www.washingtonpost.com/world/journalists-threatened-and-detained-as-countries-on-multiple-continents-restrict-coronavirus-coverage/2020/04/05/90d9953e-6eb7-11ea-a156-0048b62cdb51_story.html.

Magdy, S. Egypt says it fights fake news, critics see new crackdown. A*P News.* https://apnews.com/5b17cf57b4384f559a3035a167f8e211/Egypt-says-it-fights-fake-news,-critics-see-new-crackdown

Morgan, M. 2017. How surveillance, trolls, and fear of arrest affect Egypt's journalists. *Committee to Protect Journalists.* https://cpj.org/2017/06/how-surveillance-trolls-and-fear-of-arrest-is-affe/.

Michaelson, R. 2018. Egyptian woman Amal Fathy jailed for sexual harassment video. *The Guardian.* https://www.theguardian.com/world/2018/sep/29/egypt-amal-fathy-jailed-sexual-harassment-video.

Reporters Without Borders, 2018. Online Harassment of Journalists. *Reporters Without Borders.* https://rsf.org/sites/default/files/rsf_report_on_online_harassment.pdf.

Shea, J. 2019. Egypt's Online Repression Thwarts Both Growth and Democracy. *The Tahrir Institute for Middle East Policy.* https://timep.org/commentary/analysis/egypts-online-repression-thwarts-both-growth-and-democracy/

The Arab Weekly. 2018. Fake social media pages cause a stir in Egypt. *The Arab Weekly.* https://thearabweekly.com/fake-social-media-pages-cause-stir-egypt.

TIMEP. 2018. Case 441. *Twitter.* https://twitter.com/TimepDC/status/1072944896632328192/photo/1

TIMEP. 2019. TIMEP Brief : The Law Regulating the Press, Media, and the Supreme Council for Media Regulation. *The Tahrir Institute for Middle East Policy.* https://timep.org/reports-briefings/timep-brief-the-law-regulating-the-press-media-and-the-supreme-council-for-media-regulation/.

Walsh, D., & Rashwan, N. 2019. 'We're at War': A Covert Social Media Campaign Boosts Military Rulers. *The New York Times.* https://www.nytimes.com/2019/09/06/world/middleeast/sudan-social-media.html?action=click&module=Top%20Stories&pgtype=Homepage

Warren, R. 2018. Facebook drove Egypt's revolution. Now it's being used as a weapon to oppress women. *Wired.* https://www.wired.co.uk/article/egypt-fake-news-facebook-oppress-women.

El Salvador

Introduction

Ending the long-term dominance of the left-wing Farabundo Martí National Liberation Front (FMLN) and right-wing Nationalist Republican Alliance (ARENA) parties who had been in power since 1992, in March 2019 Nayib Bukele became president of El Salvador, representing Grand Alliance for National Unity (GANA).

Whilst social media was at the centre of his presidential campaign, during his time in office he is using social media to directly address his citizens (Esberg, 2020) and he employs Twitter as "his official communication mechanism" (Meléndez, 2020). Nevertheless, social media is increasingly being used as a battlefield for presenting opposing narratives. Both supporters and critics of President Bukele coordinate operations to favour or criticize his leadership and policies. And Bukele himself and his administration have been accused of working with troll centres, as well as coordinating amplification campaigns and attacks against journalists and the opposition.

An Overview of Cyber Troop Activity in El Salvador

Organizational Form

Troll or net centres have often been at the centre of manipulation operations in El Salvador. Indeed, President Bukele had previously paid a troll centre to target local media outlets (Esberg, 2020). In August 2020, the Legislative Assembly of El Salvador created a commission to investigate whether Bukele's government paid net centres to attack and harass journalists and the opposition (Castañeda, 2020).

Additional evidence has linked the presidential press office to online attacks against the opposition. Since 2012 the Twitter account @_brozo attacked accounts critical to Nayib Bukele. However, when in January 2019, Twitter suspended the account, the former account @PrensaBukele deleted most of its previous tweets and changed its name account to @__Brozo__. @PrensaBukele was created in early 2015 before Bukele took office as Mayor of San Salvador and it was subsequently used during his presidential campaign. After he became president, it was the first official account of the newly created president's press office led by Ernesto Sanabria (Rauda et al., 2020).

Porfirio Chica, communications and public relations strategist and owner of the media outlet Última Hora, has worked for several political campaigns in El Salvador, such as the re-election of former general attorney Luis Martínez in 2015. For that campaign, he coordinated a propaganda network including the columnist Geovani Galeas, politician Juan José Martell, Garrid Safie, Julio Valdivieso, and Félix Ulloa, among others, to boost Martínez's image in both traditional and social media. In the 2018 municipal campaign, this network targeted Will Salgado, former mayor of San Miguel. Fake accounts used hashtags, such as #Willyarobosuficiente and #Willrobo to coordinate a campaign attacking the candidate (Rauda et al., 2020). Porfirio Chica is known to be closed to former governments of Flores and Saca, and currently, to Bukele's. According to Esberg (2020) he was the first person to post #QueBonitaDictadura, the main hashtag of a coordinated campaign to favour President Bukele.

In July 2020, Facebook removed Facebook and Instagram accounts and pages that were linked to Ecuatorian Canada-based firm Estraterra. Although there is no further information about the intentions and clients of the company, some of its activities focused on El Salvador, where it published content about the Farabundo Martí National Liberation Front (Gleicher, 2020).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in El Salvador

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
	Evidence found	Evidence found	Evidence found. Among them, Estraterra		Evidence found

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

During the 2019 presidential campaign, candidates Carlos Calleja for the Nationalist Republican Alliance (ARENA), Hugo Martínez for the National Liberation Front (FMLN), and Nayib Bukele for the Grand Alliance for National Unity (GANA) widely used social media—especially Facebook, not only to disseminate their electoral messages but also to attack each other (Meléndez, 2020). Manipulation techniques in the form of fake followers and disinformation were also observed.

According to NIMD, all three candidates had followers with no posts nor profile pictures. Most of them had alphanumeric account names (Meléndez, 2020). The candidate with the most fake followers was Bukele. Indeed, he had been accumulating fake followers since his role as Mayor in Nuevo Cuscatlán (Unidad de Datos, 2018, p. 240). He accounted for 94% of the 256 thousand inactive accounts following the three candidates and 20% of his total followers (Unidad de Datos, 2018, p. 240).

In order to analyse the Twitter landscape in the run-up of the elections, Internet activist Alberto Escorcia observed the accounts of President Salvador Sánchez Cerén, candidate Nayib Bukele, and ARENA party between 20 October and 23 November 2018. He found that around 9% of messages had signs of automation. Content of Bukele and the ARENA party were amplified by recently created accounts of less than a hundred followers, although those supporting Bukele showed signs of greater coordination. Salvador Sánchez Cerén was mostly amplified by official accounts that used TweetDeck (*Simulación, Automatización y Coordinación. Una Mirada a La Conversación En Twitter En El Salvador Previo a Las Elecciones Presidenciales*, 2019).

Disinformation was a particular concern as candidates were also active in disseminating such content (Meléndez, 2020). An article published at Primero Noticias website stating that Bukele had a 'D factor', explaining that dark characteristics of his personality were widely shared. However, a great part of the publication was a copied from a BBC World article that had no reference to the candidate (Baires, 2019). Photomontages and false leaked messages were also observed (Baires, 2019).

After Bukele took office, manipulation operations by his supporters and opponents have been observed. They are often the most active during specific events or crisis, such as payment scandals or discussions over security policies (Esberg, 2020).

According to a report by the Crisis Group there is a coordinated effort to manipulate the online debate about the domestic political agenda, which has manifested in the opposing hashtags #BukeleDictador and #QueBonitaDictadura (Dictator Bukele and What a Lovely Dictatorship, respectively). The hashtag #BukeleDictador was first published in February 2020 when the government ordered the entrance of military troops to the building of the Legislative Assembly and it was also used to criticize his management of COVID-19 response. Contrastingly, #QueBonitaDictadura was used for supporters of Bukele and against critics by the press. Analysis of posts related to both hashtags between 27 April and 9 May 2020 show signs of the use of fake accounts created recently and automation. Also, between 4.4 and 5.6 percent of posts were originated from accounts that were deactivated later in May. (Esberg, 2020).

Apart from fake accounts, political elites play a significant role in amplifying content. Whilst they account for less than 1.5% of posts, their influence is disproportionate. Crisis Group report also shows that "Deputy Alexandra Ramírez, whom the government alleges coordinated the FMLN troll centre", boosted the hashtag #BukeleDictador and that Porfirio Chica was the person who first published #QueBonitaDictadura (Esberg, 2020).

The government has also made use of trolls. Nelson Rauda, journalist at media outlet El Faro, was widely criticized after an intervention during a press conference. Some content was first published at pro-Bukele website La Britany and then disseminated by public servants and the president himself, including death threats (Cascante, 2020). Two Twitter fake accounts were created to target the journalist and his family (Pozzebon, 2020)

Finally, it is worth noting that during the Coronavirus pandemic, Bukele posted tweets with misleading information. For instance, he stated that the Italian health system had collapsed and that a specific flight from Mexico to San Salvador was carrying twelve confirmed cases of Covid-19. However, the Italian embassy in El Salvador and Mexico's Foreign Minister, respectively, denied the information (Meléndez, 2020).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in El Salvador

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Bots and human Real and Fake	Support, Attacks on opposition, Driving polaritzation, Trolling	Trolls, Amplifying content	Twitter, Facebook

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

There are no details about how cyber troops in El Salvador are organized nor the resources allocated for their activities.

Table 3: Cyber Troop Capacity in El Salvador

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
		Temporary	Decentralised	Low

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

References

Baires, R. (2019, January 30). *Las noticias falsas de la campaña presidencial*. Revista Factum. https://www.revistafactum.com/noticias-falsas-campana/

Cascante, L. F. (2020, July 16). *Periodistas salvadoreños denuncian ataques del gobierno y bloqueo de información pública*. Red internacional de periodistas. https://ijnet.org/es/story/periodistas-salvadore%C3%B1os-denuncian-ataques-del-gobierno-y-bloqueo-de-informaci%C3%B3n-p%C3%BAblica

Castañeda, J. M. (2020, August 14). *El Salvador: Crean comisión para investigar 'netcenter' de Bukele*. https://www.soy502.com/articulo/salvador-crean-comision-investigar-netcenter-bukele-63338

Esberg, J. (2020, July 13). *All the President's Trolls: Real and Fake Twitter Fights in El Salvador*. Crisis Group. https://www.crisisgroup.org/latin-america-caribbean/central-america/el-salvador/all-presidents-trolls-real-and-fake-twitter-fights-el-salvador

Gleicher, N. (2020, July 8). Removing Coordinated Inauthentic Behavior. *About Facebook*. https://about.fb.com/news/2020/07/removing-political-coordinated-inauthentic-behavior/

Meléndez, J. (2020, June 29). *Learning from El Salvador's Fake News Pandemic*. NIMD. https://nimd.org/learning-from-el-salvadors-fake-news-pandemic/

Pozzebon, S. (2020). Less than social media: El Salvador's new leader takes a leaf out of the Trump playbook to use Twitter to crush freedoms. *Index of Censhorship*, *49* (2), 48-49.

Rauda, N., Arauz, S., & Reyes, D. (2020, February 7). *La cuenta en Twitter de la Secretaría de Prensa de Presidencia se transformó en @__Brozo__*. Elfaro.Net. https://elfaro.net/es/202002/el_salvador/23990/La-cuenta-en-Twitter-de-la-Secretaría-de-Prensa-de-Presidencia-se-transformó-en-@__Brozo__.htm

Simulación, automatización y coordinación. Una mirada a la conversación en Twitter en El Salvador previo a las elecciones presidenciales. (2019, January 23). LoQueSigue.Tv. https://loquesigue.tv/simulacion-automatizacion-y-coordinacion-una-mirada-a-la-conversacion-en-twitter-en-el-salvador-previo-a-las-elecciones-presidenciales/

Unidad de Datos. (2018, November 26). Más de 240,000 cuentas inactivas o falsas siguen a Nayib Bukele. *Noticias de El Salvador - elsalvador.com*. https://www.elsalvador.com/noticias/nacional/mas-de-240000-cuentas-inactivas-o-falsas-siguen-a-nayib-bukele/543201/2018/

ERITREA

Introduction

Eritrea gained independence from Ethiopia in 1993 and has since been ruled by the People's Front for Democracy and Justice (PFDJ) headed by President Isaias Afwerki as a militarized authoritarian state with no elections. The country has no independent media and most domestic journalists are regularly detained without an explanation. By the end of 2018 sixteen journalists had been under arrest, many of whom had been detained since 2001 when the government officially shut all independent media. Eritrea also requires citizens to perform national service for most of their working lives. Over the past few years, citizens have tried to leave the country in huge numbers: in a single week in September 2018 nearly 4,000 Eritreans claimed asylum in Ethiopia (the country has a population of about 5 million) (Carnegie Ethics Online Monthly Column, 2016; Freedom House, 2019).

Eritrea is one of the least connected countries in the world, with an extremely low internet penetration rate. In 2012 only about 6% of the population had mobile phones and 1% had access to the internet. Eritreans fulfilling national service are not allowed to have a mobile phone (Katlic, 2014; Winter, 2014). By 2020 the internet penetration rate has risen to 8.3% and about 0.6% of the population use Facebook (Africa Internet User Stats | Eritrea, 2020). While mobile phone subscriptions and access to the internet through dial-up or one of the few internet cafés are very expensive, another reason for limited online communication is fear of repercussions when searching for or sharing information online. Internet cafés are monitored by security agents, so any questionable behaviour would likely lead to being detained (Freedom House, 2019; Katlic, 2014).

An Overview of Cyber Troop Activity Eritrea

Organizational Form

Even though the domestic internet and social media penetration rates are so low, the Eritrean government nonetheless appears to have made sure to stay up to date with modern online manipulation and information-warfare techniques. Reports surfacing in the summer of 2019 find that the PFDJ has sent operatives to the United Arab Emirates (UAE) and Saudi Arabia to receive extensive training on tactics of internet/social media warfare. The Eritrean government established a task force under the leadership of the Minister of Information, Yemane Gebremeskel, which included Eritreans living abroad to work as ambassadors for Eritrea. It appears that this task force worked as part of a troll farm for the UAE, targeting a number of countries in the Middle East. Moreover, Eritrea seem to target the few Eritrean independent news outlets as well as activists that are currently based abroad (Awate, 2019, 2020).

Eritrea remains the most censored country in the world and domestically controls information flows through direct, legislative means as well as by having a legal monopoly on broadcast media (CPJ, n.d.).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Eritrea

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
	x				

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

The Eritrean trolling activities predominantly take place on Facebook. The platform has removed hundreds of accounts associated with the UAE’s trolling activities, many of which were run by Eritrea’s task force. Where the trolls were not engaged with UAE’s work, they targeted Eritreans residing in foreign countries on Facebook and Twitter to disrupt any discussion that goes against the government’s narratives and intimidated and harassed individuals who, for example, report on the country for Eritrean newspapers located abroad (Awate, 2019; “Eritrea Unleashes Its Troll Patrol,” 2015).

Additionally, Eritrea has been using its new knowledge to attack other governments online, mainly by spreading accusations and potential disinformation. For example, in 2018 the border between Ethiopia and Eritrea was opened for the first time since the two countries had been at war between 1998 and 2000. However, after only three months Eritrea closed it again and took to social media to accuse Ethiopia of plotting to disrupt Eritrean security by attempting to assassinate a high-ranking general with the goal of ultimately overthrowing the PFDJ’s rule. Eritrea may have had an ulterior motive to close the border and attack Ethiopia as observers note that public agitation with the Eritrean government is continuously increasing and many took advantage of the open border to leave the country (Gedab News, 2018).

Domestically Eritrea is not experiencing much cyber troop activity, which, given the low internet penetration rates, is not too surprising. To ensure control over the information citizens acquire, the Eritrean administration relies instead on intimidation and surveillance: since October 2016 state security required internet cafés (which are basically the only internet service providers in the country) to keep a detailed log on all customers including those that would go online using their own devices at cafés (Carnegie Ethics Online Monthly Column, 2016; Harnet, 2016).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Eritrea

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Human Fake accounts	Pro-government Attacking opposition (critics of country) Supressing speech	Trolling Disinformation	Facebook Twitter

Source: Authors’ evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

Given the poor domestic internet connectivity, most pro-regime trolling happens from outside of Eritrea by forces likely trained through the administration’s connections to the UAE, who are then sent abroad to get to work (Shearlaw, 2015). Even the Eritrean ambassador to Japan is alleged to be part of the task force trained by the UAE (Awate, 2019).

There is not much known about what training Eritrean operatives receive from the UAE or how their training and operation is being paid for and how much resources the Eritrean government uses to attack activists living abroad. Nevertheless, their activities seem on-going and coordinated, though the possibility remains that much of the organization and coordination is done by the UAE.

Table 3: Cyber Troop Capacity in Eritrea

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
		Permanent	Training/coordinated	Medium

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Inspired by the Arab Spring, opposition groups have started to form in Eritrea as well, and as much as possible they try to organise and share their experiences through Facebook and YouTube. However, next to the low internet penetration rates in Eritrea, low literacy levels make written communication and organisation complicated. For now, Eritreans have failed to have their voices heard though occasional whistle-blowers have reached a wider international audience online, and local activists are not giving up hoping to keep up their fight for more freedom through online means (Carnegie Ethics Online Monthly Column, 2016).

References

Africa Internet User Stats | Eritrea. (2020). https://www.internetworldstats.com/africa.htm#er

Awate. (2019, August 2). PFDJ Troll Alliance: Facebook Removes Saudi-UAE-Egypt Accounts. *Awate.Com*. http://awate.com/pfdj-troll-alliance-facebook-removes-saudi-uae-egypt-accounts/

Awate. (2020, April 23). David Copperfield, Isaias, and Dahlan. *Awate.Com*. http://awate.com/david-copperfield-isaias-dahlan/

Carnegie Ethics Online Monthly Column. (2016, December 30). Eritrea: An Exiled Nation Suspended in Liminal Space through Social Media. *Carnegie Council for Ethics in International Affairs*. https://www.carnegiecouncil.org/publications/ethics_online/0125

CPJ. (n.d.). 10 Most Censored Countries. *Committee to Protect Journalists*. Retrieved July 5, 2020, from https://cpj.org/reports/2019/09/10-most-censored-eritrea-north-korea-turkmenistan-journalist/

Eritrea unleashes its troll patrol. (2015, August 23). *The Mail & Guardian*. https://mg.co.za/article/2015-08-23-eritrea-unleashes-its-troll-patrol/

Freedom House. (2019). *Freedom House | Eritrea*. https://freedomhouse.org/country/eritrea/freedom-world/2019

Gedab News. (2018, December 27). Ethio-Eritrean Border: Haphazardly Opened Erratically Closed. *Awate.Com*. http://awate.com/ethio-eritrean-border-haphazardly-opened-erratically-closed/

Harnet, A. (2016, October 6). Eritrea: Regime orders internet service providers to keep detailed ... *[AIM] Asmarino Independent Media*. https://asmarino.com/news/4808-eritrea-regime-orders-internet-service-providers-to-keep-detailed-records-of-their-customers

Katlic, T. (2014, August 1). Understanding Eritrea's Exceptionally Limited Internet Access. *ICTworks.Org*. https://www.ictworks.org/understanding-eritreas-exceptionally-limited-internet-access/

Shearlaw, M. (2015, August 18). From online trolling to death threats – the war to defend Eritrea's reputation. *The Guardian*. http://www.theguardian.com/world/2015/aug/18/eritrea-death-threats-tolls-united-nations-social-media

Winter, C. (2014, June 27). Eritrea's Communications Disconnect. *Bloomberg.Com*. https://www.bloomberg.com/news/articles/2014-06-26/eritrea-worlds-least-connected-country-tech-wise

Ethiopia

Introduction

The Ethiopian Government maintains a repressive regime over Ethiopian political space, freedom of expression and marginalized ethnic minorities. Corruption, protest crackdowns and human rights abuses mark Ethiopia's recent political history. In May 2015, the ruling party, the Ethiopian People's Revolutionary Democratic Front (EPRDF), won 100% of parliamentary seats and proceeded to crack down on opposition political parties, journalists and peaceful protestors. Following the elections and carrying through 2016, protests took place in the Oromia and Amhara regions. State forces used fatal methods against the demonstrations, killing hundreds of protestors (Freedom House, 2019a).

With the inauguration of new Prime Minister Abiy Ahmed Ali in Spring 2018 (the old Minister had resigned over the 2015/16 unrests in the country), there were developments that raised hopes for a more democratic future in Ethiopia, such as a law giving new freedoms to NGOs. Moreover, the EPRDF went through some major reorganization moving towards a more pan-Ethiopian, rather than ethnic-based party (dominated by the Oromo ethnic group). In light of the next parliamentary election to be held in 2020, electoral law was also reformed, allowing for more freedom of expression and a multiparty election (Freedom House, 2019a). However, due to the COVID-19 pandemic, the parliamentary elections, which were set to take place in August 2020, have been postponed indefinitely. There has been public outcry over this decision, accusing the current government of using COVID-19 as an excuse to avoid democracy (Davies, 2020; Reuters, 2020).

According to the most recent Freedom House report on Ethiopia, the country's Internet penetration rate is 18.62% (of a population of over 102 million in 2017), making it one of the countries with the least internet-connectivity in the world. The country's telecommunications infrastructure is underdeveloped and the prices for Internet access are high. Internet access is controlled by state-owned Ethio Telecom which also holds a monopoly over SIM cards, which citizens must register for. Since the 2016 protests the government has announced plans to require that mobile phones be purchased from Ethiopian companies which are also complemented by a tracking system for all mobiles (Chala, 2016; Freedom House, 2019b; Human Rights Watch, 2014). Although there have been indications that the government is willing to dissolve the monopoly of the telecommunication sector by selling large holdings of Ethio Telecom (Endeshaw, 2020).

An Overview of Cyber Troop Activity in Ethiopia

Organizational Form

While there are some reports of paid social media influencers (Chala, 2018), for the most part, and similar to other repressive, autocratic regimes, the Ethiopian government has used its legal powers to control the flow of information and slowly chip away at narratives that critique or compete for attention. In October 2016, the former government declared a state of emergency in the aftermath of the destruction of government buildings and private property by protesters. This state of emergency introduced further restrictions on the rights to freedom of expression, including lockdowns on digital communication (Chala, 2016), association, and peaceful assembly, and legitimized the government's controls of information. The state of emergency lasted 10 months from October 2016 to August 2017, a period marked by mass arrests and restrictions on independent media and social media (Freedom House, 2019a). A second state of emergency lasted for four months starting in February 2018 (Freedom House, 2019b). It should be noted, however, that these events happened under the old government ruling and before Abiy took office in 2018. The state of emergency of February 2018 had also been imposed by the old government, and Abiy, as part of his political reforms, brought the state of emergency to an end earlier than legally necessary (Dahir, 2018b).

A 2014 report by the Human Rights Watch details how the Ethiopian government has controlled the media landscape. Information from sources that were independent from state-run media had become increasingly difficult to access, and journalists were facing a choice of self-censorship, arrest or exile. Human Rights Watch has gone further, reporting that diaspora journalism has been targeted, in particular television. For instance, the Ethiopian Satellite Television and the Oromia Media Network (OMN) stations were banned under the country's anti-terrorism law (Human Rights Watch, 2014).

The government of Prime Minister Abiy has been taking steps to increase press freedom since 2018. Networks such as OMN are now active again. Additionally, arrested journalists have been released, and the government held a World Press Freedom Day in May 2019. However, these developments have been overshadowed by new arrests (Freedom House, 2019a). Thus, it remains unclear whether events such as the World Press Freedom Day and the release of journalists have in fact been intended to temporarily appease public opinion.

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Ethiopia

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
	X	EPRDF			X

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

In 2016, the government shut down mobile networks for almost two months, thereby controlling spread of information digitally, and removed space for critical voices through punishing critical opinions, which was exacerbated by the conduct of arrests without court orders. According to government figures, over 10,000 citizens were detained. Access to social media and websites containing information deemed subversive was heavily restricted. In December 2017, amid anti-government protests, the government started blocking internet and social media access again, though access to many pages have since been reestablished (Freedom House, 2019a; Freedom House, 2019b).

Still, internet shutdowns take place frequently; for instance, in June 2017, during the national exams period, the Internet was shut down across the nation and between May 30 and June 8, all telecom networks were shut down following the conviction of two human rights activists for online expression in May 2017. In June 2016, the Computer Crime Proclamation was passed, criminalizing amongst others digital content that "incites fear, violence, chaos or conflict among people" and legitimizing interception of digital communications (Freedom House, 2018; Freedom House, 2019b). Freedom House reports on a lack of transparency about how such control is operationalized, exacerbated by the fact that the government denies it censors the Internet (Freedom House, 2019b). Additionally, Freedom House continues to highlight persecution cases for online activities in which activists were imprisoned without being charged or in some cases tortured. There has also been evidence that governmental agents have taken over accounts from activists that have been imprisoned, such as Yonatan Tesfaye, to monitor other dissidents and encourage them to break the law (Freedom House, 2017). Thus, while the government does not usually engage in content removal directly, it silences dissent and fosters self-censorship through its physical intimidation tactics (Freedom House, 2019b).

Critics of the government who have sought exile abroad have been targeted for producing critical content about the government. According to an article by WIRED Magazine citing research by Citizens Lab, dissidents in 20 countries, including Germany, USA and Canada were targeted by Ethiopian government agencies through spyware embedded in emails containing a malicious link (see figure 1 for all countries). The spyware – PC Surveillance System – was produced by Cyberbit, an Israeli firm and subsidiary of the defence contractor Elbit Systems (Deibert, 2017; Marczak et al., 2017).

In relation to disinformation operations, it appears that for the most part the Ethiopian government makes use of misinformation and social media largely to the extent that it blames it for violence and conflict in the country. Citing this relationship, legislation against hate speech and disinformation on social media was passed in early 2020 that has raised concerns about online freedoms (Freedom House, 2019a; Freedom House, 2019b; Internet Sans Frontières, 2020). Journalists and activists alike are worried that the legislation will be used to further limit free speech and censor online content: internet users and platform operators who violate the law face up to three years in prison and fines of up to USD $3,145. Essentially, the law could allow for the government and security forces to track down and punish critics (Al Jazeera, 2020; Cascais, 2020). However, there is also substance to the argument that ethnic tensions are being exacerbated through social media. There are numerous examples of links between social media activity and ethnic violence in recent years (Chala, 2019). It is uncertain to what extent the government's intention is to suppress ethnic violence, rather than silencing dissent.

The past government (before 2015) was known to have an army of trolls to engage in online disinformation operations, despite the country's low internet penetration rate (Freedom House, 2019b). In 2014 a report from the Ethiopian Satellite Television Service accused the Ethiopian government of training bloggers to undermine online content that was critical of the government. In the second round of recruiting 235 people were trained, such that 2,350 Facebook, Twitter and blog accounts had subsequently been opened (ECADF, 2014). It remains unclear, however, if the present government has continued with these activities, though accusations have been made (Freedom House, 2019b). In late 2017 and early 2018 information began circling online that the Ethiopian government was again hiring social media trolls. Documents were shared on Facebook that showed chat logs, and lists of names and emails who appeared to have been paid to promote the ruling government and harass opponents on social media (Chala, 2018).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Ethiopia

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Human, hacked/impersonated accounts	Support Attack Opposition Suppression	Trolls	Facebook Twitter Other blogs

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

The government continues to develop its surveillance and information flow capabilities. There is little detailed knowledge about their capacity or funding for these operations, but it does appear that Ethiopia has been receiving help from China. Chinese telecommunications firms ZTE and Huawei have reportedly been used to build both Ethiopia's telecommunications infrastructure and its surveillance capabilities through a deal worth USD $1.6 billion (Sands, 2013). A 2015 Human Rights Watch report strongly suggested that Ethiopia has been developing a centralized surveillance system developed by ZTE to monitor mobile phone networks and the internet. The system reportedly has the ability to intercept emails and web chats (Freedom House, 2019b).

These developments point to a strategy that is not focused on particular political events. The strong reactions of the government to political activism, protest and violence indicates that the country is maintaining its capacity to increase repressive activities when it deems it to be necessary. However, the extent to which this involves cyber troop capacity and maintenance is unclear. According to some of the documents leaked in late 2017, at least 13 trolls were paid a minimum of USD $300 for blog posts or Facebook messages. Whether these numbers and related activities are still on-going under the new government is unclear. Still, even after Abiy's government took over, Ethiopia's spy agency appears to have sent two employees to China for special training for roughly USD $12,000, and has paid roughly $1,200 to influential bloggers to write articles in favor of the government (Chala, 2018).

Table 3: Cyber Troop Capacity in Ethiopia

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
At least 13	USD $300 SM posts USD $1,200 articles by influencers	Permanent	Coordinated/Foreign training	Medium

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

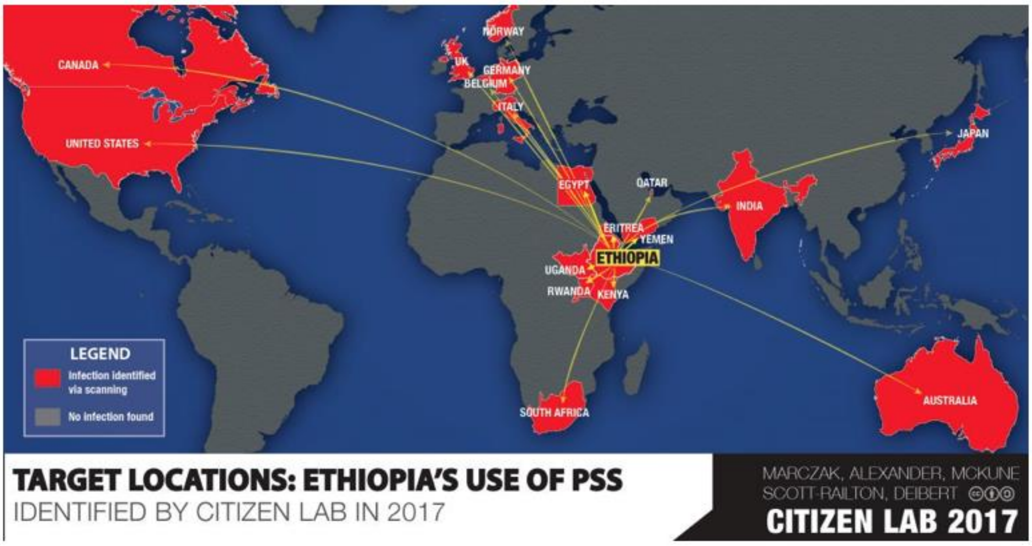


Figure 1: Countries identified by Citizen Lab to have been targeted by Ethiopia[1]

References

Al Jazeera. (2020, February 13). Ethiopia passes controversial law curbing “hate speech.” *Al Jazeera*. https://www.aljazeera.com/news/2020/02/ethiopia-passes-controversial-law-curbing-hate-speech-200213132808083.html

Cascais, A. (2020, February 23). Africa’s online hate speech laws sound alarm over press freedom | DW | 23.02.2020. *Deutsche Welle*. https://www.dw.com/en/africas-online-hate-speech-laws-sound-alarm-over-press-freedom/a-52488748

Chala, E. (2016, July 14). Ethiopia Locks Down Digital Communications in Wake of #OromoProtests. *Global Voices Advocacy*. https://advox.globalvoices.org/2016/07/14/ethiopia-locks-down-digital-communications-in-wake-of-oromoprotests/

Chala, E. (2018, January 20). Leaked Documents Show That Ethiopia’s Ruling Elites Are Hiring Social Media Trolls (And Watching Porn) · Global Voices. *Global Voices Advocacy*. https://globalvoices.org/2018/01/20/leaked-documents-show-that-ethiopias-ruling-elites-are-hiring-social-media-trolls-and-watching-porn/

Chala, E. (2019, November 22). In Ethiopia’s disinformation epidemic, the crumbling ruling coalition is the elephant in the room · Global Voices. *Global Voices*. https://globalvoices.org/2019/11/22/in-ethiopias-disinformation-epidemic-the-crumbling-ruling-coalition-is-the-elephant-in-the-room/

Dahir, A. L. (2018a, January 30). China “gifted” the African Union a headquarters building and then allegedly had it bugged. *Quartz Africa*. https://qz.com/africa/1192493/china-spied-on-african-union-headquarters-for-five-years/

Dahir, A. L. (2018b, June 4). Ethiopia will end its state of emergency early, as part of widening political reforms. *Quartz Africa*. https://qz.com/africa/1295834/ethiopias-prime-minister-abiy-ahmed-ends-the-countrys-state-of-emergency-early/

Davies, G. (2020, October 25). Ethiopian prime minister compared to Mandela now ruling with an iron fist. *ABC News*. https://abcnews.go.com/International/ethiopian-prime-minister-compared-mandela-now-ruling-iron/story?id=73763560

Deibert, R. (2017, December 6). Evidence That Ethiopia Is Spying on Journalists Shows Commercial Spyware Is Out of Control. *Wired*. https://www.wired.com/story/evidence-that-ethiopia-is-spying-on-journalists-shows-commercial-spyware-is-out-of-control/

ECADF. (2014, June 7). Ethiopia Trains Bloggers to attack its opposition. *ECADF Ethiopian News*. https://ecadforum.com/2014/06/07/ethiopia-trains-bloggers-to-attack-its-opposition/

Endeshaw, D. (2020, May 21). Ethiopia to sell 40 percent of Ethio Telecom—Minister. *Reuters*. https://www.reuters.com/article/ethiopia-telecoms-idUSL8N2D350G

Freedom House. (2017). *Freedom on the Net | Ethiopia*. https://freedomhouse.org/country/ethiopia/freedom-net/2017

Freedom House. (2018). *Freedom House | Ethiopia*. https://freedomhouse.org/country/ethiopia/freedom-world/2018

Freedom House. (2019a). *Freedom House | Ethiopia*. https://freedomhouse.org/country/ethiopia/freedom-world/2020

Freedom House. (2019b). *Freedom on the Net | Ethiopia*. https://freedomhouse.org/country/ethiopia/freedom-net/2019

Human Rights Watch. (2014). *“They Know Everything We Do.”* Human Rights Watch. https://www.hrw.org/report/2014/03/25/they-know-everything-we-do/telecom-and-internet-surveillance-ethiopia

Internet Sans Frontières. (2020, February 18). Ethiopia’s new hate speech law is a consequence of social media platforms’ limited action. *Internet Sans Frontières*.

https://internetwithoutborders.org/ethiopias-new-hate-speech-law-is-a-consequence-of-social-media-platforms-limited-action/

Maasho, A. (2018, January 29). China denies report it hacked African Union headquarters. *Reuters*. https://www.reuters.com/article/us-africanunion-summit-china-idUSKBN1FI2I5

Marczak, B., Alexander, G., McKune, S., Scott-Railton, J., & Deibert, R. (2017). *Champing at the Cyberbit: Ethiopian Dissidents Targeted with New Commercial Spyware*. The Citizen Lab. https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/

Reuters. (2020, April 1). Ethiopia postpones August election due to coronavirus. *Reuters*. https://www.reuters.com/article/us-ethiopia-election-idUSKBN21I2QU

Sands, G. (2013, September 6). Ethiopia’s Broadband Network—A Chinese Trojan Horse? *Foreign Policy Blogs*. https://foreignpolicyblogs.com/2013/09/06/ethiopias-broadband-network-a-chinese-trojan-horse/

GEORGIA

Introduction

Georgia is a “partly free” democracy with a competitive but frequently partisan media landscape, which civil society groups have warned is increasingly at risk of the political influence of oligarchs and leaders of the governing Georgian Dream party (Freedom House, 2019). In 2017, civil society groups released a joint statement expressing concern about the recruitment of political allies of Bidzina Ivanishvili, chairman of the Georgian Dream party, to senior positions at the Georgian Public Broadcaster, which the statement describes as decreasingly critical of the government (Freedom House, 2019). In 2018, threats to the Georgian media ecosystem were brought to international attention when a long-standing legal dispute about the ownership of Rustavi 2, an opposition-aligned TV station, involved the European Court of Human Rights (Freedom House, 2019). In 2019, the ECHR ruled against the owners of the TV channel in a controversial ruling (Antidze, 2019). In 2020, the government has introduced greater control over digital information infrastructure (Freedom House, 2020). This combined with greater governmental control over the independent media and judiciary, along with growing evidence of disinformation and propaganda, have caused concern for civil rights activists monitoring the country (Visegrad Insight, 2020).

Social media use by Georgia’s citizens is also high, with 60% of the country’s population (2.4 million) on Facebook. According to Visegrad Insight (2020), Facebook is the predominant social media platform, totalling around 81% of all social media (with platforms such as YouTube, Twitter and Instagram ranking under 5%).

An Overview of Cyber Troop Activity in Georgia

Organizational Form

While Georgia is subject to multiple ongoing disinformation campaigns from Russia (discussed in the Russia case study), there is also evidence of computational propaganda originating from domestic sources. The former prime minister Giorgi Kvirikashvili, who resigned in the summer of 2018 due to disagreements with the party chairman Bidzina Ivanishvili, was exposed for buying likes to promote his posts on Facebook. In June 2018, Kvirikashvili and the government more widely were found to have paid for thousands of likes from accounts in India, Bangladesh, Vietnam and Pakistan, among others, after thousands of users commented “haha” on a Facebook post criticizing non-Governmental Organizations (NGOs) (Gvadzabia, 2018). According to local news sources, the post rejected an ultimatum set by NGOs for the Justice Minister, Tea Tsulukiani, to resign for failing to nominate a candidate for the post of Chief Prosecutor. Kvirikashvili wrote that NGOs should not go beyond the mandate of their activities and criticised them for their own lack of transparency. The post spawned negative responses in comments and likes, which were countered by the allegedly bought likes (Gvadzabia, 2018).

In 2019, Facebook also removed hundreds of pages linked to the government for coordinated inauthentic behaviour. Facebook stated it removed “39 Facebook accounts, 344 Pages, 13 Groups and 22 Instagram accounts as part of a domestic-focused network that originated in the country of Georgia”. The pages were attributed to “Panda”, an advertising agency in Georgia, as well as the Georgian Dream-led government (Facebook, 2019). Many of these pages bought ads, with approximately $316,000 USD spent on ads on Instagram and Facebook (Facebook, 2019). In response to the takedown, Transparency International Georgia (2019), a human rights watchdog, called on the Prosecutor’s office to launch an investigation into the activities. However, these calls have “thus far gone unanswered” (Visegrad Insight, 2020).

In relation to Russian propaganda and disinformation in Georgia, some narratives that originated in Russian misinformation campaigns have appeared in the messaging of domestic actors, who deploy these narratives in pursuit of their own political or ideological agendas. Given the density of Russian disinformation campaigns, and cyber troop actors knowingly or not spreading these messages, it is often hard to disentangle Russian disinformation from computational propaganda that is of domestic origins (Visegard Insight, 2020).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Georgia

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
	X	X	X		

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

According to the Media Development Fund (MDF), a Georgian NGO, pro-government trolls on Facebook frequently target NGOs and journalists. Between 4 March and 5 April 2019, 15 pro-government trolls were observed. Eleven users had been stolen identities taken from Russian social networks, Odnoklassniki and VKontake; two users were accounts named after characters in TV series; one was a Facebook user; and one was a journalist and student in Batumi, Georgia (Liberali.ge, 2019). The MDF found that the trolls were mobilized against critical media outlets and journalists. In particular, the report states that the Facebook "posts/comments were directed against specific media outlets as well as specific journalists. Rustavi-2 and TV Pirveli were the targets of attacks in this regard and in individual publications, also the Liberali online edition" (Liberali.ge, 2019).

In addition to concerns about threats to the diversity of traditional media in light of government influence, according to the MDF, the government frequently employs troll factories to mobilise public opinion on social media and to criticise entities ranging from TBC bank to NGOs and media outlets. Social media trolls and sponsored posts are reportedly particularly prevalent during anti-government protests, where content is spread to share pro-government information (MDF, 2019).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Georgia

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Bots, Human	Pro-government messages, Attacks on Opposition	Amplification Strategies, Trolling, Data-Driven Strategies	Facebook, Instagram

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

There is very little data about the organizational capacity of cyber troop activity in Georgia.

Table 3: Cyber Troop Capacity in Georgia

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
	316,000 on Facebook Ads			Medium

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Other Examples of Mis-and-Disinformation

Misinformation has actively targeted foreigners. On 22 September, the online news outlets alia.ge, geotimes.ge and dainteresdit.ge shared a Facebook status that alleged that the Vashlijvari Exaltation Church had ceased to ring its bells upon the request of Iranian residents in Tbilisi. The news articles were reportedly shared thousands of times and led to heated discussions and hateful comments in the websites' comment sections and on social media. Dean Giorgi Sakhvadze of the Vashlijvari Exaltation Church denied the allegations and stated the church had not been involved in any confrontation on grounds of ethnicity or religion (Chimakadze, 2018). Once the netgazeti online newspaper reported the news was false, the Facebook user who had initially posted the story subsequently deleted her post but reportedly the online news outlets that shared the story did not correct the false claims in their stories (Chimakadze, 2018).

Similarly, a doctored image of a street sign was shared by Facebook pages in March 2018 claiming Ivane Machabli Street in Tbilisi had been renamed to Iran Street (Kokoshvili, 2018). The online news sites alie.ge, infonews.ge and guriismoambe.ge shared this story, with none of the stories providing links or evidence to support the report (Gugulashvili, 2019). Armenians, who are a minority group in Georgia, have also been targeted by online news outlets and Facebook pages. For instance, this story was posted by the Iberian Unity Facebook page in August 2017, which was shared over 3,900 times and reposted by Info9 and Rezonansi in March 2019 (Pertaia, 2019). Another example of xenophobic fake news was a story published by the website intermedia.ge that alleged that, according to a United Nations report, the Georgian ethnos was disappearing quicker than any other in the world, stating that the combination of slowing birth rates and more foreigners was responsible for this development. One fake site called theguarian.com, whose design was identical to British newspaper theguardian.com, shared a story with a fabricated interview with a British foreign service agent who allegedly stated that after the former president Mikheil Saakashvili was brought to power, the British foreign office launched a three stage plan to dissolve Russian military influence in Georgia (mediachecker.ge, 2017).

Members of the LGBTQ community are also frequent targets of online misinformation, largely peddled by online news websites and the Facebook pages of ultra-nationalist activists. For instance, on 3 September 2018, the leader of the ultra-nationalist group Georgian March, Sandro Bregadze, made a misleading statement that a gay pride event would take place at the national football stadium, Dinamo Stadium, on 9 September, which online news outlets Alia, Metronome and Kartuli Azri shared without verifying its truth. Actually, on 9 September, Georgia and Latvia were scheduled to play each other at football and in support of the Georgian footballer, Guram Kashia, who had been a public target of ultra-nationalist and homophobic groups for wearing LGBTQ armbands during matches, LGBTQ groups announced that they would attend the match with armbands and display banners saying "#guramshentanvart", Georgian for "Guram we are with you" (Mythdetector, 2018). Only a few days later, on 7

September, the online outlets, alia.ge and resonancedaily.com, published Bregadze's Facebook status in which he falsely stated that a lawsuit by LGBTQ organisations and the ombudsman will legalise same sex marriages as well as the adoption of children by same sex couples in the near future. Bregadze blamed this development on "Kashia's LGBT armband and his support!!!" while adding, "Now you can celebrate a victory over the Kazakh team manned by shepherds or the Andorran team manned by barbers and fishers!!!" (Mandaria, 2018).

GERMANY

Introduction

With an internet penetration rate of 94% in 2019 (*Eurostat - Internet Use*, 2020), and well-developed networks and ICTs the Freedom on the Net report by Freedom House (2019) places Germany above EU average. Generally, the internet is considered free, though a law which passed the Bundestag in June 2017 and came into full effect in January 2018 is viewed by some as an infringement on freedom of speech and could lead to improper censorship of online content posted by private individuals. The law, called the Network Enforcement Act, compels social media platforms with more than 2 million registered users (excluding messenger and chat app users) in Germany to establish ways to report unconstitutional speech (e.g. hate speech, defamation, libel, or slender) and delete such language within twenty-four hours of being reported (e.g. by other users) and remove content which appears to be illegal hate speech within seven days (Freedom House, 2019).

In relation to misinformation campaigns and elections, an inquiry showed that no such campaign seemed to have significantly influenced election results for the federal elections in 2017. A similar conclusion has been reached the 2019 election for the European Parliament (Freedom House, 2019; Marchal et al., 2019). Nonetheless, fake news and conspiracy stories were shared throughout both campaign seasons, and commercial botnets were found to actively promote such material (Freedom House, 2019; F-Secure Deutschland, 2017). However, microtargeting or dark advertising on social media is not as common in Germany due to electoral and data protection laws (Dachwitz, 2017). Additionally, rising political tensions with regards to the continued popularity of the right-wing populist party Alternative für Deutschland (AfD) have also fuelled the spread of misinformation, oftentimes facilitated by the AfD's social media channels. This has been particularly significant as right-wing sentiments are infiltrating the military and police (Der Spiegel, 2020a, 2020b), and fostering hate crimes, such as the shooting in Hanau in early 2020, which killed eleven people, the majority of whom were of Kurdish descent (BBC, 2020; Sheftalovich, 2020).

In relation to the COVID-19 pandemic, Germany has also been struggling with conspiracy theories and increasing resistance against preventative measures (Naumann et al., 2020). The analytic firm NewsGuard was reportedly able to track a majority of misinformation and conspiracies around the virus to the Facebook page of COMPACT Magazine (c. 94,700 followers on 01/06/2020), which has also been sharing content for the AfD (Holroyd, 2020), though there is no proof of a direct connection between the two. Nevertheless, the AfD has been the only larger party actively politicising the pandemic by criticising the government, blaming them for the current situation, supporting the partially violent protests (Kamann, 2020), and spreading conspiracies through their social media (e.g. Figure 1) (Asmann, 2020). Additionally, the Twitter accounts RT Deutsch (formerly Russia Today), has also been highly involved in sharing conspiracies, as well as two other accounts with about 20,000 followers that do not seem to have any political affiliation (Holzki, 2020).

An Overview of Cyber Troop Activity in Germany

Organizational Form

In general, it seems that the focus of the Cyber and Information Space structure within German intelligence and military is more on classic cyber security issues like network security or counterintelligence and less on information warfare and citizen surveillance (Freedom House, 2019). However, there are growing concerns that the state may try to expand its legal ability to hack into web servers and computers used by newsrooms and journalists, though such laws are currently still in draft (Freedom House, 2019) and their passing into legislation is uncertain. However, in the summer of 2020 the government finalised legislation that would German intelligence to infiltrate IT devices (e.g. computers, smartphones, etc.) through so-called "Staatstrojaner" to wiretap and record communication. The law is expected to pass without any further issues, and experts remain critical that it leaves legal and technological uncertainties unaddressed (Meister, 2020).

Meanwhile, in February 2019 the Administrative court of Cologne ruled that the German domestic intelligence service, the Office for the Protection of the Constitution (BfV), is not allowed to declare the entire AfD a case for heightened scrutiny as it would 'convey a negative effect to the public'. The AfD had previously called out the declaration as politically motivated, and subsequently went on to legally challenge it in front of the court in Cologne (Deutsche Welle, 2019; Boyd, 2019). Such examples showcase the tight judicial oversight to ensure that any infringement on freedoms is appropriate.

Misinformation from foreign countries, mainly Russia, is also becoming an increasing concern for the government. Russia has established channels such as RT and Redfish, which are especially present on Facebook and YouTube (Figure 2). The main focus of these channels has been right-wing topics supporting the party AfD or the extreme right-wing movement Patriotic Europeans Against the Islamisation of the Occident (Pegida). However, recently (with reports emerging from late 2018) they also appear seem to be taking up left-wing and green topics too. This development has led to demands from politicians across party lines to increase the governmental fight against misinformation to ensure that the public decision-making process is not affected, especially in light of the upcoming EU election. These channels present themselves as a new form of grass-roots journalism for anybody who is frustrated with mainstream media. Even politicians themselves are sometimes unaware of the background of the media sources with which they are engaging: Green Party MP Canan Bayram for example gave an interview to Redfish and was only made aware of their connection to Russia later (see Figure 3 for example post) (Wiebe, 2018; Wiebe, 2018). Additionally, a network of Twitter bots and trolls thought to be connected to the Russian Internet Research Agency have been observed to run temporary influence operations to polarise debates during elections and other political events (e.g. the refugee crisis in 2015). While many Tweets are shared in Russian and English over 100,000 were German and for the most part emanating from accounts that can be perceived as real and human-operated by most other users (Holland, 2018).

To counter such disinformation and propaganda about Germany both domestically and internationally the Ministry of Foreign Affairs established a unit for strategic communication in 2016. Their aim is to understand online communication and provide objective and reliable information through campaigns such as "Rumours about Germany". The ministry has specifically stated that this unit is to inform and not produce counterpropaganda to Russia or the Islamic State (Auswärtiges Amt, 2018; la Cour, 2019).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Germany

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
		X, Predominantly AfD			X though their connection to political parties (AfD) is unclear

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

While state actors are generally not engaged with blocking or filtering content online, in 2015 the Federal Court of Justice ruled that blocking websites was a last resort if it is only way to end copyright infringements (Auswärtiges Amt, 2018; la Cour, 2019). In February 2018, the first case of blocking was enforced by the Munich regional court for the first time, which compelled Vodafone to block kinox.to for uploading illegally owned content. Most other instances of removal online relate to search engine results rather than to content as such. Nevertheless, with the introduction of the Network Enforcement Act there have been several instances where content was removed, causing controversy amongst online communities and the act's potential chilling effects remain concerning (Freedom House, 2019).

The 2017 elections saw the use of microtargeting infrastructures provided by Facebook by all major parties, even though the creation and use of complex voter profile databases is limited due to European and German data protection laws. Nevertheless, such techniques are increasingly being used for elections, with most parties refusing to talk openly about their data-driven strategies (Dachwitz, 2017). Fake news spread by third parties remains a larger issue though, which is one of the reasons why Facebook teamed up with German news agency DPA to fight fake news with fact checking for the 2019 European Election (Der Spiegel, 2020a, 2020b). Moreover, several lawmakers have called for a crackdown on social media bots after MPs were flooded with messages on social media and via email during the debate on the UN migration pact in late 2018. It seems as if over one-quarter of the messages and tweets were from bots. Reportedly, you can buy around one thousand bots for under €10 in Germany (Deutsche Welle, 2018).

In terms of social media use by politicians and parties, most parliamentary parties have official social media accounts. The AfD in particular seems to be quite successful online, continuously scoring high engagement numbers. However, it looks as if this success is partly due to fake accounts: in early 2019 a local AfD account was caught in what has been dubbed a "fake-account-fail" where they gave positive praise in a comment on their own post (Figure 4). Other users made them aware of this error and the comment was quickly deleted. What likely happened is that the administrator of the AfD page forgot to change profiles when commenting on the post (Focus Online, 2019).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Germany

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Human Bots	Pro-Party Support Attack Opposition Driving Divisions	Trolling Conspiracy/Disinformation Data-driven Amplification	Facebook Twitter

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

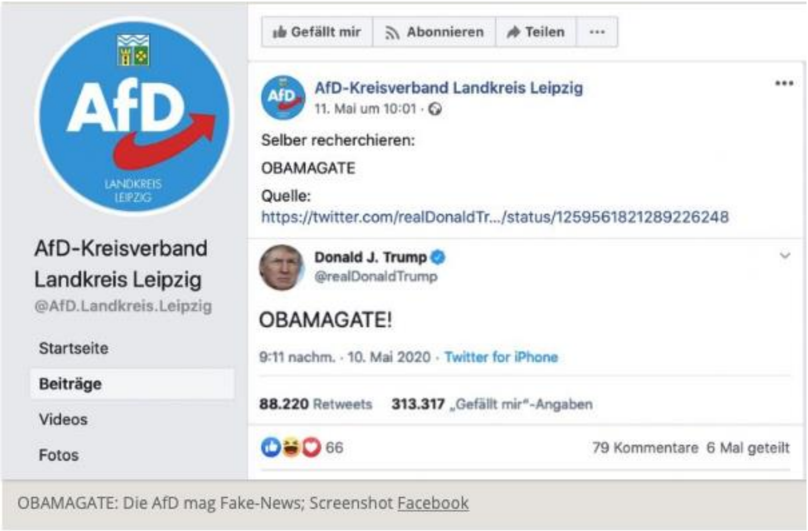
When it comes to cyber troop activity by the state itself, at present there is no evidence that Germany has or is planning to build much capacity in that regard. There are some developments, however, that could suggest the country may consider involving itself with foreign influence operations as it is trying to counter foreign disinformation campaigns and propaganda. The official narrative is to describe these efforts as working to provide objective and reliable information, rather than functioning as counterpropaganda or a counter-misinformation campaign. There is growing evidence that most major parties are employing data-driven microtargeting strategies, which are often supported by Facebook databases even though such utilization remains legally questionable. Still, budgets for such activities are growing: Allegedly the Green Party spent about one third (€ 2 million) of their campaign budget for the 2017 election on online advertising (Dachwitz, 2017).

Information operations that are currently taking place in Germany mainly stem from other country's influence operations, namely Russia, and far-right extremists, including the AfD. These activities tend to linger in the background and show temporary surges of activity during elections or other political events, such as the current COVID-19 pandemic or the refugee crisis of 2015 and 2016. Evidence shows that AfD accounts tend to jump onto favourable narratives and conspiracies to spread them more widely, while Russian activity appears a little more coordinated and deliberate in comparison.

Table 3: Cyber Troop Capacity in Germany

Team Size	Resources Spent (USD)		Activity Levels	Coordination	Capacity Measure
	$2,224,560 (Green Party allegedly)		Temporary (by AfD and foreign actors)	AfD: low Russia: liminal	

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.



AfD-Kreisverband Landkreis Leipzig
@AfD.Landkreis.Leipzig

Startseite
Beiträge
Videos
Fotos

AfD-Kreisverband Landkreis Leipzig
11. Mai um 10:01

Selber recherchieren:

OBAMAGATE

Quelle:
https://twitter.com/realDonaldTr.../status/1259561821289226248

Donald J. Trump
@realDonaldTrump

OBAMAGATE!

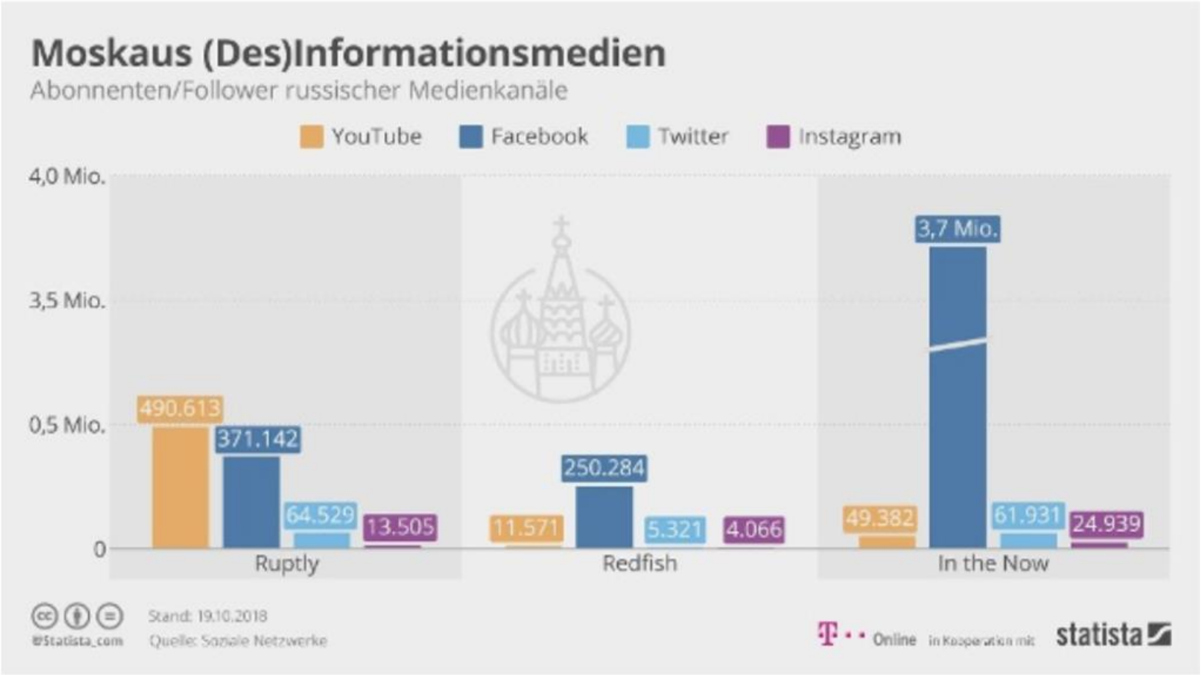
9:11 nachm. · 10. Mai 2020 · Twitter for iPhone

88.220 Retweets 313.317 „Gefällt mir"-Angaben

66 79 Kommentare 6 Mal geteilt

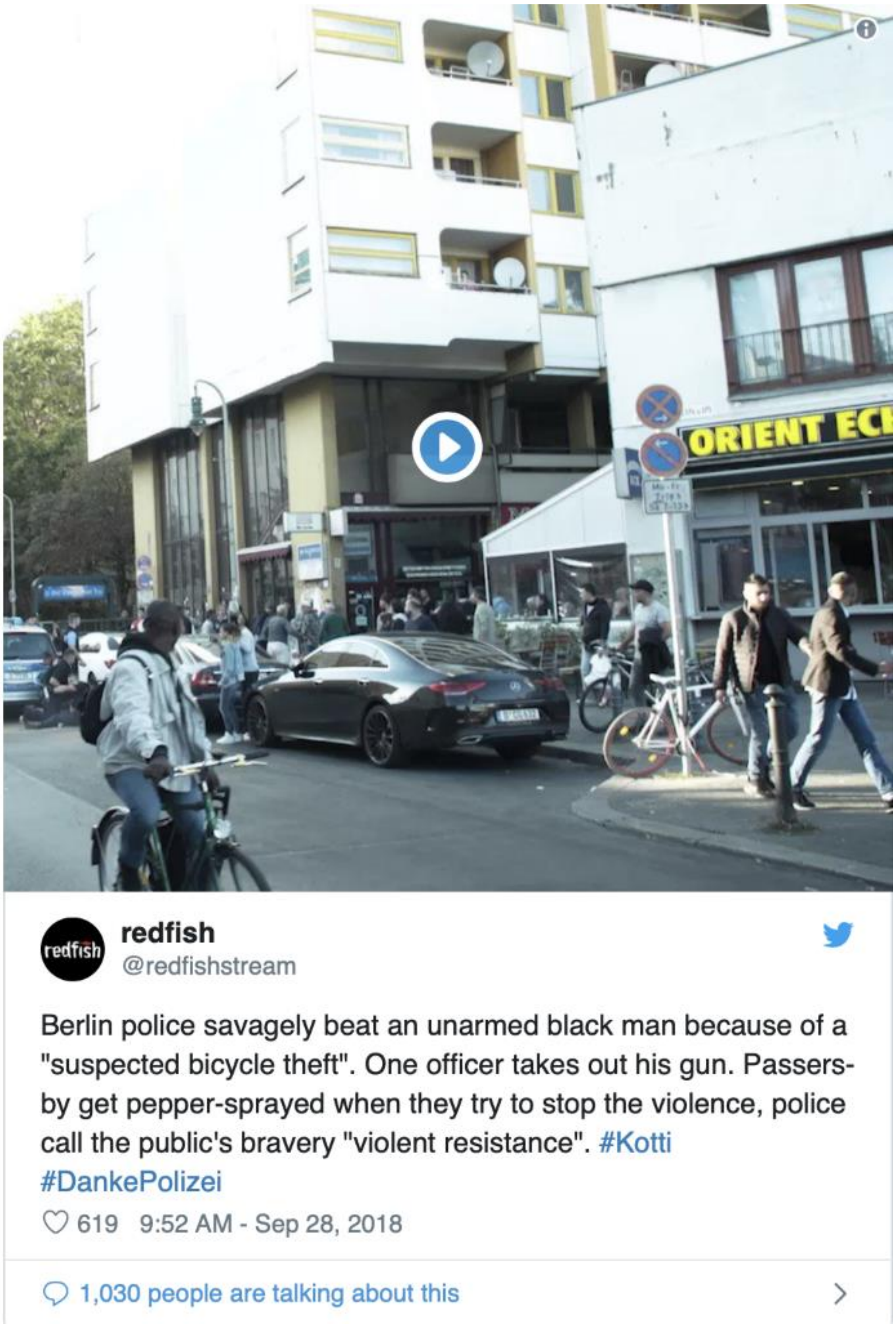
OBAMAGATE: Die AfD mag Fake-News; Screenshot Facebook

Figure 1: Local AfD Facebook page sharing conspiracies of Trump (German post stating: do your own research: OBAMAGATE) (Ansmann, 2020)



Die Kanäle von Ruptly, Redfish und "In the Now" erreichen teilweise Millionen von Menschen. (Quelle: Statista)

Figure 2: number of followers of the three main channels owned by Russia (Jan-Henrik Wiebe, 2018)



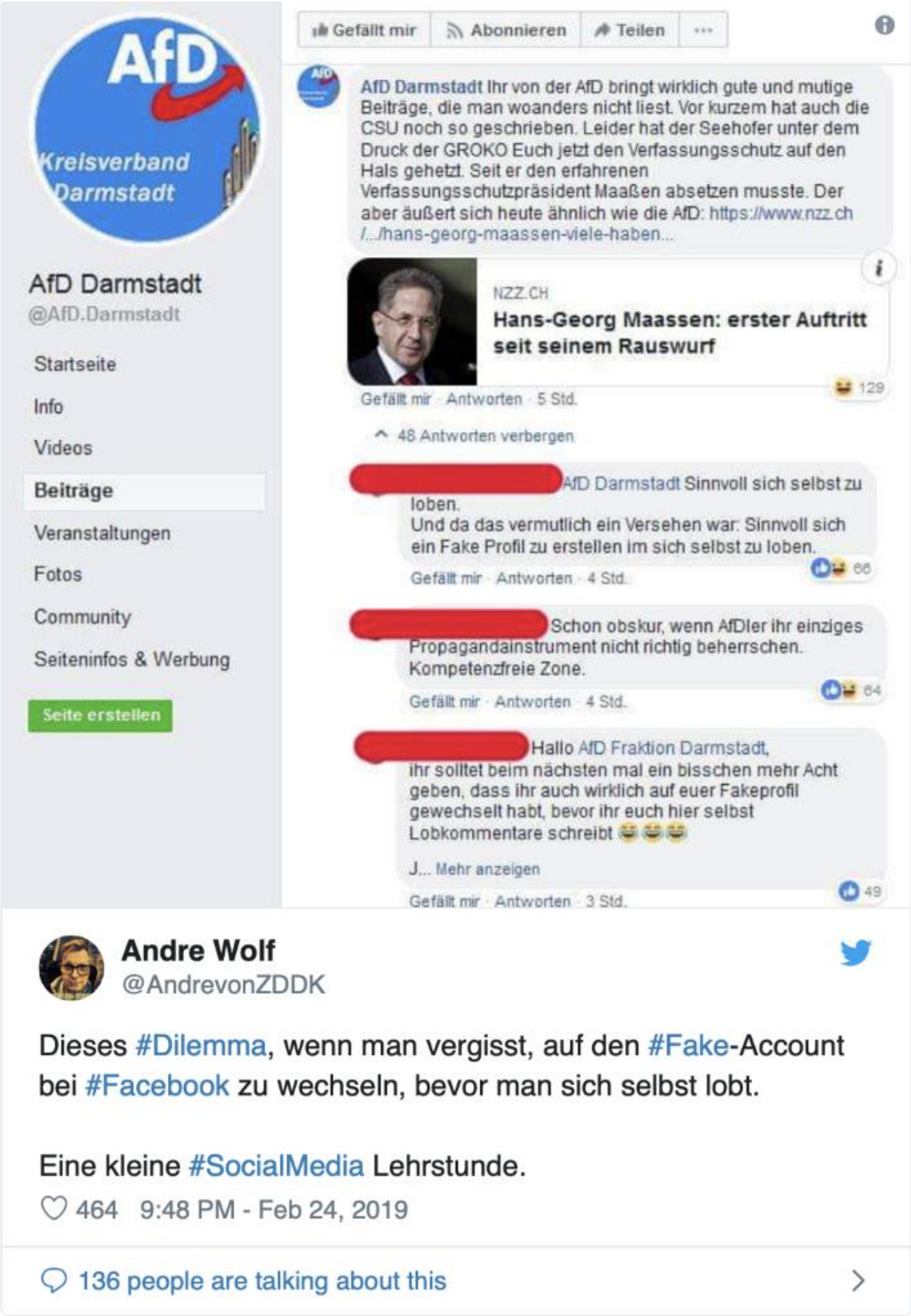
redfish
@redfishstream

Berlin police savagely beat an unarmed black man because of a "suspected bicycle theft". One officer takes out his gun. Passers-by get pepper-sprayed when they try to stop the violence, police call the public's bravery "violent resistance". #Kotti #DankePolizei

♡ 619 9:52 AM - Sep 28, 2018

1,030 people are talking about this

Figure 3: example post of Redfish, owned by Russia (post fails to mention the intense resistance to the police the suspect exhibited before the video starts) (Wiebe, 2018)



AfD Darmstadt Ihr von der AfD bringt wirklich gute und mutige Beiträge, die man woanders nicht liest. Vor kurzem hat auch die CSU noch so geschrieben. Leider hat der Seehofer unter dem Druck der GROKO Euch jetzt den Verfassungsschutz auf den Hals gehetzt. Seit er den erfahrenen Verfassungsschutzpräsident Maaßen absetzen musste. Der aber äußert sich heute ähnlich wie die AfD: https://www.nzz.ch /.../hans-georg-maassen-viele-haben...

NZZ.CH
Hans-Georg Maassen: erster Auftritt seit seinem Rauswurf

129
Gefällt mir · Antworten · 5 Std.

48 Antworten verbergen

[redacted] AfD Darmstadt Sinnvoll sich selbst zu loben.
Und da das vermutlich ein Versehen war: Sinnvoll sich ein Fake Profil zu erstellen im sich selbst zu loben.

66
Gefällt mir · Antworten · 4 Std.

[redacted] Schon obskur, wenn AfDler ihr einziges Propagandainstrument nicht richtig beherrschen. Kompetenzfreie Zone.

64
Gefällt mir · Antworten · 4 Std.

[redacted] Hallo AfD Fraktion Darmstadt,
ihr solltet beim nächsten mal ein bisschen mehr Acht geben, dass ihr auch wirklich auf euer Fakeprofil gewechselt habt, bevor ihr euch hier selbst Lobkommentare schreibt 😂😂😂

J... Mehr anzeigen

49
Gefällt mir · Antworten · 3 Std.

Andre Wolf
@AndrevonZDDK

Dieses #Dilemma, wenn man vergisst, auf den #Fake-Account bei #Facebook zu wechseln, bevor man sich selbst lobt.

Eine kleine #SocialMedia Lehrstunde.

♡ 464 9:48 PM - Feb 24, 2019

136 people are talking about this

Figure 4: AfD's "fake-account-fail" (comment by Andre Wolf reads: The dilemma of forgetting to change to your Fake-Account on Facebook before you praise yourself. A small social media lecture.) (Focus Online, 2019)

References

AfD wins case against spy agency. (2019, February 26). *Deutsche Welle*. https://www.dw.com/en/afd-wins-case-against-spy-agency/a-47695697

Ansmann, P. (2020, May 18). Die AfD setzt auf Hass: Bill Gates und #obamagate. *Ruhrbarone*. https://www.ruhrbarone.de/die-afd-setzt-auf-hass-bill-gates-und-obamagates/185140

Auswärtiges Amt. (2018, May 25). *Außenpolitik strategisch kommunizieren—Werte und Interessen gezielter vermitteln*. Auswärtiges Amt. https://www.auswaertiges-amt.de/de/aussenpolitik/themen/-/2089138

BBC. (2020, February 20). German Kurds react to Hanau shootings. *BBC News*. https://www.bbc.com/news/world-europe-51576446

Boyd, C. (2019, February 26). Germany's intelligence agency acted illegally by declaring it would monitor the anti-migrant AfD party and sent "a negative message to the public", court rules. *Daily Mail*. https://www.dailymail.co.uk/news/article-6747803/Germanys-intelligence-agency-acted-illegally-declaring-monitor-anti-migrant-AfD-party.html

Dachwitz, I. (2017, September 1). Wahlkampf in der Grauzone: Die Parteien, das Microtargeting und die Transparenz. *netzpolitik.org*. https://netzpolitik.org/2017/wahlkampf-in-der-grauzone-die-parteien-das-microtargeting-und-die-transparenz/

Der Spiegel. (2020a, August 7). Rechtsextremismus bei der Polizei: Rund 400 Verdachtsfälle in Bund und Ländern. *Der Spiegel*. https://www.spiegel.de/politik/deutschland/rechtsextremismus-bei-der-polizei-rund-400-verdachtsfaelle-in-bund-und-laendern-a-3e99a308-cf89-4e02-9ca7-ccd73f78a7dc

Der Spiegel. (2020b, August 7). Rechtsextremismus in der Bundeswehr: Erneut KSK-Soldat unter Verdacht. *Der Spiegel*. https://www.spiegel.de/politik/deutschland/bundeswehr-ksk-ausbilder-unter-rechtsextremismus-verdacht-a-42d37195-62f9-44f9-b672-b56d9e1c17c8

Euronews, & with Reuters. (2019, March 18). *Facebook teams up with German news agency DPA to fight fake news ahead of EU elections*. https://www.euronews.com/2019/03/18/facebook-teams-up-with-german-news-agency-dpa-to-fight-fake-news-ahead-of-eu-elections

Eurostat—Internet Use. (2020). Eurostat. https://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_ci_ifp_iu&lang=en

Freedom House (2019). *Freedom on the Net | Germany* . Freedom House. https://freedomhouse.org/country/germany/freedom-net/2019

F-Secure Deutschland. (2017, September 26). Wo waren die Bots? Twitter-Analyse zur Bundestagswahl 2017. *F-Secure*. https://blog.f-secure.com/de/wo-waren-die-bots-twitter-analyse-zur-bundestagswahl-2017/

Germany | Freedom House. (2019). Freedom House. https://freedomhouse.org/country/germany/freedom-world/2020

Germany mulls crackdown on social media bots. (2018, December 16). *Deutsche Welle*. https://www.dw.com/en/germany-mulls-crackdown-on-social-media-bots/a-46764545

Holland, M. (2018, October 24). Russische Trolle in Deutschland: Per Twitter die öffentliche Meinung vergiften. *heise online*. https://www.heise.de/newsticker/meldung/Russische-Trolle-twitterten-auf-Deutsch-als-normale-Nutzer-und-lokale-Boten-4200551.html

Holroyd, M. (2020, May 6). "Super-spreaders" of COVID-19 misinformation on Facebook identified. *Euronews*. https://www.euronews.com/2020/05/06/coronavirus-super-spreaders-of-covid-19-misinformation-on-facebook-identified

Holzki, L. (2020, May 20). Twitter und Facebook: Studie: Das sind Deutschlands größte Verbreiter von Verschwörungstheorien. *Handelsblatt*. https://www.handelsblatt.com/technik/it-internet/twitter-und-facebook-studie-das-sind-deutschlands-groesste-verbreiter-von-verschwoerungstheorien/25842870.html

Kamann, M. (2020, May 11). Anti-Lockdown-Demos: AfD und die neuen Verschwörungstheoretiker. *DIE WELT*. https://www.welt.de/politik/deutschland/plus207902751/Anti-Lockdown-Demos-AfD-und-die-neuen-Verschwoerungstheoretiker.html

Kurz, C. (2015, November 26). BGH-Entscheidung zu Netzsperren: Die nichtsnutzige digitale Sichtschutzpappe ist zurück. *netzpolitik.org*. https://netzpolitik.org/2015/bgh-entscheidung-zu-netzsperren-die-nichtsnutzige-digitale-sichtschutzpappe-ist-zurueck/

la Cour, C. (2019, October 3). Governments countering disinformation: The case of Germany. *StopFake*. https://www.stopfake.org/en/governments-countering-disinformation-the-case-of-germany/

Marchal, N., Kollanyi, B., Neudert, L.-M., & Howard, P. N. (2019). *Junk News During the EU Parliamentary Elections: Lessons from a Seven-Language Study of Twitter and Facebook* (Data Memo 2019.3; p. 6). Oxford Internet Institute. https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/05/EU-Data-Memo.pdf

Meister, A. (2020, June 18). Verfassungsschutzrecht—Wir veröffentlichen den Gesetzentwurf, mit dem alle Geheimdienste Staatstrojaner bekommen. *netzpolitik.org*. https://netzpolitik.org/2020/mit-diesem-gesetz-bekommen-alle-geheimdienste-staatstrojaner/

Naumann, A., Brause, C., Fuest, B., & Hock, A. (2020, May 3). Fake News in der Corona-Krise: Die tägliche Dosis Lügen. *DIE WELT*. https://www.welt.de/politik/deutschland/plus207687573/Fake-News-in-der-Corona-Krise-Die-taegliche-Dosis-Luegen.html

Peinlicher Fake-Account-Fail: So lobt sich die AfD selbst auf Facebook. (2019, February 26). *Focus Online*. https://www.focus.de/digital/internet/peinlicher-fake-account-fail-so-lobt-sich-die-afd-selbst-auf-facebook_id_10375909.html

Sheftalovich, Z. (2020, February 20). At least 11 dead in shootings in Germany’s Hanau: Police. *POLITICO*. https://www.politico.eu/article/at-least-8-dead-in-shootings-in-germanys-hanau-reports/

Wiebe, Jan-Henrik. (2018, October 19). Der Informationskrieg ist für Rechtsstaaten ein Problem. *T-Online*. https://www.t-online.de/nachrichten/deutschland/gesellschaft/id_84640062/russlands-medienzentrale-in-berlin-der-informationskrieg-ist-fuer-rechtsstaaten-ein-problem-.html

Wiebe, Jan-Hnerik. (2018, November 16). Mitten in Berlin: Russlands heimliche Medienzentrale in Europa. *T-Online*. https://www.t-online.de/nachrichten/deutschland/id_84584050/mitten-in-berlin-russlands-heimliche-medienzentrale-in-europa.html

GHANA

Introduction

According to Freedom House, Ghana is a ’Free’ democracy that has been holding peaceful competitive elections since 1992. There are two major political parties, the New Patriotic Party (NPP), which is currently in power, and the National Democratic Congress (NDC), the main opposition. For the most part civil liberties and personal freedoms are protected in Ghana, though discrimination, weaknesses in judicial independence, and political corruption remain issues (Freedom House, 2019). Moreover, minority members in Ghana’s parliament are expressing concerns about the state of democracy in Ghana, citing accusations that the government is ignoring interference in the activities of the Electoral Commission (Graphic Online, 2020).

Press and media freedoms are enshrined in Ghana’s constitution, and Ghana has a diverse and vibrant media landscape. Nevertheless, the government does occasionally restrict media freedom by harassing and arresting journalists. For example, Freedom House notes that “in June 2019, personnel from the Ministry of National Security arrested two journalists from the news website ModernGhana.com in connection with an article on the minister; the reporters were allegedly tortured during interrogation and released within two days.” Moreover, an NPP member of Parliament had publicly encouraged violence against journalists (Freedom House, 2020; Freedom House, 2019). In addition, online fake news and election interference are a concern in Ghana. The Ghanaian Electoral Commission has announced that it will build a media monitoring team to identify disinformation ahead of the 2020 elections that will be held on 7th December (Ngnenbe, 2019). Social media are popular in Ghana. Nearly 70% of Ghanaian citizens use WhatsApp and/or Facebook (Gadjanova et al., 2019) and social media are becoming an increasingly common source for news. At the same time social media are increasingly being used to spread fake disinformation (MyJoyOnline.Com, 2020).

An Overview of Cyber Troop Activity Ghana

Organizational Form

Compared with other countries with case studies cited in the Cyber Troops Report, the Ghanaian government does not engage in cyber troop activity to the same extent. Instead, the Ghanian police often attempt to try and control information flows in a more direct manner. There are cases in which journalists have been arrested on spurious grounds, and in 2016 the Inspector General of the Ghanaian police raised the possibility of shutting down all social media in Ghana during election day. Officially, this was set out as a means of ensuring a peaceful election, but both domestic and international reactions were very critical as shutting down social media would have seriously limited online political discourse. In response to criticism the police assured that access to social media would not be limited (Graphic Online, 2016).

In Ghana various political institutions, organisations, and actors have sought to use social media to their benefit. The Ghanaian Electoral Commission has used social media to disseminate information, educate voters and cut the costs it has incurred through more traditional advertising campaigns (Ngnenbe, 2019). Political parties, particularly the main two, are also known to employ social media strategies for their campaigns, and observers have noted that both parties have been busy building “battalions of social media armies” ahead of the 2020 election. Compared to the last election, held in 2016, the 2020 campaigns are expected to be much more coordinated, particularly on the part of the NDC. The NDC’s social media use was considered to be ineffective in 2016, which is thought to be one of the reasons why the NPP succeeded in winning a majority of the votes that year.

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Ghana

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
	x	x			x

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Ahead of the 2020 elections, Ghana is expecting a surge in fake news, disinformation and political propaganda. Both main parties are preparing for taking using social media for their campaigns. According to a study published by the University of Exeter, the NPP has already compiled a social media team with over 700 people (Gadjanova et al., 2019). Facebook and WhatsApp are the two main platforms where political messages as well as disinformation are spread. At present it appears that automated techniques are not used by domestic actors in Ghana. Rather, it is human actors that spread information through fake and real accounts. However, Ghana is no stranger to data-driven techniques such as microtargeting (Ahiabenu, 2019). The NPP and NDC are also maintaining an international outreach element to their campaigns. For example, the NPP has a UK page called "NPP UK Communications"[1].

Meanwhile, the growing interest in online campaigning has created a market for digital entrepreneurs in Ghana. Young, tech-savvy individuals hope to find work with local or national politicians to maintain their online presence. Some citizens volunteer to set-up and maintain social media accounts for political actors. Interestingly, others take a different route and attempt to extort money from politicians by threatening to circulate negative information (true or false) about them (Gadjanova et al., 2019).

Finally, it appears that Russia has been leveraging tech-savvy citizens in Ghana. In early 2020 a CNN investigation led to Facebook removing 203 pages and accounts from Facebook and Instagram that were operating from Ghana and Nigeria, on the basis that they were for coordinated inauthentic behavior in relation to Russian influence operations. Most of the accounts were fake and were being used to manage pages posing as blogs or non-governmental organizations. Additionally, CNN found a similar network on Twitter, and the platform subsequently removed 71 accounts that had a total of 68,000 followers. All the accounts that were removed were focusing their activity on the United States on behalf of Russia. CNN's investigation also showed that the people working as trolls in Ghana seem to have had no idea that their work was connected to Russian influence operations (Frimpong, 2020; Polglase et al., 2020).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Ghana

Account Types	Messaging and Valence	Communication Strategies	Platforms
Human Fake accounts	Support Attack Opposition	Disinformation Data-driven strategies	Facebook WhatsApp Instagram

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

There are no exact numbers available on the resources spent on social media campaigning by political parties in Ghana. However, it is important to note that even though these platforms make it easier to reach a broader audience, resources and capacity remain an issue. The research published by the University of Exeter notes that while the two major parties are heavily investing in social media campaigns, smaller parties simply do not have the resources to become similarly active online.

For now, it also appears that online influence campaigns do not have a substantial presence in everyday lives of Ghanaians. Rather, such efforts are mobilized during politically sensitive times, such as elections, and subsequently calm down afterwards.

Table 3: Cyber Troop Capacity in Ghana

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
		Temporary	Coordinated	

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

In relation to the COVID-19 pandemic, Ghana is experiencing a surge in conspiracy and fake news being spread about the virus. The most common topic about which conspiracy and misinformation are spread are fake cures. It appears that several doctors in Ghana have taken advantage of the situation to scam patients out of money by advertising cures to the virus (Owoseye, 2020; The Media Online, 2020). Meanwhile formal sources for information on the virus seem to be scarce and the void has been filled with informal news, often times causing fear, discrimination, stigmatization and confusion (APO Group, 2020).

References

Ahiabenu, K. (2019, June 20). What is political micro targeting? *Graphic Online*. https://www.graphic.com.gh/features/features/what-is-political-micro-targeting.html

APO Group. (2020, June 11). Gov'ts must fight COVID misinformation. *BusinessGhana*. http://www.businessghana.com/site/news/general/215149/Gov

Freedom House. (2020). *Freedom in the World: Ghana*. Freedom House. https://freedomhouse.org/country/ghana/freedom-world/2020

Frimpong, E. D. (2020, March 13). Facebook removes 203 pages and accounts in Ghana and Nigeria for coordinated inauthentic behaviour from Russia. *Graphic Online*. https://www.graphic.com.gh/news/general-news/facebook-removes-203-pages-and-accounts-in-ghana-and-nigeria-for-coordinated-inauthentic-behaviour-from-russia.html

Gadjanova, E., Lynch, G., Reifler, J., & Saibu, G. (2019). *Social Media, Cyber Battalions, and Political Mobilisation in Ghana*. University of Exeter. https://doi.org/10.13140/RG.2.2.24383.25766

Ghana | Freedom House. (2019). Freedom House. https://freedomhouse.org/country/ghana/freedom-world/2019

Graphic Online. (2020, February 20). Minority defends boycott of 2020 State of the Nation Address. *Graphic Online*. https://www.graphic.com.gh/news/general-news/minority-defends-boycott-of-2020-state-of-the-nation-address.html

Ngnenbe, T. (2019, September 19). EC to 'arrest' fake news. *Graphic Online*. https://www.graphic.com.gh/news/politics/ghana-news-ec-to-arrest-fake-news.html

Owoseye, A. (2020, July 1). *Undercover journalists expose Ghana's COVID-19 scam*. https://www.premiumtimesng.com/health/400515-undercover-journalists-expose-ghanas-covid-19-scam.html

Polglase, K., Shukla, S., Mezzofiore, G., & Lister, T. (2020, April 11). How Russian meddling is back before 2020 vote. *CNN*. https://www.cnn.com/2020/03/12/world/russia-ghana-troll-farms-2020-ward/index.html

Police Service rescinds decision to ban social media. (2016, June 27). *Graphic Online*. https://www.graphic.com.gh/news/general-news/police-service-rescinds-decision-to-ban-social-media.html

Social media increasingly used to spread fake news in Ghana. (2020, June 8). *MyJoyOnline.Com*. https://www.myjoyonline.com/news/national/social-media-increasingly-used-to-spread-fake-news-in-ghana-afrobarometer/

The Media Online. (2020, July 1). BBC Africa Eye and Anas Aremeyaw Anas expose Covid-19 scam. *The Media Online*. themediaonline.co.za/2020/07/bbc-africa-eye-and-anas-aremeyaw-anas-expose-covid-19-scam/

Greece

Introduction

Computational propaganda and information manipulation online have swiftly moved into Greek public life in the past few years. Given the politically and financially unstable situation of the country in the recent past, fake news and online conspiracy theories have found fertile ground in Greece and further complicated the country's situation. About 71% of Greek internet users now use social media as their main source for news (MANDRAVELIS, 2020; ΓΕΩΡΓΑΚΟΠΟΥΛΟΣ, 2019). The independent watchdog organisation Freedom House (2020) reports that Greece's parliamentary democracy is characterised by vigorous competition between political parties with generally free and independent media coverage. Nevertheless, lately there have been several political controversies in Greece based on fake news. This development is becoming increasingly expensive (literally, but also in terms of political and societal costs). Some experts even claim that social media and fake news are so influential in Greece that they are starting to distort democracy (Konstantopoulou, 2018; News IT, 2019). A recent survey, however, showed that about 80% of Greeks are aware they should not believe everything they read online (MANDRAVELIS, 2020), while more than half of Greek respondents in a Eurobarometer survey reported coming across fake news daily (Net Politics, 2019). In July 2019, the country held a legislative election which incumbent prime minister Alexis Tsipras from the leftist SYRIZA party lost to Kyriakos Mitsotakis from the centre-right liberal conservative party New Democracy (BBC News, 2019).

The recent COVID-19 pandemic has been affecting Greece as well, albeit to a lesser degree than some other countries. The government was swift to order a lockdown, and for the most part citizens did their part to ensure the situation did not get out of hand. Many sought to share their support online, through hashtags such as #menoumespiti (#westayathome) and by organising help for those in need via online platforms such as Facebook (ARTE & Balkan Insight, 2020; Malichudis, 2020). However, as schools started to open for the new academic year, a surge of conspiracies, many of which question whether the virus is real, have led to public unrest as the government is scrambling to curb the spread of hoaxes through, for example, Facebook groups (The National Herald, 2020a, 2020b). Additionally, with a large population of refugees provided for in camps, the situation remains tense, especially after Turkey declared the border to Greece open in an attempt to allow refugees to cross into EU territory. The dispute between the two countries is still on-going and has led to a surge in conspiratorial content (Menke & Neufeld, 2020).

An Overview of Cyber Troop Activity in Greece

Organizational Form

When Tsipras took office, he vowed to support modern and independent news, but instead old media oligarchs remained in place and new "Tsipras-era" ones are establishing themselves and continue to control the main media outlets. In 2016 the government held auctions for television licenses, which were officially overseen by the independent National Council for Radio and Television, however, critics have accused the government of using the procedure to alter the media landscape in their favour (ΓΕΩΡΓΑΚΟΠΟΥΛΟΣ, 2019). Additionally, while some European countries (e.g. Germany and France) passed domestic laws against fake news (which are not without controversy), Greece is keeping with EU coordinated measures such as National Election Networks to support the national election processes across the EU (Karaoulanis, 2019). Thus far, the new government has not passed any impactful legislation in relation to fake news or disinformation campaigns.

A continuous hot topic in the country is corruption and unfortunately past prime minister Tsipras and his SYRZIA party did not seem to be keeping their promise of fighting it (In Box News, 2019; Kourdistoportocali, 2019; Κανέλλης, 2019; Κουνιάς, 2019). The new government has seen to improve the situation however, corruption continues to be a concern (Freedom House, 2020). Additionally, the country is currently preoccupied with something akin to a cyberwar with Turkey, after the Turkish President declared the border between Turkey and Greece open in February 2020 in hopes of letting through refugees to the European Union. The EU and Greece maintain that the border remains closed. The dispute has led to a surge in reports and allegations spread online, many of which are unverifiable, leading to the Greek Foreign Ministry to repeatedly debunking and dismissing fake reports, often resorting to Twitter to do so (Ekathimerini, 2020a, 2020b). At the same time riots and violence are breaking out within the border and other refugee camps (Menke & Neufeld, 2020).

Just like in most European countries, Greek political parties are increasingly using online platforms to guide public opinion. Some evidence even suggests that all major parties have "dealing rooms" where people sit and coordinate the dispersal of news and texts to influence voters, order trolls and block certain news. These activities mainly focus on individuals who are undecided and did not want to vote (ΚΑΡΑΙΣΚΑΚΗ, 2019).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Greece

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
	Foreign Ministry	X			X

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Most Greek parties seem to have started to employ bots to ensure their voters stay party supporters by feeding them the stories they want to hear and thus assuring them in their views (ΚΑΡΑΙΣΚΑΚΗ, 2019). A recent example of computational propaganda comes from the Rhodes local elections of 2018 where online trolling seems to have gotten out of hand. Specific people (both politicians but also private individuals) were allegedly targeted with hate campaigns. While initially the trolls worked in small units or individually, they quickly started coordinating and formed troll farms. Organizers created webpages where they would leave directions as to whom should be targeted and state political goals (Αθανασίου, 2018). However, there are few little national reports on these activities and the exact size of the operations is unknown, thus these reports, which are quite vague, should be read with care.

Before the national election, local papers were assuming that Tsipras was looking at a bad defeat and was allegedly preparing for a campaign "American style": hiring a large foreign company to run an online campaign, focusing on social media and microtargeting as these are strategies which had proven effective in US elections. In the meantime, fake news and deliberate misinformation campaigns continue to operate at full speed: According to an analysis by Crisis Monitor a total of 3.868 fake news mentions were published between 1-10 March 2019, with Twitter having the largest volume. It appears that Greece has experienced all the main components of most modern information wars during elections; trolls, spam bots, chat bots (reportedly over 33,000 were created on Facebook in 2016 alone), fake news and general propaganda (Crisis Monitor, 2019).

More recently, an investigation by Balkan Insight showcased how far-right nationalists are utilising automated armies on social media to amplify their agendas and ideas, particularly in relation to the on-going tensions of the country name of their neighbour, North Macedonia (Zafeiropoulos, 2019). Additionally, there have been reports of SYRIZA, now in opposition to the government, fabricating accusations against the Greek government, particularly the Tourism Ministry, to attack their spending plans and general politics (iefimerida.gr, 2020; Newsteam Spoilers, 2020).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Greece

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Human Bots	Support Attack Opposition	Disinformation Trolls Amplifying content	Twitter Facebook

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

While there are reports on cyber troop activities from several political parties, there is fairly little known on how they pay for such campaigns, particularly because their financial situations have not look too promising in recent years (Κουνιάς, 2019; Λυγερού, 2019). Moreover, for the most part, such party-based activities are temporary and organised around elections and other political events.

In light of recent border tensions with Turkey, the Greek government appears to be gearing up a little bit: reports have surfaced that the National Intelligence Service has hired eighty new hackers to support the growing conflict between Greece and Turkey. Much of the disagreement is now being carried out online and has degenerated into a cyberwar of cyber-attacks between the two countries, reportedly even Anonymous Greece has joined in (Antonopoulos, 2020a, 2020b; ΠΟΛΙΤΙΚΗ, 2020).

Table 3: Cyber Troop Capacity in Greece

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
80 new recent hires[1]		Temporary	Decentralised	

[1] Their jobs seem to focus on hacking, engagement with information warfare unclear

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

References

Analytics: Εκλογές πλησιάζουν, Fake news, bots και trolls στο προσκήνιο. (2019). Crisis Monitor. https://www.crisismonitor.gr/2019/03/12/analytics-ekloges-plisiazoyn-fake-news-bots-kai-trolls-sto-proskinio/

Antonopoulos, P. (2020a, June 14). Greece hires 80 new hackers as cyberwar with Turkey intensifies. *Greek City Times*. https://greekcitytimes.com/2020/06/14/greece-hires-80-new-hackers-as-cyberwar-with-turkey-intensifies/

Antonopoulos, P. (2020b, December 6). Turkish media lie about cyberattack against Greek ministry after Turkish hackers humbled by Anonymous Greece. *Greek City Times*. https://greekcitytimes.com/2020/06/13/turkish-media-lie-about-cyberattack-against-greek-ministry-after-turkish-hackers-humbled-by-anonymous-greece/

ARTE, & Balkan Insight. (2020, June 1). Coronavirus Concerns Grow in Migrant, Refugee Camp in Greece | Balkan Insight. *Balkan Insight*. https://balkaninsight.com/2020/06/01/coronavirus-concerns-grow-in-migrant-refugee-camp-in-greece/

BBC News. (2019, July 8). Centre-right regains power in Greece. *BBC News*. https://www.bbc.com/news/world-48902766

Ekathimerini. (2020a, March 1). Greece calls out Turkish "disinformation" on migrants | Kathimerini. *Ekathimerini*. http://www.ekathimerini.com/250095/article/ekathimerini/news/greece-calls-out-turkish-disinformation-on-migrants

Ekathimerini. (2020b, May 23). Ministry dismisses reports of 'invasion' of Greek territory as 'fake news' | Kathimerini. *Ekathimerini*. http://www.ekathimerini.com/252981/article/ekathimerini/news/ministry-dismisses-reports-of-invasion-of-greek-territory-as-fake-news

Freedom House. (2020). *Freedom House | Greece*. https://freedomhouse.org/country/greece/freedom-world/2020

iefimerida.gr. (2020, June 6). Πέτσας κατά ΣΥΡΙΖΑ για την καμπάνια του τουρισμού: Fake news, υιοθετεί ό,τι διακινούν τα trolls του διαδικτύου | ΠΟΛΙΤΙΚΗ. *iefimerida.gr*. https://www.iefimerida.gr/politiki/petsas-syriza-kampania-toyrismoy-trolls

In Box News. (2019, March 30). Παιχνίδια με πρόωρες εκλογές από τον Σύριζα—Μάιο ή Οκτώβριο; *In Box News Greece*. https://www.inboxnews.gr/politiki/paihnidia-me-proores-ekloges-apo-ton-syriza-maio-i-oktovrio

Karaoulanis, T., & Καραουλάνης, Θ. (2019, March 14). fake news και παραπληροφόρηση: η ΕΕ ετοιμάζεται να αντιμετωπίσει την εχθρική προπαγάνδα. *Euractiv*. https://www.euractiv.gr/section/ekloges/news/fake-news-kai-parapliroforisi-i-ee-etoimazetai-na-antimetopisei-tin-echthriki-propaganda/

Konstantopoulou, Z. (2018, September 7). If you love Greece, help us get rid of Alexis Tsipras and his zombie party. *The Guardian*. https://www.theguardian.com/commentisfree/2018/jul/09/greece-alexis-tsipras-syriza-austerity-eu

Kourdistoportocali. (2019, March 30). Μαρινάκης>Ο Τσίπρας έδωσε δώρα 750 εκατ. Ευρώ στον Κόκκαλη. *Kourdistoportocali*. https://kourdistoportocali.com/news-desk/marinakiso-tsipras-edose-dora-750-ekat-evro-ston-kokkali/

Malichudis, S. (2020, March 30). Getting By In Greece, Under Lockdown | Balkan Insight. *Balkan Insight*. https://balkaninsight.com/2020/03/30/getting-by-in-greece-under-lockdown/

MANDRAVELIS, V. (2020, June 3). Greeks wise to online fake news, Vangelis Mandravelis | Kathimerini. *Ekathimerini*. http://www.ekathimerini.com/253392/article/ekathimerini/business/greeks-wise-to-online-fake-news

Menke, M., & Neufeld, S. (2020, May 27). What's going on at the Greek-Turkish border? *The New Federalist*. https://www.thenewfederalist.eu/greek-turkish-border-what-s-going-on-there

Net Politics. (2019, May 23). Europe’s Elections: The Fight Against Disinformation. *Council on Foreign Relations*. https://www.cfr.org/blog/europes-elections-fight-against-disinformation

News IT. (2019, August 4). Σκουρλέτης: Ποτέ άλλοτε δεν υπήρχαν τόσα fake news. *News It Newsrook*. https://www.newsit.gr/politikh/skourletis-pote-allote-den-ypirxan-tosa-fake-news/2754698/

Newsteam Spoilers. (2020, June 6). Ο ΣΥΡΙΖΑ υιοθετεί τα fake news των trolls του διαδικτύου. *Spoilers*. https://spoilers.gr/o-syriza-uiothetei-ta-fake-news-ton-trolls-tou-diadiktuou/

The National Herald. (2020a, August 21). Greek Police Probe Facebook Anti-Mask Campaign Aimed at Schools. *The National Herald*. https://www.thenationalherald.com/archive_general_news_greece/arthro/greek_police_probe_facebook_anti_mask_campaign_aimed_at_schools-743139/

The National Herald. (2020b, August 23). Greek Cybercops Push Prosecution of COVID-19 Conspiracy Sites. *The National Herald*. https://www.thenationalherald.com/archive_general_news_greece/arthro/greek_cybercops_push_prosecution_of_covid_19_conspiracy_sites-751740/

Zafeiropoulos, K. (2019, December 18). Alexander the Bot: The Twitter War for the Macedonian Soul. *Balkan Insight*. https://balkaninsight.com/2019/12/18/alexander-the-bot-the-twitter-war-for-the-macedonian-soul/

Αθανασίου, Δ. (2018, September 28). Με troll farms τα στρατόπεδα των υποψηφίων στις εκλογές της αυτοδιοίκησης στη Ρόδο Πηγή:www.dimokratiki.gr. *Dimokratiki*. https://www.dimokratiki.gr/28-09-2018/me-troll-farms-ta-stratopeda-ton-ypopsifion-stis-ekloges-tis-aytodioikisis-sti-rodo/

ΓΕΩΡΓΑΚΟΠΟΥΛΟΣ, Θ. (2019, August 3). Εκλογές, ψέματα και πλατφόρμες. *Kathimerini*. http://www.kathimerini.gr/1013722/opinion/epikairothta/politikh/ekloges-yemata--kai-platformes

Κανέλλης, Β. Σ. (2019, December 2). *«Ιερό» κόλπο Τσίπρα για να κάνει 10.000 προεκλογικές προσλήψεις*. https://www.in.gr/2019/02/12/politics/kyvernisi/iero-kolpo-tsipra-gia-na-kanei-10-000-proslipseis-apo-tin-piso-porta-sxedio-gia-tous-misthous-ton-ieromenon/

ΚΑΡΑΙΣΚΑΚΗ, Τ. (2019, March 25). Η αναμέτρηση Ευρώπης—Fake news. *Kathimerini*. http://www.kathimerini.gr/1016041/gallery/texnologia/diadiktyo/h-anametrhsh-eyrwphs---fake-news

Κουνιάς, Δ. (2019, July 4). ΑΠΟΚΑΛΥΨΗ: Το «κόλπο» για τα δάνεια του ΣΥΡΙΖΑ. *Parapolitika*. https://www.parapolitika.gr/article/to-kolpo-gia-ta-dania-tou-siriza

Λυγερού, Ν. (2019, March 18). Τα επιτελικά σχέδια του ΣΥΡΙΖΑ για τις εκλογές. *SL Press Greece*. https://slpress.gr/politiki/ta-epitelika-schedia-toy-syriza-gia-tis-ekloges/

ΠΟΛΙΤΙΚΗ. (2020, June 13). «Νέο αίμα» στον ελληνικό κυβερνοστρατό: Με 80 χάκερ στελεχώνεται η ΕΥΠ. *Έθνος*. https://www.ethnos.gr/politiki/110338_neo-aima-ston-elliniko-kybernostrato-me-80-haker-stelehonetai-i-eyp

Guatemala

Introduction

Guatemala has been facing major political challenges for a substantial period of time. Over the years, these have ranged from an armed conflict that lasted more than thirty years (1960 – 1996) to the continuing influence of criminal organizations that have gained control of state institutions. Most recently, the country has been immersed in corruption scandals and the undermining of checks and balances. The International Commission against Impunity in Guatemala (CICIG) was created in 2006 by the United Nations and Guatemala as an independent body to support national institutions in their investigations, such as that of the bribery and tax evasion network that involved the political elite, and prosecution of serious crimes, including the genocide trials against Efraín Rios Montt. In early 2019, however, President Jimmy Morales unilaterally terminated the agreement whilst accusing the CICIG of acting against the constitution.

Since 2012 there has been evidence of surveillance programs targeting journalists, and in 2017 the media outlet Nómada was subject to DDoS attacks over a period of several months, one of them they had published a damning account of government inaction and negligence related to a fire at a children's public shelter (Committee to Protect Journalists, 2020). Since 2016 coordinated social media activities aiming to create disinformation and attack the opposition have boosted operations of what have locally been termed as net centres.

Guatemala has low rates of internet access, with only 52.7% of the population online («Informe», 2019). Facebook is the most used social media platform, while Twitter has a low level of penetration. Social media, however, is not the main source of information about politics, with only 9.2% of the population using it for this purpose («Informe», 2019). Nonetheless, during Jimmy Morales' administration (2016-2020), political violence on social media was constant and there were episodes of "coordinated, state aligned campaigns of online disinformation" (Abbas et al., 2019) and harassment and organized online attacks on opposition figures, especially environmental and indigenous activists (Committee to Protect Journalists, 2020). Abbas et al. (2019) highlight the serious risk posed by online harassment in the national context of historical violence and genocide. Indeed, their report suggests that standards for moderation on social media platforms lack contextualized rules. Whilst the "vocabulary of coded speech" of attacks and harassment might be considered unproblematic for content moderators, in Guatemala, where "violence is condoned and perpetrators are often not charged or prosecuted", this vocabulary might be dangerous (Abbas et al., 2019).

Finally, it is worth noting that the legal framework in Guatemala does not incorporate digital attacks as types of crimes nor does it counterbalance potential attempts of organized online harassment campaigns (Committee to Protect Journalists, 2020).

An Overview of Cyber Troop Activity in Guatemala

Organizational Form

In early 2019, the International Commission against Impunity in Guatemala (CICIG) released a report on bots and net centres. They had already been in operation for years. However, while Luis Assardo mentioned initial operations already evident in 2008 in online newspaper comments (*Los Netcenters: Negocio de manipulación—Luis Assardo—Medium*, s. f.), more sustained social media manipulation has been recorded since 2016 («Informe», 2019). Since then, there have been multiple attacks on anti-corruption activists, CICIG officials, and opposition figures in general.

Currier & Mackey (2018) suggested that a portion of the pro-government propaganda during Morales' administration originated from within the government itself. This allegation was reinforced by the link established between a Twitter account under the pseudonym DictaLord and Marvin Palacios Castillo, who was closely connected with the political elite in Guatemala and had two contracts "related to social media monitoring" (Currier & Mackey, 2018). It has also been alleged that Elsie Sierra, news director at Channel 13, recruited people to work at net centres and connected them with the Secretary of Communication to the Presidency to manage pro-Morales social media accounts (Nómada, 2018).

Additionally, Currier & Mackey (2018) highlight the involvement of business elites, comprised of former military figures, who invest in these campaigns. In line with this, the CICIG report («Informe», 2019) specified that the primary clients of these net centres are public servants, politicians, and members of the business community. However, no individual names were specified and, in spite of the state-aligned campaigns, the connections to the government are not clearly established.

Although most journalists state that the level of activity of net centres have decreased since the 2019 general elections, "the infrastructure to attack journalists is still there" (Committee to Protect Journalists, 2020).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Guatemala

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
2016	Evidence found	Evidence found	Evidence found		Evidence found

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

The report by the CICIG («Informe», 2019) provided evidence of the existence of individuals or companies that work to discredit, attack and disseminate disinformation, especially against anti-corruption activists, via social media, including such platforms as Facebook, Twitter, and the messaging app WhatsApp. Additionally, social media accounts and email accounts have been hacked or "communications intercepted" (Committee to Protect Journalists, 2020).

Net centres make use of fake accounts to amplify pro-government messages and attacks on opposition. Moreover, opponents are not only subject to account hacking, online stalking, and image manipulation, but also direct intimidation and threats (Abbas et al., 2019). Forms of online harassment include the dissemination of memes and the labelling of targets as terrorists, leftists, foreign invaders, and more, reinforcing the polarized rhetoric of the civil war period. The 2019 Annual Report of the Office of the Special Rapporteur for Freedom of Expression at the Inter-American Commission on Human Rights made special reference to the concerns that journalists were being targeted often with vocabulary associated with war, such as "enemies of the country" and "guerrilla", as well as other militarized terminology (IACHR, 2020).

There were also cases of defamation transmitted over anonymous blogs (IACHR, 2020). Other messages urged people to physically attack or condemn targeted individuals (Committee to Protect Journalists, 2020). When Iván Velásquez, head of the CICIG, was declared persona non grata by President Morales, fake accounts targeted defamation campaigns against Velásquez, with messages disseminated on Twitter, Facebook, and WhatsApp both by these accounts and others related to right-wing commentators (Abbas et al., 2019; Currier & Mackey, 2018). Thelma Aldana, former Attorney General of Guatemala, was also subject to collateral aggression (Currier & Mackey, 2018), and when she ran for president in 2019 she was "one of the most targeted individuals in Guatemala" (Abbas et al., 2019). In fact, it was during the presidential elections in 2015 and 2019 that attacks increased (Committee to Protect Journalists, 2020). As Edison Lanza stated, stigmatization and defamation were not only present on social media but also in Morales' own statements (IACHR, 2020). He labelled journalists and the media as "unfair", "illegal", "liars", and expressed intentions of attacking those who criticized the government, including La Hora, Guatevisión, Prensa Libre, and Emisoras Unidos (IACHR, 2020).

Human rights defenders, such as Helen Mack (Abbas et al., 2019) and Juan Francisco Sandoval (Head of the Special Prosecutor's Office Against Impunity) (Comisión Internacional contra la Impunidad en Guatemala, 2019), and journalists were also targeted by net centres.

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Guatemala

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Bots, Human. Fake and hacked.	Pro-government, pro-party, Attack opposition, Suppressing speech	Disinformation, Trolls, Amplifying content	Twitter, Facebook, WhatsApp

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

According to several reports (Currier & Mackey, 2018; *Los Netcenters: Negocio de manipulación*—Luis Assardo—Medium, s. f.), it is understood that net centres are related to "more conventional online marketing businesses". A report by CICIG («Informe», 2019) found that most coordinated accounts are localized in Guatemala City, Xela, and increasingly, Cobán.

Each operation involves between fifteen and twenty people, who manage in total 100-200 fake accounts on Twitter and Facebook (Currier & Mackey, 2018; «Informe», 2019). Multiple accounts are also managed by different people («Informe», 2019), and they have a greater level of activity from Monday to Friday from 6 am to 6 pm. Employees are mostly university students, who receive between Q3.000 and Q4.000 per month (around $380-520) («Informe», 2019).

These net centres are paid more than $280,000 for their services (Abbas et al., 2019), around $7,000 per month («Informe», 2019). Most specifically, for the full-time pro-candidate and attack campaigns during general elections in 2015, net centres asked for $375,000 (Currier & Mackey, 2018). As suggested by Assardo, "there were two big net center operations that worked for all the major candidates" (Currier & Mackey, 2018). After 2015, net centres expanded to include foreign clients.

In terms of tasks, employees receive a handbook with amplification strategies and pre-established scripts, comments, links, and targeted users, among other things. Moreover, net centres use a third-party database with phone numbers that are then used to target campaigns via WhatsApp (Currier & Mackey, 2018).

Table 3: Cyber Troop Capacity in Guatemala

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
15-20 per operation	$280,000-375,000 per campaign $7,000 per month	Permanent, with peaks during critical events, such as trials or elections.	Centralised	Medium

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

References

Abbas, M., Al-Wohaibi, E., Donovan, J., Hale, E., Marugg, T., Sykes, J., Land, M. K., & Wilson, R. A. (2019). Invisible Threats: Online Hate Speech Against Human Rights Defenders in Guatemala. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3483258

Committee to Protect Journalists. (2020). *Trust deficit: Guatemala's new president must overcome skepticism to improve press freedom*. Committee to Protect Journalists. https://cpj.org/reports/2020/03/guatemala-giammattei-journalists-online-harass-discredit-corruption-environment.php

Currier, C., & Mackey, D. (2018, April 7). The Rise of the Net Center: How an Army of Trolls Protects Guatemala's Corrupt Elite. *The Intercept*. https://theintercept.com/2018/04/07/guatemala-anti-corruption-trolls-smear-campaign/

IACHR. (2020). *Annual Report 2019. Report of the Office of The Special Rapporteur for Freedom of Expression.* (OEA/Ser.L/V/II. Doc. 5.). http://www.oas.org/en/iachr/docs/annual/2017/docs/AnnexRELE.pdf

Informe: Bots, netcenters y el combate a la impunidad. (2019, May 20). ⚖ *CICIG*. https://www.cicig.org/cicig/informes_cicig/informes-tematicos/bots-netcenters-y-el-combate-a-la-impunidad/

Los Netcenters: Negocio de manipulación—Luis Assardo—Medium. (s. f.). https://medium.com/@luisassardo/los-netcenters-negocio-de-manipulaci%C3%B3n-2140cf7262fc

Nómada. (2018, February 20). Acusan a directora de Canal 13 de contratar netcenteros para el Gobierno. *Nómada*. https://nomada.gt/pais/la-corrupcion-no-es-normal/acusan-a-directora-de-canal-13-de-contratar-netcenteros-para-el-gobierno

Honduras

Introduction

In 2009, a military coup removed President Manuel Zalaya. Since then, Honduras has struggled with fragile democratic institutions. The first elections after the coup in which there was participation by opposition parties were held in 2013 and right-wing Juan Orlando Hernández won. He was re-elected in 2017, but there were claims of fraud. The government and the Organization of American States established in 2016 the Mission to Support the Fight against Corruption and Impunity in Honduras (MACCIH), which was ended in January 2020.

Additionally, poverty and inequality have been persistent historical problems. The country has also one of the highest rates of violence in the world and, in addition to impunity of crimes and abuses committed by the judiciary and the police, it is one of the most dangerous places to be a journalist, an activist or a woman (Human Rights Watch, 2019). Because of this, there are substantial flows of emigrants and asylum-seekers. In 2019, after the Congress passed two bills on health and education reforms, a wave of anti-government protests took place. Honduran security forces used excessive force and several people were injured and, by the end of the year, at least six people were killed (Human Rights Watch, 2019). In this context, freedom of expression is often undermined.

An Overview of Cyber Troop Activity in Honduras

Organizational Form

Online attacks towards journalists are on the rise, usually with death threats content (2019 World Press Freedom Index | Reporters Without Borders, 2019). Those media outlets and journalists that are critical of the government or that cover sensitive topics are often subject to threats, blocking, harassment and event conviction. It was documented that the government, through its National Direction of Research and Intelligence, paid 355,000 euros to Hacking Team in 2014 for its Galileo platform (Pérez de Acha, 2016) to hack and spy on opposition.

As regards online social media manipulation, there is evidence that the government used Facebook and Twitter to generate support (Cryst & García Camargo, 2020) as early as 2015 (Garay, 2019) and with significant operations around the 2017 elections that also attacked opposition (Cryst & García Camargo, 2020). It is documented that the government pays for social media ads and fake profiles (Garay, 2019), as well as content creators, influencers, and journalists (Cryst & García Camargo, 2020).

Finally, it has been noted that Archimedes Group, a private Israeli firm managed Facebook groups aligned to the government. However, there is no evidence of who was the client of the company.

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Honduras

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
2015	Evidence found		Archimedes Group		Content creators, social media influencers and journalists

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

The government uses Facebook and Twitter to generate support. During the citizens protests of 2015, a network of pro-government bots (JOHBots, as they would then be identified as) coordinated to amplify content (Garay, 2019).

During the 2017 elections around a hundred clusters of rudimentary Twitter bots coordinated "to provide a positive social media fog in what turned out to be a violent post-electoral circumstance" (Gallagher et al., 2019). As analysed by Erin Gallagher (2018), groups of accounts share common characteristics. For instance, of the active accounts between 25 and 29 December 2017 that mentioned Juan Orlando Hernández, there was a group that used profile pictures of attractive women with cover photos and that were created on 10 or 17 June 2015. Their tweeting schedules are also similar: from 9 to 5 during weekdays. Other groups shared surnames, such as Santos or Rivera.

In May 2019, Facebook announced that it had removed Facebook pages that were being used to "mislead others about who they are or what they are doing" and were managed by the firm Archimedes Group, a private Israeli firm (@DFRLab, 2019). The operations were being deployed in the content of the protests over health and education reforms. They were mostly used to spread content aimed at polarizing and driving division in Honduras, and targeted ads with pro-government and anti-opposition content. Some content, for instance, targeted former President and leader of the opposition, Zelaya, labelling him a drug consumer, or attacked deputy Olivia Zúniga Cáceres with misogynist messages (Garay, 2019). In July 2019, there was a new takedown announcement by Facebook. The company indicated that part of the activities was linked to social media managers of the government (Facebook, 2019).

In early 2020, Twitter deleted 3,104 fake accounts attributed to the social media manager of Juan Orlando Hernández because they were undermining the public conversation. According to the company, their creation was traced to a single IP range in Honduras. A report by the Stanford Internet Observatory (Cryst & García Camargo, 2020) lists accounts of public institutions, such as that of the National Television Station, and television and media personalities, among the ones taken down. They were mostly pro-government messages, and the most recent accounts had an automated appearance both in the way they were created and in the content posted. Moreover, it is worth noting that the peaks of their date of creation were related to controversial events, such as the sanctioning of "the president's re-election bid", the results of the 2017 elections, and the drug trafficking trial of Tony Hernández, brother of the President (Cryst & García Camargo, 2020). Nevertheless, some accounts of intellectuals, artists, and left-wing activists critical to the government were also taken down. As suggest by the report of the Stanford Internet Observatory, this cluster might have coordinated activities, although more evidence is needed (Cryst & García Camargo, 2020).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Honduras

Account Types	Messaging and Valence	Communication Strategies	Platforms
Automated, Human Fake	Pro-government, Attacks on opposition	Creation of disinformation, data-drive strategies, Amplification strategies	Twitter, Facebook

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

The report by the Stanford Internet Observatory that analysis accounts taken down by Twitter in 2020 identified that some of them belonged to content creators, social media influencers and journalists. The study indicated that Q'Hubo (@qhubochano) and other television networks, for instance, post pro-government content "in exchange for tax write-offs" (Cryst & García Camargo, 2020).

As regards operations managed by Archimedes Group, Facebook identified that the company spent $812,000 to promote content in targeted countries between 2012 and 2019, however, it remains unknown how much of the that budget corresponds to the operation in Honduras nor who was the client that paid for it (@DFRLab, 2019). As regards the accounts taken down in July, Facebook informed that in total they spent $23,000 on ads paid in US dollars and local currency (Facebook, 2019).

Table 3: Cyber Troop Capacity in Honduras

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
		Temporary	Centralised	Low

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

References

2019 World Press Freedom Index | Reporters Without Borders. (2019). Reporters Without Borders. https://rsf.org/en/ranking

Cryst, E., & García Camargo, I. (2020). *#VivaJOH o #FueraJOH. An analysis of Twitter's takedown of Honduran accounts.* Standford Internet Observatory. https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/04022020-hondurastakedown.pdf

@DFRLab. (2019, July 2). *Archimedes Ran Politically Charged Facebook Ads in Crisis-Torn Honduras*. Medium. https://medium.com/dfrlab/archimedes-ran-politically-charged-facebook-ads-in-crisis-torn-honduras-1137f355e159

Facebook. (2019, July 25). *Removing Coordinated Inauthentic Behavior in Thailand, Russia, Ukraine and Honduras*. https://about.fb.com/news/2019/07/removing-cib-thailand-russia-ukraine-honduras/

Gallagher, E., Suárez-Serrato, P., & Velazquez Richards, E. I. (2019). Socialbots Whitewashing Contested Elections; A Case Study from Honduras. *Third International Congress on Information and Communication Technology*, 547-552. https://doi.org/10.1007/978-981-13-1165-9_50

Gallagher, Erin. (2018, January 25). Honduras: Network visualizations of JOHbots. *Medium*. https://medium.com/@erin_gallagher/honduras-network-visualizations-of-johbots-909bdda5adc0

Garay, C. (2019, August 6). La manipulación de un presidente impopular en redes sociales. *Contra Corriente*. https://contracorriente.red/2019/08/06/la-manipulacion-de-un-presidente-impopular-en-redes-sociales/

Human Rights Watch. (2019). *World Report 2020: Rights Trends in Honduras*. Human Rights Watch. https://www.hrw.org/world-report/2020/country-chapters/honduras

Pérez de Acha, G. (2016). *Hacking Team Malware para la Vigilancia en América Latina*. Derechos Digitales. https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf

HUNGARY

Introduction

According to Freedom House, Hungary, with a government currently led by Prime Minister Viktor Orbán, is the only partly free democracy in the European Union. Orbán's government rules with a supermajority/constitutional majority through the Fidesz–KDNP coalition, a government that has been criticized for dismantling Hungary's democratic institutions as well as its independent media (Freedom House, 2020). Orbán's government has also been accused of playing a role in the spreading of fake news via social media platforms as well as more traditional channels.

An Overview of Cyber Troop Activity in Hungary

Organizational Form

During the Victor Orbán-led government in Hungary there has been a decline in the number of independent media outlets. 2016 saw the closure of *Népszabadság*, the largest, independent daily newspaper (Freedom House, 2020), and many national, regional and local media have either closed or come to be controlled by oligarchs with ties to Orbán. The most striking development has been the consolidation of 476 media outlets within the Central European Press and Media Foundation (in Hungarian, KESMA), whose chairman was previously a Fidesz party legislator (Besser, 2019). With its control of various newspapers, radio stations, and websites, critics have dubbed KESMA a pro-government media conglomerate.

When the Hungarian government created KESMA, it announced that it was in the national strategic interest that Hungarian newspapers be owned by Hungarian nationals, and that as such they amount to "critical infrastructure" (Aries, 2019). With this decision, the Hungary Competition Authority closed its investigation on the merger. However, according to a 2020 Hungarian court ruling this was deemed unlawful. In a study undertaken by Budapest-based Mertek Media Monitor, the total pro-Fidesz media portfolio, made up of public service media, KESMA-owned media and pro-government media not under the remit of KESMA, encompasses 77.8% of the entire news and public affairs segments in the Hungarian media (Mertek, 2019a). Mertek economist Agnes Urban noted that these outlets are not simply in tune with promoting Hungarian government rhetoric but are also dependent on the funding that it provides (Aries, 2019). According to a report undertaken by the investigative website Atlatszo, government funds amounting to over USD $250 million over the course of the past eight years have been spent on advertising campaigns to promote the government's policies (Attila, 2019). Mertek's report noted that more than half of the advertising revenues of KESMA-owned media outlets came from the Hungarian government (Mertek 2019a). As such, these funds are arguably a form of state subsidy that is illegal under EU law (Mertek 2019b). Critics have also characterized KESMA as a "media empire" that allows for the spread of "fake news and misinformation" through "state-sponsored media itself" (Besser, 2019).

In a report undertaken by GLOBESEC on information operations and disinformation campaigns during the European elections in Central Europe, the main public broadcast news channel hirado.hu, and the leading commercial online news site origo.hu, were both listed in the top 15 pro-Kremlin disinformation channels in Hungary on Facebook. Both these news outlets are under the umbrella of KESMA, and both have been criticized for promoting conspiracist theories, including the likes of those attacking George Soros and those of the EU's support for illegal immigration, and promoting pro-Russian disinformation media in the hope that it will become a key part of media consumption in Hungary (Sawiris et al., 2019).

According to a study by the European Values think-tank, a "large portion of mainstream media in Hungary are under the control of the government, some of them using Russian quasi media like Sputnik or RT as their sources. In certain instances, known Russian disinformation centers are welcomed" (Freedom on the Net, 2019). These disinformation outlets significantly contribute to the political campaign, and as such, the Orbán government has made no attempts to counter disinformation coming from Russia (Sawiris et al., 2019).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Hungary

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
	x	Fidesz-KDNP	KESMA		x

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Misinformation and conspiracy theories:

According to the Center for Media, Data and Society, the part-public-part-private pro-government media conglomerate has created a narrative that helps the government promote the populist agenda of Prime Minister Orbán and his party Fidesz. Most of what these news outlets promote is considered pro-government propaganda, and the most essential element of this propaganda is the dissemination of false and misleading information online (Gajdos, 2019).

Misinformation and pro-government messages were particularly dominant during the run-up to the May 2019 European Parliament Election. The Hungarian government was criticized for spreading campaign posters on Facebook that depicted the former president of the European Commission, Jean-Claude Junker, with George Soros under the caption "you too have a right to know what Brussels is preparing!" (BBC, 2019), and which was also intended to undermine the European Commission's scheme to redistribute asylum seekers. A spokesperson for Orbán, Zoltan Kovacs, defended the poster by stating that "Brussels continues to want to support illegal immigration, which is something the Hungarian people must know about" (Ibid). The European Commission rejected this statement as "fake news" and "ludicrous conspiracy theories" (Ibid).

The government has also been criticized for posting misinformation on its official Facebook page. For instance, in 2018, the government posted a video in English attacking Guy Verhofstadt, the Chief Brexit Negotiator for the European Union. However, the statements and images of Verhofstadt were found to have been taken out of context, and were found to be dated to 2014 (Graham-Harrison & Walker, 2019). Despite official complaints Facebook did not remove the video. As *The Guardian* suggests, the choice of English language (with an American accent) indicates that the video's target audience was probably not Hungarian (Ibid).

One of the main narratives that has been promoted by these media outlets and the government has focused on promoting the notion that globalists, liberal elites, and refugees conspire to be enemies of the Hungarian people and state, with a particular emphasis on George Soros as a key actor in the conspiracy, a Jewish Hungarian–American billionaire. For instance, the Hungarian government rejected the 2019 Freedom House report by claiming that it was part of the "empire" of George Soros (Simon, 2019). In 2018, the Hungarian government introduced "Stop Soros" laws, criminalizing the provision of assistance to asylum seekers by Hungarian nationals (Reuters in Budapest, 2018). Furthermore, during his campaign for the 2019

European elections, Orbán criticized "the interference of that global, liberal mafia … players outside Hungary, manipulating huge funds, seeking to wage a campaign and interfere with the Hungarian elections" and argued that "Europe's borders must be protected against the invasion of migrants" (MTI-Hungary Today, 2019).

According to the Political Capital Institute, During the 2019 municipal elections KESMA launched a disinformation campaign against the opposition. The leading mainstream online pro-government news outlet, Origo.hu, stated that the mayoral candidate of Hodmezovasarhely, Peter Marki-Zay, would flood Hungary with immigrants by building a system modelled upon Canada's immigration system. Marki-Zay had in fact only argued that Hungary needed to establish a more tolerant society akin to Canada (Political Capital, 2019). Moreover, pro-government online portal PestiSracok alleged that Peter Niedermuller, the opposition's mayoral candidate in the capital's 7th district, was mobilizing 90,000 foreign-born/non-citizen voters living in Budapest to decide the outcome of the mayoral races. This conspiracy theory was subsequently used by the Fidesz campaign chief and MP, Lajos Kosa (Ibid). In another case, pro-government news outlet Magyar Nemzet spread the conspiracy theory that Gergely Karacsony, the opposition's candidate for lord mayor, was planning a deal with the president of the European commission that would settle Muslim migrants in Budapest and other cities as a precondition for receiving EU funds (Zgut, 2019). According to Political Capital "the most successful type of media related to the above-mentioned conspiracy theories were memes about immigration that were centrally disseminated by the official Facebook account of Fidesz and dutifully shared by dozens of local party affiliates' accounts across the country" (Political Capital, 2019).

Beyond controlling narratives in municipal elections, the highly centralized nature of the Hungarian media space has enhanced the dissemination of pro-Russian messages in mainstream pro-government outlets. These include major conspiracy theories such as the portrayal of the Ukrainian Maidan revolution as the "CIA executed plan of George Soros" to install a "puppet government", with predictions of similar "Maidan-like" attempts to destabilize Hungary and overthrow its government. By expressing a pro-Kremlin geopolitical orientation, these Hungarian news sites echo the Fidesz party's pro-Russian and Eurosceptic turn as well as Orbán's praise for the Kremlin for withstanding the "Western attempts of isolation and regime change" (Gyori and Syrovatka, 2019).

Conspiracy theories have a huge impact on public opinion. As a poll by Political Capital found, anti-Soros, anti-Muslim conspiracy theories are extremely widespread in amongst Hungarians, and especially in the supporters of the governing party (Political Capital, 2018).
Trolls and the manipulation of media:

Facebook in particular has been a popular platform for manipulation by the government and pro-government outlets. An investigation by the political weekly HVG found that governmental parties were the most successful at manipulating the electorate via Facebook during the last parliamentary election campaign (and that this was partially because they had the greatest resources to draw upon). One important tool was masked political messages: the promotion through advertising revenue of KESMA-produced media content that didactically pushed the government's eurosceptic and anti-immigration rhetoric (Marton, 2019). According to an investigation by the online political news site 444.hu, the government also employed a network of trolls to share and engage with pro-Fidesz content (444.hu, 2018). These unpaid users were reportedly given directives to post particular content within a specified timeline.

Moreover, detailed instructions were given on how to create images and memes (Freedom on the Net, 2019).

According to the Director of the Political Capital Institute, Peter Kreko, these trolls were used both in domestic politics and abroad. For example, profiles that flooded the platform during protests against development plans in the city of Keszthely and which labelled the protesters as "brain dead" were in fact fake profiles created mere months before. According to Kreko, the comments were intended to undermine the credibility of the protesters in order to keep citizens from participating in debates. These fake comments were then quoted by the government-controlled media outlet PestiSracok to justify the claim that citizens in the city supported the Fidesz-backed mayor's plans (Kreko et al., 2019). In another example, comments flooded the Facebook profile of former MEP Judith Sargentini after a debate in the European Parliament condemning the Hungarian government's rule of law record. These comments came from mostly fake profiles and were heavily repetitious, and were again quoted in order to provide proof that Hungarians support their government, this time in the pro-government outlet Origo (Ibid).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Hungary

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Real, Fake	Pro-government messages, attacks against opposition, smear campaigns, supressing participation, manipulating online conversations, promoting specific narratives	Trolls, disinformation, conspiracy theories, paid promotion of political messages in the government-friendly media	Facebook, government owned, and partially government owned news websites

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

During the European elections in 2019, Facebook came under fire for failing to partner with Hungarian domestic fact-checking organizations (Graham-Harrison & Walker, 2019). Facebook responded that it had not identified credible partners, which many journalists concerned with the spread of government-backed misinformation on the platform during the elections deemed to be an unsatisfactory response. However, Facebook was also in turn criticized by pro-government think tanks and media outlets for politicization. The newspaper *Magyar Nemzet* criticized Facebook for becoming a political actor. Moreover, the think tank Századvég published a report in April 2019 criticizing Facebook's "principles of political correctness" which had made Hungarian politicians and public figures "victims of censorship". According to a poll by the think tank, 79% of Hungarians found it unacceptable that social media platforms, such as Facebook, can "delete content based on its own political views", voicing anger at the suspension or banning of content and users for sharing anti-immigrant content (Ibid). This government-organized think-tank calls for regulation that would allow national authorities, in line with Hungarian legal framework, to make the final say on what can be removed from FB.

Google has also come under criticism for initially granting the New Wave Media group a financial award under its Digital News Innovation Fund, which is designed to "help journalism thrive in the digital age" (Bayer, 2019). However, the New Wave Media group has been criticized by journalists and researchers for publishing fake news. According to critics, Origo is a vehicle for government propaganda and a major recipient of government advertising. Gábor Polyák, head of Hungarian watchdog Mérték Media Monitor, described Origo as "an emblematic player of the Fidesz propaganda media", which spreads "thousands of pieces of news about migrants in an extremely negative context [that is] accompanied by false videos and photos". According to Politico, Origo has repeatedly been found guilty by judges of incorrectly portraying facts about government critics. In response, Google subsequently withdrew the grant given to the New Wave Media group (Ibid).

In the midst of the COVID-19 Pandemic, Hungary's parliament has passed a new set of measures in the battle against the spread of misinformation regarding the coronavirus that include jail time of up to five years. Since the introduction of the new measures, several people have been arrested for spreading false information or for "obstructing" the prevention of coronavirus (Kaszas 2020). Most of the people detained have been relesed and many of the cases dropped (Mertek 2020). However, the measures were also significant in that they gave new powers to the prime minister, Viktor Orbán, to rule by decree under a state of emergency, with no clear limits (Walker & Rankin, 2020). At the same time, the Hungarian government was also involved in spreading obviously misleading information about the causes of the virus, claiming that illegal migration is the main driver (Kreko & Szicherle, 2020).

References

Aries, Q. 2019. Europe's Failure to Protect Liberty in Hungary. *The Atlantic*.https://www.theatlantic.com/international/archive/2019/12/eu-hungary-press-freedom/603985/.

Attila, B. 2019. The government of Hungary spent €216 million on propaganda and fearmongering in the past 8 years. *Atlatszo*. https://english.atlatszo.hu/2019/01/11/the-government-of-hungary-spent-e216-million-on-propaganda-and-fearmongering-in-the-past-8-years/.

Bayer, L. 2019. Google pulls grant to Hungarian publisher over fake news allegations. *Politico.* https://www.politico.eu/article/google-withdraws-grant-to-hungary- news-site-over- fake-news-anti-semitism/.

BBC News. 2019. EU blasts Hungary 'fake news' on migrants. *BBC.* https://www.bbc.com/news/world-europe-47294183.

Besser, L. 2019. Hungary's Viktor Orbán has attempted to dissolve Europe's values — but Brussels is fighting back. *ABC News.* https://www.abc.net.au/news/2019-05- 27/inside-the-illiberal-hungary-of-viktor-Orbán/11151500.

Freedom on the Net. 2019. Hungary. *Freedom House*. https://freedomhouse.org/country/hungary/freedom-net/2019#footnote17_inypy4h.

Freedom House. 2020. Hungary. *Freedom House.* https://freedomhouse.org/country/hungary/freedom-world/2020

Gajdos, R. 2019. We need a Fact-Checking Website in Hungary and Here's Why. *Center for Media, Data and Society*. https://cmds.ceu.edu/we-need-fact-checking-website- hungary-and-heres-why

Graham-Harrison, E., & Walker, S. 2019. Hungary: the crucible for faulty efforts by Facebook to banish fake news. *The Guardian.* https://www.theguardian.com/world/2019/may/18/hungary-crucible-facebook- attempt-banish-fake-news.

Gyori, L., & Syrovatka, J. 2019. Russian propaganda in the Czech Republic, Slovakia and Hungary. *Security and Human Rights Monitor.* https://www.shrmonitor.org/russian-propaganda- in-the-czech-republic- slovakia-and-hungary/

Kaszas, F. 2020. Police Investigating Facebook Users for 'Spreading Fake News' Causes Uproar in Hungary". *Hungary Today*. https://hungarytoday.hu/coronavirus-fake- news-hungary-police/.

Kreko, P., Racz, A., & Szicherle, P. 2019. Political Trolling in Hungary. *Disinfo Portal*. https://disinfoportal.org/political-trolling-in-hungary/

Kreko, P., & Szicherler, P. 2020. Gone Viral. *Eurozine*. https://www.eurozine.com/gone-viral/

Marton, G. 2019. A Fidesz gyilkos kampánygépet csinált a Facebookból, és most retteg, hogy elveszíti. *hvg*. https://hvg.hu/itthon/20190416_EP_valasztasok_Fidesz_Orbán_Viktor_Facebook_KESMA_Szazadveg_manipulacio.

Mérték Médiaelemző Műhely. 2019a. Fidesz-friendly media dominate everywhere. *Atlatszo*. https://mertek.atlatszo.hu/fidesz-friendly-media-dominate-everywhere/.

Mérték Médiaelemző Műhely. 2019b. State advertising spending in Hungary – an unlawful form of state aid. *Mérték Médiaelemző Műhely*. https://mertek.eu/en/2019/01/29/state-advertising-spending-in-hungary-an-unlawful-form-of-state-aid/.

Mérték Médiaelemző Műhely. 2020. Police Action Against Alleged Fake News in Hungary. *Mérték Médiaelemző Műhely*. https://mertek.eu/en/2020/05/13/police-action-against-alleged-fake-news/

MTI-Hungary Today. 2019. EP Election – Orbán Encourages 'Anti-Migration' Voters to Participate. *Hungary Today*. https://hungarytoday.hu/ep-election-Orbán-encourages-anti-migration-voters-to-participate/.

Political Capital 2018. Összeesküvés-elméletek, álhírek, babonák a magyar közvéleményben. *Political Capital*.https://www.politicalcapital.hu/rendezvenyek.php?article_read=1&article_id=2323.

Political Capital. 2019. The Hungarian government's disinformation campaign during the 2019 municipal elections. *Political Capital Policy Research & Consulting Institute*. https://www.politicalcapital.hu/library.php?article_read=1&article_id=2467

Reuters in Budapest. 2018. Hungary passes anti-immigration 'Stop Soros' laws. *The Guardian*. https://www.theguardian.com/world/2018/jun/20/hungary-passes-anti-immigrant-stop-soros-laws.

Reuters World News. 2019. EU's Juncker takes aim at Hungary's Orbán over fake news. *Reuters*. https://www.reuters.com/article/us-eu-cyber-disinformation/eus-juncker- takes-aim-at-hungarys-Orbán-over-fake-news-idUSKBN1OD1U8.

Sawiris, M., Duskova, L., Syrovatka, J., & Gyori, L. 2019. European Elections in Central Europe: Information Operations and Disinformation Campaigns. GLOBSEC. https://www.globsec.org/wp-content/uploads/2019/05/EP-Elections_Information-Operations-Disinformation-Campaigns-1.pdf

Simon, Z. 2019. Hungary Becomes First "Partly Free" EU Nation in Democracy Gauge. *Bloomberg*. https://www.bloomberg.com/news/articles/2019-02-05/hungary-becomes-first-partly- free-eu-nation-in-democracy-gauge.

Walker, S. & Rankin, J. 2020. Hungary passes law that will let Orbán rule by decree. *The Guardian*. https://www.theguardian.com/world/2020/mar/30/hungary-jail-for- coronavirus-misinformation-viktor-Orbán.

Zgut, E. 2019. Shifted into Higher Gear. *Visegrad Insight*. https://visegradinsight.eu/shifted-into- higher-gear/.

444.hu. 2018. A Fidesz egyik Facebook-katonája elmesélte, milyen virtuális hadsereget hozott létre a part. *444.hu*. https://444.hu/2018/01/30/a-fidesz-egyik-facebook-katonaja-elmeselte- milyen-virtualis-hadsereget-hozott-letre-a-part.

INDIA

Introduction

Fact-checking organisations reported that in India, every major event in 2019 —from the general election, to the Pulwama terrorist attack, to the protests about the Citizenship Amendment Act—has been the subject of extensive mis- and disinformation across social media platforms. Jency Jacob, managing director of fact-checking site BOOM, said that 2019 had been "the busiest year for us so far" (Chaturvedi, 2019). Internet freedom has decreased for the fourth year in a row, and Freedom House (2019) noted that "manipulated content, disinformation, and misinformation plague the online environment in India".

On 14 February 2019, a terrorist attack by Pakistan-based terrorist organization Jaish-e-Muhammad in Pulwama district of Kashmir, killing forty Indian soldiers and triggering a wave of online disinformation. Within 24 hours of the attack, a doctored image of opposition Indian National Congress (INC) party leader Rahul Gandhi standing next to the suicide bomber was debunked by BOOM (Funke & Benkelman, 2019). The Hindi text accompanying the photo questioned whether the INC party was involved—a deliberate attempt at using the attack to incite political tensions (AFP India, 2019a). Despite vigorous efforts to counter the spread of false and misleading content, disinformation filtered through to credible news outlets, with mainstream channels in India and Pakistan publishing news stories that amplified rumours and misinformation about the attack (AFP India, 2019b).

The seventeenth Lok Sabha, the 2019 Indian general election, took place from April 11 to May 19, 2019. This was described as the largest exercise of democracy in history—due to the 900 million eligible voters, including 340 million Facebook users and 230 million WhatsApp users. Prime minister Narendra Modi's Hindu nationalist Bharatiya Janata Party (BJP) remained in power following a landslide victory. The low barriers to entry, availability of resources, and low levels of regulation on networks such as Facebook, Twitter and WhatsApp provided ample opportunities for propaganda. An enormous population constituted of a variety of castes, religions, and languages, with varying levels of digital literacy, provided a fertile ground for disinformation. This, combined with the fact that political parties deliberately exploited these vulnerabilities as part of their campaign strategies, meant that computational propaganda played a key role in all aspects of Indian politics.

Cyber troop capacity grew significantly in the lead-up to the 2019 general election. While there were only a few actors involved in social media manipulation in 2017, political parties are now working with a wide range of actors including private firms, volunteer networks, and social media influencers to shape public opinion over social media. At the same time, more sophisticated and innovative tools are being used to target, tailor, and refine messaging strategies including data analytics, targeted advertisements, and automation. The increasing amount of money being spent on growing team sizes, advertising campaigns, and hiring private firms combined with the application of a variety of more sophisticated computational techniques underscores the growing capacity of cyber troops operating in India.

An Overview of Cyber Troop Activity in India

Organizational Form

India has a long history of political parties using social media for political campaigning. The two main political parties, incumbent Prime Minister Narendra Modi's Bharatiya Janata Party (BJP), and opposition Indian National Congress (INC) party, both have 'IT cells' that are known to use automation, trolling and disinformation techniques. These IT cells have existed since the early days of social media—the BJP's IT cell was founded in 2007 (Dasgupta, 2018). Political parties in India have also been known to work with private firms. Cambridge Analytica "worked extensively in India" according to whistle-blower Christopher Wylie (Crabtree, 2018). The Indian IT firm Silver Touch was responsible for building Modi's NaMo app, and was linked to fake Facebook accounts (Gleicher, 2019). Influencers on social media platforms are increasingly used to amplify political messages organically to a wider audience. For example, Delhi marketing firm OMLogic Consulting has worked for both the BJP and INC to utilize the power of YouTube and Instagram influencers (Chaturvedi, 2019).

Cyber troop activity in India is predominantly of domestic origin. The deliberate spread of disinformation by politicians and political parties has often led to misinformation due to hyper-connectivity and digital illiteracy. However, there have also been foreign interference attempts attributed to Pakistan through a network of fake accounts and Facebook pages about issues to do with India's general election (Kalra & Sayeed, 2019). Following the Kashmir attack, individuals linked to the Pakistan Army used Facebook and Instagram accounts to inflame tensions with India and push claims over Kashmir (@DFRLab, 2019). In response, the defence ministry reportedly approved a new Information Warfare branch in the army, to combat misinformation, propaganda, and psychological operations (Gurung, 2019). This announcement came in March 2019, directly following the wave of propaganda following the Balakot air strikes by the Indian Air Force in February 2019.

As well as the BJP campaigning in India, the 'Overseas Friends of the BJP (UK)' (OFBJP) said it was campaigning for the Conservative Party in the UK's 2019 general election. They targeted Conservative candidates in forty-eight marginal seats, and it was reported that messages were circulating on WhatsApp groups among British Hindus urging them to vote against the Labour Party (Siddique, 2019).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in India

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
2007	Indian Army's Information Warfare branch	BJP, INC	Cambridge Analytica, Silver Touch, OMLogic Consulting, The Ideaz Factory, Infocrunch Analytics		Evidence Found

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Disinformation

Disinformation is prolific in India partly because originates from mainstream media, politicians, and as part of official election strategies. Economic Times and India Today, the latter of which even has its own fact-checking project, published—both in print and in a video—a photo that allegedly showed the February terrorist attacker in a combat uniform; however, in reality it originated from an unknown source on Twitter and was determined as fake (Funke & Benkelman, 2019). BOOM claim that political parties have "begun building teams for the specific purpose of pushing out a huge volume of propaganda and disinformation" (McLaughlin, 2018). Both the BJP and INC accuse each other of propagating "fake news" while denying they do so themselves (Kalra, 2018). And Amit Malviya, head of the BJP's IT cell, publicly acknowledged that there was "some scope for misinformation" during the 2019 election (Dasgupta, 2018).

International disinformation campaigns with links to India have also been reported. An influence network linked to Indian actors was identified by the EU Disinfo Lab, comprising over 265 fake local news sites in more than sixty-five countries. For example, the website EP Today (a self-proclaimed magazine for the European Parliament in Brussels) is managed by Indian stakeholders with ties to a large network of think tanks, NGOs, and companies from the Srivastava Group. The network was found to cover Indian-related demonstrations and events, as well as anti-Pakistan content (EUDisinfoLab, 2019).

Automation

Automation is used by political actors in India to create inorganic popularity around an individual, organization, or message. During the 2014 general election, the BJP were accused of paying to boost their popularity artificially on social media. On Twitter, Prime Minister Narendra Modi is second only to United States President Donald Trump as the most followed politician, with 45.9 million followers; however, a study by Twiplomacy claimed that as many as 60% of these come from fake accounts (Twitter Audit, 2018). There is evidence of active networks of Twitter bots being deployed during the election to boost Modi's popularity. In February 2019, the hashtag #TNwelcomesModi received 777,000 mentions over two days, referencing Modi's visit to Tamil Nadu, a southern Indian state. In response, #GoBackModi was mentioned 447,000 times by INC-supporting accounts (@DFRLab, 2019). Despite the high levels of automation on Twitter, this activity did not reach very many people, as the unsophisticated fake accounts had few followers. Following the Indian government's digital blackout in Jammu and Kashmir, social media accounts have been amplifying political hashtags such as #KashmirWelcomesChange and #KashmirWithModi. The hashtags were shared by media outlets (e.g. @TimesNow, 9.2 million followers), but also by "a range of anonymous accounts that exhibited suspicious and bot-like tendencies" (@DFRLab, 2020).

Trolling

Trolling tactics have been used to suppress political speech and dissenting opinions. In the book *I am a Troll*, Indian journalist Swati Chaturvedi details the creation of the BJP's IT cell, also known as the 'BJP troll army,' which was formed in 2007 by Prodyut Bora to smear and threaten opponents online (Dasgupta, 2018). Today, around three hundred workers use "strategies meant to inflame sectarian differences, malign the Muslim minority, and portray Modi as saviour of the Hindus" (Riley, Michael et al., 2018). These attacks vary in their sophistication: from crudely automated criticism, such as #GoBackModi, to highly personalized attacks on individuals.

Trolls target political opponents and journalists—especially prominent female figures—with sexual harassment and abuse. Sometimes individuals are threatened with real-life physical attacks by online trolls (Gopalakrishnan, 2018). For example, the Office of the United Nations Commissioner for Human Rights called for the government to protect journalist Rana Ayyub, after her face was superimposed on pornographic clips and she received rape and murder threats following false quotes attributed to her on social media (Shaheen, 2018). Kavita Krishnan, a politician and activist, said she received nonstop harassment on Twitter from an “organized army of far-right trolls” which belongs to the BJP (Mackintosh & Gupta, 2020). Amnesty International (2020) conducted research into online harassment and found that one in every seven tweets mentioning women politicians in India was ‘problematic’ or ‘abusive,’ and that one in every five problematic tweets was sexist or misogynistic. While both parties deny supporting online trolls, these accounts are often aligned with party agendas and the leaders provide tacit support. For example, Prime Minister Modi follows known troll accounts on Twitter, and drew criticism for hosting one hundred and fifty social media influencers at his residence in 2015, many of whom used sexual slurs to harass women online (Safi, 2018).

Manipulated Content

Doctored photos and videos circulate widely on social media, as both a means of political persuasion and to attack opponents. This is particularly concerning as senior politicians often share these images from personal accounts. For example, an edited video purported to show INC leader for East Uttar Pradesh Priyanka Gandhi teaching children abusive political slogans was shared by Smriti Irani, a serving cabinet minister for the BJP. However, the full unedited video reveals that Gandhi can be seen telling the children to stop using abusive language (@DFRLab, 2019). Similarly, Divya Spandana, director of social media and communications for the INC, shared a doctored photo of Prime Minister Modi that drew a comparison with Adolf Hitler (Sidharth, 2019).

A significant technological development has been the first use of a deepfake video as part of an Indian election campaign. Ahead of the legislative assembly elections in Delhi, on 7 February 2020, two deepfake videos of BJP President Manoj Tiwari criticising the Delhi government were circulated on WhatsApp (Christopher, 2020). This was organised by the Delhi BJP IT Cell and political communications firm The Ideaz Factory. It utilised deepfake technology to create a video in which the politician speaks a local Hindi dialect—Haryanvi. Concerns about the manipulative potential for deepfakes have grown, but this particular application of deepfakes is part of a campaign to reach different linguistic voter bases. Neelkant Bakshi, of the BJP Delhi IT cell, said the deepfakes were distributed to 5,800 WhatsApp groups in Delhi, reaching fifteen million people (Christopher, 2020). Deepfakes have previously been used for manipulated pornographic content. India’s youngest parliamentarian, Chandrani Murmu, was subject to her face being superimposed onto an obscene video ahead of her election in 2019 (Mackintosh & Gupta, 2020).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in India

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Human, Fake, Automated	Pro-Party Messages, Attacks on Opposition, Polarization Strategies, Trolling and Harassment	Facebook pages & ads, disinformation & misinformation websites, memes, doctored videos, WhatsApp groups, deepfakes, amplification	Facebook, Instagram, Twitter, WhatsApp, NaMo

Source: Authors’ evaluations based on data collected. Blank spaces indicate no evidence was found.

Social Media Platforms

Chat applications are an important platform for spreading disinformation about Indian politics. At least fifty thousand election-related WhatsApp groups were created by both the BJP and INC during the May 2018 Karnataka state elections (Freedom House, 2018). The social media chief of the BJP declared 2018 the year of India's first 'WhatsApp elections', and has reportedly "drawn up plans to have three WhatsApp groups for each of India's 927,522 polling booths" (Perrigo, 2019). A so-called 'cell phone pramukh' will operate a number of these groups and drive the party's WhatsApp-based campaign by circulating specially designed campaign material (Uttam, 2018). Parties are even using data analytics to form WhatsApp groups based on demographic and socio-economic factors, using information from the electoral roll to sort the population into groups based on factors such as caste and affluence, to achieve micro-targeted messages (Singh, 2019).

Following the 2019 election, researchers at the Tow Center for Digital Journalism analysed 1.09 million campaign-related WhatsApp messages and found that 52% of content was either images, videos, or links. They also discovered that 35% of the media items in the dataset had been forwarded messages (Bengani, 2019). Ahead of the 8 February 2020 elections in Delhi, it was reported that dozens of WhatsApp groups were being created, containing up to two hundred and fifty members and spreading messages that condemned mainstream media and promised to provide 'real' news (Sircar, 2020).

WhatsApp is increasingly scrutinized by the Indian government. Mob lynchings caused thirty deaths throughout India in 2018, which reportedly resulted directly from misinformation spread over the app – leading them to be known as 'WhatsApp killings' (Safi, 2019). In one video that went viral in June 2018, footage of a child abduction was accompanied by text about 'kidnappers' arriving in the city to abduct children; however, it was actually a child abduction awareness video created in Pakistan. In line with their trolling tactics, political differences are exacerbated by inciting Hindu–Muslim tensions on WhatsApp. For example, right-wing Hindu groups circulated a video on WhatsApp depicting a Muslim mob attacking a Hindu woman, but it was footage of a lynching in Guatemala. Automation has also been attempted—during the state elections in 2018, the platform's systems detected an attempt by someone in Karnataka to create dozens of WhatsApp groups in quick succession (Goel, 2018).

In April 2019, Facebook took down 687 pages and accounts linked to the IT cell of the INC which posted about political issues, the upcoming elections, and criticism of the BJP. Facebook also suspended fifteen pro-BJP pages, groups, and accounts, and one pro-BJP Instagram account linked to Silver Touch. These accounts were removed because they engaged in "coordinated inauthentic behaviour" (Gleicher, 2019).

Alongside evidence of computational propaganda on Twitter, Facebook and WhatsApp, Modi has his own app, NaMo, which launched in June 2015 and has over 10 million downloads. NaMo is a platform used by Modi to communicate with his followers. However, he has received a significant amount of criticism for bypassing traditional media channels and evading media scrutiny through its use (S. Bansal, 2019). And despite the Indian government putting pressure on social media platforms to control disinformation, there is a lack of content moderation on the NaMo app making it susceptible to propaganda. One of the most prolific accounts on this app, The India Eye, was responsible for 40% of the 744 posts on NaMo's default feed. Alt News, a fact-checking organization in India, uncovered extensive misinformation peddled by The India Eye on their Facebook page: at least six of the twenty most shared posts between September and November 2018 were inaccurate or misleading, exposing its two million followers to misinformation (S. P. and S. Bansal, 2019). Alt News discovered The India Eye had links with Silver Touch, the private firm linked to fake accounts on Facebook and Instagram. It is also claimed that Silver Touch created the NaMo app itself (Patel & Chaudhuri, 2019).The India Eye's Facebook page was taken down by Facebook and is part of a wider propaganda network linked to Silver Touch (Gleicher, 2019).

Organizational Capacity and Resources

Networks of paid workers and volunteers disseminate disinformation across social media, responding in real time to political developments. The organization of propaganda efforts appears to be both centrally coordinated and volunteer-run. India's vast size and regional politics means that propaganda efforts are geographically coordinated. There is evidence of specific regional cells, such as the Gujarat Congress IT cell's 'Cyber Army' (@DFRLab, 2019), the BJP Delhi IT cell, and the BJP's fifty-member team in an office in Bangalore (Niranjankumar, 2018). A former troll said that he was given a half-dozen Facebook accounts and eight cell phones as part of a three hundred-person team in a BJP IT cell (Riley et al., 2018).

Alongside paid workers, individuals can volunteer to assist in 'WhatsApp Group Management', being 'active on Facebook & Twitter' or 'Content Creation' among others, according to a volunteer sign-up form (Niranjankumar, 2018). There is a blurring of attribution between paid IT cell workers and volunteer movements. The former head of the BJP IT cell, Arvind Gupta, said in 2016 that neither the party nor IT cell had ever encouraged trolling and that online support came from a grass-roots movement (Riley et al., 2018). Relying on volunteers and paid workers allows the blurring of boundaries between campaigning, trolling and propaganda.

Political parties used Facebook to target political advertisements at voters. Following the takedown of fake accounts in April 2019, according to Facebook the INC-linked accounts spent US$39,000, and the BJP-linked accounts spent US$70,000 from 2014 to 2019 in political advertisements (Gleicher, 2019). However, since 21 February 2019, when Facebook began to track political advertising, the total spending for political advertisements in India totalled 103 million rupees, approximately US$1.5 million (Goel & Frenkel, 2019). There is a lack of transparency on who is amplifying political advertisements; while the top three advertisers in India were all aligned with the BJP's election agenda, none explicitly disclose their affiliation.

Table 3: Cyber Troop Capacity in India

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
Multiple teams ranging in size from 50-300 people	$1.5 million on political advertisements. Contracts with several firms for unknown amounts.	Permanent, Increases around political events (e.g. elections)	Medium levels of coordination between cyber troops. Geographically organized.	Medium-High

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Government and Private Responses

There have been several public and private initiatives designed to curb the spread of low-quality information online. Fact-checking has been an important response and several media organizations, such as BOOM (Boom Live) and Alt News, have been established to verify photos and rumours spread on social media. A number of social media platforms and the Internet and Mobile Association of India (IAMAI) released a Voluntary Code of Ethics in March 2019, outlining how the Election Commission of India can notify platforms to remove content (Freedom House, 2019).

Given its importance to Indian politics and everyday life, WhatsApp has received the most public criticism. Following the rumours spread on WhatsApp, the Indian IT ministry issued several warnings, stating irresponsible messages were not being "addressed adequately by WhatsApp", and that in the absence of adequate checks, WhatsApp would be considered an "abettor" of rumour propagation and subject to legal consequences (BloombergQuint, 2018). In response, WhatsApp added a 'forwarded' tag to messages, limited to five the number of times a message can be forwarded, and launched an advertisement campaign giving "easy tips" to spot fake news (Waterson, 2018). Restrictions have proved ineffective, and technical tools to circumvent these restrictions are advertised to campaigners—such as one charging a fee of 0.04 rupees ($0.0005) per message per individual, to allow a message to be forwarded thousands of times (Gilbert, 2019).

The day following the Kashmir terrorist attack, India's Central Reserve Police Force set up a team of twelve soldiers to fact-check social media posts (Bagri, 2019). Army Chief General Bipin Rawat said that "Our adversary will utilise social media for psychological warfare. We must also leverage social media to our advantage" (Gurung, 2018). Given the heightened tensions with Pakistan following the Kashmir attack, the Indian army is now considering how to use social media to its strategic advantage.

Battling disinformation is particularly difficult in India: dozens of languages make both automated and human moderation difficult, and the use of end-to-end encryption by WhatsApp restricts the platform's ability to counter disinformation. Alt News even found that two of Facebook's media partners, India Today Group and Jagran Media Network, published false information about the Kashmir attack (Goel & Frenkel, 2019). This demonstrates the difficulty in countering disinformation, and that such efforts are carried outagainst ingrained and institutionalized practices.

References

AFP India. (2019a, February 18). *No, this is not a photo of Indian politician Rahul Gandhi with the perpetrator of a deadly suicide attack in Kashmir*. AFP Fact Check. https://factcheck.afp.com/no-not-photo-indian-politician-rahul-gandhi-perpetrator-deadly-suicide-attack-kashmir

AFP India. (2019b, February 26). *No, these videos do not show Indian, Pakistani warplanes in Kashmir*. AFP Fact Check. https://factcheck.afp.com/no-these-videos-do-not-show-indian-pakistani-warplanes-kashmir

Amnesty International. (2020). *Trolling Verified: Troll Patrol India's Findings On Online Abuse*. Amnesty International. https://amnesty.org.in/trolling-verified-troll-patrol-indias-findings-on-online-abuse-twitter/

Bagri, N. T. (2019, March 15). When India and Pakistan clashed, fake news won. *LA Times*. https://www.latimes.com/world/la-fg-india-pakistan-fake-news-20190315-story.html

Bansal, S. (2019, January 27). *Narendra Modi App Has A Fake News Problem*. HuffPost India. https://www.huffingtonpost.in/entry/narendra-modi-app-has-a-fake-news-problem_in_5c4d5c86e4b0287e5b8b6d52

Bansal, S. P. and S. (2019, April 1). Misinformation Is Endangering India's Election. *The Atlantic*. https://www.theatlantic.com/international/archive/2019/04/india-misinformation-election-fake-news/586123/

Bengani, P. (2019). *India had its first 'WhatsApp election.' We have a million messages from it*. Tow Center for Digital Journalism. https://www.cjr.org/tow_center/india-whatsapp-analysis-election-security.php

BloombergQuint. (2018, July 19). *Mob Lynchings India: Government Wants WhatsApp To Do More Than Being Just A Mute Spectator*. https://www.bloombergquint.com/law-and-policy/mob-lynchings-whatsapp-at-risk-of-being-labelled-abettor

Chaturvedi, A. (2019, March 1). Ahead of general elections, parties tap social media influencers. *Economic Times*. https://economictimes.indiatimes.com/news/politics-and-nation/ahead-of-general-elections-parties-tap-social-media-influencers/articleshow/68208863.cms

Christopher, N. (2020, February 18). Deepfakes by BJP in Indian Delhi Election Campaign—VICE. *VICE*. https://www.vice.com/en_in/article/jgedjb/the-first-use-of-deepfakes-in-indian-election-by-bjp?wp-linkindex=16&utm_campaign=Disinformation_Newsletter_wc_03_Mar_2020_Prospects&utm_content=bbc-monitoring.co.uk&utm_medium=email&utm_source=BBC_Monitoring

Crabtree, J. (2018, July 11). *Cambridge Analytica must answer India, says Minister Prasad*. CNBC. https://www.cnbc.com/2018/07/11/cambridge-analytica-must-answer-india-says-minister-prasad.html

Dasgupta, P. (2018, June 25). 'It's Like Frankenstein's Monster': The Founder Of BJP's IT Cell Says PM Modi's Team Started The Rot | HuffPost India. *Huffington Post*. https://www.huffingtonpost.in/2018/06/22/its-like-frankensteins-monster-the-father-of-the-bjps-it-cell-says-team-modi-started-the-rot_a_23464587/?guccounter=1

@DFRLab. (2019, April 1). #ElectionWatch: Inauthentic Activity in India. *DFRLab*. https://medium.com/dfrlab/electionwatch-inauthentic-activity-in-india-8940588e09b5

@DFRLab. (2019, April 1). *Pakistan Army's Covert Social Network – DFRLab – Medium*. https://medium.com/dfrlab/pakistan-armys-covert-social-network-23ce90feb0d0

@DFRLab. (2020, January 17). *Case study: Politically charged pro-India hashtags amid Kashmir's digital blackout*. Medium. https://medium.com/dfrlab/case-study-politically-charged-pro-india-hashtags-amid-kashmirs-digital-blackout-670f81ae150d

EUDisinfoLab. (2019, November 26). Uncovered: 265 coordinated fake local media outlets serving Indian interests. *EU DisinfoLab*. https://www.disinfo.eu/publications/uncovered-265-coordinated-fake-local-media-outlets-serving-indian-interests

Freedom House. (2018, November 1). *Freedom on the Net 2018—India*. Freedom House. https://freedomhouse.org/report/freedom-net/2018/india

Freedom House. (2019). *India | Freedom House*. https://freedomhouse.org/country/india/freedom-net/2019

Funke, D., & Benkelman, S. (2019, February 21). 'No image can be taken on face value': Fake photos flood social media after a terrorist attack in India. *Poynter*. https://www.poynter.org/fact-checking/2019/no-image-can-be-taken-on-face-value-fake-images-flood-social-media-after-a-terrorist-attack-in-india/

Gilbert, D. (2019, April 11). Modi's trolls are ready to wreak havoc on India's marathon election. *Vice News*. https://news.vice.com/en_us/article/597mwk/modis-trolls-are-ready-to-wreak-havoc-on-indias-marathon-election

Gleicher, N. (2019, April 1). *Removing Coordinated Inauthentic Behavior and Spam From India and Pakistan*. https://newsroom.fb.com/news/2019/04/cib-and-spam-from-india-pakistan/

Goel, V. (2018, May 16). In India, Facebook's WhatsApp Plays Central Role in Elections. *The New York Times*. https://www.nytimes.com/2018/05/14/technology/whatsapp-india-elections.html

Goel, V., & Frenkel, S. (2019, April 11). In India Election, False Posts and Hate Speech Flummox Facebook. *The New York Times*. https://www.nytimes.com/2019/04/01/technology/india-elections-facebook.html

Gopalakrishnan, R. (2018, April 26). *Indian journalists say they intimidated, ostracized if they criticize Modi and the BJP - Reuters*. Reuters. https://www.reuters.com/article/us-india-politics-media-analysis/indian-journalists-say-they-intimidated-ostracized-if-they-criticize-modi-and-the-bjp-idUSKBN1HX1F4

Gurung, S. (2018, September 4). Social media could be used in combating proxy war: Army Chief. *Economic Times*. https://economictimes.indiatimes.com/news/defence/soldiers-should-get-access-to-social-media-within-line-of-control-army-chief/articleshow/65668575.cms

Gurung, S. (2019, March 9). Defence ministry approves information warfare branch for Indian army. *Economic Times*. https://economictimes.indiatimes.com/news/defence/defence-ministry-approves-information-warfare-branch-for-indian-army/articleshow/68329797.cms

Kalra, A. (2018, December 20). Insight: An online battle for 900 million hearts and minds - India... *Reuters*. https://in.reuters.com/article/india-election-socialmedia-idINKCN1OJ0DR

Kalra, A., & Sayeed, S. (2019, April 1). Facebook deletes accounts linked to India's Congress party,... *Reuters*. https://www.reuters.com/article/facebook-accounts-india-idUSKCN1RD1R2

Mackintosh, E., & Gupta, S. (2020, January 22). Troll armies, 'deepfake' porn videos and violent threats. How Twitter became so toxic for India's women politicians. *CNN*. https://www.cnn.com/2020/01/22/india/india-women-politicians-trolling-amnesty-asequals-intl/index.html

McLaughlin, T. (2018, September 5). The Plan to Save India From Disinformation. *The Atlantic*. https://www.theatlantic.com/international/archive/2018/09/fighting-whatsapp-disinformation-india-kerala-floods/569332/

Niranjankumar, N. (2018, May 1). With 23,000 WhatsApp Groups, BJP's Final Push To Woo Voters In Karnataka. *Boom Live*. https://www.boomlive.in/with-23000-whatsapp-groups-bjps-final-push-to-woo-voters-in-karnataka/

Patel, J., & Chaudhuri, P. (2019, February 7). 'The India Eye' – The Fake News Factory Promoted by NaMo App. *The Wire*. https://thewire.in/media/the-indian-eye-fake-news-factory-namo-app-silver-touch

Perrigo, B. (2019, January 25). How Whatsapp Is Fueling Fake News Ahead of India's Elections. *Time*. http://time.com/5512032/whatsapp-india-election-2019/

Riley, M., Etter, L., & Pradhann, B. (2018, July 19). A Global Guide to State-Sponsored Trolling. *Bloomberg*. https://www.bloomberg.com/features/2018-government-sponsored-cyber-militia-cookbook/

Riley, Michael, Etter, Lauren, & Pradhan, Bibhudatta. (2018, July 19). *A Global Guide to State-Sponsored Trolling*. https://www.bloomberg.com/features/2018-government-sponsored-cyber-militia-cookbook/

Safi, M. (2018, June 26). Indian foreign minister the latest victim of social media attacks on women. *The Guardian*. https://www.theguardian.com/world/2018/jun/26/indian-foreign-minister-sushma-swaraj-trolls-social-media

Safi, M. (2019, February 6). WhatsApp ‘deleting 2m accounts a month’ to stop fake news. *The Guardian*. https://www.theguardian.com/technology/2019/feb/06/whatsapp-deleting-two-million-accounts-per-month-to-stop-fake-news

Shaheen, K. (2018, June 18). *Turkey elections 2018: Everything you need to know*. Guardian. https://www.theguardian.com/world/2018/jun/18/turkey-elections-2018-everything-you-need-to-know

Siddique, H. (2019, November 11). British Indians warn Hindu nationalist party not to meddle in UK elections. *The Guardian*. https://www.theguardian.com/politics/2019/nov/11/british-indians-warn-hindu-party-not-to-meddle-in-uk-elections

Sidharth, A. (2019, April 29). Congress IT cell head tweets photoshopped image drawing a parallel between PM Modi and Hitler. *Alt News*. https://www.altnews.in/congress-it-cell-head-tweets-photoshopped-image-drawing-a-parallel-between-pm-modi-and-hitler/

Singh, S. S. (2019, February 21). *A former BJP data analyst reveals how the party’s WhatsApp groups work*. Quartz India. https://qz.com/india/1553765/bjps-whatsapp-ops-is-what-cambridge-analytica-can-only-dream-of/

Sircar, A. (2020, January 20). In poll-bound Delhi, Modi fans are carpet bombing student rebels on WhatsApp. *Quartz India*. https://qz.com/india/1786296/ahead-of-elections-pro-caa-whatsapp-propaganda-spreads-in-delhi/

Twitter Audit. (2018, February 21). World Leaders and their Fake followers Some of the most followed world leaders and their share of bot followers as determined by http://twitteraudit.com. Graphics prepared by @Saosasha @gzeromedia #DigitalDiplomacypic.twitter.com/viid9ZTReV [Tweet]. *@Twiplomacy*. https://twitter.com/Twiplomacy/status/966226775683534848?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E966226775683534848&ref_url=http%3A%2F%2Fwww.newindianexpress.com%2Fnation%2F2018%2Fmar%2F14%2F60-per-cent-of-pm-narendra-modis-twitter-followers-are-fake-twiplomacy-1786939.html

Uttam, K. (2018, September 29). For PM Modi’s 2019 campaign, BJP readies its WhatsApp plan. *Hindustan Times*. https://www.hindustantimes.com/india-news/bjp-plans-a-whatsapp-campaign-for-2019-lok-sabha-election/story-lHQBYbxwXHaChc7Akk6hcI.html

Waterson, J. (2018, November 12). WhatsApp struggling to control fake news in India, researchers say. *The Guardian*. https://www.theguardian.com/technology/2018/nov/12/whatsapp-struggling-control-fake-news-india-bbc-study-hindu-nationalism-cheap-mobile-data

Indonesia

Introduction

Indonesia is the largest majority-Muslim country in the world, with a population of over 267 million, and ranked fifth in the world in terms of total internet users, behind only the US, India, and China, and Brazil. Indonesia is also one of the largest social media markets in the world (Clement, 2019). According to research by Data Reportal, there were over 160 million social media users in Indonesia in January 2020 (Kemp, 2020) With a penetration rate of over 88%, YouTube was found to be the most used social network in Indonesia. However, Facebook and WhatsApp are also very popular, with approximately 40% of Indonesians using WhatsApp (Green House 2019).

Though the country has made significant democratic progress since the fall of its authoritarian regime in 1998, Indonesia still faces challenges that have been exacerbated by a well-established and sophisticated infrastructure of online manipulation. Such manipulation has been part of the country's political landscape for at least a decade, but the buildup for the April 2019 General Elections presented evidence of an intricately advanced framework of actors, organizations, and cashflow. The elections between the incumbent president Joko "Jokowi" Widodo and the former army general Prabowo Subianto, resulted in a second term for Widodo (Lipson, 2018).

An Overview of Cyber Troop Activity in Indonesia

Organizational Form

Political fake news and coordinated manipulation of online content by the government and other political actors in Indonesia has been evident at least since the 2014 presidential elections (Freedom of the Net, 2019). In recent years political cyber troop activity in Indonesia has undergone changes and developments. Specifically, there has been a movement away from the control of cyber troop activity by political campaign teams towards the influence of professional independent contractors (Renaldi, 2018). According to Ross Tapsell, an expert on politics and media at Australia National University, it has become common for candidates in Southeast Asia to hire campaign strategists to handle their online campaigns, who in turn orchestrate an army of people to spread political content on social media. This makes it difficult to find direct links between this online activity and the candidates themselves. Both competitors in the 2019 elections regularly denied hiring contractors to propagate fake news. However, there has been an array of social media operations spreading propaganda online on behalf of both President Joko Widodo and his opponent Prabowo Subianto (Potkin & Da Costa 2019).

A large volume of social media manipulation in Indonesia originates at the hands of "buzzer" groups, named after the online buzz they create. Buzzer groups are teams of individuals, sometime influencers, who are contracted to create a buzz around a particular topic or individual. Typically, each group is comprised of a team leader, who receives tasks and funds from clients and manages the team, and team members, who each operate numerous social media accounts on multiple platforms (Potkin & Da Costa, 2019). Evidence from one buzzer team reveals that members were employed in a "luxury house" in Jakarta and operated from several rooms. One room was charged with spreading positive content about their client, while another room focused solely on promoting negative content to smear their client's rival (Lamb, 2018a).

It is illegal under Indonesian law to create and spread disinformation online. However, operating a social media account under a fake identity is somewhat tolerated as long it is not considered theft of a real person's identity. Therefore, buzzer teams can and do take advantage of this legal loophole, and while denying any use of fake content, teams supposedly may operate thousands of accounts under fake identities. Spokespeople from Twitter, Facebook, and WhatsApp have stated that they are aware of these cases and actively delete such accounts in Indonesia, but they have not shared the number of account that have been removed (Potkin & Da Costa, 2019).

Volunteers also play a role in the country's social media manipulation. Many eager activists volunteer to serve on the digital frontline of their political agenda and promote the appropriate content. Political campaigns often have thousands of volunteers who are either organized directly by the campaign team, or by seemingly unrelated organizations. For example, Prabowo's Digital Team Coordinator denied that his campaign uses buzzer teams, but did admit to the use of "digital volunteers" (Potkin & Da Costa, 2019). Another example of volunteer organizing is a Prabowo-supporting volunteer group called Pride, which allegedly has thousands of members across Indonesia and coordinates its activity using thousands of WhatsApp groups. Moreover, one of Pride's volunteer team leaders, who has confirmed the use of WhatsApp groups to coordinate volunteer activity, is the founder of a digital marketing agency (Renaldi, 2018).

Cyber activity in Indonesia can also be found in civil society groups that work to promote specific political individuals or values. One such group that stands out is the Muslim Cyber Army, or MCA. The MCA is an online organization that engages in disinformation and doxing to promote the primacy of Islam and Islamic values in Indonesian society. Unlike common buzzer groups, the MCA is often described as having no formal structure or leadership, no central headquarters, and no dependence on cashflow. Some think of it as resembling the international hacktivist group Anonymous in terms of its organizational form (Juniartu 2018). Research conducted by the Southeast Asia Freedom of Expression Network found that the organization can be broadly divided into four clusters of smaller groups, which center their activity around Islamism, but each also add their own emphasis. Many of these smaller organizations have similar names, such as the Srikandi Muslim Cyber Army, the United Muslim Cyber Army, the Legend MCA, and Muslim Coming (Ibid). An investigation by *The Guardian* found links between the MCA and some opposition parties, military leaders, and influential Islamist activists. Additionally, the police said they are aware of at least one politically influential financier who backs the organization, though details were not provided (Lamb, 2018b).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Indonesia

Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
	Prabowo Subianto, Basuki Tjahaja Purnama, Joko Widobo	Buzzer groups, InsightID	Muslim Cyber Army, Srikandi Muslim Cyber Army, the United Muslim Cyber Army, the Legend MCA, and Muslim Coming	Volunteers, influencers, Pride

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Automated accounts: There is a variety of social media manipulation strategies and techniques being used by the various groups, with some groups using multiple techniques simultaneously, and others focusing on one. An increasingly common strategy is the use of automated bot-like accounts to promote hashtags, and spam online discourse with a particular message, which in turn makes it seem like a natural topic of discussion organically chosen by Indonesian netizens. Research conducted before the 2019 elections by the DFRLab found that about 25% of tweets posted between March 10th and April 10th (a week before the elections) that promoted the hashtag #JokowiLagi ("Jokowi again"), were posted using automating programs, alongside a significant amount of duplicated content. The research further found that programs like TweetCaster, IFTTT, and Twittbot.net were common for automating the posting and retweeting of hashtags. There is still insufficient evidence that links these bots to political actors, however, since parties have become more reliant on buzzer teams to amplify messages, it could be possible that these operations were conducted by a buzzer team working for the Jokowi campaign (DFRLab, 2019). Evidence of bot-like manipulation has also been revealed leading up to the 2017 Jakarta Gubernatorial elections, where researchers for the Centre for Innovation Policy and Governance found that at least some buzzers teams had created hundreds of bots to promote the campaign of Basuki "Ahok" Purama (Lamb, 2018a).

A notable case study of effective bot activity in the Indonesian general elections was the targeting of Sandiaga "Sandi" Uno, Prabowo's running mate, days after the campaign period began in September 2018. Two websites that were dedicated to attacking him, skandalsandiaga.com and sandiagaundercover.com, suddenly went viral on social media platforms and were heavily promoted with the hashtag #SkandalSandiaga. An analysis by Drone Emprit found that most of the accounts behind the campaign had no followers, were created in the same month, and tended to have profile pictures of women, all indicating that these were automated accounts (Renaldi 2018).

Another illuminating case study of bot-activity occurred in the Eastern region of West Papua. An investigation by the BBC and the Australian Strategic Policy Institute traced a network of bot accounts to InsightID, a Jakarta-based media company. These accounts spanned across at least four platforms spreading pro-government content about the region. One strategy they utilized was latching onto hashtags in support of the separatist movement and spamming them with positive stories, such as government investments in the region. Alternatively, bots would spread pictures with false captions that would suggest that the UN Human Rights commissioner responded "positively" to the state's treatment of the region, while she was in fact "disturbed" by it. These accounts also spent heavily on paid ads in the US, UK, and Europe, with the intention of skewing international perceptions regarding the region in favor of the government. Facebook stated that it shut down more than 100 accounts from this group, which also reportedly spent significant amounts of money on advertisements (Strick & Syavira, 2019).

Fake accounts: Hashtags are also promoted via buzzer teams using less technologically sophisticated techniques, but rather manually through authentic-looking accounts. In order to boost their authenticity, team members are often encouraged to use real profile pictures taken from Google, friends, or random Facebook and WhatsApp groups. Many choose to use pictures of beautiful women, which typically draw more attention. Evidence from one buzzer team suggests that members were provided with a hashtag list for promotion on a daily basis, which in a coordinated effort reached thousands of tweets a day, significantly increasing a hashtag's chances of reaching trending status (Lamb, 2018a).

Buzzer team members are also tasked with promoting news content, starting conversations, and engaging in comment sections of articles and threads. Additionally, the work of buzzer groups often begins long before the campaign season. Preparatory work includes the identification of potential collaborators and influencers, following accounts of politicians and gently beginning to interact, thus creating an illusion that these accounts are real characters who have emerged organically (Renaldi, 2018). Examples of coordinated activity by such accounts vary widely. Some accounts focus on day-to-day praise for leaders, and conveying messages that aren't necessarily related to elections but rather seem to be the common thoughts of an average citizen. One buzz group member said that there are accounts that his group manages that tweet about government-led infrastructure developments, Widodo diplomacy success, and national unity (strongly implying that the central government also utilizes buzz groups) (Lamb, 2018a). Other accounts were found to post identical tweets with identical political content, such as articles or pictures, within a very close timeframe. This kind of behavior typically implies that a either a single person or a tight network of people operate the accounts, often coordinated through WhatsApp (DFRLab 2019).

Disinformation: In addition to coordinated content promotion, spreading fake news is also a common strategy used by social media manipulators in Indonesia. Many groups deliberately spread fake news in order to discredit political opponents and to escalate ethno-religious tensions. Saracen, for example, was an online syndicate that spread bluntly fake stories that evoked racist and sectarian sentiments. At its height, the organization's Facebook page had over 800,000 followers and thousands more on other platforms (Renaldi 2017). Other notable examples of fake news included the widely spread rumors that before the 2014 elections that Widodo is opposed to Islam, is ethnically Chinese and is a communist. The rumors were so widely shared that some citizens still say that Widodo is a member of the banned Indonesian Communist Party (Lamb, 2019b).

Incitement: Some strategies promote de facto violence in the offline world. A strategy commonly associated with the MCA, known as doxing, involves collecting personal information of individuals accused of insulting Islam and circulating it with harmful intent. The MCA maintained a Facebook page dubbed "Database of People Wanted by the Muslim Community", which included sensitive personal information of the group's targets (Juniarto, 2018). In 2017, there were over 100 known cases in which doxing by the MCA led to intimidation and violent attacks, as well as the video recording of confessions under duress (Lamb, 2018b). The MCA has also released videos of targeted people under the caption "Blasphemer Hunter Team", urging viewers to report other people who insulted the religion (Ibid).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Indonesia

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Fake, Real, Bots	Anti-opposition, Pro-party, pro-government, Incitement, smear campaigns	Disinformation, Amplification of content, promoting hashtags	Facebook, Twitter, YouTube, WhatsApp

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

The buzzer ecosystem involves a significant amount of money, especially around the campaign season. One buzzer team leader, whose team worked for the Widodo campaign (with no known formal connection, however), stated that his team's price for a "complete package", which includes research, posts, and videos, costs USD $14,000 a month. A salary of a member of that team may vary between USD $65 and over USD $3,000 per project, typically depending on the reach of his accounts (Potkin & Da Costa, 2019). ABC claims to be aware of political parties offering buzzers USD $500 for sharing a single post (Lipson, 2018). On another team, operating in the 2017 Jakarta gubernatorial elections, team members were paid approximately USD $280 a month to post up to 120 posts a day through multiple accounts. Alternatively, campaign coordinators also approach people with influential accounts, unrelated to any organized propaganda effort, and "buy" tweets from them for up to USD $1,400 per tweet, or offer a monthly salary (Lamb, 2018a). For example, Denny Siregar, a famous author and political commentator said that he was offered USD $1,000 a month to become a buzzer himself, when he had 625,000 followers on Facebook and over 560,000 on Twitter (Ibid).

Information about the average size and capacity of individual buzzer teams varies, but ballpark estimations could be made with the available data. As such, it seems that an average buzzer group has approximately 15-20 members who each operate multiple social media accounts (Potkin & Da Costa, 2019; Lamb, 2018a). In terms of capacity, one buzzer team member reported that his group of 20 members can promote a particular message over 2,400 times a day (Lamb, 2018a).

Unlike buzzer teams, the size of volunteer groups varies quite significantly. While groups like the MCA are hard to quantify, campaign officials occasionally reveal the number of volunteer groups in order to discredit allegations of hiring buzzer teams. As such, Prabowo's official group of "digital volunteers" added up to at least 10,000 members, as per his Digital Team Coordinator (Potkin & Da Costa, 2019). Similarly, the pro-Prabowo volunteer group Pride allegedly has 12,000 members (Renaldi, 2018).

Table 3: Cyber Troop Capacity in Indonesia

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
Average buzzer group- 15-20 employees, Prabowo Pride volunteer group over 12000 members,	Buzzer salary – 65-3000 per project, Buzzer team price per month – 15,000$ 280 $ a month for 120 posts a day, One influencer tweet – 1400$, InsightID campaign – 300,000$			One buzzer group capable of promoting a message 2400 times a day

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

The Indonesian government has restricted internet access for citizens on several occasions. In some regions since 2018, internet shutdowns became a pre-planned occurrence implemented during large religious festivities, such as Nyepi. Also known as the Hindu Day of Silence, Nyepi is widely celebrated in the Hindu-majority island of Bali, where the internet was shut down for 24 hours after a request by the authorities (Lamb, 2018c).

The outcome of the 2019 elections led to a public uproar wds after Prabowo that declared he would challenge the results. Deadly riots soon broke out in his support, leaving 6 dead and over 200 wounded. Fake news and conspiracy theories virally spread in the early stages of the riots, claiming the police were shooting protesters inside mosques, and that many of them were secretly Chinese soldiers (Coconuts Jakarta 2019). The rapid spread of fake news urged the authorities to restrict the use of WhatsApp and Instagram for two days in an attempt to prevent the spread of more disinformation and decrease the level of violence (Singh & Russell, 2019). Another instance of an internet shutdown occurred three months later, with the intention of silencing protests in West Papua. Thousands took to the streets in late August 2019 to protest against government discrimination and in favor of self-determination and independence. In addition to security forces, the government responded with connectivity blockings until authorities deemed the security situation in the region "recovered" (Netblocks 2019).

References

Clement, J. 2019. Social Network Users in Selected Countries in 2018-2023. *Statista*. https://www.statista.com/statistics/278341/number-of-social-network-users-in-selected-countries/

Coconuts Jakarta. 2019. Police deny entering mosques in pursuit of rioters as hoaxes about secret Chinese soldiers go viral. *Coconuts Jakarta*. https://coconuts.co/jakarta/news/police-deny-entering-mosques-in- pursuit-of-rioters-as-hoaxes-about-secret-chinese-soldiers-go-viral/

DFRLab.2019. Social Media Spam Tactics in Indonesia. *Medium*. https://medium.com/dfrlab/social-media-spam- tactics-in-indonesia-1fd0beb8d5dd

Freedom House. 2019. Freedom of the Net: Indonesia. *Freedom House*. https://freedomhouse.org/country/indonesia/freedom-net/2019#footnote3_1f5qztt

Green House. 2019. Indonesia's Social Media Landscape: An Overview. *Green House*. https://greenhouse.co/blog/indonesias-social-media-landscape-an-overview/#:~:text=Facebook%2Downed%20WhatsApp%20and%20Japanese,has%2090%20million%20Indonesian%20users..

Juniarto, D.2018. The Muslim Cyber Army: what is it and what does it want. *Indonesia at Melbourne*. https://indonesiaatmelbourne.unimelb.edu.au/the-muslim-cyber-army-what-is-it-and-what-does-it-want/

Kemp, S. 2020. Digital 2020: Indonesia. *DataReportal*. https://datareportal.com/reports/digital-2020-indonesia.

Lamb, K. 2018a. 'I felt disgusted': inside Indonesia's fake Twitter account. *The Guardian*. https://www.theguardian.com/world/2018/jul/23/indonesias-fake-twitter-account-factories-jakarta- politic

Lamb, K. 2018b. Muslim Cyber Army: a 'fake news' operation designed to derail Indonesia's leader. *The Guardian*. https://www.theguardian.com/world/2018/mar/13/muslim-cyber-army-a-fake-news- operation-designed-to-bring-down-indonesias-leader

Lamb, K. 2018c. Bali switches off internet services for 24 hours for New Year's quiet reflection. *The Guardian*. https://www.theguardian.com/world/2018/mar/15/bali-switches-off-internet-services-24-hours-new- year

Lamb, K. 2019. Fake news spikes in Indonesia ahead of elections. *The Guardian*. https://www.theguardian.com/world/2019/mar/20/fake-news-spikes-in-indonesia-ahead-of-elections.

Lipson, D. 2018. Indonesia's 'buzzers' paid to spread propaganda as political elite wage war ahead of election. *ABC*. https://www.abc.net.au/news/2018-08-13/indonesian-buzzers-paid-to-spread-propaganda-ahead- of-election/9928870.

NetBlocks. 2019. Internet disrupted in Papua, Indonesia amid protests and calls for independence. *Netblocks.* https://netblocks.org/reports/internet-disrupted-in-papua-indonesia-amid-mass-protests-and-calls-for- independence-eBOgrDBZ.

Potkin, F., & Da Costa, A. B. 2019. In Indonesia, Facebook and Twitter are ‘buzzer; battlegrounds as elections loom. *Reuters*. https://www.reuters.com/article/us-indonesia-election-socialmedia-insigh/in-indonesia- facebook-and-twitter-are-buzzer-battlegrounds-as-elections-loom-idUSKBN1QU0AS

Renaldi, A. 2017. Saracen is shut down. But can we ever really beat fake news? *Vice*. https://www.vice.com/en_asia/article/3kk7v5/saracen-has-been-shut-down-but-can-we-ever-really- beat-fake-news

Renaldi, A, 2018. This is pure business. It has nothing to do with personal politics: Inside the hoax industry. *Vice.* https://www.vice.com/en_asia/article/pa58g7/inside-indonesia-hoax-black-campaign-industry- presidential-elections-jokowi-prabowo

Sheany. 2018. Muslim Cyber Army more harmful than Saracen, human rights group says. *Jakarta Globe.* https://jakartaglobe.id/news/muslim-cyber-army-more-harmful-than-saracen-human-rights-group-says/

Singh, M., & Russell, J. 2019. Indonesia restricts WhatsApp, Facebook and Instagram usage following deadly riots. *Tech crunch*. https://techcrunch.com/2019/05/22/indonesia-restricts-whatsapp-and-instagram/

Strick, B., & Syavira, F. 2019. Papua unrest: Social media bots skewing the narrative. *BBC News.* https://www.bbc.com/news/world-asia-49983667

IRAN

Introduction

The Islamic Republic of Iran has gained prominence as a sophisticated computational propaganda actor. The manipulation of social media takes place in the context of domestic Internet controls which have resulted in repeated shutdowns—most recently in response to anti-regime protests in November 2019. The extent of Iran's foreign influence campaigns has also been revealed through repeated platform suspensions by Facebook and Twitter for coordinated inauthentic behaviour.

Mis- and disinformation about the coronavirus pandemic have spread in Iran. The low turnout in the February 2020 parliamentary elections was blamed on the "negative propaganda" of Iran's enemies by Supreme Leader Ayatollah Ali Khamenei (Hafezi, 2020). Health-related misinformation allegedly lead to more than seven hundred deaths in Iran after fake rumours spread claiming that methanol could cure coronavirus (Forrest, 2020). Reports have also indicated that Iran has used the coronavirus pandemic to propagate anti-American and anti-Israeli narratives, such as the conspiracy that coronavirus is a "biological ethnic weapon" (Aarabi, 2020).

An Overview of Cyber Troop Activity in Iran

Organizational Form

The state has been monitoring Iranian social media activity to dismantle protests since 2010 (Murphy & Dodds, 2020). There are multiple organizations tasked with this social media manipulation, but their size and organization are disputed. A report by the Atlantic Council (2020) found evidence that Iran was operating Facebook and Twitter sock-puppet accounts created in 2010. The report suggested that Iran's digital influence efforts involve "different elements of Iran's digital apparatus" which evidence the involvement of multiple government agencies. The BBC (2017) reported that the government announced a 'Cyber Basij' had 18,000 online volunteers to flag questionable content online.

Platform suspensions have been linked to two media actors. Accounts have been attributed to the Islamic Republic of Iran Broadcasting Corporation (IRIB), the Iranian state media organization (Nimmo, Eib, et al., 2020). An IRIB network dismantled in April 2020 had been active since 2011. A further network of accounts has been dubbed the International Union of Virtual Media (IUVM) after the main media outlet involved in disseminating disinformation (Nimmo, Francois, et al., 2020). This entity is a "prolific operator" that has taken a geopolitical approach reflecting that of the Iranian government, and has been linked to accounts on Facebook, Google, and Twitter.

The Islamic Revolutionary Guard Corps (IRGC) is alleged to be partly responsible for Iran's offensive cyber capabilities. The Telecommunications Company of Iran was wholly acquired by the IRGC in 2009, strengthening its power and oversight over Iran's communications (Murphy & Dodds, 2020). Iran has also actively engaged in cyberwarfare under the IRGC. Hacking divisions are commonly called 'kittens' and have engaged in cyberattacks and cyber espionage, including by setting up fake personas on platforms like Facebook and LinkedIn.

The People's Mujahedin Organization (Mujahedin-e Khalq, or MEK) has an active online presence from their base in Tirana, Albania. The MEK is an exiled opposition group that has been designated a terrorist organisation (Benjamin, 2016). The Guardian reported that former

MEK member Hassan Heyrani said that there were several thousand accounts managed by about 1,000-1,500 MEK members in Tirana. They posted pro-Rajavi and anti-Iran propaganda in English, Farsi and Arabic on Facebook, Twitter, Telegram, and newspaper comment sections with fake accounts (Merat, 2018). Marc Owen Jones, an academic who investigates political bots, found that thousands of suspicious accounts emerged in early 2016 located in Iran, and posting in support of Trump and the MEK. Most accounts tweeting the hashtags #FreeIran and #Iran_Regime_Change from December 2017 to May 2018 were created within a four-month window, suggesting automated activity (Merat, 2018).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Iran

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
2009	IRIB, IRGC	MEK		Media (IUVM, Liberty Front Press TV) – level of state coordination unknown	

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Political Control

Iran has made repeated attempts to control the free flow of information on the Internet. This has been seen in Internet crackdowns during moments of political significance, such as the blocking of Facebook and Twitter during the 2009 elections, and internet shutdowns and throttling in the aftermath of the 2009 and 2013 elections. Social media as a tool for political control came to public attention during the 2009 Green Movement protests, when the rich and active blogosphere—that had for a decade been indirectly political—became explicitly used as a political tool for mobilization against the regime. Social media was dominated by pro-opposition users and reformists who shared images of the Green Movement to the outside world. Iran began systematically monitoring social media activity to demobilise protests, and criminalised online activism in 2010, legislated through the Computer Crimes Law (Article 19, 2012).

During the January 2018 protests, dozens of Twitter bots used tactics that ranged from calling widely shared videos of rallies fake to discouraging potential protestors from joining. Accounts were created by pro-regime users to guide protestors to the wrong locations and give the impression that the protests were on a small scale. One account posted in response to a video from a protest in Rasht, Gilan, "I just arrived here, there is nothing going on". The exact same messages by the same accounts could be seen commented on many videos between 1 and 4 January. The hashtag most associated with the events, #nationwide_protests has been used more than 470,000 times, but an analysis shows a large number of posts in favour of the demonstrations originated from Saudi Arabia (BBC, 2018).

Anti-regime protests broke out in November 2019 following a decision to triple the price of fuel overnight (Kadivar, 2019). This was met with a country-wide Internet shutdown, which some observers called the largest internet shutdown ever observed in Iran (Qiblawi, 2019). Communications apps such as WhatsApp, Telegram and Skype were unavailable—whilst Iranian messaging apps worked, many avoided them as they are controlled by state agencies or partly state-owned companies. According to former head of Iran's Chamber of Commerce, Mohessen Jalalpour, the five-day blackout cost the Iranian economy $1.5 billion (Kalbasi, 2019).

Electoral Campaigning

The presidential elections in May 2017, in which incumbent reformist President Hassan Rouhani was opposed by conservative Ebrahim Raeisi, saw attempts of manipulation by political forces. On Instagram, both reformist and conservative accounts produced a high volume of content, for example the pro-Rouhani account @nedayeeslahat appears to have been automated, posting fifty-two times between 13 and 17 May, including seven posts within forty seconds. Campaining occurred on Twitter during the 2016 parliamentary elections, as analysed in the report #IranVotes 2016, which found evidence of botnets and sock-puppet accounts (Marchant et al., 2016).

Messaging Apps

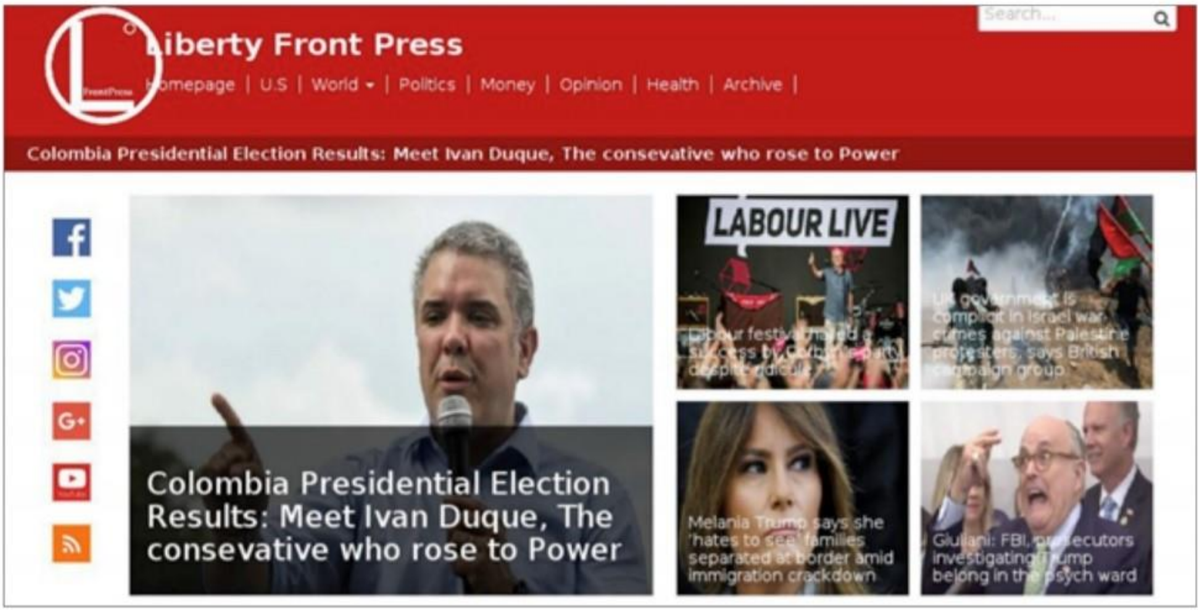
Telegram has forty million Iranian users (Sardarizadeh, 2019). Mahsa Alimardani, a researcher at the Oxford Internet Institute, said that “the regime has spent most of its time trying to manipulate or control the narrative on Telegram,” and that pro-Iranian government narratives have spread across Persian-language Telegram channels (Gallagher, 2020). Telegram was used in the 2017 presidential election, with both major campaigns deploying automated accounts to disseminate political messages (Freedom House, 2019). Conservative activists deployed a fake Rouhani bot with a very similar handle to the official account to spread anti-Rouhani content including cartoons, news from conservative news' agencies, Qur’anic citations and hadiths, and miscellaneous apolitical memes (Marchant et al., 2016). However, there is no indicator of the number of users or the impact of this account, and Telegram bots are distinct from the behaviour of Twitter bots.

In December 2016, Iran’s Supreme Cyberspace Council announced that Iranian-owned Telegram channels with more than five thousand members must obtain a permit from the Ministry of Culture and Islamic Guidance (Center for Human Rights in Iran, 2017). Authorities moved to ban Telegram altogether in April 2018, and it has been subject to temporary blocks in response to protests in the past (BBC Monitoring, 2018). Pavel Durov, CEO of Telegram, wrote in a blog post that the company had complied with Iranian government requests to shut down Telegram channels that called for violence during the protests (Frenkel, 2018).

Media Outlets

Social media accounts amplify state-sponsored narratives that are disseminated by media outlets. For example, IRIB is directly involved in the dissemination of disinformation and propaganda (Nimmo, Eib, et al., 2020). Following the August 2018 takedown of Iranian state-linked accounts by Twitter, Ben Nimmo stated that whilst other nations’ operations engage people and use sophisticated messaging, the Iranian operation used social media to message people and amplify links to disinformation websites. While there was a high number of tweets, they were of limited impact as the accounts simply shared links to pro-Iranian websites rather than creating personas to engage with audiences (Leprince-Ringuet, 2018). Approximately a third of the one million Iranian tweets released by Twitter contained links to AWDnews.com, part of the network of sites exposed by FireEye. One inauthentic news website discovered by FireEye was ‘Liberty Front Press’ (www.libertyfrontpress.com) which publishes political news related to the USA (Figure 1). Liberty Front Press has also maintained social media accounts on Twitter, Facebook, Instagram, Google Plus and YouTube (FireEye, 2018).

Figure 1: Liberty Front Press (FireEye, 2018)


Search...
Liberty Front Press
Homepage | U.S | World ▾ | Politics | Money | Opinion | Health | Archive |
LABOUR LIVE

Colombia Presidential Election Results: Meet Ivan Duque, The consevative who rose to Power

Colombia Presidential Election Results: Meet Ivan Duque, The consevative who rose to Power

Labour festival hailed a success by Corbyn's party despite ridicule

UK government is complicit in Israel war crimes against Palestine protesters, says British campaign group

Melania Trump says she 'hates to see' families separated at border amid immigration crackdown

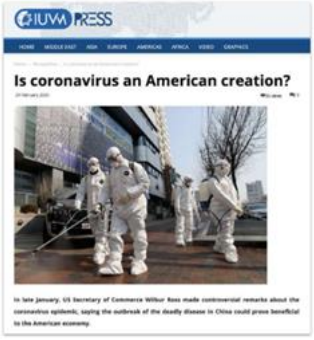
Giuliani: FBI, prosecutors investigating Trump belong in the psych ward

The International Union of Virtual Media (IUVM) is a prolific operator that creates web-based content that amplifies pro-government narratives, which is then posted across social media account posing as independent news outlets or journalists. Content includes video reports, news articles, and memes that are propagated across multiple IUVM-branded websites and covertly managed social media accounts. Graphika's investigation noted that the operation is "significant and manned by a well-resourced and persistent actor, but its effectiveness should not be overstated" (Nimmo, Francois, et al., 2020).

Disinformation

In an operation dubbed 'Endless Mayfly', an Iranian actor was involved in 'ephemeral disinformation' according to a May 2019 report by Citizen Lab. The Iranian-aligned network of websites and online personas was used to spread false and divisive information targeting Saudi Arabia, the United States and Israel. They discovered 135 articles, seventy-two domains and eleven personas that have been active since early 2016. The authors classified this as 'ephemeral disinformation' as the actor deleted content and redirected users to make attribution more difficult (Lim et al., 2019).

Amidst the global COVID-19 pandemic, a US State Department report from their Global Engagement Center warned that Iran had been leveraging coronavirus to launch propaganda and disinformation targeting the US (Swan, 2020). Likewise, Graphika found evidence that an Iranian influence actor had responded to coronavirus by "shifting its messaging to blame the United States and praise the role of China". An example of this propaganda can be seen in Figure 2 (Nimmo, Francois, et al., 2020).



Is coronavirus an American creation?

In late January, US Secretary of Commerce Wilbur Ross made controversial remarks about the coronavirus epidemic, saying the outbreak of the deadly disease in China could prove beneficial to the American economy.

Figure 2: Coronavirus disinformation from IUVM Press

Impersonating Journalists

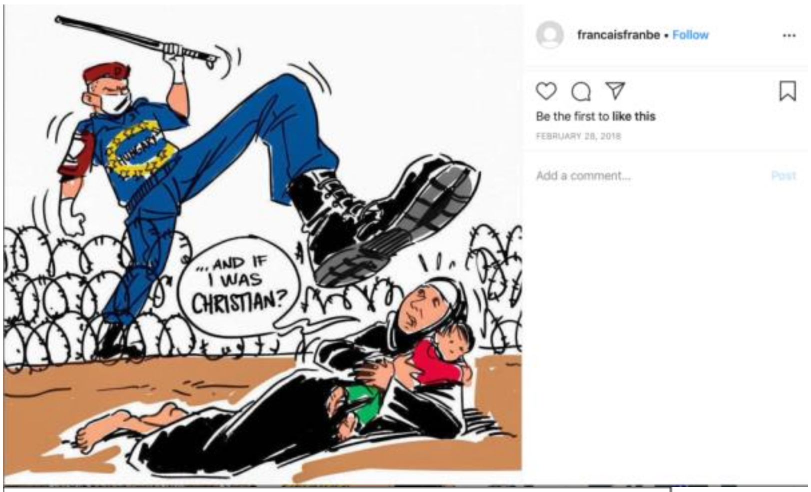
A tactic favoured by pro-Iranian accounts has been to impersonate prominent public figures such as journalists, academics, or activists, in an operation dubbed ‘Distinguished Impersonator’ by FireEye. Researchers found direct overlap between six personas operating on Facebook, Instagram, and Twitter. Whilst they have not been able to connect this operation directly to the Iranian government, the content was directly in line with Iranian political interests, such as anti-Saudi, anti-Israeli, and anti-Trump messaging. Tactics included amplifying favourable authentic content and disseminating news articles and videoclips from Western media that aligned with Iranian interests (Revelli & Foster, 2020).

Fake Accounts

The extent of Iran’s computational propaganda efforts is evidenced by multiple takedowns of accounts across Facebook, Instagram, and Twitter in the period 2018-2020. Facebook first announced in August 2018 that it had removed 652 Iran-based pages, groups and accounts that were part of a network linked to Iranian state media organisation IRIB (Facebook, 2018a). The network targeted people across the Middle East, Latin America, UK, and US. Twitter and Google also suspended an expansive network of accounts and websites that had links to the IRIB (Lapowsky, 2018). Kent Walker, Google’s senior vice president for global affairs, said they had “identified and terminated a number of accounts linked to the IRIB” which had been sharing English-language political content in the US (Timberg & Romm, 2019).

Twitter made public in October 2018 an Iranian foreign influence operation comprising 770 users and one million tweets. The social media accounts targeted Saudi Arabia, mentioning ‘Saudi’ nearly ninety thousand times. Researchers from the Computational Propaganda project at the Oxford Internet Institute found that Arabic was the third most used language in the data set, more than 69% of the links shared were to pro-Iran Arabic-language news websites, and the most widely shared websites pushed an Iranian political narrative (Elswah et al., 2019). Analysis by the Atlantic Council’s Digital Forensic Research Lab stated that Iranian Twitter accounts peaked earlier than the Russian troll accounts—surging in activity in 2014 and during a smaller peak in October 2017 (@DFRLab, 2018).

Iran’s foreign minister Mohammad Javad Zarif accused Twitter of double standards by shutting down the accounts of ‘real’ Iranians while letting an army of fake bot accounts continue. He tweeted “How about looking at actual bots in Tirana used to prop up ‘regime change’ propaganda spewed out of DC? #YouAreBots”. Iranian media accused the MEK, Israel and Saudi Arabia of being behind social media campaigns that have called for the overthrow of the Islamic government (Stubbs & Bing, 2018).



francaisfranbe • Follow

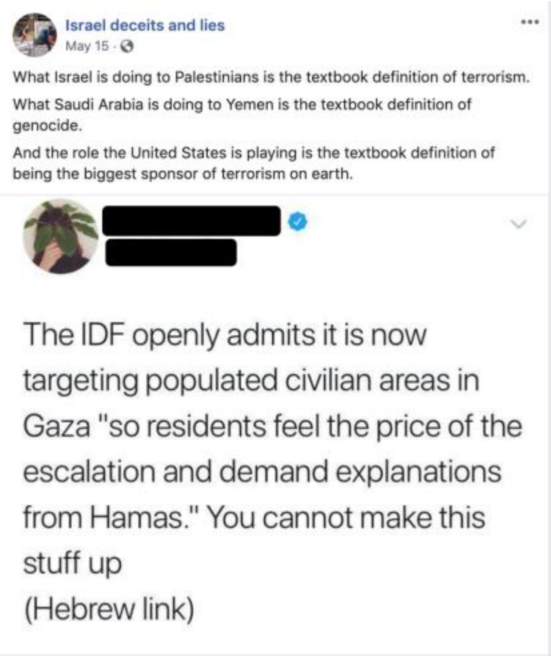
Be the first to like this

FEBRUARY 28, 2018

Add a comment...

Post

Figure 3: Inauthentic coordinated content removed from Facebook



Israel deceits and lies

May 15 ·

What Israel is doing to Palestinians is the textbook definition of terrorism.

What Saudi Arabia is doing to Yemen is the textbook definition of genocide.

And the role the United States is playing is the textbook definition of being the biggest sponsor of terrorism on earth.

[redacted]

The IDF openly admits it is now targeting populated civilian areas in Gaza "so residents feel the price of the escalation and demand explanations from Hamas." You cannot make this stuff up

(Hebrew link)

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Iran

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Fake, Human, Automated, Impersonation	Pro-Government, Attacking Opposition, Suppressing Speech, Polarising messages Attacking government	Creation of Disinformation, Amplifying authentic and inauthentic content, Impersonating journalists, trolling	Facebook, Twitter, Instagram, Telegram, Google

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

Iran's disinformation efforts initially developed to manipulate domestic political conversations, before gradually expanding to include more languages, themes, and targets (Timberg & Romm, 2019). Through Facebook and Instagram account takedowns, we can ascertain that accounts attributed to Iran have targeted:

Afghanistan, Albania, Algeria, Argentina, Bangladesh, Bahrain, Bolivia, Bosnia, Brazil, Ecuador, Egypt, France, Germany, Ghana, India, Indonesia, Iran, Iraq, Israel, Italy, Kazakhstan, Libya, Mauritania, Mexico, Morocco, Nigeria, Pakistan, Palestine, Peru, Qatar, Saudi Arabia, Serbia, Senegal, Sierra Leone, Somalia, South Africa, Spain, Sudan, Syria, Tanzania, Tunisia, United Kingdom, United States, Venezuela, Yemen and Zimbabwe.

It can also be calculated that cumulatively, networks attributed to Iran have spent US$58,702 on ads, and that 1,509 Facebook accounts, 884 Facebook pages, 82 Facebook groups and 386 Instagram accounts originating from Iran have been suspended. Twitter has suspended 8,166 accounts that it has linked to Iran. (These figures were calculated from the account suspensions detailed below.)

Table 3: Cyber Troop Capacity in Iran

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
	US$58,702	High		High

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

A summary of publicly disclosed takedowns of Iran-linked accounts:

- In October 2018, Facebook shut down thirty Facebook pages, thirty-three Instagram accounts and three Facebook groups, that were followed by around one million users in the US and UK and attributed to Iranian actors (Facebook, 2018b).
- In January 2019, Facebook removed 783 pages, groups, and accounts. Around two million accounts followed at least one of the pages, and $30,000 was spent on Facebook and Instagram ads. The activity targeted countries across the Middle East, Europe, Asia, Africa, and Central America (Gleicher, 2019a).
- In January 2019, building on the takedowns in August 2018, Twitter suspended a further 2,617 accounts (Roth, 2019a).
- In March 2019, Facebook removed 513 pages, groups, and accounts for coordinated inauthentic behaviour operating in Egypt, India, Indonesia, Israel, Italy, Kazakhstan, and across the Middle East and North Africa. Around 1.4 million accounts followed one or more of these pages, and US$15,000 was spent on advertisements (Facebook, 2019a).
- In May 2019, Facebook removed fifty-one accounts, thirty-six pages, seven groups and three Instagram accounts involved in coordinated inauthentic behaviour (Facebook, 2019b).
- In May 2019, FireEye uncovered a network of fake American personas on accounts made between April 2018 and March 2019, which it suspects is organized in support of Iranian political interests. These accounts impersonated individuals, including Republican political candidates, to disseminate favourable messaging towards Iran (Revelli & Foster, 2019).
- In June 2019, Twitter removed nearly 4,800 accounts with ties to the Iranian government. These accounts shared global news content in line with the geostrategic views of Iran, engaged in discussions related to Israel, and targeted political and social conversations in Iran and globally (Roth, 2019b).

- In October 2019, Facebook removed three networks of accounts for coordinated inauthentic behaviour, which targeted the US, North Africa, and Latin America (Gleicher, 2019b).
- In February 2020, Facebook removed six accounts and five Instagram accounts for foreign interference targeting the US (Facebook, 2020a).
- In April 2020, Facebook removed 389 accounts, 118 pages, twenty-seven groups and six Instagram accounts for engaging in foreign interference. Facebook linked this activity to the IRIB (Facebook, 2020b).

References

Aarabi, K. (2020, March 19). Iran Knows Who to Blame for the Virus: America and Israel. *Foreign Policy*. https://foreignpolicy.com/2020/03/19/iran-irgc-coronavirus-propaganda-blames-america-israel/

Article 19. (2012). *Islamic Republic of Iran: Computer Crimes Law*. Article 19. https://www.article19.org/data/files/medialibrary/2921/12-01-30-FINAL-iran-WEB%5B4%5D.pdf

Atlantic Council. (2020). *Iranian digital influence efforts: Guerrilla broadcasting for the twenty-first century—Atlantic Council*. https://atlanticcouncil.org/in-depth-research-reports/report/iranian-digital-influence-efforts-guerrilla-broadcasting-for-the-twenty-first-century/

BBC. (2017, February 8). ‘بسیج مجازی؛ ۱۸ هزار داوطلب تخلفات اینترنتی را گزارش می‌دهند’. *BBC News □□□□□*. https://www.bbc.com/persian/iran-38909342

BBC. (2018, January 7). *Iran messaging battle on social media*. https://www.bbc.com/news/world-middle-east-42566083

BBC Monitoring. (2018, April 25). *Iran pushes app with ‘Death to America’ emoji*. https://www.bbc.com/news/blogs-news-from-elsewhere-43891478

Benjamin, D. (2016, December 13). Yes, We Do Know the MEK Has a Terrorist Past. *POLITICO Magazine*. https://www.politico.com/magazine/story/2016/12/mek-backtalk-iranian-group-214526

Center for Human Rights in Iran. (2017, January 10). Iran’s Telegram Registration Requirement Widens Governmental Snooping Powers. *Center for Human Rights in Iran*. http://www.iranhumanrights.org/2017/01/irans-telegram-registration-requirement-widens-governmental-snooping-powers/

@DFRLab. (2018, October 17). #TrollTracker: Twitter’s Troll Farm Archives. *DFRLab*. https://medium.com/dfrlab/trolltracker-twitters-troll-farm-archives-17a6d5f13635

Elswah, M., Howard, P., & Narayanan, V. (2019). *Iranian Digital Interference in the Arab World – The Computational Propaganda Project* (Computational Propaganda Research Project). Oxford Internet Institute. https://comprop.oii.ox.ac.uk/research/working-papers/iranian-digital-interference-in-the-arab-world/

Facebook. (2018a, August 21). Taking Down More Coordinated Inauthentic Behavior. *About Facebook*. https://about.fb.com/news/2018/08/more-coordinated-inauthentic-behavior/

Facebook. (2018b, October 26). Taking Down Coordinated Inauthentic Behavior from Iran. *About Facebook*. https://about.fb.com/news/2018/10/coordinated-inauthentic-behavior-takedown/

Facebook. (2019a, March 26). Removing Coordinated Inauthentic Behavior from Iran, Russia, Macedonia and Kosovo. *About Facebook*. https://about.fb.com/news/2019/03/cib-iran-russia-macedonia-kosovo/

Facebook. (2019b, May 28). Removing More Coordinated Inauthentic Behavior From Iran. *About Facebook*. https://about.fb.com/news/2019/05/removing-more-cib-from-iran/

Facebook. (2020a, March 2). February 2020 Coordinated Inauthentic Behavior Report. *About Facebook*. https://about.fb.com/news/2020/03/february-cib-report/

Facebook. (2020b, May 5). April 2020 Coordinated Inauthentic Behavior Report. *About Facebook*. https://about.fb.com/news/2020/05/april-cib-report/

FireEye. (2018). *Suspected Iranian Influence Operation*. https://www.fireeye.com/blog/threat-research/2018/08/suspected-iranian-influence-operation.html

Forrest, A. (2020, April 28). 700 dead in Iran after drinking toxic alcohol to 'cure coronavirus'. *The Independent*. https://www.independent.co.uk/news/world/middle-east/coronavirus-iran-deaths-toxic-methanol-alcohol-fake-news-rumours-a9487801.html

Freedom House. (2019). *Freedom on the Net | Iran*. Freedom House. https://freedomhouse.org/country/iran/freedom-net/2019

Frenkel, S. (2018, January 2). Iranian Authorities Block Access to Social Media Tools. *New York Times*. https://www.nytimes.com/2018/01/02/technology/iran-protests-social-media.html

Gallagher, R. (2020, January 8). Iran's Infamous Disinformation Apparatus Isn't Going Into Overdrive—Yet. *Bloomberg.Com*. https://www.bloomberg.com/news/articles/2020-01-08/iranians-seen-holding-back-on-disinformation-campaigns

Gleicher, N. (2019a, January 31). Removing Coordinated Inauthentic Behavior From Iran. *About Facebook*. https://about.fb.com/news/2019/01/removing-cib-iran/

Gleicher, N. (2019b, October 21). Removing More Coordinated Inauthentic Behavior From Iran and Russia. *About Facebook*. https://about.fb.com/news/2019/10/removing-more-coordinated-inauthentic-behavior-from-iran-and-russia/

Hafezi, P. (2020, February 23). Iran announces low poll turnout, blames coronavirus 'propaganda'. *Reuters*. https://www.reuters.com/article/us-iran-election-khamenei-idUSKCN20H09Z

Kadivar, M. A. (2019, November 27). Analysis | Iran shut down the Internet to stop protests. But for how long? *Washington Post*. https://www.washingtonpost.com/politics/2019/11/27/iran-shut-down-internet-stop-protests-how-long/

Kalbasi, K. (2019, November 25). Iranians endure internet shutdown with despair and disarray. *Atlantic Council*. https://www.atlanticcouncil.org/blogs/iransource/iranians-endure-internet-shutdown-with-despair-and-disarray/

Lapowsky, I. (2018, October 26). Iran's New Facebook Trolls Are Using Russia's Playbook. *Wired*. https://www.wired.com/story/iran-facebook-trolls-using-russia-playbook/

Leprince-Ringuet, D. (2018, October 25). Iran has its own fake news farms, but they're complete amateurs. *Wired UK*. https://www.wired.co.uk/article/iran-fake-news

Lim, G., Maynier, E., & Scott-Railton, J. (2019, May 14). *Burned After Reading: Endless Mayfly's Ephemeral Disinformation Campaign—The Citizen Lab*. Citizen Lab. https://citizenlab.ca/2019/05/burned-after-reading-endless-mayflys-ephemeral-disinformation-campaign/

Marchant, J., Sabeti, A., Bowen, K., Kelly, J., & Jones, R. H. (2016). *#IranVotes: Political Discourse on Iranian Twitter During the 2016 Parliamentary Elections*. Small Media. https://smallmedia.org.uk/media/projects/files/IranVotes_2016.pdf

Merat, A. (2018, November 9). Terrorists, cultists – or champions of Iranian democracy? The wild wild story of the MEK. *The Guardian*. https://www.theguardian.com/news/2018/nov/09/mek-iran-revolution-regime-trump-rajavi

Murphy, M., & Dodds, L. (2020, January 8). How Iran built an online disinformation machine to rival Russia's. *The Telegraph*. https://www.telegraph.co.uk/technology/2020/01/08/iran-built-online-disinformation-machine-rival-russias/

Nimmo, B., Eib, S., Ronzaud, L., Ferreira, R., Lederer, T., & Smith, M. (2020). *Iran's Broadcaster: Inauthentic Behavior*. https://graphika.com/reports/irans-broadcaster-inauthentic-behavior/

Nimmo, B., Francois, C., Eib, C. S., & Ronzaud, L. (2020). *Iran's IUVM Turns To Coronavirus*. Graphika. https://graphika.com/reports/irans-iuvm-turns-to-coronavirus/

Qiblawi, T. (2019, November 18). Iran's 'largest internet shutdown ever' is happening now. Here's what you need to know. *CNN*. https://www.cnn.com/2019/11/18/middleeast/iran-protests-explained-intl/index.html

Revelli, A., & Foster, L. (2019, May 28). Network of Social Media Accounts Impersonates U.S. Political Candidates, Leverages U.S. and Israeli Media in Support of Iranian Interests. FireEye. https://www.fireeye.com/blog/threat-research/2019/05/social-media-network-impersonates-us-political-candidates-supports-iranian-interests.html

Revelli, A., & Foster, L. (2020, February 12). 'Distinguished Impersonator' Information Operation That Previously Impersonated U.S. Politicians and Journalists on Social Media Leverages Fabricated U.S. Liberal Personas to Promote Iranian Interests. FireEye. https://www.fireeye.com/blog/threat-research/2020/02/information-operations-fabricated-personas-to-promote-iranian-interests.html

Roth, Y. (2019a, January 31). *Empowering further research of potential information operations*. https://blog.twitter.com/en_us/topics/company/2019/further_research_information_operations.html

Roth, Y. (2019b, June 13). Information operations on Twitter: Principles, process, and disclosure. *Twitter*. https://blog.twitter.com/en_us/topics/company/2019/information-ops-on-twitter.html

Sardarizadeh, S. (2019, February 15). Warsaw summit: Were hashtags amplified on Iranian Twitter? – BBC Monitoring. *BBC Monitoring*. https://monitoring.bbc.co.uk/product/c200mbyv

Stubbs, J., & Bing, C. (2018, November 30). Special Report: How Iran spreads disinformation around the world. *Reuters*. https://www.reuters.com/article/us-cyber-iran-specialreport-idUSKCN1NZ1FT

Swan, B. W. (2020, April 21). State report: Russian, Chinese and Iranian disinformation narratives echo one another. *POLITICO*. https://www.politico.com/news/2020/04/21/russia-china-iran-disinformation-coronavirus-state-department-193107

Timberg, C., & Romm, T. (2019, July 25). It's not just the Russians anymore as Iranians and others turn up disinformation efforts ahead of 2020 vote. *Washington Post*. https://www.washingtonpost.com/technology/2019/07/25/its-not-just-russians-anymore-iranians-others-turn-up-disinformation-efforts-ahead-vote/

IRAQ

Introduction

The state has historically dominated the public information landscape within Iraq. Despite attempts to foster a more pluralistic media landscape after the 2003 Iraq war and the fall of the Ba'athist regime, an increase in sectarian conflict in 2005 led to further limitations on media freedoms (Al-Kaisy, 2019). Media outlets supporting the dominant Shi'a narratives were banned from Sunni areas, while Shi'a districts banned Sunni outlets (Al-Kaisy, 2019). Iraqi citizens thus had limited access to varied information sources. Today, the online information landscape in Iraq continues to be shaped by its fragile, sectarian political system. Issues of corruption, polarisation and a lack of trust in governing institutions have led to a rapid growth in politically charged domestic computational propaganda campaigns.

Freedom House (2020) reports Iraq as "not free", despite holding regular competitive elections, frequent security threats and pervasive corruption undermine these democratic efforts. Recently, between October and December 2019, widespread anti-government protests took place in Baghdad. In response to these protests, Iraqi military killed 500 protestors and injured 19,000 (Freedom House, 2020). Amidst the protests, Major General Abdul Karim Khalaf, who was previously Minister of Information in 2003, stated that live bullets and tear gas were not used by security forces (Crisp & al-Salhy, 2020). These claims amounted to disinformation, as they were contrary to extensive video evidence, which showed the military killing and wounding demonstrators with tear gas and live bullets (Crisp & al-Salhy, 2020).

Following the protests, Adel Abdul Mahdi resigned from the post of Prime Minister, along with his cabinet. There was a subsequent struggle to form a new government, resulting in the appointment of Mustafa Al-Kadhimi, former director of the Iraqi National Intelligence Service, to the post of Prime Minister (Alshamary, 2020).

Throughout these shifts in power, however, there has remained the pervasive presence of so-called "electronic armies" to conduct computational propaganda campaigns (Niqash, 2017). These armies are mostly controlled by competing political groups within Iraq, and are used to fabricate news stories to defame their political opponents (Niqash, 2017).

An Overview of Cyber Troop Activity in Iraq

Organizational Form

Iraq's cyber troops operate primarily through Facebook pages (Niqash, 2018b). The lack of reliable, accessible news sources mean that these Facebook pages have become a key information source for Iraqi citizens (Crisp & al-Salhy, 2020). These pages have large audiences, with followings ranging from 100,000 to 400,000 (Kholoud Al-Amry, 2019). Traditional media will often publish information from these Facebook pages, enabling cyber troop content to reach a broad audience (Mawazin News, 2019).

Many of these Facebook pages are run by professional bloggers using common Iraqi names as pseudonyms (خلود العامري, 2019). These bloggers often create these pages, acquire large followings, then rent these pages to politicians or political parties (Niqash, 2018b). The Iraq Independent High Electoral Commission acknowledged that while some media organisations engage in cyber troop activity, the vast majority of cyber troops are funded by political parties . Politicians can either rent entire Facebook pages or pay per post (Niqash, 2018b). If the pages are rented to politicians, the administrators of these pages often receive monthly salaries from these politicians (خلود العامري, 2019).

Other pages, however, are directly affiliated with politicians or political groups and act as advertising platforms (Niqash, 2018b). However, there now exists a more varied cyber troop landscape, and pages have since emerged that are designed to criticise the former Prime Minister. One such page titled “Siyasi Hashash” (Addict Politician) reached a following of 331,000 in 2017, and other pages such as “Al-Abadi Wadihan” (Al-Abadi is Clear) continue to publish critical content (خلود العامري, 2019).

One of the groups spending the most on Facebook cyber troops is Kata’ib Hezbollah, a Shia paramilitary group that is part of the Popular Mobilisation Forces (Crisp & al-Salhy, 2020).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Iraq

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
2010	Military	A wide range of political actors and parties	Private bloggers	Kata’ib Hezbollah	

Source: Authors’ evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

A report by the local media monitor Iraqi Media House (IMH) into cyber troop activity found that political Iraqi cyber troops pursued three main goals: (1) generating inauthentic engagement to give the impression of widespread public support; (2) defaming political adversaries through the generation of false information; (3) diverting online discussion away from politically sensitive discussions (Al-Badeel Iraq, n.d.).

Of these goals, defaming political adversaries is the one most frequently pursued by Iraqi cyber troops. There are many reported examples of Iraqi political groups using false information to defame opponents. One such example of an “aggressive campaign using fabricated news”, in the words of Kurdistan Democratic Party’s Iraqi presidential candidate Fouad Hussein, is a series of reports by local media regarding Hussein’s links to the Israeli Mossad intelligence service, and further claims that his wife is Christian rather than Jewish (Al-Quds al-Arabi, 2018b). It is important to note that this publication cannot speak to the accuracy of these claims. In another example, former Iraqi Prime Minister Adel Abdul Mahdi denied claims that he had given away land in the fortified Green Zone to Hezbollah militia (Iraqi News Agency, 2020).

In contrast to these examples of defamation attempts, the Iraqi military attempted to use cyber troops for reputation-building. The website Al-Sumaria News published a story claiming that the Iraqi army had been awarded a prize for the best army in the world. Furthermore, the article claimed that the award for the best military commander in the world had been given to deputy Iraqi Council-Terrorism Service, Abdul-Wahab al-Saedi (Al-Badeel Iraq, n.d.). These rumours were later refuted by the media (Al-Badeel Iraq, n.d.).

As previously outlined, the primary computational propaganda tool in Iraq is Facebook. The pages generated on Facebook by professional bloggers and political actors gather followers rapidly after their creation, party through the use of paid social media advertisements, and party through the publication of innocuous content such as comic strips to attract users. Some pages also post fabricated documents to attract audiences, this could include documents reporting financial corruption that have not previously been published by mainstream media. Other pages digitally edit official documents to give their platforms false credibility (خلود العامري, 2019). Some pages publish specific content to attract audiences, such as hate speech, abuse against specific politicians and calls for violence against political actors.

These calls for violence are most frequently targeted toward female political candidates running in Iraqi parliamentary elections (Niqash, 2018a). A report into these campaigns found that they were systematic, and targeted toward the 2,000 female political candidates (Al-Ittihad, 2018). A report found that defamation attempts against female candidates can include the publication of sexual videos, allegedly involving these candidates. The report could not verify the clips, but quoted a female candidate stating that "some parties try to defame her to make sure she cannot win the elections" (Al-Quds al-Arabi, 2018a).

Groups with their own cyber troop capacities, such as Hezbollah, employ a team to run the Facebook pages. Team members are given a mobile phone, an iPad and a Visa card to pay for post boosts to attract audiences (Crisp & al-Salhy, 2020). These teams are provided with training to avoid censorship (Crisp & al-Salhy, 2020). Hezbollah focusses on posting disinformation that undermines the reputation of political rivals.

While Facebook is the main platform used by cyber troops in Iraq, some pages also have documented links to other sites, such as Twitter and YouTube (2,21). Video footage of politicians statements is often edited to focus on the most sensationalist quotes, then published on these YouTube channels (2,21). An IMH report noted that the group Fursan al-Karahiyah (Knights of Hate) often engaged in such multi-platform posting (Iraqi Media House, n.d.).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Iraq

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
	Distraction, attacking opposition, generating support	Disinformation, amplifying content	Facebook, YouTube, Twitter

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

In May 2020, Facebook removed a total of 324 pages, 71 accounts, 5 groups and 31 Instagram accounts identified as Iraqi cyber troops (Crisp & al-Salhy, 2020). Facebook noted that the accounts were followed by 4.4 million accounts. These Facebook pages have been very successful in engaging audiences. One of the most active pages is called "Haramiyah" (Thieves), and is followed by around 573,000 accounts (خلود العامري, 2019).

Maliki-affiliated Facebook page administrators, along with cyber troop writers and analysts were reportedly been paid $1,600 or more per month for their efforts. Since the decline of Maliki's influence, there have been reports of journalists charging $1,000 a month to campaign on behalf of an Islamic party (Yaqein, 2018). Alternatively, a political party may pay around $1,000 for several posts on a popular Facebook page each month (Niqash, 2018c).

In addition to these costs, most politicians or political parties have designated office space for their cyber troop employees (خلود العامري, 2019). Reports claim that Hezbollah has approximately 400 employed cyber troop staff, tasked with operating the network of fake Facebook pages and accounts (Crisp & al-Salhy, 2020).

Some of these political interest groups operate permanent cyber troop campaigns, however other pages emerge during security crises, elections or political power struggles. In one instance, cyber troop campaigns were mobilised by various political actors during the passage of a contentious draft law (خلود العامري, 2019).

Table 3: Cyber Troop Capacity in Iraq

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
		Permanent	Professional Facebook page administrators	High

References

Al-Badeel Iraq. (n.d.). !! "أكذوبة الجيش العراقي "يحصل على جائزة الأفضل بالعالم دون منازع http://www.albadeeliraq.com/ar/node/761

Al-Ittihad. (2018, April 23). الانتخابات العراقية «الأشرس» والنساء في عين العاصفة.

Al-Kaisy, A. (2019). A fragmented landscape: Barriers to independent media in Iraq.

Al-Quds al-Arabi. (2018a, April 19). مرشح لرئاسة العراق: زوجتي مسيحية وليست يهودية.. وهناك حملة مدعومة ضدي.

Al-Quds al-Arabi. (2018b, September 26). مرشح لرئاسة العراق: زوجتي مسيحية وليست يهودية.. وهناك حملة مدعومة ضدي.

Alshamary, M. (2020, November 13). Six months into his premiership, what has Mustafa al-Kadhimi done for Iraq? *Brookings*. https://www.brookings.edu/blog/order-from-chaos/2020/11/13/six-months-into-his-premiership-what-has-mustafa-al-kadhimi-done-for-iraq/

Crisp, W., & al-Salhy, S. (2020, June 14). Iraqi groups paying Facebook millions to churn out fake news. *The Telegraph*. https://www.telegraph.co.uk/business/2020/06/14/iraqi-groups-paying-facebook-millions-churn-fake-news/

Freedom House. (2020). *Iraq*. Freedom House. https://freedomhouse.org/country/iraq/freedom-world/2020

Iraqi Media House. (n.d.). "الجيوش الإلكترونية"... أخبار مفبركة تجتاح "فيسبوك".

Iraqi News Agency. (2020, May 22). *Iraq denies Shia militia granted land in Green Zone*.

Mawazin News. (2019, January 31). الاعلام العراقي الحقيقي في مواجهة خطر الجيوش الالكترونية. https://www.mawazin.net/Details.aspx?jimare=32207

Niqash. (2017, April 12). "الترويج لشائعات وأخبار كاذبة: الساسة العراقيون يتقاتلون عبر "جيوش الكترونية.

Niqash. (2018a, April 16). بين التسقيط والاستهزاء: حملات تسقيط وتشهير ضد المرشحات العراقيات. https://www.niqash.org/ar/articles/politics/5891/

Niqash. (2018b, April 25). مصادر غامضة وأهداف واضحة :الأخبار الزائفة.. نشاط مافياوي وراء شاشات الكومبيوتر.

Niqash. (2018c, April 25). مصادر غامضة وأهداف واضحة :الأخبار الزائفة.. نشاط مافياوي وراء شاشات الكومبيوتر.

Yaqein. (2018, April 29). الانتخابات العراقية.. كيف يستخدم المرشحون الجيوش الالكترونية في حملاتهم؟. https://yaqein.net/investigations/106558

خلود العامري. (2019, March 27). ‘جيوش إلكترونية’ عراقية تدير حروب السياسيين على مواقع التواصل. *The Independent (Arabic Language)*.

Israel

Introduction

Israel's computational propaganda efforts fall under three main categories: (1) propaganda which is aimed at social media users outside of the country (Hasbara/public diplomacy), (2) political campaign propaganda which is aimed at local Israeli citizens, and (3) the "alternative enforcement" method which Israel's attorney generals' office developed together with platforms such as Facebook and YouTube to ensure better coordination between the platforms and Israel in locating malicious online behaviour directed toward Israel.

An Overview of Cyber Troop Activity in Israel

Organizational Form

Hasbara (Public Diplomacy): The first of these efforts falls mainly within the broader effort of public diplomacy (in Hebrew, *hasbara*). In recent years this has become more professionalized and centralized in character (Aouragh, 2016). Israel's public diplomacy efforts are divided roughly into four different and coordinated organizations: The Ministry of Foreign affairs, the Office of Hasbara, the Hasbara array in The Office of the Prime Minister, and the Israel Defense Forces Spokesperson's Unit. The general aims of public diplomacy efforts are addressed mostly to foreign audiences and include the promotion of pro-Israeli narratives and countering BDS (boycott, divestment and sanctions) propaganda messages, whose threats aim at delegitimizing Israel (Toker, 2012).

The main government organizations working in the field of hasbara work on different audiences. For example, the Ministry of Foreign Affairs is primarily focused on spreading messages to other Israeli delegations around the world that are at the forefront of foreign media. The Hasbara array in the Prime Ministers Office focuses on the Jewish diaspora and pro-Israeli organizations around the world. It is also in charge of coordinating responses to foreign media in Israel. These organizations find themselves the most active during major regional conflicts as they become a major player in the "narrative war" with Palestinian diplomatic and propaganda efforts. During these conflicts, public diplomacy works towards justifying and explaining the Israeli position on the nature of the conflicts. The Israel Defense Forces Spokesperson's Unit is one of the most active organizations during these conflicts and uses digital means to spread messages about Israel's military activity and attempts by terrorist organizations to attack Israeli civilians (Toker, 2012).

The Ministry of Strategic Affairs is another government office that has become increasingly more involved in Hasbara. In recent years the ministry, which started out as an office without substantial political importance, has become the leading office in the development of online Hasbara strategies, especially in regards to efforts concerned with the global BDS organization. One of the main activities the office has supported is the promotion of a Hasbara app called act.il, to be used by supporters around the world to help spread pro-Israel and anti-BDS messages online. The app is supported by the ministry and was developed by three organizations in Israel and the US: The Israeli-American Council, the Maccabee Task Force, and the Interdisciplinary Center Herzliya University. On the ministry's website there is additional recommended content to be used by apps users for sharing on social media (Sommer, 2017).

Beyond official government diplomacy organizations, Israel has developed a large network of coordinated volunteer groups in Israel and around the world, comprising mainly of students, whose main task is to spread pro-Israel messages and counter anti-Israel and BDS messages online. Most of these coordinated volunteer networks began during the Operation Pillar of Defense and Operation Protective Edge between Israel and Gaza in 2012 and 2014, in which the office of the Prime Minister budgeted ILS 3 million shekels towards building a "shadow unit" with the Israeli Student Union to manage hasbara efforts on social media. The initiative included: paying students through scholarships to take part in spreading pro-Israel messages, combatting anti-Israel narratives online, and the development of a government unit of interactive media to be in charge of the governments Hasbara in the social media realm (Ravid, 2013).

This campaign continued through 2015 in which the National Hasbara Office funded a joint initiative between students and the Stand With Us organization to allow students to take part in Israel's public diplomacy efforts online. According to the office, this decision comes after the previous volunteer campaigns were found to have played a crucial and successful role in "spreading reliable information and a balanced discourse on social media" (Zarhia, 2015). These new campaigns were to be coordinated together with several international Jewish organizations, such as the World Union of Jewish Students, the Jewish National Fund, the Jewish Agency, and the World Jewish Congress (Ibid).

Political social media manipulation: The second segment of computational propaganda in Israel, as mentioned above, is more directly related to the issue of political social media manipulation aimed at influencing Israeli citizens' public opinions, mostly during election periods. Various parties and politicians in Israel have taken part in this kind of computational propaganda, though direct links are yet to be evidenced.

In the past year Israel had three general elections, which led to increases in coordinated online behavior. Some of the first evidence of social media manipulation were found during Israel's municipal elections in 2018, leading to Facebook taking down thousands of fake accounts (Ginosar and Liberman, 2018). Manipulation of online media for political interests was also evident in the national elections in 2019. An investigation by the *Yediot Aharonot* newspaper revealed a large network of fake Twitter accounts that were promoting Prime Minister Benyamin Netanyahu's campaign and attacking his opponent, Benyamin Gantz. Even though no direct connection was found between the Likud party's campaign and the coordinated network, people close to the campaign, including the prime minister's son, Yair Netanyahu, have shared messages posted by these accounts. For example, the holder of one of the central accounts, named "BOND", revealed that he is a "covert activist" for the Likud party and that his online activity is funded. The exposure of this network has raised suspicions of a range of criminal offenses, including violations of Israel's Propaganda Law, violations of election financing, violations of privacy, and more (N12 News 2019).

Alternative Enforcement: The third type of computational propaganda identified in this case study does not fall under the category of social media manipulation and is mostly aimed at law enforcement and online safety purposes that are not intended for political benefit.

During the 2015-2016 wave of terrorist stabbing attacks against Israelis the distribution of online content inciting young Palestinians to continue the attacks was evident. By consequence, the Israeli government worked with Facebook to create joint teams to work together in fighting against online incitement. Facebook receives recommendations from Israel on the removal of accounts and posts. Palestinian activists have been critical of this arrangement, arguing that has been used as a means suppressing their freedom of speech on Facebook (Barak, 2020).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Israel

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
	Ministry of Foreign Affairs, The office of Hasbara, The Hasbara array in The Office of The Prime Minister, Israel Defence Forces Spokesperson's Unit, Ministry of Strategic Affairs	Likud	Media Group	The Israeli-American Council, the Maccabee Task Force, Interdisciplinary Centre Herzliya University, Stand With Us, Israeli Student Union, World Union of Jewish Students, the Jewish National Fund, the Jewish Agency, the World Jewish Congress, Inter-disciplinary Centre for Innovation and Leadership	Volunteer students

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Coordinated inauthentic behavior: During the 2018 municipal elections an investigation undertaken by the newspaper *Yediot Aharonot* revealed the various strategies and tactics being used by political strategy companies in the online sphere to boost their clients' campaigns. Some of the strategies that were revealed included: using trolls to harass and spread lies about other candidates, creating "armies" of fake accounts to spread misinformation, the creation of "avatar troops" to gather political information on social media users, and creating various fake Facebook pages to gain followers in order to eventually use these pages to boost their campaigns (Ginosar and Liberman, 2018).

Ran Tennenbaum, the CEO of Media group, revealed in an interview cited in the investigation that his company holds around 120 avatars. He explains that these avatars are used to identify users' political opinions, identities, and psychological profiles to be used later for political campaigning and advertising (Ginosar and Liberman, 2018). Michal Adar, a political strategist, also explained the focus on many occasions was on trying to find dirt on political rivalries and then spread it via social media (Ibid). Rotem Gaz, someone who had worked as an online campaign worker, listed various strategies being used today by political candidates online. According to Gaz, candidates are willing to spend a lot of money on buying likes and inauthentically boosting their online profile. Another strategy that is used is the buying of software that artificially spreads a political opponent's name online. By doing so, Google's algorithm tags the word as being more popular than it actually is, and subsequently charges the opponent for advertising, therefore crushing the opponent's advertising budget (Goichman 2018).

The network of fake accounts created during the 2019 national elections also appeared to tweet in a coordinated manner while using messages taken from the Likud party's campaign. For example, many tweets mentioned the Likud slogan "will fall like a house of cards", referencing the campaign's slogan used to downplay the indictments against Netanyahu. Other messages used were mostly misinformation and attacks on Netanyahu's opponent, Benyamin Gantz (N12 News, 2019).

Hasbara/Diplomacy: The main strategy of the act.il Hasbara app, deployed by the Ministry of Strategic Affairs, is to promote the spread of pro-Israel messages on social media. Users receive a list of tasks and receive points when they are completed. The app searches the social media network for negative, anti-Semitic, and anti-Israel online content, and notify its users who are then prompted to comment on the post and try to change the narrative. Users with the most points at the end of each month are recognized and virtually decorated. The main point of the app is to build an online community of Israel supporters (Bz, 2017).

Facebook takedowns: There have been a number of takedowns relating to Israel-based activity in the past year. On May 2019, Facebook took down 265 Facebook and Instagram accounts involved in coordinated inauthentic behavior. The activity originated in Israel and focused on Nigeria, Senegal, Togo, Angola, Niger, and Tunisia. The network used fake accounts to run pages to distribute their content and artificially increase engagement. The administrators frequently posted about local politicians, political news, elections, candidate views, and criticism of opponents. The investigation found that the activity was linked to an Israeli commercial entity, Archimedes Group. No direct relationship with the government has been evidenced (Facebook 2019).

In 2019 Facebook took down more than 82 accounts it suspected were fake and which were attempting to discourage Israeli-Arabs from voting. According to an investigation undertaken by Democratic Bloc, the suspected profiles encouraged an election boycott. The accounts were suspected of actively commenting on pages in order to undermine Israeli-Arab politicians and their parliamentary work (Yaron, 2019). In 2020 Facebook removed a number of fake accounts that were promoting incitement against Prime Minister Netanyahu. Posts being uploaded by these accounts included pictures of Netanyahu next to pictures of Hitler and various threats on his life (ynet, 2020).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Israel

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Fake accounts, real accounts	Pro Netanyahu messages, misinformation on opposition, Pro-Israel messages, spreading dirt on political opponents, supressing voting	Coordinated behaviour, disinformation, amplification of likes, organized online Hasbara, creating info-graphs, targeting social media users.	Twitter, Facebook

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

Rotem Gaz, the ex-online campaign worker cited above, also revealed that if he was to keep working in the field, he could have expected to have made around USD $60,000 in contributing to online activity by using various methods, such as bots, scripts, and spreading dirt on candidates (Goichman, 2018). According to Gaz, candidates can spend around USD $6,000-25,000 for an online campaign (Ibid).

According to the investigation by *Yediot Aharonot* and *The New York Times*, the coordinated inauthentic network of fake accounts that was active during the 2019 national elections disseminated over 130,000 tweets promoting Prime Minister Benyamin Netanyahu. The report noted that the fake messages reached over 2.5 million Israelis online (N12, 2019).

In recent years Israel has invested millions of dollars in developing a wide network of organizations and individuals to extend the government's influence in the online arena. Their job is to spread the voice of the Israeli government through civilians instead of official government organizations (Bz, 2019). In 2019 the Office of Strategic Affairs, whose primary role has become the development of Israel's Hasbara in the digital sphere, received a budget of over USD $21.9 million (Kahane 2020). The budget used to promote the Hasbara app act.il was close to USD $2 million, whereas funding from outside organizations came to around USD $29,500. This money goes to the ongoing management of the project, social media advertisement, and the operation of three "war rooms", one in Israel and two in the US. The Ministry has also spent over USD $450,000 on seminars and training at youth groups, coordinated through civilian organizations such as the Maccabiah organization, in Israel and abroad, with a view to training young people to become online ambassadors for Israel. In recent years, the ministry has also given the "Inter-disciplinary Center for Innovation and Leadership" around USD $600,000 to train Israeli high schoolers to become online ambassadors. The youth will be in charge of building the campaigns, however the content is defined by the ministry (Bz, 2017).

In 2015 the government allocated USD $300,00 to the civil organization Stand With Us to help promote the integration of university students in the online Hasbara mission. The Project's goal was to create a network of volunteers composed of groups of students who are online influencers around the world. The students meet roughly three times each month for training on the type of content to be promoted and the various technological means to be used. During "emergency times," in which regional conflict sparks up, the students are meant to work in the format of "situation rooms". Each campus has an organizer who undertakes special training three times a year (Zarchia, 2015).

Table 3: Cyber Troop Capacity in Israel

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
	• Candidates can spend around 6000 $ - 25,000$ for an online campaign, • The office of the Prime Minister budgeted 3 million shekels to build a shadow unit of online hasbara • The ministry of strategic affairs spent over 2 million dollars on promoting the act.il app,			

	450,000$ on seminars and training of youth groups to be online ambassadors and 600,000$ to the “Inter-disciplinary Centre for Innovation and Leadership” to train Israeli high schoolers. • The government allocated 300,00$ to “Stand With Us” to help promote the integration of university students in the online Hasbara mission.			

References

Aouragh, M. 2016. Hasbara 2.0: Israel’s Public Diplomacy in the Digital Age. Middle East Critique, 25(3), pp. 271-297.

Facebook. 2019. Removing coordinated inauthentic behavior. Facebook. https://about.fb.com/news/2019/05/removing-coordinated-inauthentic-behavior-from-israel/.

Yaron, O. 2019. Israel Election 2019: Facebook Removes Fake Accounts Encouraging Arabs Not to Vote. Haaretz.https://www.haaretz.com/israel-news/elections/.premium-israel-election-2019-facebook-removes-accounts-encouraging-arabs-not-to-vote-1.7856351.

גינוסר, ש., וליברמן, ג. 2018. כך מחסלים מועמד: הצצה לתעשיית ההכפשות ברשת. *ידיעות אחרונות*. https://www.ynet.co.il/articles/0,7340,L-5324713,00.html

גויכמן, ר. 2018. תעריף החיסול ברשת של מועמד בבחירות: 20-80 אלף שקל. מאקו. https://www.mako.co.il/nexter-internet/Article-5ef6d862a19b661006.htm

חדשות 12. מערך החשבונות המזויפים למען ראש הממשלה. חדשות 12. https://www.mako.co.il/news-israel-elections/elections_2019-q2_2019/Article-3a101ea2c07d961004.htm .

ב"ז, א. 2017. צבא האמת של מדינת ישראל. העין השביעית. https://www.the7eye.o rg.il/272146 ץ

כהנא, א. 2020. קיצוץ במדרש שנאבק ב-BDS. ישראל היום . https://www.israelhayom.co.il/article/729733

טוקר, נ. 2012. ההסברה הישראלית למדה לתקוף בחזה: צה"ל מנצח על הטוויטר. דה מרקר. https://www.themarker.com/advertising/1.1870129 .

זרחיה, צ. 2015. המדינה תקצה במיליון שקל לדיפלומטיה ציבורית ברשתות החברתיות. דה מרקר. https://www.themarker.com/news/1.2538175 .

ברק, מ. 2020. פייסבוק חוסמת את פלסטין: הפלסטינים נגד הצנזורה ברשתות החברתיות. מרכז משה דיין. https://dayan.org/he/content/5465 ץ

סומר, א., ק. 2017. נשים מפתות וסאטירה על פעילי זכויות אדם: האפליקציה של ישראל נגד ה-BDS. הארץ. https://www.haaretz.co.il/news/politics/.premium-1.4175468

רביד, ב. משרד ראש הממשלה מקים יחידת צללים של סטודנטים להסברה מוסווית ברשת. הארץ. https://www.haaretz.co.il/news/politics/.premium-1.2095791

Italy

Introduction

Generally, the Internet is freely accessible in Italy and the Italian government does not engage in any kind of censorship or blocking. The Internet penetration rate of the country is higher than the global average, but lower than the EU average. In addition, there is a north/south divide in penetration rate, with the north having a higher rate on average compared to the south.

In terms of legislation there has been some controversy and criticism from international organizations and the United Nations. In November 2017, the Italian government adopted a law requiring telecommunication services to retain telephone and Internet data for up to six years. With little parliamentary debate taking place on the new legislation, the general public were unhappy about the situation and staged demonstrations. Moreover, the United Nations Human Rights Committee has raised concerns about Italian legislation relating to two issues in 2017: firstly, the fact that defamation is a criminal offence in Italy and civil libel suits against journalists and online activists continuously put great financial strain on the online media landscape of the country; and secondly, that Italian intelligence employs hacking methods and intercepts personal communications without explicit statutory authorization. However, in 2016 the Supreme Court of Italy ruled hacking by intelligence agencies as constitutional. Italian politicians have subsequently tried to regulate hacking but have thus far been unsuccessful.

It is worth mentioning that nearly all politicians in Italy have established a presence on major social media platforms (Facebook, Twitter). Populist candidates, such as Luigi Di Maio and Matteo Salvini, were able to harness the frustration of the electorate by posting live videos on Facebook discussing issues such as migration and corruption to score high engagement numbers. Even after the election, leading politicians regularly take their debates about legislation to social media, not just to comment on current issues and express their views, but also to accuse each other of political propaganda and engaging in heated debates online.

Meanwhile, the Italian government has taken official action against fake news, instituting educational initiatives in schools by adding media literacy to school curricula. They have also established a unit within the Polizia Postale (Postal and Communications Police), encouraging cooperation between ISPs (including social media platforms, and Facebook in particular), citizens and police to report fake news, leading to public refutations and removal requests. The project—called 'The Red Button'—was launched in January 2018 to allow citizens to report fake news on a portal provided by the police. The National Anti-Crime Information Center for Critical Infrastructure Protection (CNAIPIC) was tasked with analysing the reported content. There has been some criticism regarding the vague language defining fake news and the job of the CNAIPIC. Moreover, the Reuters report *Measuring the reach of "fake news" and online disinformation in Europe* relativized the impact of such sites in Italy, both in terms of average monthly reach and time spent on those websites, although the Facebook interactions of false news sites exceeded those produced by the most popular news brands.

An Overview of Cyber Troop Activity in Italy

Organizational Form

Social media manipulation in Italy is repeatedly described as an "ecosystem", coordinating different types of initiatives mostly affiliated with populist forces such as the Lega Nord (Northern League) and the Movimento Cinque Stelle (M5S, 5 Stars Movement). Public concern has arisen specifically in relation to three crucial political events: the 2017

Constitutional Referendum, the general elections on 4 March 2018, in which M5S came first and League jumped from 4% to 17% of votes, and the 2019 European Parliament elections, in which League obtained 34% of votes.

According to WIRED, Web365 and NextMediaWeb, both agencies owned by Giancarlo and Davide Colono, managed a network of websites that promoted nationalist and Islamophobic content, often associated with Lega Nord's narrative (Fontana, 2020). After the network was revealed in 2017, the two entrepreneurs updated it with a more complex and decentralized structure. Similarly, Planet Share, an agency owned by Andrea Caroletti, has established a network of around 140 domain sites that follow a similar logic and interact with Colono's networks (Fontana, 2020). As reported by Fontana (2020), the visible website of Planet Share was registered by Web365. Andrea Caroletti also chairs La Luce di Maria, a not-for-profit cultural association that organizes pilgrimages and has a website and a Facebook page with more than 1.4 million followers. Through its Facebook page it shares conservative and anti-scientific content, as well as content produced by the above mentioned Web365 and Planet Share networks (Fontana, 2020).

M5S leadership have been identified as being behind some of the websites revealed in 2017, including its co-founder Gianroberto Casalleggio (Tze Tze[1] and La Fucina[2] websites are owned by his firm Casaleggio Associati). Other sites shared IP addresses, Google Analytics and AdSense IDs with Beppe Grillo's blog and M5S official websites (Bayer et al., 2019).

Misinformation and fake news remain a concern for the country: in addition to campaigns organized by domestic teams, data released in early 2018 also suggest that the same Russian company (Internet Research Agency, IRA) which was behind disinformation campaigns during the 2016 US election was also responsible for thousands of tweets and profiles in Italy. The US information website Fivethirtyeight.com released nine Excel spreadsheets containing millions of tweets and profiles which US special counsel Robert Mueller strongly suspects are from the IRA and some of the content is in Italian. So far there does not appear to have been official response from the Italian government. While it is unlikely that the Lega party or Five Star Movement directly supported or paid for these tweets, most of the content shared by IRA profiles was supportive of these two parties and a report from the Atlantic Council suggests close ties between both parties and several Russian individuals. In the case of Lega, a recording shows evidence of negotiations of a deal to send millions of dollars to the party to sustain their European election campaign, which was permissible due to a legal loophole that until January 2019 permitted foreign funding to political parties (Nardelli, 2019). With the COVID-19 crisis, several allegations of Russian disinformation in Italy have also been raised (Pellegatta, 2020). Following disinformation campaigns related to COVID-19, there are additional allegations that China has used bots to undertake pro-Chinese and anti-European Union propaganda (Carrer & Bechis, 2020; DFRLab, 2020). The official Twitter account of the Embassy of China in Italy has been identified as a key driver of the campaign. Also related to the publications were hashtags associated to Lega Nord. Moreover, in Twitter's disclosure of state-backed operations by China in June 2020, it can be observed that *Italy* and *Italia* occur several times in tweets where the help received by the Chinese authorities was praised (Twitter Safety, 2020).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Italy

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
2016		Evidence found	Web365, NextMediaWeb, and Casaleggio Associati		

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

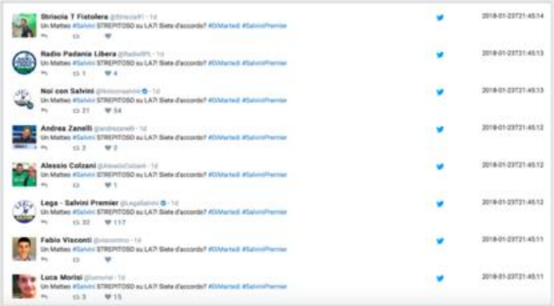
Strategies, Tools, and Techniques

Lega Nord and the Five Star Movement made use of both common and uncommon techniques of social media manipulation, especially on Facebook, mainly during the general election in 2018 and European Parliament elections in 2019. Disinformation campaigns on social media have already been documented in 2016 in the context of the Italian Constitutional Referendum (Bayer et al., 2019).

There is evidence, for instance, that Lega Nord used an automated system called La Bestia to monitor news and social networks and thus coordinate their communication. This technique enabled them to be the first to comment on the news, forcing opponents into reactive strategies, polarizing discussions, and amplifying their messages (Joint Research Centre (European Commission), 2019). But the app also enabled the automated cross-posting of social media activities. Volunteers authorized an app to automatically like or embed the party and Matteo Salivini's posts (Bayer et al., 2019).

Lega Nord use real accounts from private individuals who turned themselves into bots, "selfbots" as the Digital Forensic Research Lab (DFRLab, 2018) calls them, which then all tweet the same messages (Figure 1). There is usually a "herder" or teacher, which creates new accounts or repurposes hijacked accounts for their botnet. However, while these selfbots send out automated messages, they remain human accounts, as, outside these tweets, they post individual content created by the actual users.

Figure 1: "Selfbot" network tweeting the same message at the same time



Striscia T Fiatolera · 1d
Un Matteo #Salvini STREPITOSO su LA7! Siete d'accordo? #DiMartedì #SalviniPremier
2018-01-23T21:45:14

Radio Padania Libera · 1d
Un Matteo #Salvini STREPITOSO su LA7! Siete d'accordo? #DiMartedì #SalviniPremier
1 4
2018-01-23T21:45:13

Noi con Salvini · 1d
Un Matteo #Salvini STREPITOSO su LA7! Siete d'accordo? #DiMartedì #SalviniPremier
21 54
2018-01-23T21:45:13

Andrea Zanelli · 1d
Un Matteo #Salvini STREPITOSO su LA7! Siete d'accordo? #DiMartedì #SalviniPremier
2 2
2018-01-23T21:45:12

Alessio Colzani · 1d
Un Matteo #Salvini STREPITOSO su LA7! Siete d'accordo? #DiMartedì #SalviniPremier
1
2018-01-23T21:45:12

Lega - Salvini Premier · 1d
Un Matteo #Salvini STREPITOSO su LA7! Siete d'accordo? #DiMartedì #SalviniPremier
32 117
2018-01-23T21:45:12

Fabio Visconti · 1d
Un Matteo #Salvini STREPITOSO su LA7! Siete d'accordo? #DiMartedì #SalviniPremier
2018-01-23T21:45:11

Luca Morisi · 1d
Un Matteo #Salvini STREPITOSO su LA7! Siete d'accordo? #DiMartedì #SalviniPremier
3 15
2018-01-23T21:45:11

Source: *DFR Lab (https://medium.com/dfrlab/electionwatch-italys-self-made-bots-200e2e268d0e) January 25, 2018*

One other technique used by both parties is that of coordinating networks of websites that post fabricated content, support their narratives, and discredit their opponents. These are purposefully pushed by social media accounts as well as by leading politicians (Bayer et al., 2019). Although their interaction rates are high, analysis by the Reuters Institute for the Study of Journalism has shown that these websites have a minor reach compared to mainstream media outlets (Freedom House, 2019).

In 2019, after the activist group Avaaz reported on some of these networks, Facebook removed twenty-three accounts that were violating the company's authenticity policy and were associated with both parties (Freedom House, 2019). Gianroberto Casaleggio, one of the co-founders of M5S, was already associated with social engineering techniques to manipulate opinions within forums and newsgroups at the end of the 1990s (Joint Research Centre (European Commission), 2019). With the creation of M5S and in the run-up to the elections, a broader propaganda machine was established. M5S has since at least 2016 been affiliated with a series of blogs, "independent news" outlets and social accounts that often share misleading or alarmist stories about corruption and anti-politics—especially in the early days of the movement—, tragic events and hyper partisan pieces about immigration, echoing nationalist and Islamophobic rhetoric, and conspiracy theories in the run-up to the general elections. On the other hand, Lega Nord was linked to a network of websites that were not party-related, but that shared the same Google codes. Some of these websites had pro-Putin and conspiracy theories content, other pro-party, anti-immigration and Islamophobic one (Bayer et al., 2019).
Giglietto et al. (2019) analysed political news stories published or shared in pages, groups and verified public profiles in both Facebook and Instagram in the run up to the 2018 general election and the 2019 European election. Identified networks shared the same link within a limited timeframe, indicating a baseline of "coordinated link sharing" (Giglietto et al., 2019). Most of the activities were aligned to Lega Nord and anti-migration, especially among highly coordinated networks. Moreover, several websites and Facebook pages were blacklisted by fact-checking websites (Giglietto et al., 2019).

In line with this, in a thorough analysis of the media landscape during the 2018 general elections, Giglietto et al. (2018) highlighted that Lega had "the highest number of media source adjudicated while the sources in the M5S category gathered the highest volume of overall Facebook interactions". Furthermore, they identified three sources among the top twenty-five URLs: Ilfatto.org, which they explicitly indicate as having content that may be "inaccurate or completely made up"; Italia24ore.com, which is categorized as a for-profit fake news site; and inews24.it, which is part of an anti-immigrant network of websites and Facebook pages (Giglietto et al., 2018). It is also worth noting that they state that Italian extreme-right groups organized via 4chan, 8chan, and Telegram in crafting the content and strategies to influence public opinion and favour League and the Brothers of Italy parties (Ebner and Davey, 2018, as cited in Giglietto et al., 2018).

As regards Twitter, according to Pierri et al. (2020), during the five-month period leading up to the 2019 European Parliament elections, there was a small proportion of tweets linked to disinformation websites, which mainly focused on polarizing content related to immigration, national safety and nationalism. They were mostly related to Lega Nord—"the main cited leader"— and M5S's narratives and sometimes targeted Partito Democratico (Pierri et al., 2020). The report indicates that there is little evidence of bot activity during this period.

Lastly, it is worth mentioning that, in addition to the already mentioned disinformation campaign which appears to have originated abroad, NewGuard has also identified a network of ten Facebook pages that appear to be diverse in content (e.g. fashion, aphorisms, lifestyles, and others) but have recently started to spread disinformation about COVID-19, such as that which suggests that lemon and water could defeat the virus or that the government denied tests on migrants, and link to articles at ViralMagazine.it and FanMagazine.it (Padovese & McDonald, 2020). These pages often post content favourable to Salvini and his agenda.

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Italy

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Bots, Human, Fake and Real	Distracting messages, Driving divisions and polarization, Pro-government, Attacks on opposition	Disinformation, Amplifying content	Facebook, Instagram, Twitter

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

There is not much evidence on resources spent by Lega Nord or Movimento 5 Stelle on propaganda operations. However, it is important to note that most activities are primarily associated with critical events, such as general and European elections.

As regards the companies behind some of the identified networks of disinformation websites, WIRED highlights that the website MeteoWeek— managed by Planet Share but with connections with Web365— offered €200 for web content editors, whose main responsibility was to write original articles of at least 380 words (Fontana, 2020).

Table 3: Cyber Troop Capacity in Italy

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
		Temporary (mostly during elections)		Low

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

References

Bayer, J., Bitiukova, N., Bárd, P., Szakács, J., Alemanno, A., & Uszkiewicz, E. (2019, febrero). *Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States*. https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2019)608864

Carrer, G., & Bechis, F. (2020, March 30). *Così la Cina fa propaganda in Italia, con i bot. Ecco l'analisi su Twitter di Alkemy per Formiche*. Formiche.net. https://formiche.net/2020/03/cina-propaganda-twitter-bot-alkemy/

DFRLab. (2018, January 25). #ElectionWatch: Italy's Self-Made Bots. *DFRLab*. https://medium.com/dfrlab/electionwatch-italys-self-made-bots-200e2e268d0e

DFRLab. (2020). *China exploits Italian coronavirus outbreak to expand its influence*. Medium. https://medium.com/dfrlab/china-exploits-italian-coronavirus-outbreak-to-expand-its-influence-967a6998fea3

Ebner, J., & Davey, J. (2018). Mainstreaming Mussolini. How the Extreme Right Attempted to "Make Italy Great Again" in the 2018 Italian Election. Institute for Strategic Dialogue.

Nardelli, A. (2019, July 10). *Revealed: The Explosive Secret Recording That Shows How Russia Tried To Funnel Millions To The "European Trump"*. BuzzFeed News. https://www.buzzfeednews.com/article/albertonardelli/salvini-russia-oil-deal-secret-recording

Fontana, S. (2020, January 13). Come Salvini tiene in vita il network di disinformazione più grande d'Italia. *WIRED*. https://www.wired.it/attualita/politica/2020/01/13/network-disinformazione-lega-web365/?refresh_ce=

Freedom House. (2019). *Freedom of the Net | Italy*. Freedom House. https://freedomhouse.org/country/italy/freedom-net/2019

Giglietto, F., Iannelli, L., Rossi, L., Valeriani, A., Righetti, N., Carabini, F., Marino, G., Usai, S., & Zurovac, E. (2018). *Mapping Italian News Media Political Coverage in the Lead-Up of 2018 General Election*. https://www.ssrn.com/abstract=3179930

Giglietto, F., Righetti, N., & Marino, G. (2019). Understanding Coordinated and Inauthentic Link Sharing Behavior on Facebook in the Run-up to 2018 General Election and 2019 European Election in Italy [Preprint]. SocArXiv. https://doi.org/10.31235/osf.io/3jteh

Joint Research Centre (European Commission). (2019). *Understanding citizens' vulnerability to disinformation and data-driven propaganda*. European Commision. https://op.europa.eu/en/publication-detail/-/publication/3ada7fb3-7d04-11e9-9f05-01aa75ed71a1/language-en/format-PDF/source-115672948

Nardelli, A. (2019, July 10). *Revealed: The Explosive Secret Recording That Shows How Russia Tried To Funnel Millions To The "European Trump"*. BuzzFeed News. https://www.buzzfeednews.com/article/albertonardelli/salvini-russia-oil-deal-secret-recording

Padovese, V., & McDonald, K. (2020, May 5). Super-diffusori in Italia – NewsGuard. *News Guard Tech*. https://www.newsguardtech.com/it/super-diffusori-in-italia

Pellegatta, A. (2020, March 30). Russia exploits Italian coronavirus outbreak to expand its influence [Medium]. *DFRLab*. https://medium.com/dfrlab/russia-exploits-italian-coronavirus-outbreak-to-expand-its-influence-6453090d3a98

Pierri, F., Artoni, A., & Ceri, S. (2020). Investigating Italian disinformation spreading on Twitter in the context of 2019 European elections. *PLoS ONE, 15*(1). https://doi.org/10.1371/journal.pone.0227821

Twitter Safety. (2020, June 12). *Disclosing networks of state-linked information operations we've removed*. https://blog.twitter.com/en_us/topics/company/2020/information-operations-june-2020.html

KAZAKHSTAN

Introduction

Computational propaganda takes place in the context of tight political and Internet controls in Kazakhstan. Freedom House cited Kazakhstan as one of the countries experiencing the biggest decline in Internet freedoms this year, partly a result of the political upheaval in 2019 (Freedom House, 2019). Popular unrest was triggered by the resignation of President Nursultan Nazarbayev -- after 29 years in power -- in March 2019. An election in June 2019 confirmed his successor as Kassym-Jomart Tokayev, with over 70% of the vote. During this period many social media platforms were temporarily inaccessible, including Facebook, Instagram, and WhatsApp (Freedom House, 2019).

There is evidence of networks of fake accounts that promote the government online. They are commonly referred to as 'nurbots' (нурбот), after the ruling Nur Otan Party. Despite their prevalence, nurbots have "never gotten a lot of attention from either local or international media" (Kozhanova, 2019).

Disinformation is widespread, resulting in a team of journalists launching the first fact-checking organisation in Central Asia: Factcheck.kz. Their goal is to fight against unreliable information, information manipulation, and fake news. Factcheck.kz publishes in Kazakh, Russian and English, and translated articles were used for this report. Further evidence is drawn from a series of interviews with a former nurbot farm employee, released by the human rights media project The Analytical Center for Central Asia (ACCA). Expert consultations were also undertaken to confirm these findings, as in response to an ACCA article, Samat Nurtaza, one of the accused individuals of the Institute of Eurasian Integration, wrote a refutation on Facebook dismissing the article as "fake and misinformation" (ACCA, 2020b).

An Overview of Cyber Troop Activity in Kazakhstan

Organizational Form

Media companies controlled by the Ministry of Information incorporated positive messaging and trolling within their remit as early as 2013. Some of their social media accounts were traced to IP addresses located in government buildings. This led to an increase in operational security by government actors through distributed Internet modems to obfuscate their efforts.

There has been a shift towards outsourcing these capabilities, and there are now multiple organisations that allegedly run nurbot farms. The ACCA reports that the first farm appeared in response to claims about national security concerns, under Karim Masimov, the head of the National Security Committee (ACCA, 2020a). This would place the emergence of the first nurbot farm around approximately 2016-17. Previously, bot farms have been part of the Nur Otan Party, run by the youth wing of the party, Zhas Otan. Currently, it is claimed by the ACCA that there are bot farms linked to the National Security Committee, KazMedia (supervised by the president's adviser Erlan Karin), and the Institute of Eurasian Integration. The Institute of Eurasian Integration is supervised by Samat Nurtaza and Anuar Shotbai, both reported to be close to Erlan Karin, and it is reported that around 50 remote workers are coordinated from this Institute (ACCA, 2020c). Similarly, KazMedia has around 100 employees that each manage ten accounts on different social networks.

Factcheck.kz uncovered "a whole network of fake accounts that are used to promote official pages, state programmes, institutions and party initiatives" (Factcheck, 2019b). The

Factcheck.kz investigation uncovered links to a company called SMMNETWORK LLP and media agency Mir Press LLP, which are both well-funded according to the investigation. These media agencies manage and support the Facebook pages of the Foundation of the First President, the Nur Otan Party, and Facebook campaigns against exiled opposition politician Mukhtar Ablyazov. Activity on these Facebook pages is often exclusively created by nurbots.

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Kazakhstan

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
2013	National Security Committee,	Nur Otan Party, President Nursultan Nazerbayev, Karim Masimov	SMMNETWORK LLP, Mir Press LLP, Vision Pro LLP, KazMedia, Institute of Eurasian Integration	Zhas Otan (youth wing of Nur Otan)	

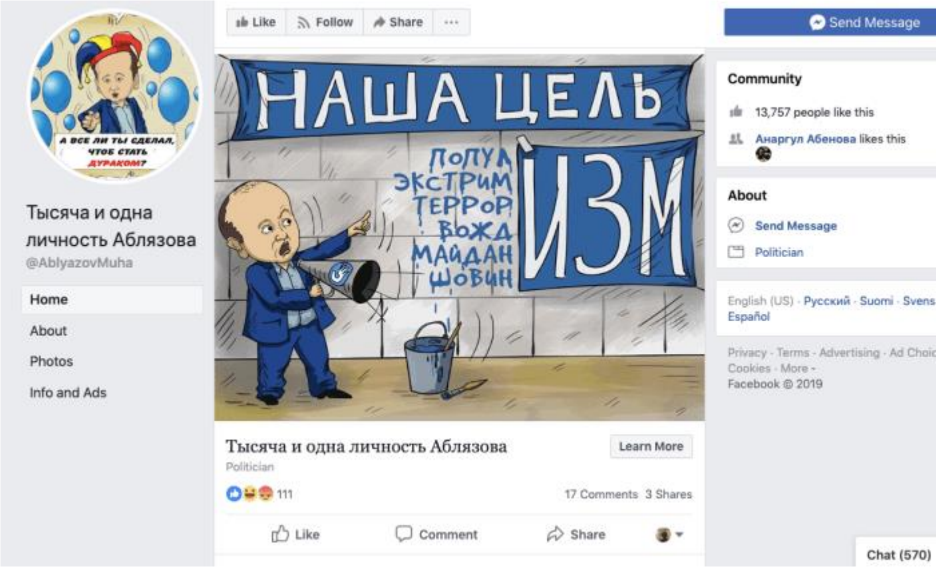
Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Fake accounts

It is claimed that nurbots are engaged in "state propaganda, aggravating the situation, [and] distracting attention" (ACCA, 2020a). The nurbots are run by humans, rather than automation, meaning that there are "practically no identical comments" as a "copywriter or a group of copywriters cooperate with bot handlers" (Factcheck, 2019b). They actively comment on Facebook and Instagram, targeting pages such as the page of the Nur Otan Party and the Foundation of the First President. Inorganic comments often blend in with the organic comments of the population, as many commenters on the Nur Otan Party page are not nurbots. However, the majority of comments are inorganic. After analysing dozens of posts on the page for the Foundation of the First President, Factcheck.kz found "only a few comments from live accounts". The nurbots also fill the comment sections on Kazakh news sites. For example, on a video of one of former Kazakh President Nursultan Nazaerbayev's public speeches, there were similar comments in support of the president (Kozhanova, 2019). An analysis of these nurbots in *The Diplomat* suggests that the purpose of the nurbots is to divert attention from crises (e.g. currency issues), strengthen images of success (e.g. praising sports stars) and praising Nazerbayev. Nurbots are increasingly expected to be present in the comments of many websites, and people often reply 'nurbot' to those who comment seemingly suspicious praise -- to discredit the legitimacy of the comment (Kozhanova, 2019).

Nurbots engage with the opposition party Democratic Choice of Kazakhstan (DCK). A dedicated Facebook page, 'Sushi Bolota' (Drain the Swamp) targets the DCK and its exiled leader Mukhtar Ablyazov. An example of an anti-Ablyazov page can be seen in figure 1. There is evidence of trolling, as nurbots often attack and insult people online (Factcheck, 2019b).



Тысяча и одна личность Аблязова
@AblyazovMuha

Community
13,757 people like this
Анаргул Абенова likes this

About
Send Message
Politician

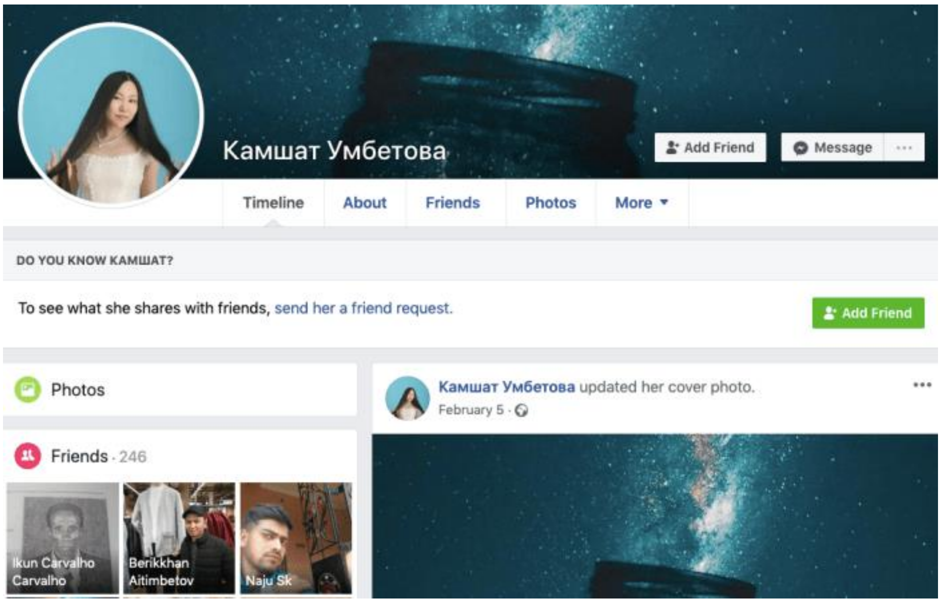
English (US) · Русский · Suomi · Svens
Español

Privacy · Terms · Advertising · Ad Choic
Cookies · More ·
Facebook © 2019

Тысяча и одна личность Аблязова
Politician
111
17 Comments 3 Shares

Figure 1: An anti-Ablyazov page (Factcheck, 2019b)

Nurbot accounts use profile pictures stolen from Turkic ethnic minorities in Russia, and Kyrgyz users of VKontakte, as their appearance resembles that of Kazakhs. A typical fake account, under the name Kamshat Umbetova, can be seen in Figure 2. It was noted by Kazakh experts that there are approximately 500,000 active Facebook users in Kazakhstan; meaning any accounts that are recently created, have little organic content, or a low number of mutual friends is treated with suspicion. Thus, the efficacy of these fake accounts is questioned.



Камшат Умбетова

DO YOU KNOW КАМШАТ?

To see what she shares with friends, send her a friend request.

Friends · 246

Ikun Carvalho Carvalho
Berikkhan Aitimbetov
Naju Sk

Камшат Умбетова updated her cover photo.
February 5

Figure 2: A Fake Facebook account (Factcheck, 2019b)

Fake accounts are acknowledged as a major issue in Kazakhstan. A member of the board of Kazakhstan's National Association of Professional Social Media Marketing, Kazybek Shaykh, said that "statistical data shows that such [fake] news is often spread through fake accounts" (Tengrinews.kz, 2019). Fake accounts have been set up in the name of leading Kazakh politicians. In April 2019, Prime Minister Askar Mamin's press office issued a statement saying that the Instagram account 'mamin_onlain' was fake, and urged users to only engage in the verified accounts of the Prime Minister on Facebook, VKontakte, Twitter, YouTube and Periscope (Sputnik, 2019). In response to consistent allegations of fake accounts, deputy chairman of the Nur Otan Party, Maulen Ashimbayev, said that the party did not use anonymous commentators or fake accounts to promote the party. However, he said that the party did encourage its members to be active on social media (Tengrinews.kz, 2019).

Fake accounts employ different strategies depending on the platform. Mass-reporting of content has proved successful on Instagram, which has resulted in livestreams being taken down -- suggesting that there is a high-level of coordination. Activist videos uploaded onto YouTube are often disliked. Telegram channels have hundreds of thousands of bots to inflate the number of members, and information is deliberately leaked through these channels to manipulate public opinion. There is also speculation that several Telegram channels are linked to Russia, evidenced by their use of Russian -- rather than Kazakh Russian -- as would be expected from a Kazakh channel.

Disinformation on Messaging Apps

The most prolific platform for manipulation is WhatsApp. This is due to the ubiquity of WhatsApp in Kazakhstan, the end-to-end encryption preventing fact-checking, and the familial networks that facilitate the fast dissemination of information. As trust in government institutions remains low, great trust is often placed in the secrecy and intimacy of WhatsApp groups among friends and family.

Two themes emerge from Factcheck.kz's debunking of disinformation on WhatsApp: fake stories often originate or spread to other Central Asian or Eurasian states; and stories are sometimes circulated so widely that institutions and officials are compelled to respond.

- In September 2018, a message spread through WhatsApp that reported that ISIS terrorists were pretending to be doctors and injecting people with a virus. This story originated in Russia, but the location of the headline was cropped out and it was spread in Kazakhstan (Factcheck, 2018a).
- A warning spread on WhatsApp about a "dangerous gang of paedophiles" luring children into their cars. This was debunked as fake, with the warning dating back to 2009 and having already been exposed as fake in Kazakhstan, Kyrgyzstan, Ukraine, Belarus and Russia (Factcheck, 2018b).
- A message claimed that "all means of communication are connected to government systems". Factcheck.kz determined that this first appeared in Russia in 2017, and had spread over Viber and WhatsApp across Ukraine, Kyrgyzstan and Kazakhstan. The Kazakh Interior Ministry was compelled to deny the rumours that control was tightening over social networks (Factcheck, 2019a).
- A message claimed that people who worked from 1991-2018 were receiving 560,000 tenge ($1,475) by the State Social Insurance Fund. The Fund's official website issued a statement denying this information (Factcheck, 2018c).
- In February 2020, ethnic clashes resulting in 10 deaths were reportedly spurred by rumours and videos on WhatsApp. Ethnic Kazakhs clashed with Dungans, a Muslim group of Chinese origin, in south-Eastern Kazakhstan. A video of three unarmed Dungans attacking Kazakh police was posted by witnesses and went viral on social media, including WhatsApp (Radio Free Europe, 2020). President Tokayev instructed security agencies to prosecute those sending hate speech, provocative rumours, and disinformation (BBC, 2020).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Kazakhstan

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Human, Fake	Pro-Government, Attacking Opposition, Distracting Messages, Trolling, Polarising	Comments on Kazakh news sites, Facebook and Instagram, Mass reporting of content	Facebook, Instagram, WhatsApp, Telegram, VKontakte

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

The Eurasian Institute for Integration receives state grants for research, which is then funnelled into the bot farms. Workers are alleged to receive a monthly salary of between 50-100 thousand tenge ($130-260) (ACCA, 2020a).

Table 3: Cyber Troop Capacity in Kazakhstan

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
~150				Low/Medium

Social media is used by the population to organise against the regime. This was seen during the demonstrations in 2019, with the use of the hashtags #qazaqkoktemi (Kazakh Spring) and #menoyandim (I've woken up). A movement called 'Wake Up, Qazaqstan' emerged, calling for democratic reforms (Lillis, 2019). The hashtag #уменяестьвыбор ('I have a choice') began circulating on social media, with students gathering and staging protests under the hashtag #seruen ('a walk') – as activists claimed they could not be detained for walking (Abdurasulov, 2019). Given the lack of funding, Amirzhan Kosanov, opposition candidate in the 2019 presidential election, used social media such as WhatsApp to organise his campaign and received a surprisingly high 16% of the vote. Given the potential power of social media for activism, it was reported that in December 2018 the government had purchased a $4.3 million automated tool to track political discontent on social media, using deep learning that detects content discrediting the regime (Freedom House, 2019).

References

Abdurasulov, A. (2019, June 7). The rare protests in a country that bans dissent. *BBC News*. https://www.bbc.com/news/world-asia-48545166

ACCA. (2020a, February 13). Who is behind the secret bot farms in Kazakhstan? *ACCA*. https://acca.media/en/who-is-behind-the-secret-bot-farms-in-kazakhstan/

ACCA. (2020b, February 21). Bot farms of Kazakhstan rebelled against ACCA. *ACCA*. https://acca.media/en/bot-farms-of-kazakhstan-rebelled-against-acca/

ACCA. (2020c, March 7). Bot farms in Kazakhstan (sequel). *ACCA*. https://acca.media/en/bot-farms-in-kazakhstan-sequel/

BBC. (2020, February 9). Ethnic clashes in Kazakhstan kill 10. *BBC News*. https://www.bbc.com/news/world-asia-51425938

Factcheck. (2018a, September 11). Фейк I Террористы ИГИЛ вводят вирус под видом врачей. *Factcheck.kz*. https://factcheck.kz/health/fejk-%ce%b9-terroristy-igil-vvodyat-virus-pod-vidom-vrachej/

Factcheck. (2018b, September 28). Зомби-фейк | Рассылка-предупреждение о банде педофилов. *Factcheck.kz*. https://factcheck.kz/glavnoe/zombi-fejk-rassylka-preduprezhdenie-o-bande-pedofilov/

Factcheck. (2018c, November 19). Фейк I Выдача ГФСС пособий в размере 560000 тг. *Factcheck.kz*. https://factcheck.kz/glavnoe/fejk-%ce%b9-vydacha-gfss-posobij-v-razmere-560000-tg/

Factcheck. (2019a, January 15). Фейк | Все средства связи подключаются к правительственным системам слежки. *Factcheck.kz*. https://factcheck.kz/glavnoe/fejk-vse-sredstva-svyazi-podklyuchayutsya-k-pravitelstvennym-sistemam-slezhki/

Factcheck. (2019b, April 2). Ферма вождя: Кто управляет нурботами и нурняшками. *Factcheck.kz*. https://factcheck.kz/glavnoe/ferma-vozhdya-kto-upravlyaet-nurbotami-i-nurnyashkami/

Freedom House. (2019). *Freedom on the Net | Kazakhstan*. Freedom House. https://freedomhouse.org/country/kazakhstan/freedom-net/2019

Kozhanova, N. (2019, February 20). *Finding Kazakhstan's Troll Farms*. The Diplomat. https://thediplomat.com/2019/02/finding-kazakhstans-troll-farms/

Lillis, J. (2019, June 10). Nazarbayev ally wins big in Kazakhstan election after hundreds arrested. *The Guardian*. https://www.theguardian.com/world/2019/jun/09/hundreds-arrested-as-kazakhs-protest-against-rigged-election

Radio Free Europe. (2020). *Kazakh Police Arrest Ethnic Dungan Brothers Blamed For Sparking Deadly Clashes*. RadioFreeEurope/RadioLiberty. https://www.rferl.org/a/kazakh-police-arrest-ethnic-dungan-brothers-blamed-for-sparking-deadly-clashes/30441254.html

Sputnik. (2019, April 2). *Аккаунт казахстанского премьера в Instagram оказался поддельным*. https://ru.sputniknews.kz/politics/20190402/9722803/askar-mamin-instagram-akkaunt-feik.html

Tengrinews.kz. (2019, March 15). *Fake news: Для чего нужна информационная гигиена*. https://tengrinews.kz/kazakhstan_news/fake-news-dlya-chego-nujna-informatsionnaya-gigiena-365111/

KENYA

Introduction

While Kenya is officially a democratic country it continues to struggle with corruption and police brutality and is considered only partly free by Freedom House (Freedom House, 2019a). Nevertheless, the country has a vibrant media landscape, though concerns about costs, speed and quality of internet access remain prevalent (Freedom House, 2019b). Kenya has seen its fair share of fake news and misinformation campaigns during the 2017 presidential election where opposing parties hired bloggers, social media influencers, and political consulting companies to support online campaign efforts with their social media insights (Nyabola, 2019). Moreover, Kenya has been struggling with Twitter bots (Muli, 2019), which had quite significant influence on online discourse with 25% influence during the August 2017 election and 28% influence during the rerun of the election in October 2017 (Freedom House, 2018b). Notably, it appears that many of the influential voices on Twitter during the election were located not only outside of Kenya, but outside Africa entirely (Mbah, 2018). Generally, this election was characterized as the Kenyan election most affected by fake news (Dahir, 2017).

In terms of access, while a majority of Kenyans have phone subscriptions (Freedom House (2019b) found a subscription penetration rate of 100.1% in late 2018) and access to the Internet, there is still a gender and urban/rural divide. Facebook and WhatsApp continue to be the most popular platforms used (Elliott, 2017). In general, Kenya does not filter or block Internet access, however, the government does regularly remove content or requests for content to be removed from platforms such as Facebook (Freedom House, 2019b). During the COVID-19 pandemic, WhatsApp has become a breeding ground for harmful misinformation about the virus. It seems the Kenyan government has been struggling to curb the spread of fake information and news and is now hoping for a technical solution from Facebook (which owns WhatsApp) (Ngila, 2020) and relying on volunteers and activists to debunk false claims (Smith, 2020).

An Overview of Cyber Troop Activity in Kenya

Organizational Form

During the general elections in 2017 both main parties (the ruling Jubilee Party and the main opposition party Orange Democratic Movement (ODM)) reportedly used bots and fake accounts or bloggers on Facebook (Mayoyo, 2017), with Jubilee, for example, hiring Cambridge Analytica. News websites, including Foreign Policy Journal (fp-news.com) and CNN Channel 1 (cnnchannel1.com), were set up to spread fake news during the election. The sites' branding resembles official international media outlets (Nyabola, 2019). The ruling Jubilee party had been engaging in online influence operations as early as 2015, when reports surfaced that they hired a group known as '36 bloggers' to polish the crumbling image of the government at the time (Kenya Today, 2015).

Kenya's government has also become an avid surveillant of its citizens' communication in recent years (Freedom House, 2019a). Several state actors carry out surveillance essentially free from any judicial oversight. The main intelligence agency is the National Intelligence Service (NIS), which is responsible for both national security and foreign intelligence. The NIS has direct access to Kenya's telecommunication network and Internet providers. In addition to the activities of the NIS the Kenyan police services also have a surveillance mandate, allowing them to collect information about serious crimes, including cybercrime. In 2012 the Kenyan Communication Commission (a state-owned corporation) announced the establishment of a system allowing authorities to monitor incoming and outgoing digital communication. All

Internet service providers were requested to cooperate as the Commission deemed this step necessary due to a continued rise in cybercrime (Privacy International, 2017). In late 2016 the Communication Authority (CA) (the governmental regulatory body of Kenya's communication sector) finalized a contract with a private Israeli web intelligence company webintPro to use their software in future projects (Rubinstein, 2019). There remains some hope for privacy, as the High Court of Kenya ruled a Device Management System to access mobile subscriber data directly unconstitutional in April 2018 (High Court of Kenya, 2018).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Kenya

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
	Military/ Intelligence	Jubilee ODM	PR/Social media insight companies		Bloggers

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

According to a GeoPoll survey conducted in May 2017, 90% of Kenyans reported they had encountered false information regarding the 2017 election, 87% of whom reported the information as deliberately false. Social media consistently ranked lower than mainstream media on trust (Elliott, 2017). On Twitter, content was spread with two core hashtags: #ElectionsKE and #ElectionsKE2017. Social media has been used in a quite strategic manner by Kenyan politicians, who have used both social media influencers with large followings as well as bots to amplify their messages and trend hashtags (BBC News, 2017; Otieno, 2019; Wright, 2018).

In general, it seems Kenya is not working on psyops operations fighting propaganda as other African countries (e.g. Nigeria) allegedly are, with such operations having become more widespread to fight IS and Al-Shabaab (Anzalone, 2020; Mutambo, 2019). The only information controlling measures the Kenyan military and intelligence have been accused of are spying on journalists, political actors and activists as well as pressuring them in an effort to control public news narratives at times (Freedom House, 2018b). It appears that the authorities' standard strategy for dealing with news agencies or activists posting information or organizing events which do not sit well with the government is to accuse them of spreading hate speech, rumours and propaganda.

In light of the government's tendency to accuse activists or news organizations of spreading rumours and propaganda, several groups, including Freedom House and the New York-based Committee to Protect Journalists, have criticized the Computer Misuse and Cybercrime Act which passed into legislation in May 2018 for repressing online liberties even further (Freedom House, 2018a). The act imposes up to 10 years of prison and hefty fines for the publication of "false" or "fictitious" information that results in "panic" or is "likely to discredit the reputation of a person" ("Kenya President Signs Controversial Social Media Bill into Law", 2018). In June 2018, the Bloggers Association of Kenya successfully petitioned some of the provisions of the law, which was suspended while awaiting further decision by the High Court of Kenya. On 20 February 2020 the Court declared the law constitutional (Itimu, 2020).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Kenya

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Human Bots	Support Attacking Opposition Suppression	Disinformation Trolls	Twitter WhatsApp Facebook

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

It seems most of the activities surrounding the latest election ceased after the election was done, but their effects continue; elections are becoming more and more expensive as candidates are no longer just politicians but brands that are carefully managed by growing online campaign teams. Such "brand-management" continues outside of election cycles through, for example, Twitter profiles. In terms of resources, the Jubilee party reportedly spent $6m on Cambridge Analytica during the 2017 election, with Kenyan politicians spending an average of $50m on their campaigns (though it is unclear how much of that would be spent on online influence campaigns) (Nyabola, 2019).

Table 3: Cyber Troop Capacity in Kenya

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
	$6 Mio.	Temporary	Liminal	

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

References

Anzalone, C. (2020). Addressing the Enemy: Al-Shabaab's PSYOPS Media Warfare. *CTCSENTINEL*, *13*(3). https://ctc.usma.edu/wp-content/uploads/2020/03/CTC-SENTINEL-032020.pdf

BBC News. (2017, June 26). Kenya's election: Your questions answered. *BBC News*. https://www.bbc.com/news/world-africa-39810869

Constitutional Petition In the matter of the Legal and Constitutional validity of the Governments' decision through the Communications Authority of Kenya to secretly acquire capability for spying on the population by tapping the networks of Mobile Phone providers, No. 53 (High Court of Kenya April 19, 2018). https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2018/05/KENYA-JUDGMENT-ON-RIGHT-TO-PRIVACY-DEVICE-MANAGEMENT-SYSTEM.pdf

Dahir, A. L. (2017, June 25). Raila Odinga and Uhuru Kenyatta are being hit by fake news in Kenya's election campaign—Quartz Africa. *Quartz Africa*. https://qz.com/africa/1011989/fake-news-and-misinformation-are-upstaging-kenyas-upcoming-high-stakes-election/

Elliott, R. (2017, July 18). GeoPoll and Portland launch a Survey Report on Fake News in Kenya. *GeoPoll*. https://www.geopoll.com/blog/geopoll-and-portland-launch-a-survey-report-on-fake-news-in-kenya/

Freedom House. (2018a). Kenya: Cybercrimes Law Restricts Media Freedom. *Freedom House*. https://freedomhouse.org/article/kenya-cybercrimes-law-restricts-media-freedom

Freedom House. (2019a). *Freedom House Report 2019 | Kenya*. https://freedomhouse.org/country/kenya/freedom-world/2020

Freedom House. (2019b). *Freedom On the Net 2019 | Kenya*. https://freedomhouse.org/country/kenya/freedom-net/2019

Freedom House. (2018b). *Freedom on the Net: Kenya*. https://freedomhouse.org/report/freedom-net/2018/kenya

Itimu, K. (2020, February 20). High Court Declares the Computer Misuse and Cybercrimes Law "Constitutional." *Techweez*. https://techweez.com/2020/02/20/court-declares-computer-and-cybercrimes-law-constitutional/

Kenya President signs controversial social media bill into law. (2018, May 15). *Premium Times Nigeria*. https://www.premiumtimesng.com/foreign/africa/268656-kenya-president-signs-controversial-social-media-bill-into-law.html

Kenya Today. (2015, October 26). Government's 36 bloggers FINALLY report to work today. *Kenya Today*. https://www.kenya-today.com/news/governments-36-bloggers-finally-report-to-work-today

Mayoyo, P. (2017, April 21). Fake news by bloggers could mess 2017 elections. *The Standard*. https://www.standardmedia.co.ke/business/article/2001237115/fake-news-by-bloggers-could-mess-2017-elections

Mbah, F. (2018, July 18). How the diaspora influenced 2017's elections in Africa: Report. *Al Jazeera*. https://www.aljazeera.com/news/2018/07/diaspora-influenced-2017-elections-africa-report-180717185153249.html

Muli, F. (2019, December 3). Kenyans On Twitter Lose Followers As Company Suspends Thousands Of Accounts. *KahawaTungu*. https://www.kahawatungu.com/kenyans-twitter-lose-followers-suspends-accounts/

Mutambo, A. (2019, July 2). Kenya joins coalition against Isis. *Daily Nation.* https://www.nation.co.ke/news/Kenya-joins-coalition-against-Isis/1056-4971788-mmlsmsz/index.html

Ngila, F. (2020, April 23). WhatsApp chats targeted in bid to stop fake news. *Daily Nation*. https://www.nation.co.ke/health/WhatsApp-chats-targeted-in-bid-to-stop-fake-news/3476990-5531362-kxxix6z/index.html

Nyabola, N. (2019, February 15). The spectre of Cambridge Analytica still haunts African elections. *Aljazeera*. https://www.aljazeera.com/indepth/opinion/nigerian-elections-money-190215080009476.html

Otieno. (2019, September 7). Rise of online campaign platforms tests Kenya's anti-hate watchdogs. *The East African*. https://www.theeastafrican.co.ke/tea/news/east-africa/rise-of-online-campaign-platforms-tests-kenya-s-anti-hate-watchdogs-1426684

Privacy International. (2017). *Track, Capture, Kill: Inside Communications Surveillance and Counterterrorism in Kenya*. https://privacyinternational.org/sites/default/files/2017-10/track_capture_final.pdf

Rubinstein, A. (2019, February 14). How Israeli Spies Meddle in Elections and Hack Activists with Impunity. *MintPress News*. https://www.mintpressnews.com/how-israel-spies-meddle-in-elections-and-hack-activists-with-impunity/255099/

Smith, G. (2020, April 25). Stamping out misinformation in Kenya's COVID-19 fight. *Al Jazeera*. https://www.aljazeera.com/news/2020/04/stamping-misinformation-kenya-covid-19-fight-200424195805081.html

Wright, G. (2018). *Kenya: Data and Digital Election Campaigning*. Tachtical Tech. https://ourdataourselves.tacticaltech.org/posts/overview-kenya/

KUWAIT

Introduction

Kuwait operates a hybrid governance structure, with a constitutional emirate working alongside a semi-democratic political system (Selvik, 2011). Executive power lies with the Sabah family monarchy which appoints the cabinet of ministers. The prime minister is appointed by the emir, but the elected parliament is still able to challenge the government (Freedom House, 2020). However, political parties are banned in Kuwait, which has prevented the formation of a coherent political opposition (MacDonald, 2020).

Kuwait is the only Arab State in the Arabian Gulf to be labelled "partly free" by Freedom House (Freedom House, 2020). However, it is important to note that recently Kuwait has been increasingly constraining freedoms of speech and assembly (Freedom House, 2020). Media freedom is limited within Kuwait, and legislation penalises critics of the emir, Islam or calls for the removal of the Sabah monarchy (BBC News, 2020; Freedom House, 2020). There are also legal penalties for spreading particular information online. Aisha al-Rasheed, a well-known journalist in Kuwait, was detained for social media postings where she criticised government corruption (Freedom House, 2020).

In September 2020 Sheikh Nawaf took over as emir, following the death of his half-brother Sheikh Sabah al-Ahmed al-Jaber al-Sabah. Sheikh Nawaf has ascended to power during a time when Kuwait is struggling to manage its budget deficit, given the recent fall in oil prices and the COVID-19 pandemic (MacDonald, 2020).

An Overview of Cyber Troop Activity in Kuwait

Organizational Form

Cyber troops are called "electronic flies" by Kuwaiti media, rather than bots, as officials claim that all bots in Kuwait were eliminated three years ago (Al-Qabas, 2019b). One example of a campaign by the "electronic flies" spread rumours that Kuwait was insisting Egyptian workers return to Egypt, even covering the travel and quarantine expenses for these workers. The campaign sought to build on pre-existing anti-immigrant sentiment in Kuwait, which has heightened during the pandemic (Sabr, 2020).

Inauthentic social media campaigns are both the result of, and contributing to, Kuwait's political instability. Kuwaiti media advisor Ahmed al-Eissa claimed that inauthentic Twitter campaigns were a prominent factor in the 2011 protests which led to the dissolution of parliament, and the frequent government reshuffles and parliamentary elections in the following years (Al-Rai, 2019; Freedom House, 2020). Political figures are said to be responsible for inciting social media campaigns to achieve particular political agendas. One example of this was the prevalence of Twitter campaigns after two ministers, Sheikh Mohammed al-Abdullah (Minister of State for Cabinet Affairs, formerly minister of information and minister of health) and Sheikh Suleiman al-Homoud (former minister of information and former minister of state for youth and sports) were questioned in parliament (Al-Qabas, 2019b). Reports claim that these campaigns contributed significantly to their subsequent dismissal (Al-Qabas, 2019b).

In another example, the website of Kuwaiti newspaper Al-Qabas outlines ten issues it claims have attracted the most bots and inauthentic users online (Al-Qabas, 2019b). One such issue is the topic of early retirement, which it claims was at the centre of a Twitter campaign seeking to put pressure on government and parliamentary factions to amend existing retirement legislation (Al-Qabas, 2019b). While it is difficult to directly link these campaigns to politicians, it appears that political actors are engaging in the propagation of social media campaigns to achieve political agendas.

The Kuwaiti government has been accused by MPs of supporting inauthentic social media accounts that seek to provoke and attack other nation-states, weakening formerly relations with these states (Masr al-Arabia, 2019). MP Al-Hamidi al-Subai claimed that the government supports the actions of these inauthentic accounts (Masr al-Arabia, 2019). Subai further asserted that the person operating the Twitter account Al-Majlis, which reports on parliamentary news, is known to and protected by the interior ministry. He accused the account of inciting sedition (Masr al-Arabia, 2019).

Political actors are also increasingly making use of media teams and private companies to conduct their online campaigns, leading to an increasingly professionalised computational propaganda industry within Kuwait (Al-Qabas, 2019b). Politicians will often employ media teams, which operate over 250 accounts. These accounts are used to ensure particular hashtags are on social media trending lists (Al-Qabas, 2019b). Fake social media pages run by foreigners are often employed by MPs and ministers to defame opponents (Masr al-Arabia, 2019).

Finally, influencers are also actively spreading misinformation within Kuwait. Influencer Fouz al-Fahad was investigated by Kuwaiti authorities for promoting an unlicenced COVID-19 test on Snapchat (Al Arabiya, 2020). Alongside these misinformation accusations, a number of Kuwaiti influencers have also been accused of operating an online money laundering scheme (MENAbytes, 2020).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Kuwait

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
	Evidence found	Evidence found	Evidence found	Muslim Brotherhood and Hezbollah	Evidence found

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

As noted previously, much of the computational propaganda in Kuwait is targeted at particularly controversial political topics, such as Egyptian migrant workers. Another targeted topic is the "Bidun issue", which involves calling on government to pardon citizen's loans (Al-Rai, 2019). Reports claim that bots are used to target these issues, ensuring that particular hashtags are trending and artificially generating engagement and awareness of these issues (Al-Rai, 2019). There appears to be a significant amount of artificial engagement on Twitter surrounding this issue, with one identified bot account tweeting "over 3,000 tweets in just 18 days, with a rate of 166 tweets per day, i.e. about 10 tweets per hour" on the Bidun issue (Al-Rai, 2019).

This illustrates the use of artificial amplification through hashtag targeting, one of the most commonly used strategies by Kuwait cyber troops. Bot accounts are used to amplify a hashtag focussed on, for example, defaming a political opponent or insulting a nation-state (Al-Qabas, 2016a). As was illustrated in the Egyptian migrant worker case, these hashtags may increase the spread of messages designed to “incite sedition” between Kuwait and Egypt (Sabr, 2020). Inauthentic social media accounts are used to “settle personal and political scores”, even using blackmail against influential officials and ministers (Al Jazeera, 2019). News-focussed Facebook pages are also used to spread misinformation. One such post incorrectly reported the death of the emir (Facebook, 2017).

The increasing use of bot accounts to spread politically-charged misinformation has created a large market for these bot accounts within Kuwait (Al-Qabas, 2016b). Tareq al-Mulla, professor of information technology at Kuwait University, is quoted stating that within Kuwait there is a large market for accounts with large followings on Twitter, YouTube, SoundCloud and even accounts with large numbers of professional connections on LinkedIn (Al-Qabas, 2016b).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Kuwait

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Inauthentic human accounts and bot accounts	Inauthentic amplification, attacking opposition	Disinformation, amplification	Facebook, Twitter, YouTube, SoundCloud, LinkedIn

Source: Authors’ evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

While there is no public data on the numbers of people or accounts used by Kuwaiti politicians and government to operate computational propaganda campaigns, as was noted previously, political actors often employ media teams which operate over 250 accounts (Al-Qabas, 2019b). Furthermore, the department of cyber-crime in Kuwait reported in January 2019 that it had shut down hundreds of bot accounts, mostly on Twitter (Al-Qabas, 2019a). The department also recorded a further 2,000 cases of online libel, slander, blackmail and impersonation between January and October 2018 (Al-Qabas, 2019a).

Table 3: Cyber Troop Capacity in Kuwait

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
Up to 250 accounts per politician		Temporary issue-based	No evidence	Medium

References

Al Arabiya. (2020, March 26). Kuwait investigates influencer over promoting 'Covid-19 test’. *Al Arabiya*. https://monitoring.bbc.co.uk/product/c201khdy

Al Jazeera. (2019, November 14). مواقع التواصل الاجتماعي في الكويت.. ثروات وتصفية حسابات. *Al Jazeera*.

Al-Qabas. (2016a, March 27). الحسابات الوهمية على مواقع التواصل.. سوق رائجة. *Al-Qabas*. https://alqabas.com/article/8145

Al-Qabas. (2016b, March 27). الحسابات الوهمية على مواقع التواصل.. سوق رائجة. *Al-Qabas*. https://alqabas.com/article/8145

Al-Qabas. (2019a, January 8). الحسابات الوهمية».. معول هدم بيد مثيري الفتن». *Al-Qabas*. https://alqabas.com/article/623636

Al-Qabas. (2019b, January 23). قضايا جذبت الذباب الإلكتروني 10. *Al-Qabas*. https://alqabas.com/article/628900

Al-Rai. (2019, November 3). «أحمد عيسى: حسابات وهمية على «تويتر» تُضخّم قضية «البدون». *Al-Rai*. https://www.alraimedia.com/Home/Details?id=8abeb6d9-be0b-4e72-ace2-a2089dd19da1

BBC News. (2020, October 1). Kuwait country profile. *BBC News*. https://www.bbc.co.uk/news/world-middle-east-14644252

Facebook. (2017, April 22). اخبار كاذبة: نشرت عدة صفحات اخبار غير صحيحة او ما يسمى كذبة نيسان هدفها التلاعب بمشاعر المتابعين. https://www.facebook.com/algrbiaalhadath/posts/791389034373932/

Freedom House. (2020). *Kuwait*. Freedom House. https://freedomhouse.org/country/kuwait/freedom-world/2020

MacDonald, F. (2020, September 30). New Kuwait Emir Takes Over Economy Constrained by Politics. *Bloomberg.Com*. https://www.bloomberg.com/news/articles/2020-09-30/kuwait-s-new-emir-takes-over-an-economy-paralyzed-by-politics

Masr al-Arabia. (2019, January 9). بسبب الحسابات الوهمية.. أزمة جديدة بين الحكومة والنواب بالكويت. *Masr Al-Arabia*.

MENAbytes. (2020, July 28). *Kuwaiti ecommerce platform Boutiqaat under investigation for money laundering, public prosecutor orders freeze on bank accounts*. KrASIA. https://kr-asia.com/kuwaiti-ecommerce-platform-boutiqaat-under-investigation-for-money-laundering-public-prosecutor-orders-freeze-on-bank-accounts

Sabr. (2020, May 1). المحامي العبدالله: مانسب من تصريحات لغصون الخالد حول وجود رسالة للرئيس المصري غير صحيح وسنقاضي أصحاب الحسابات. *Sabr*. https://www.sabr.cc/2020/05/02/440153/

Selvik, K. (2011). Elite Rivalry in a Semi-Democracy: The Kuwaiti Press Scene. *Middle Eastern Studies*, *47*(3), 477–496.

KYRGYZSTAN

Introduction

Attempts to manipulate public debates and control the flow of online information are reported in Kyrgyzstan, where freedom of expression and the degree of press freedom is greater than in other Central Asian states (Rysaliev et al., 2012). Anonymous fake commentators are reported as the most widespread form of computational propaganda. According to Yulia Barabina, who leads the press office of former presidential candidate Jenishbek Nazaraliev, anonymous online posts are triggered by political events such as elections and disputes—a tactic which is used by the government as well as other political parties (Rysaliev et al., 2012). Alongside domestic manipulation, Kyrgyzstan has been the target of foreign influence operations. In January 2019, Facebook removed a network of accounts that originated in Russia and targeted Central Asian states including Kyrgyzstan (Gleicher, 2019).

Censorship and attempts to control the Internet have increased following the government's fight against extremism (Freedom House, 2019). Most recently, in response to the prevalence of fake social media accounts, the Kyrgyz parliament adopted a new law 'On Manipulating Information' on 25 June 2020. This is part of a series of legislation proposed by the government in response to the coronavirus pandemic. The aim of the law is to address false and inaccurate information spreading online. Internet users would have to make their identity clear when using social media platforms, and the creation of anonymous accounts may be treated as a criminal offence. The civil society organisation Article 19 (2020) has cautioned that it contains vague and overboard terms, giving authorities the power to block Internet sites and shut down social media accounts.

This law could stifle Kyrgyzstan's nascent investigative journalism community, which is most active online and on social media (Simpson, 2020). Investigative journalist outlets are subject to harassment, physical attacks and cyber-attacks (Reporters Without Borders, 2020). Bolot Temirov, the founder and chief editor of Kyrgyz website Factcheck (Factcheck.kg), was assaulted by three men in January 2020. This comes after Factcheck and other websites had reported on the corruption scandal around the influential former customs official Raimbek Matraimov, leading to the suggestion that the assault was in response to Temirov's investigative work (CPJ, 2020).

An Overview of Cyber Troop Activity in Kyrgyzstan

Organizational Form

Cyber troop activity is reported to originate from both the government and opposition parties. The earliest reports of the use of trolls were the linked to the 2010 parliamentary elections in which "trolls for virtually all the main players were visible on many Russian- and Kyrgyz-language websites" according to Yulia Barabina. Temirov claims that "we have the teams of the ex-president and current president actively opposing [each other] in cyberspace" including the use of creating "fake reports" (Центр-1, 2018). Factcheck's research found in July 2018 that a small-scale network of fake accounts on Facebook supported President Sooronbay Jeenbekov, alongside another network supporting his rival, the former President Almazbek Atambayev (Freedom House, 2019).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Kyrgyzstan

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
2010	X	President Sooronbay Jeenbekov, former President Almazbek Atambayev			Freelance trolls

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Fake Accounts

According to Azattyk (the Kyrgyz service of Radio Liberty), Kyrgyz activists have noted that fake accounts spreading false information are active in the country. Human rights activist Aziza Abdirasulova said that websites and social networks should be more stringent in stopping accounts without a name or photo from registering (Азаттык, 2018). It is alleged that these anonymous accounts not only respond to existing news, but help set the agenda by leaking stories to the media (Rysaliev et al., 2012). Anonymous, fake accounts respond to criticism online—an investigation into a corruption scandal surrounding the Matraimov family prompted an "army of trolls and fake accounts" coming to their defence on social media (Kaktus, 2019). In response to this problem, one of the country's most popular forums, Diesel, has imposed a month-long waiting period for each new user. An MP for the Social Democratic Party of Kyrgyzstan, Asilbek Zheenbekov, suggested monitoring social networks to combat anonymous, fake accounts which disseminate false information during election campaigns (Кабар, 2018).

Disinformation

In response to the circulation of disinformation in Kyrgyzstan, Factcheck was set up to debunk online rumours (Центр-1, 2018). The organisation's chief editor Bolot Temirov says he receives five to six fake reports a day, some originating on WhatsApp and other messaging apps. Government ministries also intervene to correct mis- and disinformation. A message spreading on WhatsApp claimed that the Ministry of Labour and Social Development was handing out 70,000 soms [US$1,000] to people who worked between 1991-2018. This was denied by the ministry in an official statement (Мокренко, 2018). The Ministry of Internal Affairs (2018) also issued a statement warning against anonymous posts from Telegraph (telegra.ph), which circulated deliberately false information targeting government and law enforcement officials.

Polarization

Freedom House (2019) suggested that Internet users self-censor on issues concerning ethnic relations, as online forums are strictly moderated to limit hateful content. Interethnic relations in the South are a sensitive matter as that region is where the majority of the country's Uzbek minority lives. A court in Batken sentenced a man to four years in prison for inciting ethnic hatred on WhatsApp after circulating a video of a fight between "two different ethnic groups" and calling for the "elimination of an ethnic minority" in the region (RFE/RL, 2019).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Kyrgyzstan

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Fake, Human	Pro-government messaging, attacks on opposition, trolling	Disinformation, Trolls	WhatsApp, Facebook

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

Analysts believe there are "probably only 25 to 30 people acting as trolls for the government". Sergei Makarov, found of the New Media Institute, said trolls are typically freelancers in their late twenties, work as journalists, lawyers, economists or in business, are educated and politically aware, and charge $200-700 for an online campaign (Rysaliev et al., 2012).

Table 3: Cyber Troop Capacity in Kyrgyzstan

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
25-30				Low

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

References

Article 19. (2020, July 3). *Kyrgyzstan: Law "On Manipulating Information" must be vetoed*. ARTICLE 19. https://www.article19.org/resources/kyrgyzstan-law-on-manipulating-information-must-be-vetoed/

CPJ. (2020, January 9). Investigative journalist Bolot Temirov assaulted in Kyrgyzstan—Committee to Protect Journalists. *Committee to Protect Journalists*. https://cpj.org/2020/01/investigative-journalist-bolot-temirov-assaulted-i/

Freedom House. (2019). *Freedom on the Net | Kyrgyzstan*. Freedom House. https://freedomhouse.org/country/kyrgyzstan/freedom-net/2019

Gleicher, N. (2019, January 17). Removing Coordinated Inauthentic Behavior from Russia. *About Facebook*. https://about.fb.com/news/2019/01/removing-cib-from-russia/

Kaktus. (2019, June 24). В соцсетях в защиту Матраимовых заработала армия троллей и фейковых аккаунтов. Фактчек. *Кактус*. https://kaktus.media/doc/393387_v_socsetiah_v_zashity_matraimovyh_zarabotala_armiia_trolley_i_feykovyh_akkayntov._faktchek.html

Ministry of Internal Affairs. (2018, December 29). *МВД опровергает распространяемую в социальных сетях ложную и дискредитирующую информацию*. https://mvd.gov.kg/index.php/rus/mass-media/all-news/item/8624-mvd-oprovergaet-rasprostranyaemuyu-v-sotsialnykh-setyakh-lozhnuyu-i-diskreditiruyushchuyu-informatsiyu

Reporters Without Borders. (2020). *Kyrgyzstan | RSF*. Reporters Without Borders. https://rsf.org/en/kyrgyzstan

RFE/RL. (2019, February 7). *Kyrgyz Court Jails Man For Using WhatsApp To 'Incite Ethnic Hatred'*. RadioFreeEurope/RadioLiberty. https://www.rferl.org/a/kyrgyz-court-jails-man-for-using-whatsapp-to-incite-ethnic-hatred-/29757536.html

Rysaliev, A., Tokbaeva, D., & Olimova, L. (2012, February 12). *Central Asia's 'Troll Wars'*. Institute for War and Peace Reporting. https://iwpr.net/global-voices/central-asias-troll-wars

Simpson, N. (2020, July 8). *Fake News, Real Censorship: A New Bill Threatens Freedom of Speech in Kyrgyzstan*. Foreign Policy Research Institute. https://www.fpri.org/article/2020/07/fake-news-real-censorship-a-new-bill-threatens-freedom-of-speech-in-kyrgyzstan/

Азаттык. (2018, April 16). В КР активизировались фейк-аккаунты? *Радио Азаттык (Кыргызская служба Радио Свободная Европа/Радио Свобода)*. https://rus.azattyk.org/a/kyrgyzstan-social-media-fake/29169794.html

Кабар. (2018, February 17). ИАЦ 'Кабар': Контроль социальных сетей – борьба с фейковыми новостями. *Информационное Агентство Кабар*. http://kabar.kg/news/kontrol-sotcial-nykh-setei-bor-ba-s-feikovymi-novostiami/

Мокренко, А. (2018, December 6). *Очередной фейк. В WhatsApp распространяют информацию о пособии от Минтруда*. 24.kg. https://24.kg/obschestvo/103230_ocherednoy_feyk_vWhatsApp_rasprostranyayut_informatsiyu_oposobii_otmintruda/

Центр-1. (2018, July 13). «Фейковые» новости в современном мире – оружие массового психоза?.. *Центр-1 / Centre1.com - Новости*. https://centre1.com/kyrgyzstan/fejkovye-novosti-v-sovremennom-mire-oruzhie-massovogo-psihoza/

Lebanon

Introduction

Lebanon is considered a partly-free country by the Freedom House report. Lebanon has been shaped by sectarian politics and feuds since before its independence from the French mandate in 1943 (Freedom House, 2019). Lebanon has extremely diverse religious demographics, with substantial followers of the Druze faith, Christians of various denominations, and Muslims of both Sunni and Shia Islam. These differences play an integral role in the country's politics (Central Intelligence Agency, 2020).

Lebanon's divided political landscape is in turn strongly reflected in the country's media landscape. With the combination of an absence of media regulation and the concentration of political and economic power within the hands of a small number of families, media outlets are strongly aligned with particular ethno-religious sects, political parties, and prominent individuals. Almost 80% of the most influential media outlets in the country are directly owned by political parties, members of parliament, parliamentary candidates, and even the state itself (Reporters Without Borders, 2018). These outlets represent the majority of TV viewership, print readership, and radio listenership. In the past decade this media landscape has come to be replicated in the online world, resulting in the ownership of many high-profile online news platforms by political actors (Ibid). For these reasons there is a general lack of trust in mainstream media, and social media platforms such as Facebook and WhatsApp have become the primary sources of information for many Lebanese citizens (Lewis, 2019).

The general state of online freedom in Lebanon remains fairly unstable and unpredictable. In January 2019, Lebanon's Telecommunications Minister allegedly ordered the country's telecom operators to block Grindr, a popular dating platform for the LGBT+ community. Additionally, in December 2018 the courts decided to block the Israeli-based hosting platform Wix, on the grounds that it violates the Israel Boycott Law of 1963, a move which caused financial problems for Lebanese businesses that were hosted on the platform (Freedom House, 2019).

Since early 2017, the capacity for online freedom of expression began to severely deteriorate. The Lebanese Cybercrime Bureau has increasingly approached and pressured social media users to apologize and delete their posts. While most users are unharmed, other users have found themselves detained and interrogated for publishing content that criticizes the government or religious authorities in the country. In March 2019, a journalist was sentenced to three months in jail for a post he posted on Facebook that criticized the arrest of a Syrian tattoo artist. Another journalist was sentenced, in absentia, to four months in prison for a Facebook post that criticized the president (Freedom House, 2019)

This year, Lebanon's politics were impacted by three main events: (1) a series of mass civil demonstrations that erupted in October 2019, triggered by planned taxes on various goods, including online phone calls through apps like WhatsApp; (2) the August 2020 Beirut port blast that killed over 178 people, left 6,500 injured and 300,000 people homeless; and (3) the spread of the coronavirus pandemic. The demonstrations were seemingly non-sectarian, which in effect united the citizens around a shared cause and threatened those in power. Meanwhile, the Beirut Port blast left a vast number of Lebanese citizens in exceptionally vulnerable positions (World Health Organization, 2020). These recent developments have played a significant role in cyber troop activity.

An Overview of Cyber Troop Activity in Lebanon

Organizational Form

Though the manipulation of social media is becoming increasingly prevalent in Lebanon, its sources and organizational form remain unclear and somewhat underdeveloped in comparison with neighboring countries. At this stage it is fairly difficult to track down the spread of misinformation to a particular organizational form. However, one origin that does stand out is Hezbollah, a militarized movement. The organization has many governance duties in Lebanon, is well-connected to foreign resources and operates an efficient media empire that it uses to disseminate its political messages and ideology around the world, and not just Lebanon (Atallah, 2019; Haaretz, 2019).

The epicenter of this network is the Al-Manar Arabic-speaking satellite television station, with an estimated budget of USD $15 million, financed predominantly by foreign actors, most notably Iran. The organization's media network is supplemented by radio stations, print publications, and dozens of websites in various languages (Clarke, 2017). Through these media channels Hezbollah also indirectly operates hundreds of social media accounts that promote the organization's propaganda without it being explicitly obvious that Hezbollah is playing a coordinating role, an approach is vital given that since Hezbollah is classified as a terrorist organization in the US, and as such prohibited from being promoted on platforms such as Facebook, YouTube, and Twitter (Frenkel & Hubbard 2019).

In an attempt to harness technology to spread its message, Al-Manar launched a smartphone application in 2012 that was dedicated to live streaming its content internationally. Four days after the app became available Apple withdraw it from its iTunes store, with Google following suit two days later by withdrawing the app from the Google Play store. Google's Head of Communications for the MENA (Middle East and North Africa) region commented that "We remove applications the violate our policies, such as apps that are illegal or that promote hate speech" (Al Tamimi, 2012).

Hezbollah also maintains partnerships with media organizations that are seemingly outside of its official network. This provides a means of circumventing scrutiny by social media moderators. One such example is the Attansakiyeh group, which operates news sites and an extensive social media presence on all platforms (Martinez, 2019). The Attansakiyeh group's mission statement says it aims to counter distortions on social media that target the "Resistence", and there is widespread evidence that Attansakiyeh has links to Hezbollah. The organization often posts pro-Hezbollah content on Facebook, Twitter, Instagram, Telegram, and YouTube, including posts that glorify Hezbollah leaders and deceased Hezbollah figures (Ibid).

In October 2016 the group partnered with Hezbollah's media outlets to organize a gathering for MP Hassan Fadlallah. Attansakiyeh was also found to be conducting fundraising events and projects related to Hezbollah, such as the "Popular Campaign to Support Resistance and Confront the U.S Siege", in which the money was donated to accounts that provide Hezbollah with funds. Other campaigns loosely affiliated with Attansakiyeh that were launched on social media in 2019 have included the #ResistenceChallenge campaign, which was intended to help boost financial support and donation to Hezbollah. The hashtag challenge went viral and was reposted by many supporters, with pictures of individuals donating money to the Islamic Resistance Support Association (Martinez, 2019)

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Lebanon

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
		Hezbollah	Attansakiyeh, Al-Manar		

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

<u>WhatsApp disinformation:</u> Among the various social media platforms available, WhatsApp seems to be the popular tool of choice for the spread of misinformation, especially in light of the recent protests. According to experts the majority of disinformation being spread has two main goals: 1) the delegitimization of the protesters; and 2) the spreading of panic about day-to-day life in the country, with the intention of deterring citizens from taking to the streets (Lewis, 2019).

A notable example is a message that rapidly spread via WhatsApp during the 2019 protests on October 30th. The message suggested that members of Hezbollah were going to shut down the entire country if the Lebanese Army did not ensure that the roadblocks of protestors were removed. This message was later claimed to be fake with a clear intention to amplify fear and force the government to clamp down on protests. Another message that was spread on the same day warned about a violent attack by government supporters: *"Tell as many people as you can. The Khandaq people are gathering and it looks like they're going to attack,"*. Referring to people from Al-Kandhaq, a Shiite district of Beirut that is known as a district with ties to Hezbollah, who were vehemently opposed to the protests, and who had organized violence against the protesters (Lewis, 2019). Other messages that were circulated on WhatsApp included references to claims that the internet was going to be shut down, that the army was going to declare a state of emergency, and warnings that demonstrations were going to descend into violence.

<u>Misinformation:</u> Official media outlets in the country are also susceptible to social media manipulation, providing an indication of its prevalence. One such example was a fake letter of resignation by Lebanon's Minister of Interior, Raya Hassan. The letter went viral on Twitter, Facebook, and WhatsApp and was subsequently published in an article by CNN Arabic. Hassan soon clarified that the letter was fake, but the case indicates the vulnerability of even the most highly respected media outlets in the country (Tardaguila, 2019).

Moments after the Beirut port explosion, videos of the events taken by residents began to circulate online. Whilst most of the videos merely captured the events, rumors about the cause of the blast also began to go viral (Spring, 2020). Initial rumors suggested that the blast took place at a firework factory. However, rumors quickly escalated to include claims that the event was caused by a nuclear bomb, because of the white mushroom-like cloud that was seen in the footage. This specific rumor was tweeted by a verified Twitter account with over 100,000 followers and gained thousands of shares and likes (Ibid). Even though weapons experts debunked the possibility of a nuclear bomb, stating that a nuclear blast would have been accompanied by a blinding white flash and a surge of heat, claims blaming the "nuclear bomb" on the US, Israel, and Hezbollah continued to spread. These claims were shared by various partisan web sites (Ibid).

Other conspiracy theories were promoted by far-right groups on Facebook, 4chan, Reddit, and Telegram. These messages mainly focused on spreading false claims that the blast was caused by an Israeli bomb or missile attack on a Hezbollah weapons depot. For example, a photograph was spread of Israel's Prime Minister, Benjamin Netanyahu, apparently pointing at the exact site of the explosion during an address to the UN General Assembly in 2018. This photo was used as proof that Israel was to blame for the blast. However, Netanyahu was actually pointing to a completely different district in the city of Beirut, a district that he claimed was a location where Hezbollah was hiding weapons (Spring, 2020).

Network Data from NetBlocks internet observatory confirmed that internet connectivity in Lebanon fell significantly in the aftermath of the explosion. The Internet outage was attributed to the impact of the blast on nearby network infrastructure (NetBlocks, 2020). Lebanon's Prime Minister, Hassan Diab, handed in his resignation following demonstrations over corruption and negligence blamed for the blast (AFP 2020).

Bots and fake accounts: According to research by the Samir Kassir Eyes Center for Media Freedom, Hezbollah stands out as a particularly efficient organization at using digital tools to spread its messages. For example, on October 25th 2019, during a speech made by Hezbollah's secretary general, there was evidence of a mass distribution of hashtags in his favor. However, up to 80% of the accounts spreading these hashtags were created on the same day, indicating the use of bots (Atallah, 2019).

One particular example was the rising prevalence of accounts tweeting the hashtag "In Nasrallah We Trust" (#السيد_نصرالله_ثقتنا), in reference to Hezbollah's leader, Hassan Nasrallah. In research conducted by reporters at Euronews regarding the prevalence of bots in Lebanon's online sphere, results showed numerous accounts of hashtags being tweeted in an identical pattern and in similar intervals, both with pro- and anti-government hashtags. The research further emphasized that accounts tweeting "In Nasrallah We Trust" were overwhelmingly displaying automated behavior (Skinner, 2019).

Harassment: Another technique used in the country is the harassment of journalists via online platforms, especially female, both by straightforward spamming and by spreading disinformation about them personally. For female journalists, this often involves extreme vulgarity, as seen in the case of Dima Sadek, a famed Lebanese reporter, in which fake images of Sadek in compromising positions were distributed. Other journalists were also the target of various conspiracy theories, such as claims that they are agents for foreign powers, most notably Israel (Caramazza, 2019).

Incitement: Hezbollah-affiliated social media accounts, including those by Al-Manar, often includes content that incites violence. One such example was a Twitter post with a picture of the ruins of the US Embassy in Beirut, after the detonation of a car bomb by Hezbollah in 1983 that killed over 300 people. The picture was supplemented with a caption reading "This is how embassies should be disciplined. This is what Imad taught us", in reference to the Hezbollah military commander behind the attacks, Imad Mughniyeh. On November 2019, Twitter suspended several accounts affiliated with Hezbollah, including Al-Manar's official account in Arabic, English, French and Spanish, and accounts of figures associated with the organization (The Meir Amit Intelligence and Terrorism Information Center, 2019). A Twitter spokesperson later commented that "there is no place on Twitter for illegal terrorist organizations and violent extreme groups" (Haaretz, 2019).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Lebanon

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Bots, human accounts	Harassment, pro Hezbollah messages, Incitement	Disinformation, distracting hashtags, fundraising, trolling	Twitter, WhatsApp, Facebook, YouTube, Instagram

References

Agence France Presse. 2020. Beirut Blast Conspiracy Tales Abound on Social Media. *Barron's.* https://www.barrons.com/news/beirut-blast-conspiracy-tales-abound-on-social-media- 01597240205.

Al Tamimi, J. 2012. Google and Apple ban web application for Hezbollah TV station. *Gulf News.* https://gulfnews.com/technology/google-and-apple-ban-web-application-for-hezbollah-tv- station-1.1059565

Atallah, N. M. 2019. How internet has become a Battleground in the Lebanese revolution. *LeCommerce.* https://www.lecommercedulevant.com/article/29508-how-internet-has-become-a- battleground-in-the-lebanese-revolution

Caramazza, Gaia. 2019. Lebanon's social media looks like the Wild West, and women journalists are in the crosshairs. *The New Arab*. https://english.alaraby.co.uk/english/indepth/2019/12/4/Lebanons-women-journalists-being- harassed-for-reporting-the-truth

Central Intelligence Agency. 2020. The World Factbook: Lebanon. *CIA.* https://www.cia.gov/library/publications/the-world-factbook/geos/le.html

Clarke, C. P. 2017. How Hezbollah came to dominate information warfare. *The Jerusalem Post.* https://www.jpost.com/opinion/how-hezbollah-came-to-dominate-information-warfare- 505354

Freedom House. 2019. Freedom on the Net: Lebanon. *Freedom House.* https://freedomhouse.org/country/lebanon/freedom-net/2019

Frenkel, S., & Hubbard, B. 2019. After Social Media Bans, Militant Groups Found Ways to Remain. *The New York Times*. https://www.nytimes.com/2019/04/19/technology/terrorist-groups-social-media.html.

Haaretz.2019. Twitter Suspends Hezbollah and Hamas Affiliated accounts. *Haaretz.* https://www.haaretz.com/us-news/twitter-suspends-hezbollah-and-hamas-affiliated-accounts- 1.8069241

Lewis, E. 2019. WhatsApp as a tool for fear and intimidation in Lebanon's protests. *Coda*. https://www.codastory.com/disinformation/whatsapp-lebanon-protest/

Martinez, H. 2019. Hashtaggers For Hezbollah? How Social Media Fundraising Can Skirt the Rules. *Bellingcat.* https://www.bellingcat.com/news/2019/08/27/hashtaggers-for-hezbollah-how-social-media-fundraising-can-skirt-the-rules/

NetBlocks. 2020. Internet connectivity in Lebanon impacted following blast. *NetBlocks.* https://netblocks.org/reports/internet-connectivity-in-lebanon-impacted-following-blast-YAE2RvB3.

Reporters Without Borders. 2018. Lebanese Media – A Family Affair. *Reporters Without Borders.* https://rsf.org/en/news/lebanese-media-family-affair

Skinner, H. 2019. Lebanon protests: are bots fueling counter demonstrations. *Euro News* https://www.euronews.com/2019/10/25/lebanon-protests-are-bots-fuelling-counter-demonstrations

Spring, M. 2020. Beirut explosion: How conspiracy theories spread on social media. *BBC.* https://www.bbc.com/news/53669029.

Tardaguila, C. 2019. A fake resignation letter made its way into CNN in Arabic and has spurred false news in Lebanon. *Poynter*. https://www.poynter.org/fact-checking/2019/a-fake-resignation- letter-made-its-way-into-cnn-in-arabic-and-has-spurred-false-news-in-lebanon/?dg

The Meir Amit Intelligence and Terrorism Information Center. Hezbollah's Media Empire. *The Meir Amit Intelligence and Terrorism Information Center*. https://www.terrorism-info.org.il/en/hezbollahs- media-empire/.

World Health Organization. 2020. Lebanon Emergency Appeal 2020. *WHO.* https://www.who.int/emergencies/funding/appeals/lebanon-explosion-2020

LIBYA

Introduction

Following the toppling of Muammar Gaddafi's regime in 2011, the social media platforms that helped Libya's revolution are now used to sow political discord and incite violence (Ghanmi, 2016). Democracy Reporting International (DRI) (2019) noted that since 2014, social media has been used for propaganda purposes by militias. This is particularly true on Facebook, the predominant social media platform—with 67% of Libya's 6.5 million population on the platform. A reliance on social media for information has been influenced by the fact that prior to 2011 the dominant source of information was the government. Mohamed Kassab (2019), a disinformation researcher, suggests that decades of information deprivation have made the Libyan population susceptible to mis- and disinformation.

Disinformation is not a recent tactic in Libya—New York Times reporters have claimed it was exploited by the competing factions and overlapping agendas of Gaddafi loyalists, opposing tribes, western guerrillas, eastern rebels and NATO allies during the 2011 upheaval (Kirkpatrick & Nordland, 2011). This is compounded by the fact that the Libyan media plays a pivotal role in shaping public perceptions and building political constituencies. For example, Al Nabaa was a staunch supporter of revolutionary units such as the Libyan Shield Force and Libya Awalan was strongly anti-Islamist and a supporter of Haftar's actions in Benghazi (Hargreaves, 2015). Wollenberg and Richter (2020) argue that the structures of the Libyan media system reflected the anatomy of the political conflict, as political parallelism shaped Libya's newly liberated media system.

The continuing civil war between two competing governments, combined with extensive foreign interference in both the conflict and the media landscape, have provided a fertile ground for computational propaganda. At a seminar on combatting the use of media and social media to promote violence in Libya organised by the United Nations Support Mission in Libya, US diplomat Stephanie Williams said that "hate speech, incitement, rumours, misinformation, and fabricated news are just a few examples of the content dominating social media in Libya" (Al Arab, 2019). The two main political groups are the House of Representatives (which is supported by General Khalifa Haftar, head of the self-styled Libyan National Army (LNA)), and the UN-backed Government of National Accord (GNA). On 4 April 2019, Haftar launched an attack on Tripoli, the location of the GNA, which was "accompanied by an equally zealous online campaign" (Democracy Reporting International, 2019b). Researchers at the Digital Forensic Research Lab (DFR Lab) identified ten hashtags that supported Haftar's military campaign and attacked the GNA and its allies (Kassab & Carvin, 2019). This assault has seen both sides of the conflict attempting to amplify favourable narratives on social media (Kassab, 2019).

An Overview of Cyber Troop Activity in Libya

Organizational Form

Cyber troop activity originates from multiple groups in Libya. CNN Arabic reported that there are "electronic militias" behind suspicious pages and fake accounts (Ghanmi, 2016). It is claimed that both sides of the conflict have effectively weaponized social media (Kassab, 2019). Mahmud Shamman, a former information minister, said that "electronic armies are owned by everyone, and used by everyone without exception" (Walsh & Zway, 2018). Abdel-Rahman Al-Shater, a member of the State's Supreme Council, tweeted about "Haftar's electronic flies"—a common term in the region for fake accounts (Asstor, 2019). Haftar's LNA reportedly has a special online unit that searches Facebook for indications of dissent or suspected Islamists—many of whom have been arrested, jailed, or forced to flee. Similarly, the Special Deterrence Force, a militia led by Abdulrauf Kara, polices conservative religious values on Facebook (Walsh & Zway, 2018). Some Facebook users are known as 'keyboard warriors' because of their attempts to manipulate information to widen ethnic divides or weaken state institutions (Freedom House, 2019).

Media Outlets

Much of the reporting on Saif al-Islam Gaddafi, Muammar Gaddafi's son, originates from Russian state media outlets RT and Sputnik (Democracy Reporting International, 2019b). In a DRI report, it was found that digital media was dominated by 218tv, a media outlet based in Jordan and funded by the Emirati government. Following Haftar's Tripoli assault, DRI found that 50% of the social media engagements they analysed were attributable to 218tv. The outlet paid considerable attention to Gaddafi, and ran "inflammatory material" such as accusing then-UN envoy Ghassan Salamé of bias against Haftar (Democracy Reporting International, 2019b).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Libya

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
2014	GNA, LNA	Khalifa Haftar, Saif al-Islam Gaddafi	Fabrika Trollei (Aleksandr Prokofyev)	Special Deterrence Force, 218tv	'Keyboard Warriors'

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Disinformation

DRI (2019a) found that mis- and disinformation have a constant presence in Facebook discussions. A common tactic is the repurposing of photos and videos. The official Facebook page of the Al-Marsa Brigade shared a photograph of a funeral parade claiming to be for French soldiers killed fighting alongside Haftar; however, it was actually from a parade in 2012 to honour four French soldiers killed in Afghanistan (Kassab, 2019). In another case, the LNA captured a Portuguese mercenary that was supporting the GNA and a fake Facebook account purporting to be a popular TV station falsely claimed that the individual was only conducting migrant smuggling surveillance. The false story went viral, was amplified by a Saudi news network and reported in the UK's Daily Mail (Stanford Internet Observatory, 2019).

Violence

Rival militant groups use social media platforms to disseminate hate speech, boasts, taunts and threats—such as vowing to "purify" Libya of its opponents (Walsh & Zway, 2018). Indeed, activists and human rights defenders have been assassinated after being tracked and monitored using their personal social media accounts (Ghanmi, 2016). Footage of war crimes is frequently shared to enrage supporters and generate online engagement. An investigation by BBC Arabic (2019) found video evidence of war crimes in Libya being shared widely on Facebook and YouTube. Both the LNA and GNA have been found to repurpose footage to defame the other side (Kassab, 2019).

Harassment

Self-censorship is common out of fear of harassment and violence, particularly among journalists who face arrest and arbitrary detention (Freedom House, 2019; Ramali, 2019). Harassment is also gendered, with women reported to avoid engaging with public Facebook groups and pages and having a stronger presence on private women-only groups. An attempt by a group of women to organise a Twitter meet up in a Benghazi café was prevented by Ministry of Interior forces (Democracy Reporting International, 2019a).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Libya

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Real, Fake, Human, Automated	Pro-government messages, attacks on opposition, polarization,	Creation of disinformation, mass reporting of content, amplification strategies	Facebook, Twitter

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

Table 3: Cyber Troop Capacity in Libya

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
		Ongoing during conflict, peaked around Haftar's Tripoli assault		

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Regional Interference

As the civil war involves proxy and regional actors, Libya has been subject to foreign interference. Tweets in support of Haftar's assault on Tripoli have originated from Egypt, the UAE and Saudi Arabia, whilst tweets that promoted an anti-LNA discourse and supporting the GNA originated from Qatar and Turkey (Democracy Reporting International, 2019b). Research by the Stanford Internet Observatory found that pro-Haftar tweets originating from Egypt, the UAE and Saudi Arabia started in 2013 and worked to discredit peace conferences before they even took place. Pro-Haftar activity was concentrated in 2019, and most of the activity focused on amplifying accounts outside of the inauthentic network (Grossman et al., 2020). Hashtags such as #SecuringTheCapital (#تأمين العاصمة) and #WeSupportTheArabLibyanArmy (#ندعم_الجيش_العربي_الليبي) were amplified by bot accounts ahead of Haftar's assault (Kassab & Carvin, 2019). Some of these accounts had previously participated in pro-UAE and anti-Qatar online campaigns (Stanford Internet Observatory, 2019). Hashtags were further amplified by regional Arabic media outlets; for example, Al-Ain, a UAE-based media outlet, embraced the hashtag in tweets covering Haftar's assault (Kassab & Carvin, 2019). The DFRLab identified a further network of 100 Twitter accounts that supported Haftar and the LNA, whilst criticising Qatar and promoting the UAE, in tweets in French and English (Carvin & Kassab, 2019).

It was reported that Qatari intelligence was behind the creation of a fake social media account in the name of Saif al-Islam Gaddafi. Saif al-Islam Gaddafi's lawyer stated that the account was not linked to Gaddafi and that the fake account aimed to spread misinformation and create confusion (Gamal, 2018).

Russian Interference

As well as providing military support to the conflict, Russia has assisted with information operations. A connection with Russia was confirmed in October 2019 when Facebook removed fourteen accounts, twelve pages, one group and one Instagram account that originated in Russia and targeted Libya. The accounts shared stories from RT and Sputnik and posted in Arabic. The network posted content on multiple sides of the political debate—criticising the GNA and Khalifa Haftar, but also supporting Muammar Gaddafi, Saif al-Islam Gaddafi, and Khalifa Haftar (Gleicher, 2019). It was further reported in April 2020 by the New York Times that the Kremlin controls dozens of social media accounts which promote Haftar and Saif al-Islam Gaddafi, as well as acquiring an ownership stake in a pro-Gaddafi Libyan satellite network (Kirkpatrick, 2020).

An example of Russian interference was a Facebook paged entitled ‘Mandela Libya’, which compared Saif al-Islam Gaddafi to Nelson Mandela. The page created and amplified (using sponsored ads) a poll asking citizens whether they would like Gaddafi to be elected President; with 65,125 out of 71,065 respondents voting ‘yes’. An analysis of a sample of 7,000 accounts found that 75% of those that voted were fake accounts: often newly created in December 2018, friends with each other, without profile pictures, and with similar names (Democracy Reporting International, 2019a). This page was created following Gaddafi’s visit to Moscow and has alleged links to a Russian information operations agent Aleksandr Prokofyev (Democracy Reporting International, 2019b). A Proekt report also linked the Mandela Libya page to Russian information operations (Badanin & Churakova, 2019). The site’s founder, Abdulmajid Eshoul, is claimed to have connections to Prokofyev, and the page has been linked to the Fund for the Defence of National Values—an organisation involved in Russian information operations in Libya (Democracy Reporting International, 2019b). Aleksandr Malkevich, the head of the Fund, said that two of his employees were arrested in Tripoli after meeting Gaddafi. This was confirmed as media reports indicated Libyan security services arrested two men in July 2019, accused of working for an outfit identified as ‘Fabrika Trollei’ (Troll Factory) that specialised in influencing African elections (Al-Atrush et al., 2019).

References

Al Arab. (2019, September 13). الكراهية على مواقع التواصل تمزق النسيج الاجتماعي في ليبيا |. *Al Arab*.

Al-Atrush, S., Arkhipov, I., & Mever, H. (2019, July 5). Libya Uncovers Alleged Russian Plot to Meddle in African Votes—Bloomberg. *Bloomberg*. https://www.bloomberg.com/news/articles/2019-07-05/libya-arrests-two-russians-accused-of-trying-to-influence-vote

Asstor. (2019, April 11). بوابة أسطر الاخباريةالذباب الالكتروني يقود حربا وهمية | بوابة أسطر الاخبارية. Asstor.Net. https://asstor.net/?p=7249

Badanin, R., & Churakova, O. (2019, September 12). *Шеф и повар. Часть четвертая*. Проект. https://www.proekt.media/investigation/prigozhin-libya/

BBC. (2019, April 30). Libya ‘war crimes’ videos shared online. *BBC News*. https://www.bbc.co.uk/news/av/world-africa-48105968

Carvin, A., & Kassab, M. (2019, July 31). Libyan Hashtag Campaign Has Broader Designs: Trolling Qatar. *DFRLab*. https://medium.com/dfrlab/libyan-hashtag-campaign-has-broader-designs-trolling-qatar-8b2ba69c7334

Democracy Reporting International. (2019a). *Libya Social Media Monitoring Report January 2019* (Democracy Reporting International). Democracy Reporting International. https://www.democracy-reporting.org/libya-social-media-report/january/index.html

Democracy Reporting International. (2019b). *Libya Social Media Monitoring Report Main Findings*. https://democracy-reporting.org/libya-social-media-report/main-findings/

Freedom House. (2019). *Freedom on the Net | Libya*. Freedom House. https://freedomhouse.org/country/libya/freedom-net/2019

Gamal, M. (2018, January 7). قطر وراء فبركة صفحات وهمية باسم #سيف_الإسلام_القذافي. قطر وراء فبركة صفحات وهمية باسم #سيف_الإسلام_القذافي. جريدة الشعلة الإلكترونية.

Ghanmi, M. (2016, January 28). كيف ساهمت مواقع التواصل الاجتماعي في انقسام الليبيين وتغذية العنف بينهم؟—CNN Arabic. *CNN*. https://arabic.cnn.com/world/2016/01/29/libya-social-media-violence

Gleicher, N. (2019, May 6). Removing More Coordinated Inauthentic Behavior From Russia. *About Facebook*. https://about.fb.com/news/2019/05/more-cib-from-russia/

Grossman, S., H., K., DiResta, R., Kheradpir, T., & Miller, C. (2020). *Blame it on Iran, Qatar and Turkey: An analysis of a Twitter and Facebook operation linked to Egypt, the UAE and Saudi Arabia*. https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/20200402_blame_it_on_iran_qatar_and_turkey_v2_0.pdf

Hargreaves, L. (2015). *The Role of Media in Shaping Libya's Security Sector Narratives*. International Security Sector Advisory Team (ISSAT). http://issat.dcaf.ch/Learn/Resource-Library/Policy-and-Research-Papers/The-Role-of-Media-in-Shaping-Libya-s-Security-Sector-Narratives

Kassab, M. (2019, May 24). Walking on Hot Coals: How Disinformation Is Fueling the Fight in Libya. *DFRLab*. https://medium.com/dfrlab/walking-on-hot-coals-how-disinformation-is-fueling-the-fight-in-libya-41a0474d757e

Kassab, M., & Carvin, A. (2019, July 24). A Twitter Hashtag Campaign in Libya: How Jingoism Went Viral. *DFRLab*. https://medium.com/dfrlab/a-twitter-hashtag-campaign-in-libya-part-1-how-jingoism-went-viral-43d3812e8d3f

Kirkpatrick, D. D. (2020, June 18). The White House Blessed a War in Libya, but Russia Won It. *The New York Times*. https://www.nytimes.com/2020/04/14/world/middleeast/libya-russia-john-bolton.html

Kirkpatrick, D. D., & Nordland, R. (2011, August 23). Waves of Disinformation and Confusion Swamp the Truth in Libya. *The New York Times*. https://www.nytimes.com/2011/08/24/world/africa/24fog.html

Ramali, K. (2019, June 23). *Libyan Perspectives*. Exploring Libya Online. https://libya.substack.com/p/libyan-perspectives

Stanford Internet Observatory. (2019, October 2). *Libya: Presidential and Parliamentary Elections Scene Setter*. https://cyber.fsi.stanford.edu/io/news/libya-scene-setter

Walsh, D., & Zway, S. A. (2018, September 4). A Facebook War: Libyans Battle on the Streets and on Screens—The New York Times. *New York Times*. https://www.nytimes.com/2018/09/04/world/middleeast/libya-facebook.html

Wollenberg, A., & Richter, C. (2020). Political Parallelism in Transitional Media Systems: The Case of Libya. *International Journal of Communication*, *14,* 1173–1193.

MALAYSIA

Introduction

Computational propaganda in Malaysia is not a recent phenomenon. Political parties pay online commentators, referred to as 'cybertroopers,' to defend government policies and attack the opposition (Freedom House, 2019). The prevalence of political attacks online has led Malaysians to call the interaction between supporters of the main political coalition Barisan Nasional (BN) and their opponents a "cyber-war" (Hopkins, 2014; Leong, 2015). Whilst the BN coalition have publicly admitted to cybertroopers, and parties in the Pakatan Harapan (PH) coalition have denied their presence, both sides speak of the negative impact of cybertroopers. This profile draws on Malaysian media reports from outlets such as Malaysiakini, Sinar Harian and Malay Mail. As cybertroopers are such a contentious and politicised issue, media allegations of activity cannot always be taken at face value. Indeed, this lack of trust is felt by the population: the Edelman Trust Barometer conducted in 2018 found that 63% of respondents failed to 'distinguish between rumors and good journalism' and 73% are uneasy about the adverse effects of disinformation in Malaysia (Haciyakupoglu, 2018).

In describing the role of online media in influencing the country's general elections, Malaysian outlet *The Star* notes that "In 2008, it was the blogs. Five years later, it was Facebook… And now, WhatsApp will be taking centre stage" (Tan, 2018). As early as the 12th General Election (GE12) in 2008, political support by bloggers is claimed to have played a role in the election result (Johns & Cheong, 2019). In a statement in 2011, Lim Guang Eng, the then-DAP Secretary General and former finance minister, stated that a "new army of cyber troopers… is proof that the 13th general election will be the dirtiest election yet" (Guan Eng, 2011). The 13th General Election (GE13) in 2013 saw a boom in social media usage, and BN advertising expenditure increased dramatically on Facebook and Google (Leong, 2015). Subsequently, the United Malays National Organisation (UMNO) "urged all its members to master the use of the social media" ahead of the 14th General Election (GE14) in May 2019. This election was called the "WhatsApp Election" given that the "most influential campaign propaganda was spread among the voters via the app" (Chin, 2018).

Former Prime Minister Najib Razak's BN coalition, which had ruled for 61 years, was defeated by the PH coalition in the GE14. Since then, Freedom House have claimed that disinformation and the influence of cybertroopers has decreased under the new government (Freedom House, 2019). *Malaysiakini* reported that for a few months there was "thunderous silence as the army of cybertroopers disappeared from the social media scene" (Malaysiakini, 2019b). In February 2020, the government changed to the Perikatan Nasional coalition, which includes the Barisan Nasional party.

An Overview of Cyber Troop Activity in Malaysia

Organizational Form

The Barisan Nasional (BN) coalition comprises UMNO, the Malaysian Chinese Association (MCA) and the Malaysian Indian Congress (MIC). The BN government made no secret that it had a network of paid and unpaid cybertroopers (Guest, 2018). UMNO leaders have admitted that the party has engaged cybertroopers to defend government policy and attack the opposition (Malaysiakini, 2019b). Some were located within government; the Prime Minister's Office Special Affairs Department (JASA) is alleged to have paid online activists (The Malaysian Insight, 2018). JASA is reported to have a branch in Kuala Lumpur that has hired young people for casual employment as BN cybertroopers (Nadzri, 2018). BN cybertroopers were previously coordinated by the New Media Unit (NMU), a formal unit of the UMNO Youth Wing, and in addition the coalition had a loosely associated collection of bloggers (Hopkins, 2014). Cybertroopers became formally organized under BN's IT bureau, headed by MP Ahmad Maslan. In March 2018, UMNO had called on local divisions to form IT bureaus to "counter the slander" on social media (Freedom House, 2019). BN deputy strategic communications director Eric See-To also managed social media operatives (Malaysiakini, 2019b; The Malaysian Insight, 2018). Former BN Prime Minister Najib Razak is credited as having been central to this process, earning the title 'King of Trolls' following "a series of sarcastic and cynical statements criticizing or responding to criticisms of political opponents, especially Pakatan Harapan leaders" (Malaysiakini, 2019a).

Cybertrooper activity also originates from political activist groups. Syarul Ema Rena Abu Samah, also known as Ratu Naga ('Dragon Empress') has given interviews detailing her life as a BN cybertrooper (Kamal, 2018). Reportedly, by 2013 she was organizing a network of 80 cybertroopers who ran thousands of fake social media accounts (Guest, 2018). Descriptions of UMNO's operations suggest that the party provides guidelines but does not micromanage the content they circulate. The lack of direct control grants BN and UMNO the ability to deny association when necessary (Haciyakupoglu, 2018).

Parti Rakyat Sarawak (PRS) president Dr James Masing said in 2017 that the party would continue to use cybertroopers for GE14 (Su-Lyn, 2017). The party relied on a five-member team comprising of party members that were selected based on their interests, knowledge about political issues, and activity in the state. These members allegedly underwent training in Kuala Lumpur together with UMBs from other parties prior to the 2011 state election. The UMB had been entrusted with the task of countering online allegations and slanderous statements against the party's coalition, and giving the general public "the true picture" of what was happening in the country (Yap, 2012).

In 2017, Malaysian Indian Congress (MIC) information chief Mogan said that the BN headquarter's social media department had trained 1,000 MIC leaders on social media. MIC's infozone, comprising 100 volunteers, sends messages to WhatsApp groups, promotes party events, defends party policies and attacks the opposition (Su-Lyn, 2017).

The Pakatan Harapan (PH) coalition comprises the Democratic Action Party (DAP), People's Justice Party (PKR), the Malaysian United Indigenous Party (Bersatu/PPBM), and National Trust Party (AMANAH). Before the GE14, the PH opposition was allegedly "manipulating social media to spread defamation and fake news" on the then-ruling BN coalition, including spreading false and misleading content, particularly on WhatsApp (Sinar Harian, 2018). Parti Gerakan Rakyat vice-president Dominic Lau claimed that the DAP cybertroopers, also known as the Red Bean Army, had received help from a Taiwanese-based businessman during GE13 (Haciyakupoglu, 2018). The DAP has denied the existence of the Red Bean Army, and these accusations ceased with threats of legal action.

Private Contractors

There is evidence that CA Political, an offshoot of Cambridge Analytica, supported Malaysia's BN coalition in Kedah state during the 2013 general election, with "a targeted messaging campaign highlighting their improvements since 2008", according to a statement on CA Political's website (Haciyakupoglu, 2018). Leaked documents revealed that SCL Group's Southeast Asian subsidiary had planned to be involved in GE14, with SCL approaching BN through Ahmad Zahid Hamidi (Ar, 2020). However, Cambridge Analytica and SCL Group declared bankruptcy prior to GE14.

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Malaysia

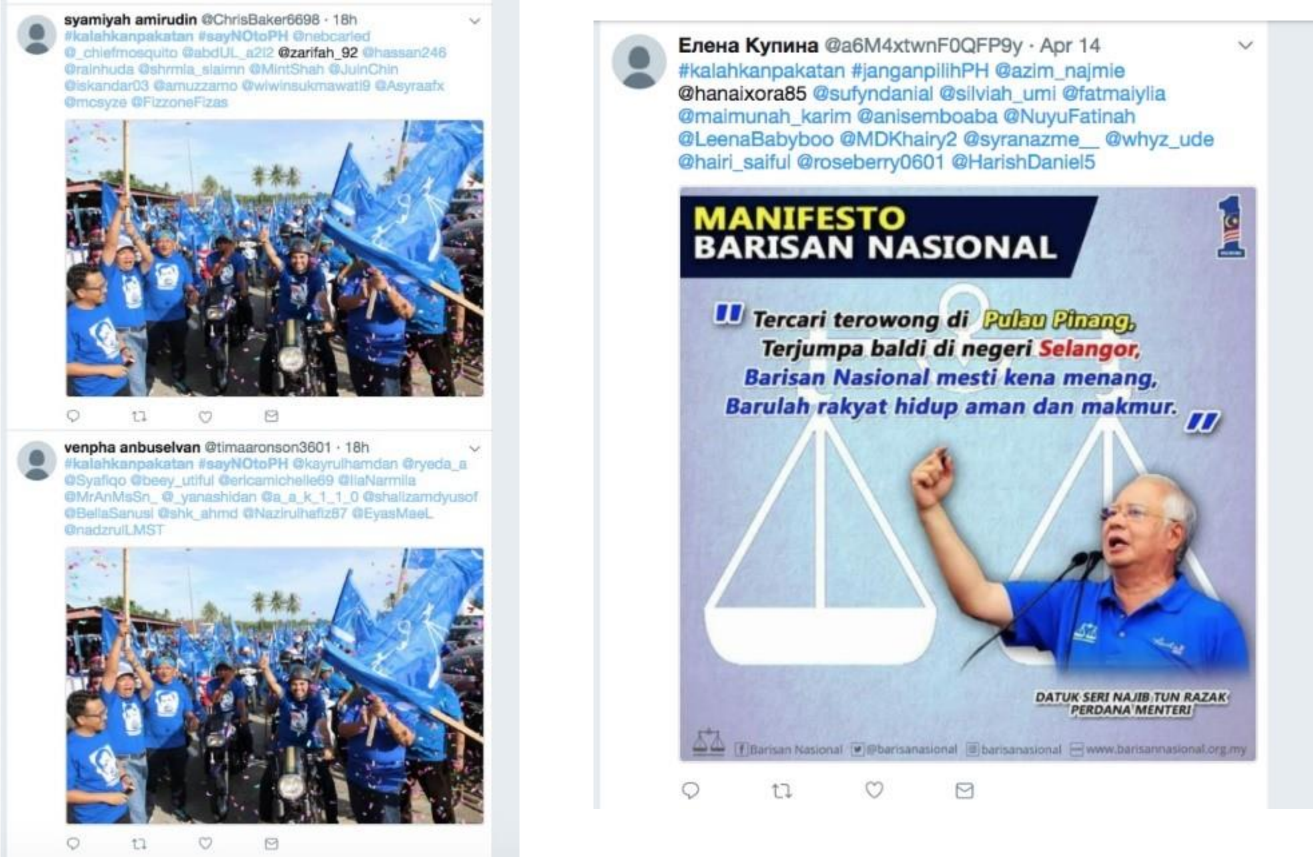
Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
2008	JASA	UMNO (IT Bureau, Youth Wing), Barisan Nasional (BN), Parti Rakyat Sarawak (PRS), Pakatan Harapan (PH), Malaysian Indian Congress (MIC), Democratic Action Party (DAP)	Cambridge Analytica	Evidence found	Evidence Found

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Bots

In the weeks before GE14, the Digital Forensic Research Lab reported that bot accounts were flooding Twitter with tens of thousands of pro-government and anti-opposition messages (DFRLab, 2018). Tweets included visuals illustrating Malaysian government policies and questioning opposition policies. Hashtags expressing disapproval of the PH opposition included #SayNoToPH and #KalahkanPakatan ('Defeat Pakatan' in Malay). These were tweeted 44,100 times by 17,600 users from April 12 to April 20, with 98% of the users appearing to be bot accounts (Ananthalakshmi, 2018). It is claimed that Twitter suspended 500 accounts involved in the messages on the Malaysian election, as they involved spam or malicious automation. UMNO's IT Bureau said it was not behind the bots and did not know who was (Ananthalakshmi, 2018). However, many of the graphics attached to the tweets credited UMNO’s information technology department and some evidenced traces of social media pages of BN-linked accounts.



syamiyah amirudin @ChrisBaker6698 · 18h
#kalahkanpakatan #sayNOtoPH @nebcarled @_chiefmosquito @abdUL_a2l2 @zarifah_92 @hassan246 @rainhuda @shrmia_slaimn @MintShah @JuinChin @iskandar03 @amuzzamo @wiwinsukmawati9 @Asyraafx @mcsyze @FizzoneFizas

venpha anbuselvan @timaaronson3601 · 18h
#kalahkanpakatan #sayNOtoPH @kayrulhamdan @ryeda_a @Syafiqo @beey_utiful @ericamichelle69 @IlaNarmila @MrAnMsSn_ @_yanashidan @a_a_k_1_1_0 @shalizamdyusof @BellaSanusi @shk_ahmd @Nazirulhafiz87 @EyasMaeL @nadzrulLMST

Елена Купина @a6M4xtwnF0QFP9y · Apr 14
#kalahkanpakatan #janganpilihPH @azim_najmie @hanaixora85 @sufyndanial @silviah_umi @fatmaiylia @maimunah_karim @anisemboaba @NuyuFatinah @LeenaBabyboo @MDKhairy2 @syranazme__ @whyz_ude @hairi_saiful @roseberry0601 @HarishDaniel5

MANIFESTO
BARISAN NASIONAL
" Tercari terowong di Pulau Pinang,
Terjumpa baldi di negeri Selangor,
Barisan Nasional mesti kena menang,
Barulah rakyat hidup aman dan makmur. "
DATUK SERI NAJIB TUN RAZAK
PERDANA MENTERI
Barisan Nasional @barisanasional barisanasional www.barisannasional.org.my

Figure 1: Bot Accounts (DFRLab, 2018)

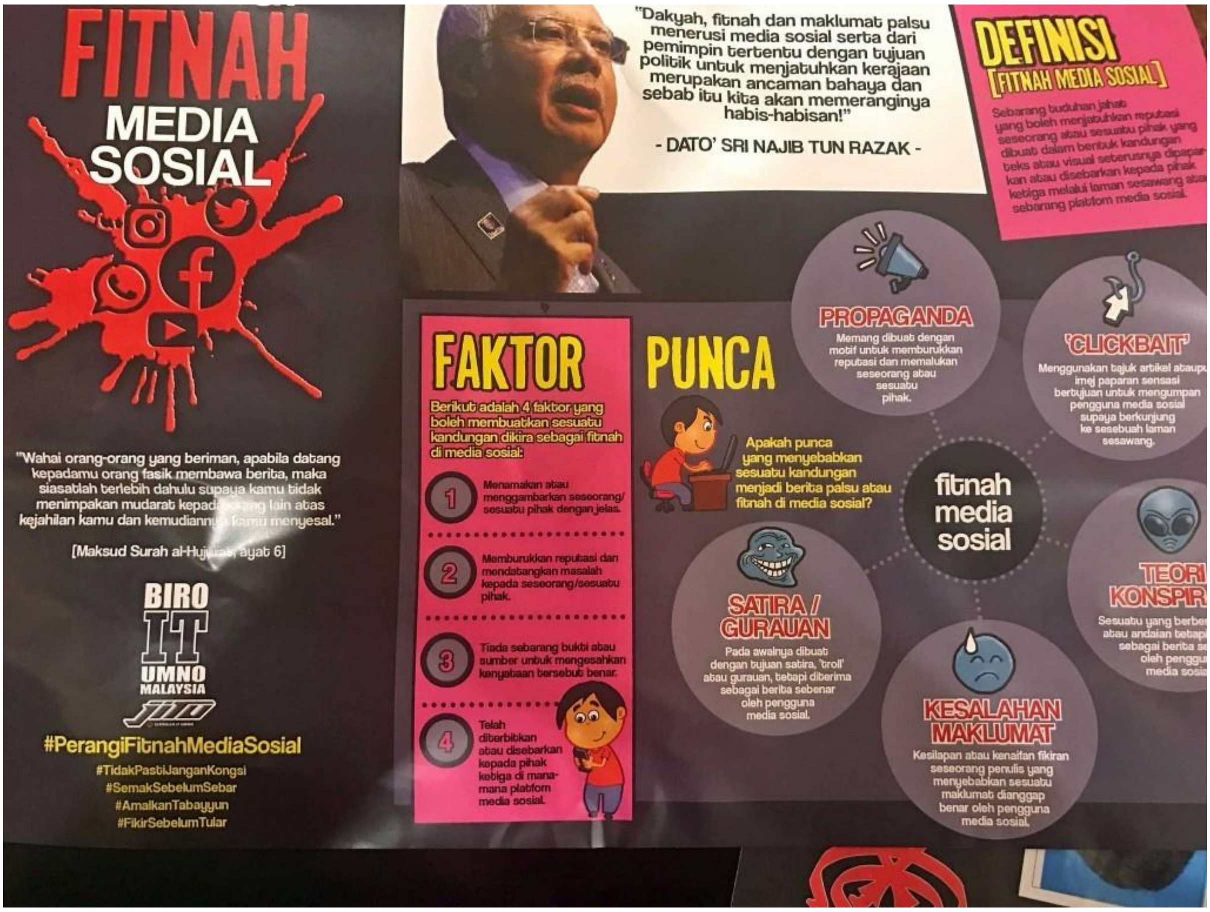
According to the investigation, nine of the top ten most active bot accounts containing anti-opposition hashtags and pro-government messages had Russian names and used Cyrillic script. Donara Barojan, a research associate at the DFRLab said: “the prevalence of bots with Cyrillic screen names does not suggest that Russian social media users are meddling in the Malaysian elections, but does indicate that whoever is behind the campaign purchased some bots created by Russian-speaking bot herders” (DFRLab, 2018).

Alongside elections, social media has been used during social movements such as Bersih (a movement for clean and fair elections) which took place from 2007 to 2016. In an analysis of Malaysian Twitter during the Bersih 3 rally, 36 users were responsible for sending 1,117 tweets, many of them duplicates across multiple accounts. These messages used the tactics of using sock-puppet accounts for astroturfing (faking opposition to the protests) and intimidation (urging people not to take part) (Johns & Cheong, 2019).

Similarly, the campaign #pualangmengundi, or “go home to vote”, aimed at connecting voters with sponsors, who otherwise could not afford plane and bus tickets to travel to vote. The hashtag trended within hours but was hijacked by bots, which overwhelmed the timeline and disrupted attempts to match sponsors with voters, flooding the timeline with thousands of pro-government messages (Seiff, 2018).

Disinformation

Opposition groups use the term ‘fake news’ to describe regime propaganda, and the regime uses the term to counter questions and critiques posed by local and international news outlets. However, disinformation is also propagated by political parties. During GE13, false information spread that 40,000 Bangladeshi nationals were being brought to Malaysia to swing the votes to benefit the BN coalition (Mohd Yatid, 2019). This story was reignited during GE14, with the unfounded rumour that Bangladeshi citizens wearing BN hats had been flown into Kuala Lumpur airport to vote.



"Wahai orang-orang yang beriman, apabila datang kepadamu orang fasik membawa berita, maka siasatlah terlebih dahulu supaya kamu tidak menimpakan mudarat kepada orang lain atas kejahilan kamu dan kemudiannya kamu menyesal."

[Maksud Surah al-Hujurat, ayat 6]

"Dakyah, fitnah dan maklumat palsu menerusi media sosial serta dari pemimpin tertentu dengan tujuan politik untuk menjatuhkan kerajaan merupakan ancaman bahaya dan sebab itu kita akan memeranginya habis-habisan!"

- DATO' SRI NAJIB TUN RAZAK -

Sebarang tuduhan jahat yang boleh menjatuhkan reputasi seseorang atau sesuatu pihak yang dibuat dalam bentuk kandungan teks atau visual seterusnya dipapar kan atau disebarkan kepada pihak ketiga melalui laman sesawang ata sebarang platfom media sosial.

Berikut adalah 4 faktor yang boleh membuatkan sesuatu kandungan dikira sebagai fitnah di media sosial:

1 Menamakan atau menggambarkan seseorang/ sesuatu pihak dengan jelas.

2 Memburukkan reputasi dan mendatangkan masalah kepada seseorang/sesuatu pihak.

3 Tiada sebarang bukti atau sumber untuk mengesahkan kenyataan tersebut benar.

4 Telah diterbitkan atau disebarkan kepada pihak ketiga di mana-mana platfom media sosial.

Apakah punca yang menyebabkan sesuatu kandungan menjadi berita palsu atau fitnah di media sosial?

PROPAGANDA: Memang dibuat dengan motif untuk memburukkan reputasi dan memalukan seseorang atau sesuatu pihak.

'CLICKBAIT': Menggunakan tajuk artikel ataupu imej paparan sensasi bertujuan untuk mengumpan pengguna media sosial supaya berkunjung ke sesebuah laman sesawang.

SATIRA / GURAUAN: Pada awalnya dibuat dengan tujuan satira, 'troll' atau gurauan, tetapi diterima sebagai berita sebenar oleh pengguna media sosial.

KESALAHAN MAKLUMAT: Kesilapan atau kenaifan fikiran seseorang penulis yang menyebabkan sesuatu maklumat dianggap benar oleh pengguna media sosial.

TEORI KONSPIR: Sesuatu yang berbe atau andaian tetapi sebagai berita se oleh penggu media sosi

Figure 2: UMNO’s fight social media slander brochures (Naidu, 2018)

Given the ubiquity of online political attacks, the head of BN’s IT bureau Ahmad Maslan launched a campaign to “fight slander on social media” (‘fitnah media sosial’). This included the dissemination of brochures which urged the public to be critical about propaganda, clickbait, conspiracy theories, satire/trolling and disinformation on Instagram, Twitter, WhatsApp, Facebook and YouTube (figure 2) (Naidu, 2018).

The Malaysian Communications and Multimedia Commission (MCMC) found in 2017 that 89% of Malaysians obtain news online, that the top social media platforms were Facebook, WhatsApp and YouTube, and have facilitated dis- and misinformation related to politics, religion, health and crime (Mohd Yatid, 2019). However, it is also important to note that the MCMC is a government unit that has a history of media control and censorship, and of suppressing dissent.

Polarisation

Racial tensions are often stoked in order to spark rifts between Malaysia's different ethnicities. Fake accounts incite tensions by targeting specific races, ethnicities and religions, and it is claimed there is a "widening divide and deteriorating tolerance on religious, racial and sexual orientation issues" (Mohd Yatid, 2019). A *Wired* article notes that "deep-rooted racial and religious tensions, a quasi-autocratic administration, a moribund mainstream press and ubiquitous social media usage have made this fertile ground for sowers of disinformation" (Guest, 2018). In 2019, a government minister of the PH government said that individuals who use social media against other races would be reprimanded by the MCMC and investigated by the Royal Malaysian Police (Nizam, 2019).

Videos created by BN cybertroopers and circulated on WhatsApp employed actors to create videos that depicted Malays as marginalised and exploited by other ethnic groups. For example, by raising issues such as the difficulty Malays face finding employment (Kamal, 2018). Twenty-four hours before polling opened for the GE13, a video circulated on WhatsApp depicting footage of a fight, which then cut to an Indian member of BN alleging he had been assaulted by DAP activists. The video was entirely fabricated by BN cybertroopers, intending to swing the Indian minority vote (Haciyakupoglu, 2018).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Malaysia

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Human, Fake, Automation	Pro-Government, Attacks on Opposition, Distracting Messages, Polarisation, Trolling	Creation of disinformation (e.g. videos), Big Data Analytics, Trolling and Harassment	Facebook, Twitter, Instagram, WhatsApp, YouTube

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

Expenditure estimations vary and are politically charged. DAP leader Lim Kit Siang estimated that former BN president Najib "must have spent tens or even hundreds of millions ringgit" on cybertroopers (Malaysiakini, 2019b). Ten million ringgit is equivalent to US$2.3 million. He alleged that the going rate for UMNO-BN cybertroopers is RM500 to RM3,000 per month (US$115-690) and that an average expenditure of RM2,000 a month for each UMNO cybertrooper would cost RM7 million per year (US$1.6 million) (Kit Siang, 2019). Another report claims that BN cybertroopers earn "tens of thousands a month" (The Malaysian Insight, 2018). *Malaysia Today* reported that the DAP had "set aside a budget of RM10 million for the next 12 months to pay each Red Bean Army or RBA cyber-trooper a salary of RM3,000 a month" (Kamarudin, 2018).

Cybertroopers are offered training and party support. UMNO's IT bureau held its largest rally of cybertroopers on 4 November 2017. The national social media convention at the Putra World Trade Centre in Kuala Lumpur was attended by over 3,500 people (Kit Siang, 2019; The Malaysian Insight, 2018). At the convention, then-deputy prime minister Seri Ahmad Zahid Hamidi called on "Umno's social media warriors" to be alert to negative news and to counter the "character assassination" of senior leaders (Su-Lyn, 2017).

Table 3: Cyber Troop Capacity in Malaysia

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
	Claimed that both BN and DAP have expenditure in the millions of dollars (unverified)	Constant, but increased around elections (2008, 2013, 2018)	High	Medium-High

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Government Responses

A 'fake news' portal called *Sebenarnya* ('the truth' in Malay) was set up in March 2017 by the MCMC to enable Malaysians to check the validity of news (Freedom House, 2019) and "combat the spreading of false news" (Malaysian Communications And Multimedia Commission, 2017). The MCMC claimed that the 'fake news' identified by their fact-checking portal "increased by almost 100%" in the lead up to GE14 (Haciyakupoglu, 2018). Further, in April 2018 the BN government enacted the Anti-Fake News Act, claiming that Malaysians encounter fake or unverified news on WhatsApp, Facebook and blogs. The law covers news, information, data, reports, images or recordings that are wholly or partly false, and states that it is an offence to possess, produce, offer or share fake news content (Freedom House, 2019). Opposition lawmaker Ong Kian Ming to tweet that it was an "attack on the press and an attempt to instill fear", and emphasizing how the law was rushed through in the weeks preceding the general election (Guardian, 2018). After an initial attempt to repeal the legislation was blocked by the BN-controlled senate, the Anti-Fake News Act was scrapped in October 2019 (Reuters, 2019).

The Ministry of Communications and Multimedia announced in 2019 that it was drafting legal amendments to restrict the spread of fake news and racially sensitive information that threaten unity and national security. The MCMC reported that 47 investigations had been opened based on social media misuse, 3,047 fake social media accounts had spread extreme messages, hatred and defamation, and 1,163 accounts had been deleted (Kementerian Komunikasi Dan Multimedia Malaysia, 2019).

According to Freedom House, several news websites (national and international outlets) were blocked in 2015 and 2016 for reporting on a billion-dollar corruption scandal (known as 1MDB) implicating former Prime Minister Najib Razak. The popular website *Malaysian Insider* was banned in February 2016 after publishing a controversial report about the 1MDB scandal. Additionally, the MCMC periodically instructs websites to remove content, including some perceived as critical of the government (Freedom House, 2019).

References

Ananthalakshmi, A. (2018, April 20). Ahead of Malaysian polls, bots flood Twitter with pro-government messages—Reuters. *Reuters*. https://www.reuters.com/article/us-malaysia-election-socialmedia/ahead-of-malaysian-polls-bots-flood-twitter-with-pro-government-messages-idUSKBN1HR2AQ

Ar, Z. (2020, January 3). How BN might have won GE14... Had Cambridge Analytica stayed alive | Malay Mail. *Malay Mail*.

https://www.malaymail.com/news/malaysia/2020/01/03/how-bn-might-have-won-ge14-had-cambridge-analytica-stayed-alive/1824311

Chin, J. (2018). The Comeback Kid: Mahathir and the 2018 Malaysian General Elections. *The Commonwealth Journal of International Affairs*, *107*(4), 535–537.

DFRLab. (2018, April 20). *#BotSpot: Bots Target Malaysian Elections – DFRLab – Medium*. Medium. https://medium.com/dfrlab/botspot-bots-target-malaysian-elections-785a3c25645b

Freedom House. (2019). *Freedom on the Net | Malaysia*. Freedom House. https://freedomhouse.org/country/malaysia/freedom-net/2019

Guan Eng, L. (2011, November 21). Najib's new army of cyber troopers with a history of dirty tricks is proof that the 13th general election will be the dirtiest election yet. http://dapmalaysia.org/english/2011/nov11/lge/lge1414.htm

Guardian. (2018, March 26). *Malaysia accused of muzzling critics with jail term for fake news*. https://www.theguardian.com/world/2018/mar/26/malaysia-accused-of-muzzling-critics-with-jail-term-for-fake-news

Guest, P. (2018, May 9). 'Queen of Dragons': The inside story of Malaysia's election fixer. *Wired UK*. https://www.wired.co.uk/article/election-malaysia-2018-general-fake-news-day-2008-syarul-ema

Haciyakupoglu, G. (2018). *The 'Fake News' Label and Politicisation of Malaysia's Elections. | StratCom* (Defence Strategic Communications). https://www.stratcomcoe.org/gulizar-haciyakupoglu-fake-news-label-and-politicisation-malaysias-elections

Hopkins, J. (2014). Cybertroopers and tea parties: Government use of the Internet in Malaysia. *Asian Journal of Communication*, *24*(1), 5–24. https://doi.org/10.1080/01292986.2013.851721

Johns, A., & Cheong, N. (2019). Feeling the Chill: *Bersih 2.0* , State Censorship, and "Networked Affect" on Malaysian Social Media 2012–2018. *Social Media + Society*, *5*(2), 205630511882180. https://doi.org/10.1177/2056305118821801

Kamal, S. M. (2018, October 5). How racial misinformation shapes politics, according to an ex-BN 'cybertrooper'. *Malay Mail*. https://www.malaymail.com/news/malaysia/2018/10/05/how-racial-misinformation-shapes-politics-according-to-an-ex-bn-cybertroope/1679778

Kamarudin, R. P. (2018, November 5). DAP's Red Bean Army given RM10 million budget. *Malaysia Today*. https://www.malaysia-today.net/2018/11/05/daps-red-bean-army-given-rm10-million-budget/

Kementerian Komunikasi Dan Multimedia Malaysia. (2019). *Pindaan undang-undang mengenai ancaman kepada perpaduan, keselamatan negara sedang digubal*. https://www.kkmm.gov.my/index.php/awam/berita-terkini/14613-bernama-05-mac-2019-pindaan-undang-undang-mengenai-ancaman-kepada-perpaduan-keselamatan-negara-sedang-digubal

Kit Siang, L. (2019, September 28). Oxford report on fake news sends timely warning to M'sia. *Malaysiakini*. https://www.malaysiakini.com/news/493635

Leong, P. (2015). Political Communication in Malaysia: A study on the Use of New Media in Politics. *EJournal of EDemocracy and Open Government*, *7*(1).

Malaysiakini. (2019a, February 3). *Najib troll lagi: Di mana saya boleh pohon permit selfie?* Malaysiakini. https://www.malaysiakini.com/news/462706

Malaysiakini. (2019b, July 14). *Kit Siang prods MCMC, cops on funders of Najib's 'cybertroopers'*. Malaysiakini. https://www.malaysiakini.com/news/483699

Malaysian Communications And Multimedia Commission. (2017, March 14). *Sebenarnya.my portal launched, in a battle against false news*. Malaysian Communications And Multimedia Commission (MCMC) | Suruhanjaya Komunikasi Dan Multimedia Malaysia (SKMM). https://www.mcmc.gov.my/en/media/press-releases/sebenarnya-my-portal-launched-in-a-battle-against

Mohd Yatid, M. (2019). Truth Tampering Through Social Media: Malaysia’s Approach in Fighting Disinformation & Misinformation. *The Indonesian Journal of Southeast Asian Studies, Vol. 2, No. 2*. https://www.researchgate.net/publication/330450786_Truth_Tampering_Through_Social_Media_Malaysia's_Approach_in_Fighting_Disinformation_Misinformation

Nadzri, M. M. N. (2018). The 14th General Election, the Fall of Barisan Nasional, and Political Development in Malaysia, 1957-2018. *Journal of Current Southeast Asian Affairs*, *37*(3), 139–171. https://doi.org/10.1177/186810341803700307

Naidu, S. (2018, January 9). Malaysian politicians gear up for online battle ahead of GE14. *Channel News Asia*. https://www.channelnewsasia.com/news/asia/malaysian-politicians-gear-up-for-online-battle-ahead-of-ge14-9844040

Nizam, O. F. (2019, April 24). Akaun palsu di media sosial cetus isu perkauman. *Berita Harian*. https://www.bharian.com.my/berita/nasional/2019/04/556873/akaun-palsu-di-media-sosial-cetus-isu-perkauman

Reuters. (2019, October 10). Malaysia parliament scraps law criminalising fake news. *Reuters*. https://www.aljazeera.com/news/2019/10/malaysia-parliament-scraps-law-criminalising-fake-news-191010024414267.html

Seiff, A. (2018, May 4). Twitter Has a Big Bot Problem in Southeast Asia. *Time*. https://time.com/5260832/malaysia-election-twitter-bots-social-media/

Sinar Harian. (2018, May 6). *Pembangkang manipulasi media sosial*. Sinarharian. https://www.sinarharian.com.my/politik/pembangkang-manipulasi-media-sosial-1.830968

Su-Lyn, B. (2017, April 11). BN reveals art of targeting voters | Malay Mail. *Malay Mail*. https://www.malaymail.com/news/malaysia/2017/04/11/bn-reveals-art-of-targeting-voters/1353587

Tan, T. (2018, April 1). It’s shaping up to be a WhatsApp election | The Star Online. *The Star*. https://www.thestar.com.my/news/nation/2018/04/01/its-shaping-up-to-be-a-whatsapp-election-platform-takes-over-from-social-media-in-dishing-out-politi/

The Malaysian Insight. (2018, June 11). As funding dries up, Umno cybertroopers fade away or switch sides | The Malaysian Insight. https://www.themalaysianinsight.com/s/53913

Yap, J. (2012, March 22). PRS’ cyber-troopers ready for coming polls. *Borneo Post Online*. https://www.theborneopost.com/2012/03/22/prs-cyber-troopers-ready-for-coming-polls/

Malta

Introduction

In November 2019 protests in Malta demanded the resignation of government officials linked with journalist Daphne Caruana Galizia's assassination in 2017 and "suspected of involvement in serious corruption schemes" (Freedom House, 2020). This followed with a series of resignations by high-profiles, including Joseph Muscat, Prime Minster of the country between 2013 and 2020. Robert Abela took office in January 2020, however, according to the Council of Europe's Group of States Against Corruption, "senior officials suspected of involvement in serious corruption schemes remained in office" (Freedom House, 2020).

In 2018 an investigation about six Facebook groups disclosed that government officials and members of the Labour Party coordinated pro-Muscat online propaganda. Not only did members in these groups spread disinformation but they also coordinated attacks and hate campaigns against the opposition, journalists, and anti-corruption activists.

An Overview of Cyber Troop Activity in Malta.

Organizational Form

As recorded by The Shift News, the ruling Labour Party has been working alongside a coordinated network of social media users that disseminate disinformation and attack the opposition in a very targeted way (The Shift News, 2018a). Members of the Labour Party and staff at ministries have been identified as managers of these Facebook groups (Demarco, 2020). Senior staff of the Muscat's government (2013-2020) who were part of them also include: Tony Zarb (former General Workers Union secretary general and government consultant), Keith Schembri (the Prime Minister's Chief of Staff), Konrad Mizzi (Minister of Tourism), Chris Cardona (Minister of the Economy), Glenn Bedingfield (Labour MP and consultant to the Prime Minister), Neville Gafa (consultant to the Prime Minister), Rosianne Cutajar (MP and communications coordinator in the Prime Minister's Office), Robert Musumeci (government consultant), Jeffrey Pullicino Orlando (chairman at Malta Council for Science and Technology), Josef Caruana (Office of the Prime Minister communications official), and Mark Farrugia (former deputy chief of staff) (Demarco, 2020; The Shift News, 2018a).

Prime Minister Joseph Muscat and President Marie-Louise Coleiro Preca were members of these groups until the network was exposed by The Shift News. As of April 2019 other members of the Party and government were still active on the groups (Taylor, 2019).

It is important to note that divisive and untrue content – including false statistics – were also disseminated by government officials through their personal social media accounts (Demarco, 2020).

Finally, it is worth noting that according to the British Parliament, the British firm Strategic Communications Laboratories, known for using behavioural research in election campaigns, advised the Labour Party "for several years before the 2013 elections" (UK Parliament House of Commons' culture committee, 2019).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Malta

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers

2013	Evidence found	Labour Party	Strategic Communications Laboratories		

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

The government of Joseph Muscat and its Labour Party used secret Facebook groups to spread and amplify its narratives, disseminate disinformation, and attack opposition. Members were also called to take actions in support of Muscat and his government (The Shift News, 2018c). At least six Facebook groups were identified and analysed. Its names ranged from United Labour Supporters and How many Labour Supporters can we find on Facebook to other Labour Supporters to Death (The Shift News, 2018a).

Among these groups a false narrative is developed. For instance, they contributed to the narrative that Malta was bankrupt and it was Joseph Muscat to save the country's economy, as well as installing the narrative that the Labour Party won the 2017 elections with a 40,000-win instead of its 35,280 votes (The Shift News, 2018c). As it was highlighted by The Shift News, the figures "became fact – even the Opposition uses that number" (The Shift News, 2018c). They also manipulated online polls in order to favour the government (Demarco, 2020). At the same time, members of these groups posted manipulated images of opponents, homophobic comments, and calls for doxing anti-corruption activists (The Shift News, 2018a). They also disseminated false information and accusations of targeted people. They led the party's online public narrative.

For instance, the campaign Truth Project was aimed at creating a counter narrative to revelations by the Daphne Project in 2018. According to Caroline Muscat, "From Facebook groups, the information is then spun by the Labour Party media, the national broadcaster TVM, then mainstream media for example on Malta Today, reproducing the narrative from different angles and platforms" (Demarco, 2020).

Secondly, government employees and officials of the Labour Party are involved in propagandist behaviours and actions aimed at discrediting, threatening, and harassing opposition and critics to the government. Additionally, they manage and moderate the Facebook groups where coordination of trolling campaigns occur (Demarco, 2020) and are characterized by abusive comments and the circulation of dehumanizing memes (Riley et al., 2018).

As stated by The Shift News These pro-government groups target specific people and "the person posting knowingly invites an extremely reactionary group of online users to hate the subject of their post" (The Shift News, 2018b). Among them, the journalist Daphne Caruana Galizia's family. She exposed corruption in Malta and was assassinated in October 2017 in a car bomb attack (Taylor, 2019). The pro-Muscat Facebook groups published posts celebrating her death and coordinated attacks on her family and called for sexual violence (The Shift News, 2018a). Two years after Caruana Galizia's death, the campaign was still active and targeting opposition and critics to the government (Demarco, 2020).

The activist Tina Urso was also a subject of attacks after she organized a protest against the Prime Minister in London for money laundry (Riley et al., 2018). Attacks ranged from misogynist insults to threats of violence and false charges, and perpetrators also posted her personal information online and manipulated her photos (Riley et al., 2018; The Shift News, 2018a). Within less than 24 hours members of the Facebook groups had amplified the calls to "share and shame" her (The Shift News, 2018a).

Other attacks were coordinated on members of the European Parliament and the European Commission, local opposition politicians, journalists, and activists (The Shift News, 2018a). Several attacks include threats to sexually abuse them and burn them (Riley et al., 2018). Most recently, there been incidents regarding calls to support Robert Abela, the Labour Leader, by Party leaders for "his stand to close the ports to migrants" and the strong enforcement on a protest by migrants at Lyster detention centre. This situation led to the increase in anti-migrants narratives online. (The Shift News, 2020).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Malta

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Human	Pro-government, pro-party, attacks on opposition, driving division, trolling	Disinformation, Trolls. Suspicion of data-driven strategies	Facebook

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

The Shift News' investigation recorded more than 60,000 members on the six identified Facebook groups (The Shift News, 2018a). At least in one of the groups, the admins checked the Labour Party membership card or the national identification card in order to accept the requests for joining the groups (The Shift News, 2018a).

Table 3: Cyber Troop Capacity in Malta

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
60,000		Permanent	Government employees and officials of the Labour Party working across a number of departments	Medium

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

References

Demarco, J. (2020, febrero 12). State-sponsored trolling continued even after Caruana Galizia's death. *The Shift News*. https://theshiftnews.com/2020/02/12/state-sponsored-trolling-continued-even-after-caruana-galizias-death/

Freedom House. (2020). *Freedom House Report 2020: Malta*. Freedom House. https://freedomhouse.org/country/malta/freedom-world/2020

Riley, M., Etter, L., & Pradhann, B. (2018, julio 19). A Global Guide to State-Sponsored Trolling. *Bloomberg*. https://www.bloomberg.com/features/2018-government-sponsored-cyber-militia-cookbook/

Taylor, A. E. (2019, abril 2). International Journalism Festival: Disinformation and censorship in Malta—The Shift News. *The Shift News*.

https://theshiftnews.com/2019/04/02/international-journalism-festival-disinformation-and-censorship-in-malta/

The Shift News. (2018a, mayo 14). Investigating Joseph Muscat's online hate machine. *The Shift News*. https://theshiftnews.com/2018/05/14/investigating-joseph-muscats-online-hate-machine/

The Shift News. (2018b, mayo 23). Manufacturing consent: How secret online groups feed the cycles of spin. *The Shift News*. https://theshiftnews.com/2018/05/23/manufacturing-consent-how-secret-online-groups-feed-the-cycles-of-spin/

The Shift News. (2018c, junio 17). Disinformation Watch #6: Orwell's nightmare – How the government controls the past to control the future. *The Shift News*.

The Shift News. (2020, abril 27). Surge in racist and hate speech online following government decisions. *The Shift News*. https://theshiftnews.com/2020/04/27/surge-in-racist-and-hate-speech-online-following-government-decisions/

UK Parliament House of Commons' culture committee. (2019). *Disinformation and «fake news»: Final Report*. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/179110.htm

Mexico

Introduction

According to Freedom House (2019), Mexico's democracy is considered partly free with regards to Internet freedom. The country has suffered from an increase in physical violence, especially related to drug trafficking, and this has led to over five hundred attacks against journalists, with at least four reporters being killed in 2018 according to an earlier Freedom on the Net report (Freedom House, 2018).

One aspect of the culture social media usage in Mexico stands out from the rest of Latin America: the country uses Twitter a lot, with a penetration rate of 49% of the population according to the Reuters Institute (Statista, s. f.). Many social media platforms are used during elections, including Twitter, Facebook, and WhatsApp. As in many Latin American countries, Mexico also has a high penetration of WhatsApp users, and 35 million out of the 60 million Mexicans are Internet users (Argüello, s. f.).

The first incident of online disinformation was recorded in Mexico in 2012, and the use of this strategy has increased since (Freedom House, 2018). In 2018, the use of automation skyrocketed as the Mexican presidential elections approached.

When disinformation was spread during the aftermath of the September 2017 earthquake, a crowd-sourced fact-checking initiative was set up by a coalition of interested parties (Argüello, s. f.). It was formed by agencies and media outlets, with the financial support of tech companies such as Google and Facebook, and organizations such as the Open Society Foundation. Named Verificado, checkers received news circulating online that had been flagged as dubious and used their network of users to fact-check information. This initiative was replicated during the Mexican elections as Verificado 2018.

The elections in 2018 marked a turning point in Mexican history and media. For the first time, a political coalition, led by Andrés Manuel López Obrador (AMLO), is represented "by parties other than the PRI and the PAN" (Gutiérrez Rentería, 2019). Whilst previously the media's advertisement was dependent on government income, this is expected to decrease by 50% (Gutiérrez Rentería, 2019).

An Overview of Cyber Troop Activity in Mexico

Organizational Form

For years it has been suggested that the Peña Nieto's government used the spying software Pegasus to harass the then-opposition. After repeated denials of their existence, in February 2019 the Attorney General's Office provided evidence for the first time of its licensing contracts for 2016 and 2017. The government has also been embroiled in criticism due to its closeness with the surveillance company Hacking Team, of which is has been the biggest client (Freedom House, 2019).

Automated accounts were also used by the Peña Nieto's administration, being initiated in 2012, as has been identified by Erin Gallagher (Ojeda de la Torre, 2020). In fact, it is known that Colombian hacker Andrés Sepúlveda received $600,000 to steal campaign strategies from opponents to Peña Nieto when he ran for president in 2012, install spyware and manipulate social media to amplify messages. He used 30,000 Twitter bots that were maintained for more than a year and set trending topics favourable to the then candidate (Robertson et al., 2016).

Researcher Luis Ángel Hurtado Razo suggests that automated accounts favourable to Peña Nieto (or as they have been called, Peñabots) were used as a way to face emerging opposition movements, such as #YoSoy132 and the protests following the disappearance of students in Ayotzinapa (Ojeda de la Torre, 2020). However, in the 2018 campaign active automated and fake accounts were related to several political parties (Freedom House, 2019). Additionally, documented evidence suggests that Peña Nieto's administration allocated 100,258,000 pesos primarily to two social media marketing agencies, Agavis Digital S.C. and 5M2 Digital S.A.P.I. de C.V., for bot-associated works (Ojeda de la Torre, 2020).

According to Brittany Kaiser (Olvera, 2020), former business developer director for Cambridge Analytica, the company had contracts with local clients for 2017 elections in the states of Mexico, Coahuila and Nayarit, as well as a potential work for Cultura Colectiva, one of the most read digital media publishers in Latin America. Although Alfredo del Mazo Maza, PRI-affiliated governor of the state of Mexico, is indicated as having been one of Cambridge Analytica's clients, the state government's Office of Social Communication denies this (Olvera, 2020). Kaiser also states that even though Cambridge Analytica held meetings with the Institutional Revolutionary Party (PRI) that were related to the 2018 presidential campaign, it did not work for the political party. Nevertheless, the PRI paid the company not to collaborate with other political parties (Olvera, 2020). As regards Cultura Colectiva, the negotiations were related to the purchase of data collected by the media publisher (Camhaji, 2019). However, the Mexican company denies it sold data to third parties.

Cultura Colectiva has also been associated with other scandals. Since its establishment in 2012, the company collected data from its users, both via its web site and Facebook, in order to target tailored content. It has been suggested that it was used for a number of targeted political campaigns (Camhaji, 2019). In the last section of this report, there is further information on the contracts between Cultura Colectiva and government institutions.

It is worth noting that Mexico has seen an increasing power struggle around disinformation. Firstly, there has been a massive expansion of the "diseconomy", an expression used to describe the burgeoning disinformation industry. One famous example of the disinformation industry is the case of Carlos Merlo of Victory Lab, known as the "fake news millionaire" in Mexico (@DFRLab, 2018). He claims to have control of millions of fake accounts and hundreds of bogus websites old enough to look authentic. Research shows that Victory Lab is likely to have orchestrated a whole network of bots to amplify content online. These botnets were hired from countries around the world, including India, Brazil, and Russia. Even though thousands of the accounts were in Russian, research has not established any tangible link between those accounts and the Kremlin (Woody, 2018).

Under the new administration, automated Twitter accounts have been identified for both pro-government and anti-government groups. However, there is no evidence of top-down funding.

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Mexico

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
2012	Evidence found during Peña Nieto's administration	Evidence found (eg. Alfredo	Evidence found (eg. Cambridge Analytica,		

		del Mazo Maza)	Andrés Sepúlveda, Cultura Colectiva, and Victory Lab)		

Source: Authors’ evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

During the 2012 and 2018 election campaigns, the Institutional Revolutionary Party (PRI) used automated accounts (Freedom House, 2019), but such accounts were also active during other significant events. For instance, Erin Gallagher found a coordinated online operation of seventy-five thousand bots to counterbalance the anti-government activist-led hashtag #RompeElMiedo (Spanish for break the fear) in December 2014.

Concerns around disinformation in the 2018 Mexican elections were mostly related to the intense use of automation and fake accounts. Artificial amplification of messages was used widely, especially to target the leading (and later elected) candidate, Andrés Manuel López Obrador.

The 2018 elections were particularly violent, and much of the aggression was fuelled by disinformation around both local and regional politics. The most notorious case was that of the gubernatorial elections in the state of Puebla, where people were attacked—and some even murdered—and ballots stolen or burned (Alberto Melchor, 2018). In these elections hundreds of electoral irregularities were reported in the dispute between candidates Miguel Barbosa and Martha Erika Alonso. Competing hashtags which claimed victory before results were announced were amplified by automated accounts. Distrust continued to worsen as the electoral court demanded a recount of the votes two and half months after election day. The battle raged on after the announcement of the official results and spiked after candidate Martha Erika Alonso and former governor Rafael Moreno Valle died in a helicopter crash. Additionally, during the 2018 elections women candidates were targeted with smear campaigns, where manipulation techniques were used to harass and sexualize them (Freedom House, 2019).

In early 2019 the first coordinated network of Twitter accounts aligned to the new administration of AMLO were observed. Semibots and human accounts attacked and aimed to suppressed speech of media and users who criticized the new president (Freedom House, 2019). Even though the hashtags #chayoteros (Spanish for journalists that take bribes) and #PrensaFifi (Spanish for posh press) had been used before, during January and February they became trending topics (Signa_Lab, 2019). The president also posted on social media “against certain journalists and news outlets that criticize him” (Freedom House, 2019). That was the case, for instance, of media outlet Reforma. In April, following AMLO’s statement, pro-government accounts attacked the editor of the outlet with the hashtag #NarcoReforma (Freedom House, 2019). However, in none of these events is there evidence of a coordinated operation from within the government.

Later that year the hashtags #PrensaSicaria, #PrensaProstituida, and #PrensaCorrupta (Spanish for hired killer media, prostituted media and corrupted media, respectively) became trending topics as a response to anti-government messages after AMLO confronted some journalists, when he put in doubt the engagement of media on veracity of information. The government, through its Secretary of Security and Civilian Protection, immediately presented a report on

the anti-government network on Twitter, stating that content was created by real users (76%) and bots (24%). Additionally, it was mentioned that the activity was highly associated with accounts owned by people associated to high-profile opposition (Redacción AN/GH, 2019).
Finally, in September 2019 the government announced the redesign of the security forces the creation of the National Guard. A number of social media accounts criticized the institution and, according to the Secretary of Security and Civilian Protection, there were five hundred thousand bots behind these operations, managed by two companies (Redacción Animal Político, 2019). However, no further evidence was shown.

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Mexico

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Bots, Human, Fake and Real	Support, Attack opposition, Suppressing	Disinformation, Data-driven strategies, Trolls, Amplifying content	Twitter, WhatsApp, Facebook

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

The 2018 Mexican elections were marked by an increase in digital campaigning expenditure, averaging 25% of campaign budgets, up from 5% six years previously. The estimates are that Andrés Manuel López Obrador spent approximately 88 million pesos, while candidates Ricardo Anaya and José Antonio Meade spent 338 million and 302 million pesos respectively (Forbes Staff, 2018).

The already mentioned Cultura Colectiva received in 2016 around 200,000 dollars (4 million pesos) from Peña Nieto's administration, 25,000 dollars from Miguel Ángel Mancera, Head of Government of the Federal District, and more than 750,000 dollars in advertisement by the Federal Government. According to the annual reports of Social Communication, it received additional 900,000 and 300,000 dollars in 2017 and 2018, respectively (Camhaji, 2019).

Table 3: Cyber Troop Capacity in Mexico

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
	Cultura Colectiva received around 2.175.000 dollars in contracts in contracts with several government institutions and public servants during Peña Nieto's administration.	Temporary	Decentralised	Medium

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

References

Alberto Melchor. (2018, July 2). *Muertos, tiroteos y robo de urnas deja la elección en Puebla | e-consulta.com 2019*. e-consulta Puebla | Referencia obligada. https://www.e-consulta.com/nota/2018-07-02/seguridad/muertos-tiroteos-y-robo-de-urnas-deja-la-eleccion-en-puebla

Andalusia Knoll Soloff. (2018, May 15). *Mexico is one of the world's most dangerous places for journalists. People are demanding action.* NBC News. https://www.nbcnews.com/news/latino/mexico-one-world-s-most-dangerous-places-journalists-people-are-n874091

Argüello, L. B., Donara Barojan, Roberta Braga, Jose Luis Peñarredonda, Maria Fernanda Pérez. (s. f.). *Disinformation in Democracies: Strengthening Digital Resilience in Latin America*. Atlantic Council. https://www.atlanticcouncil.org/publications/reports/disinformation-democracies-strengthening-digital-resilience-latin-america

Camhaji, E. (2019, April 10). 'Cultura Colectiva': El escándalo detrás de 540 millones de 'me gusta'. *El País*. https://elpais.com/internacional/2019/04/09/mexico/1554830383_929383.html

@DFRLab. (2018, June 28). #ElectionWatch: Trending Beyond Borders in Mexico. *DFRLab*. https://medium.com/dfrlab/electionwatch-trending-beyond-borders-in-mexico-2a195ecc78f4

Etelekt. (2018, July 9). *Séptimo Informe de Violencia Política en México 2018*. http://www.etellekt.com/reporte/septimo-informe-de-violencia-politica-en-mexico.html

Forbes Staff. (2018, March 30). *Cambridge Analytica trabajó con el PRI: Channel 4 News • Forbes México*. https://www.forbes.com.mx/cambridge-analytica-mexico-pri-enero-2018-channel-4-news/

Freedom House. (2019). *Mexico*. Freedom House. https://freedomhouse.org/country/mexico/freedom-net/2019

Freedom House. (2018) *Freedom on the Net 2018—Mexico*. https://freedomhouse.org/report/freedom-net/2018/mexico

Gutiérrez Rentería, M. E. (2019). *Mexico* (Digital News Report). http://www.digitalnewsreport.org/survey/2019/mexico-2019/

Numeralia Proceso Electoral 2017-2018. (s. f.). Instituto Nacional Electoral. https://www.ine.mx/wp-content/uploads/2018/08/1Numeralia01072018-SIJE08072018findocx-3.pdf

Ojeda de la Torre, I. (2020, March 1). *Peña fue el rey de los seguidores falsos y baratos en Twitter, dice experto. Hoy sólo es un fantasma*. SinEmbargo MX. https://www.sinembargo.mx/01-03-2020/3737975

Olvera, D. (2020, February 29). Cambridge Analytica se vio con Peña, el PRI y Slim en 2017, previo a la elección, confiesa ex directiva. https://www.sinembargo.mx/29-02-2020/3738856

Redacción AN/GH. (2019, November 4). Este es el estudio de redes sociales que liga a hijo de Calderón, Aurelio Nuño y Romero Hicks con granjas de bots. *Aristegui Noticias*. https://aristeguinoticias.com/0411/mexico/este-es-el-estudio-de-redes-sociales-que-liga-a-hijo-de-calderon-aurelio-nuno-y-romero-hicks-con-granjas-de-bots/

Redacción Animal Político. (2019, September 24). 500 mil bots se dedican a criticar a la Guardia Nacional, acusa el secretario Alfonso Durazo. *Animal Político*. https://www.animalpolitico.com/2019/09/guardia-naciona-bots-criticas-durazo/

Signa_Lab. (2019, February 28). Signa_Lab—Democracia, libertad de expresión y esfera digital. Análisis de tendencias y topologías en Twitter. El caso de la #RedAMLOVE. http://signalab.iteso.mx/informes/informe_redamlove.html

Statista. (s. f.). • *Mexico: Social network penetration 2018 | Statistic*. https://www.statista.com/statistics/449869/mexico-social-network-penetration/

Woody, C. (2018, January 6). McMaster: US has seen signs of Russian «subversion and disinformation» in upcoming Mexican election. *Business Insider*. http://uk.businessinsider.com/mcmaster-us-russia-interference-mexico-election-2018-1

MOLDOVA

Introduction

Moldova is a partly free democracy with a generally competitive political environment in which personal freedoms are mostly respected. However, the country suffers from pervasive corruption, non-transparent relations between political actors and private business, and a rule of law susceptible to political pressures[1]. The presence of computational propaganda in Moldova has come to light in 2019 as a result of parliamentary elections in February as the campaign time was characterised by disinformation and inauthentic activity on social media[2]. Additionally, local media outlets suffer from bias, as most are affiliated with political actors and any free and independent journalists are hampered in their work and experience harassment from state authorities; for example, under the previous administration (before 2019 elections) over 50 individuals from the opposition, civil society and mass media were wiretapped by the government[3].

Moreover, efforts of disinformation in Moldova are interconnected with Russia, as independent Moldovan media have been engaged in an information war with the Kremlin for years[4]. The Ukrainian NGO Prism, in a 2018 study on disinformation resilience in central and eastern Europe, found that Moldova was the "most exposed country in Eastern Europe to Russian propaganda" as a result of the dominance of Russian-language media, the Russian orientation of the church, and the mistrust in the political class[5]. A main issue in relation to Russian influence is that Russian-language outlets or media re-broadcasting Russian channels outnumber local ones and Russian social networks are used by many Moldovans[6].

An Overview of Cyber Troop Activity in Moldova

Organizational Form

Ahead of the parliamentary elections on 24 February 2019, a network of Moldovan troll accounts set up fake Facebook accounts to pose as legitimate voters and civic groups. These accounts disseminated fake news, disinformation and memes ahead of the elections[7]. The fake accounts also coordinated with legitimate actors to overwhelm web forums and manipulate the online debate. Facebook concluded that "some of this activity was linked to employees of the Moldovan government[8]. The government responded by suggesting that any fraudulent activity by government workers on behalf of the Democratic Party was carried out by rogue workers[9].

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Moldova

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
		x			x

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Fake accounts impersonating groups or individuals are a common tactic in Moldova. The taken down accounts on Facebook typically posted about local news and political issues, but also shared manipulated photos, divisive narratives and satire. In the takedown of activity on 13 February, Facebook removed 168 accounts, 28 pages and 8 Instagram accounts for engaging in coordinated inauthentic behaviour targeting people in Moldova[10]. According to activists involved in the takedown, these Facebook trolls operating from Moldova to attack particular actors employ the behavioral patterns of Russian trolls, though there is no proof of a training or collaboration between Russian and Moldovan trolls[11].

An example of an organization targeted by a fake account was the fact-checking group StopFals, a misinformation watchdog based in the capital, Chisinau, created to call out misinformation on social media[12]. Cornelia Cozonac, the director for the Centre of Investigative Journalism in Moldova, was impersonated when trolls made a clone of her account and posted messages in her name to attempt to discredit her. These messages were republished by obscure news websites and then amplified by other trolls on social media[13].

Next to fake accounts, fake news remains a widespread problem in Moldova. Anti-European Union messages often proliferate, such as the rumor that the EU was sending thousands of Syrian refugees into Moldova[14]. Reports allegedly coming from Russian TV and retranslated by the Moldovan TV channels claimed that there was a massive wave of Syrian refugees on the way to Moldova, with one report claiming that an "invasion of 30,000 Syrians in Moldova" would occur if the pro-European candidate were to win the election[15].

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Moldova

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Human, Bots	Supressing, Driving divisions	Disinformation, Trolls, Amplifying content	Facebook, Instagram

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

According to Facebook, the network of trolls and bots they took down spent less than $20,000 on ads on Facebook and Instagram, which were paid for in US dollars, euros and Romanian leu. While Facebook and other sources have claimed a connection to Moldovan political actors, they were quick to deny it[16]. Similarly, while the activities on Facebook were coordinated, it is not clear whether the government or other political actors had anything to do with this coordination. Thus, from a state cyber troop perspective, Moldova seems to be of liminal capacity, though disinformation and amplification techniques remain a continuous concern for the country.

Table 3: Cyber Troop Capacity in Moldova

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
		Temporary	Decentralised	Low

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

In light of the recent COVID-19 pandemic, digital rights observers have noted that Moldovan authorities have taken the virus as a reason to extend the amount of time they will take to respond to freedom of information requests, sometimes not answering at all. Media watchdogs see this as a worrying crackdown on press freedom[17].

References

Banja, L. (2019, December 25). Heroes of 2019: People Who Took Action for Positive Change. *Balkan Insight*. https://balkaninsight.com/2019/12/25/heroes-of-2019-people-who-took-action-for-positive-change/

BBC News. (2019, February 14). *Moldovan election prompts Facebook to remove accounts—BBC News*. https://www.bbc.co.uk/news/world-europe-47237920

Broderick, R. (2019, March 1). These Developers Say It Took Three Years And A Chance Meeting To Get Facebook To Deal With Their Country’s Fake News. *Buzzfeed News*. https://www.buzzfeednews.com/article/ryanhatesthis/trollless-moldova

Facebook. (2019, February 14). Removing Coordinated Inauthentic Behavior From Moldova. *Facebook Newsroom*. https://about.fb.com/news/2019/02/cib-from-moldova/

Freedom House | Moldova. (2020). Freedom House. https://freedomhouse.org/country/moldova/freedom-world/2020

IWPR. (2019, August 12). Moldova Battles Hybrid Threat. *Institute for War and Peace Reporting*. https://iwpr.net/global-voices/moldova-battles-hybrid-threat

Necsutu, M. (2018, July 26). *Moldova Highly “Vulnerable” to Russian Propaganda, Study Says | Balkan Insight*. Balkan Insight. https://balkaninsight.com/2018/07/26/moldova-the-most-vulnerable-country-to-russian-propaganda-07-26-2018/

Necsutu, M. (2019, February 14). *Facebook Shuts Moldova Officials’ “Fake News” Accounts | Balkan Insight*. Balkan Insight. https://balkaninsight.com/2019/02/14/facebook-shuts-moldova-officials-fake-news-accounts/

Nikolic, I., Barberá, M. G., Kajosevic, S., & Necsutu, M. (2020, April 6). Central and Eastern Europe Freedom of Information Rights ‘Postponed.’ *Balkan Insight*. https://balkaninsight.com/2020/04/06/central-and-eastern-europe-freedom-of-information-rights-postponed/

Polygraph.info. (2018, October 24). *The ‘Art of Fake News’ – How Independent Moldovan Media Fight Russian Disinformation*. Polygraph. https://www.polygraph.info/a/disinfo-moldova-russia/29557985.html

Synovitz, Ron. (2019, February 27). Copycat Hacks: Moldovan Facebook Trolls Used Russian Tactics To Promote Kremlin Foes. *RadioFreeEurope/RadioLiberty*. https://www.rferl.org/a/moldovan-facebook-trolls-used-russian-tactics-to-promote-kremlin-foes/29793394.html

Synovitz, Roy, & Raileanu, D. (2019, February 27). *Copycat Hacks: Moldovan Facebook Trolls Used Russian Tactics To Promote Kremlin Foes*. Radio Free Europe. https://www.rferl.org/a/moldovan-facebook-trolls-used-russian-tactics-to-promote-kremlin-foes/29793394.html

MYANMAR

Introduction

In 2015 Myanmar held an election deemed relatively free by Freedom House that left the country to the leadership of the National League for Democracy (NLD). However, the transition from military dictatorship to democracy has since come to a halt as human rights are not protected and the military retained significant influence: In 2017 military operations forced over 900,000 members of Myanmar's Rohingya minority to flee the country, while journalists, demonstrators and even ordinary people risked detention and unfair convictions if they voiced dissent. As a result, Freedom House now classifies the countries as "not free" (Freedom House, 2020a). On November 8, 2020 the country held elections which saw the NLD with their leader Aung San Suu Kyi winning 63% of the seats in the House of Nationalities and 58% in the House of Representatives, which together make up the national-level bicameral legislature in Myanmar. Next to the military, which receives 25% of seats in both Houses by default, the NLD's main opposition was the Union Solidarity and Development Party (USDP), which received 3% and 5.9% in each house respectively (Reuters, 2020).

Internet access continues to increase throughout Myanmar. In 2020 about 41% of the population used the internet as well as social media, most do so through their smartphones (Kemp, 2020). Facebook and other "zero-rate"[1] mobile apps are among the most popular to access the internet (Hynes, 2017). Yet, despite Facebook's dominance in Myanmar—a market that has been prone to ethnic violence for years—it has devoted limited resources to combat hate speech and disinformation (CBS News, 2018; Stecklow, 2018). It was not until fall of 2018 that Facebook identified and removed 28 accounts and 65 pages operated by Myanmar military personnel which had amassed over 13-million unique followers (Facebook Newsroom, 2018). For several years, coordinated disinformation campaigns on Facebook went largely unchecked, serving to foster a climate in which hate speech thrives and violence is legitimized (Fink, 2018). Facebook has since taken down several other instances of "coordinated inauthentic behavior" originating in Myanmar by military personnel (see for example Gleicher, 2020a, 2020b), and have announced measures to prepare for the 2020 elections, which include increasing the efficiency for detecting and removing hate speech, content that incites violence as well as misinformation that could lead to voter suppression (Frankel, 2020). However, with the election on the horizon, Myanmar was still seeing large amounts of mis-and-disinformation spreading online (The Economist, 2020). It is against this backdrop that we examine cyber troop activity in Myanmar.

An Overview of Cyber Troop Activity in Myanmar

Organizational Form

While Freedom House observed a relative freedom for political parties to prepare ahead of the 2015 and the 2020 election, they still noted an unfair advantage for the USDP as they receive systematic support from the military (Freedom House, 2020a). As it stands, most attempts at influencing the public or interfering with public and political activities are driven by the military, especially cyber troop activities: Over the past decade, Myanmar military has used social media to incite communal violence against minority ethnic communities in the country (Christina Fink, 2018a), with personnel posing as celebrities, pop stars and national heroes as they flooded Facebook with anti-Muslim rhetoric and calls for the ethnic cleansing of the Rohingya, a Muslim minority in Myanmar (Mozur, 2018). Dozens of accounts—created as part of a covert military propaganda operation—positioned themselves as independent sources of news and information, disseminating false, fearmongering, and incendiary content about the Rohingya (Douek, 2018; Freedom House, 2020b; Mozur, 2018).

At the same time, other governmental institutions are known to be involved with controlling and influencing the information landscape in Myanmar. State-run media controlled by the government produce a majority of information available domestically. Current law allows authorities to deny licenses and prosecute media outlets that are considered insulting to religion or a threat to national security. Online spaces are under heavy surveillance through both the government and the military and online activities can be criminally punished for similar reasons as media outlets: the government (previous to the 2020 elections) was reportedly working on a cyberlaw that would allow criticism of the state to be criminally punished (Freedom House, 2020b). The government has also engaged in internet shutdowns in some regions (Rahkine and Chin) which lasted several months from 2019 to 2020 (Freedom House, 2020a). Ahead of the November 2020 elections, online censorship drastically increased and the Ministry of Transport and Communications ordered service providers to block a total of 2,147 websites including independent and regional news outlets such as Voice of Myanmar in March 2020 (Freedom House, 2020b; ချမ်းသာ & အောင်ငြိမ်းချမ်, 2020).Given the intertwined nature of the government and the military it is hard to tell whether these activities are specifically military, or wholly state-driven.

There have also been instances of commercial disinformation in Myanmar. In early 2020 the Atlantic Council's Digital Forensic Research Lab reported a network of 23 assets being removed from Facebook for coordinated inauthentic behavior. This network seems to have worked for the telecommunication company MyTel, though it appears that the activity was focused on attacking competitors of MyTel in order to increase own user numbers and revenues, rather than being a network that MyTel offered for hire to spread disinformation in behalf of third parties (DFRLab, 2020). However, MyTel is a joint venture owned by three major groups, which include Myanmar's military and VietTel, owned by the Vietnamese Ministry of Defense. Some observers thus fear that this operation had the ultimate goal of increasing the military's control over Myanmar's internet (Long & Wazir, 2020).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Myanmar

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
	X				

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Ahead of the 2020 election Myanmar's Union Election Commission established a social media monitoring mechanism to flag and remove hateful and harmful online content, particularly on Facebook. How successful this mechanism was remains unclear, as Facebook was reluctant to cooperate at first, and has a past of not reacting to warnings of hate speech and misinformation in Myanmar, even when flagged by the government (Douek, 2018; Freedom House, 2020b; Stecklow, 2018). At the same time, this administrative effort was quite unique, as governmental institutions had thus far failed to properly address the issue of misinformation perpetuating intolerance, hate and violence online (Eleven Myanmar Asia News Network, 2018; Freedom House, 2020b; The Irrawaddy, 2018).

Such failure is not surprising, though, as both the military and government are involved in disinformation campaigns themselves. As part of the ongoing disinformation campaigns targeting the Rohingyia minority, cyber troops have used fake Facebook accounts to systematically spread disinformation for years, calling the Rohingya and other Muslims “dogs, maggots and rapists, suggest they be fed to pigs, and urge they be shot or exterminated” (Stecklow, 2018). According to some reports, nearly 700 military officials were involved in systematic disinformation campaigns, most focused on attacking Myanmar’s Rohingya minority, that continued online for five years before Facebook started banning accounts on their platform in 2018 (Freedom House, 2020b; Gleicher, 2019; McLaughlin, 2018; Mozur, 2018; Su, 2018).

Several NGOs and civil society activists prepared for the elections in November 2020 by creating fact-checking organizations and partnerships. These groups have reported seeing the spread of disinformation in the leadup to elections (The Economist, 2020). Other networks attacked the NLD at large, claiming that they plan to introduce tax laws that would leave the poor even poorer, or would restart building the Myitsone Dam with support of China, a project that has been suspended almost ten years ago (Kyaw et al., 2020).

There have also been instances of data-driven targeting strategies in Myanmar, with political advertisements being purchased by some of the fake networks operating on Facebook and other pages being taken down by Facebook specifically for coordinated inauthentic behavior rather than content violations (Facebook Newsroom, 2018). In addition, scholars suspect a mix of automated bot accounts and human curated accounts operating on social media. Fake accounts have taken on human personas and have impersonated popular celebrities and other influencers in the country (Mozur, 2018). In other instances, fake accounts posed as a subsidiary of existing media, such as a page called ‘Radio Free Myanmar’ (RFM), which imitated the logo of Radio Free Asia (a US-funded non-profit international broadcasting corporation) and published at least 10 false news stories a day, mainly attacking the NLD and civil societies including fact-checking organizations (Palatino, 2020). Interestingly, the RFM network deliberately avoided data-driven strategies and encouraged supporters to simply copy and paste their content and templates, most likely to avoid being detected and shut down (Kyaw et al., 2020). With regards to platforms, many of the campaigns in Myanmar have taken place on Facebook, as it is the most widely used platform in the country, as well as the Facebook-owned chat application WhatsApp (Malhotra, 2017; Paj, 2019).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Myanmar

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Bots, Humans	Progovernment Messaging, Attacks on Opposition, Suppressing Political Speech/Participation, Polarization	Disinformation, Data-Driven Strategies, Trolling, Amplification	Facebook WhatsApp

Source: Authors’ evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

There is very little data about the organizational capacity of cyber troop activity in Myanmar. Facebook has taken down accounts linked to military cyber troops, with less than $1,200 spending on political advertisements. However, the MyTel disinformation campaign disclosed by Facebook spent approximately $2,255,000 on Facebook ads.

Table 3: Cyber Troop Capacity in Myanmar

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
	<$1,200 on Facebook Ads	Permanent	Coordinated	High

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

References

CBS News. (2018, August 21). Facebook failing to tackle hate speech in Myanmar, investigative report finds. *CBS News*. https://www.cbsnews.com/news/facebook-failing-to-tackle-hate-speech-in-myanmar-investigative-report-finds/

Christina Fink. (2018a). Myanmar: Religious Minorities and Constitutional Questions. *Asian Affairs*, *49*(2), 259–277. https://doi.org/10.1080/03068374.2018.1469860

Christina Fink. (2018b). Dangerous Speech, Anti-Muslim Violence, and Facebook in Myanmar. *Columbia Journal of International Affairs*, *71*(1.5). https://jia.sipa.columbia.edu/dangerous-speech-anti-muslim-violence-and-facebook-myanmar

DFRLab. (2020, December 2). Facebook shut down commercial disinformation network based in Myanmar and Vietnam. *Medium*. https://medium.com/dfrlab/facebook-shut-down-commercial-disinformation-network-based-in-myanmar-and-vietnam-d8c07c518c04

Douek, E. (2018, October 22). Facebook's Role in the Genocide in Myanmar: New Reporting Complicates the Narrative. *Lawfare*. https://www.lawfareblog.com/facebooks-role-genocide-myanmar-new-reporting-complicates-narrative

Eleven Myanmar Asia News Network. (2018, June 9). Facebook closes some accounts of Myanmar hard-liners. *Nation Thailand*. https://www.nationthailand.com/breakingnews/30347347

Facebook Newsroom. (2018, August 28). *Removing Myanmar Military Officials From Facebook*. https://newsroom.fb.com/news/2018/08/removing-myanmar-officials/

Frankel, R. (2020, August 31). How Facebook Is Preparing for Myanmar's 2020 Election—About Facebook. *About Facebook*. https://about.fb.com/news/2020/08/preparing-for-myanmars-2020-election/

Freedom House. (2020a). *Freedom House | Myanmar*. Freedom House. https://freedomhouse.org/country/myanmar/freedom-world/2020

Freedom House. (2020b). *Freedom on the Net | Myanmar*. Freedom House. https://freedomhouse.org/country/myanmar/freedom-net/2020

Gleicher, N. (2019, August 21). Taking Down More Coordinated Inauthentic Behavior in Myanmar. *About Facebook*. https://about.fb.com/news/2019/08/more-cib-myanmar/

Gleicher, N. (2020a, February 12). Removing Coordinated Inauthentic Behavior From Russia, Iran, Vietnam and Myanmar. *About Facebook*. https://about.fb.com/news/2020/02/removing-coordinated-inauthentic-behavior/

Gleicher, N. (2020b, October 27). Removing Coordinated Inauthentic Behavior. *About Facebook*. https://about.fb.com/news/2020/10/removing-coordinated-inauthentic-behavior-mexico-iran-myanmar/

Hynes, C. (2017, September 22). Internet Use Is On The Rise In Myanmar, But Better Options Are Needed. *Forbes*. https://www.forbes.com/sites/chynes/2017/09/22/internet-use-is-on-the-rise-in-myanmar-but-better-options-are-needed/

Kemp, S. (2020). *Digital 2020: Myanmar*. Datareportal. https://datareportal.com/reports/digital-2020-myanmar

Kyaw, B., Naung, P. H., & Nachemson, A. (2020, October 9). Radio Free Myanmar: Disinformation network spreads false news and hate speech. *Frontier Myanmar*. https://www.frontiermyanmar.net/en/radio-free-myanmar-disinformation-network-spreads-false-news-and-hate-speech/

Long, K., & Wazir, B. (2020, July 23). Military-backed company in Myanmar seeks control of the country's internet. *Coda Story*. https://www.codastory.com/authoritarian-tech/myanmar-fake-news/

Malhotra, A. (2017, October 24). Watching the Rohingya crisis through WhatsApp. *Deutsche Welle*. https://www.dw.com/en/watching-the-rohingya-crisis-through-whatsapp/a-41092184

McLaughlin, T. (2018, July 6). How Facebook's Rise Fueled Chaos and Confusion in Myanmar. *Wired*. https://www.wired.com/story/how-facebooks-rise-fueled-chaos-and-confusion-in-myanmar/

Mozur, P. (2018, October 18). A Genocide Incited on Facebook, With Posts From Myanmar's Military. *The New York Times*. https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html

Paj, P. (2019, July 8). We Need to Deal With WhatsApp's Misinformation Problem. *Pro Market.Org*. https://promarket.org/2019/07/08/we-need-to-deal-with-whatsapp-misinformation-problem/

Palatino, M. (2020, October 23). Fighting disinformation and fact-checking the Myanmar election · Global Voices. *Global Voices*. https://globalvoices.org/2020/10/23/fighting-disinformation-and-fact-checking-the-myanmar-election/

Reuters. (2020, November 10). Aung San Suu Kyi's ruling party claims resounding election win in Myanmar. *CNN*. https://www.cnn.com/2020/11/09/asia/myanmar-election-results-nld-intl-hnk/index.html

Stecklow, S. (2018, August 18). Why Facebook is losing the war on hate speech in Myanmar. *Reuters*. https://www.reuters.com/investigates/special-report/myanmar-facebook-hate/

Su, S. (2018, August 16). Update on Myanmar. *About Facebook*. https://about.fb.com/news/2018/08/update-on-myanmar/

The Economist. (2020, October 24). In Myanmar, Facebook struggles with a deluge of disinformation. *The Economist*. https://www.economist.com/asia/2020/10/22/in-myanmar-facebook-struggles-with-a-deluge-of-disinformation

The Irrawaddy. (2018, June 12). WhatsApp the Media Platform of Choice for ARSA. *The Irrawaddy*. https://www.irrawaddy.com/news/burma/whatsapp-the-media-platform-of-choice-for-arsa.html

United Nations Human Rights Council. (2018). OHCHR | Myanmar: UN Fact-Finding Mission releases its full account of massive violations by military in Rakhine, Kachin and Shan States. United Nations Human Rights Council. https://www.ohchr.org/EN/HRBodies/HRC/Pages/NewsDetail.aspx?NewsID=23575&LangID=E

ချမ်းသာ, & အောင်ငြိမ်းချမ်. (2020, March 26). ရခိုင်သတင်းဌာန ၂ ခု၊ AA တို့၏ ဝက်ဘ်ဆိုက်များကို ဖုန်းအော်ပရေတာ ၂ ခုက ပိတ်. *Myanmar Now*. https://www.myanmar-now.org/mm/news/3391

The Netherlands

Introduction

The Netherlands is considered a free and democratic country with a Freedom House Index of 99/100 in the 2020 report. As with many established democracies, there are few reports on government-organized misinformation or online propaganda campaigns in the Netherlands. Still, Dutch political parties (especially the nationalist Party for Freedom (PVV)) actively use social media to communicate with their voters. While the country prides itself on protecting political rights and civil liberties, in recent times online political debate has been dominated by worries of immigration and anti-Islamic sentiment (Freedom House, 2020).

An Overview of Cyber Troop Activity in the Netherlands

Organizational Form

Recent reports have focused on Geert Wilders, chairman of the PVV, as most disinformation - mainly Islamophobic content - originates from him. However, parties from across the political spectrum are present on major social media platforms and interact with voters, presenting their viewpoints and occasionally attempting to influence public debate. At the same time, the Netherlands is also facing trolling and misinformation attacks which are likely to have originated from the Russian Internet Research Agency (IRA).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in the Netherlands

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
		x			

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

In light of a published list of candidates running in state elections in 2019, the newspaper Dagblad van het Noord found right-wing, anti-Islamic tweets from several candidates campaigning for border control (Bakker, 2019). Nevertheless, Wilders remains on the forefront of attacking the Islam, and recently took to attacking the religion as being the main reason behind rising antisemitism in the Netherlands during a parliamentary debate in February ("Debate in Dutch Parliament about antisemitism on the rise in The Netherlands", 2020). His words have since been picked up by newspapers in Israel who champion him as “the Netherland’s most informed and intellectually courageous politician on the subject of Islam” (Bostom, 2020). Wilders continues to ridicule Islam and held a Prophet Mohammed cartoon competition (Figure 1) in late December 2019, to demonstrate the importance of freedom of speech (Reuters, 2020). Initially, he had tried to run the competition in 2018, but cancelled it after reportedly receiving death threats (Osborne, 2018).

In November 2018, the Turkish Islamic Cultural Federation (TICF) which represents 144 Dutch mosques, sent a request to Twitter asking them to shut down Wilders’ Twitter account as he was violating Twitter’s terms of use with his anti-Islamic messages (Pieters, 2018a). The TICF said it would consider legal action should Twitter not take any action (France24, 2018), however, since the early November 2018 request there have been no reports of them taking any further steps. In May 2019 Wilders’ account was suspended by Twitter (Figure 2), reportedly over a Tweet attacking the progressive-left party Democrats 66 (D66) (Schumacher, 2019). The suspension did not last long though, and at present his account is active again.

Concerning misinformation and trolling activities by the IRA, the first incident, traced back to the IRA in 2016, has been dubbed the 'Dutch Terror Threat' ("Behind the Dutch Terror Threat Video: The St. Petersburg 'Troll Factory' Connection," 2016), which was reported on in last year's Cyber Troop case study report. In general, however, investigations have found that Russian trolling activity in the Netherlands has not led to a 'Trump effect' and remains relatively uninfluential (DutchNews.nl, 2018).

As a reaction to these trolling activities from Russia and misinformation campaigns from the PVV, the Dutch government decided to launch an Anti-Fake-News campaign on social media lasting four months during both the state elections in March and the EU parliamentary elections in May 2019 (Pieters, 2018b).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in the Netherlands

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Human	Attacking, Driving Divisions	Disinformation	Twitter

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

For the most part, Dutch political parties regularly engage with their voters through social media, mainly Twitter. Wilders has seen his Twitter following shrink throughout 2018 as Twitter culled fake accounts. Wilders lost about 15% of his twitter followers in summer 2018 (150,000 followers), while Prime Minister Rutte lost only a handful of followers (DutchNews.nl, 2018).

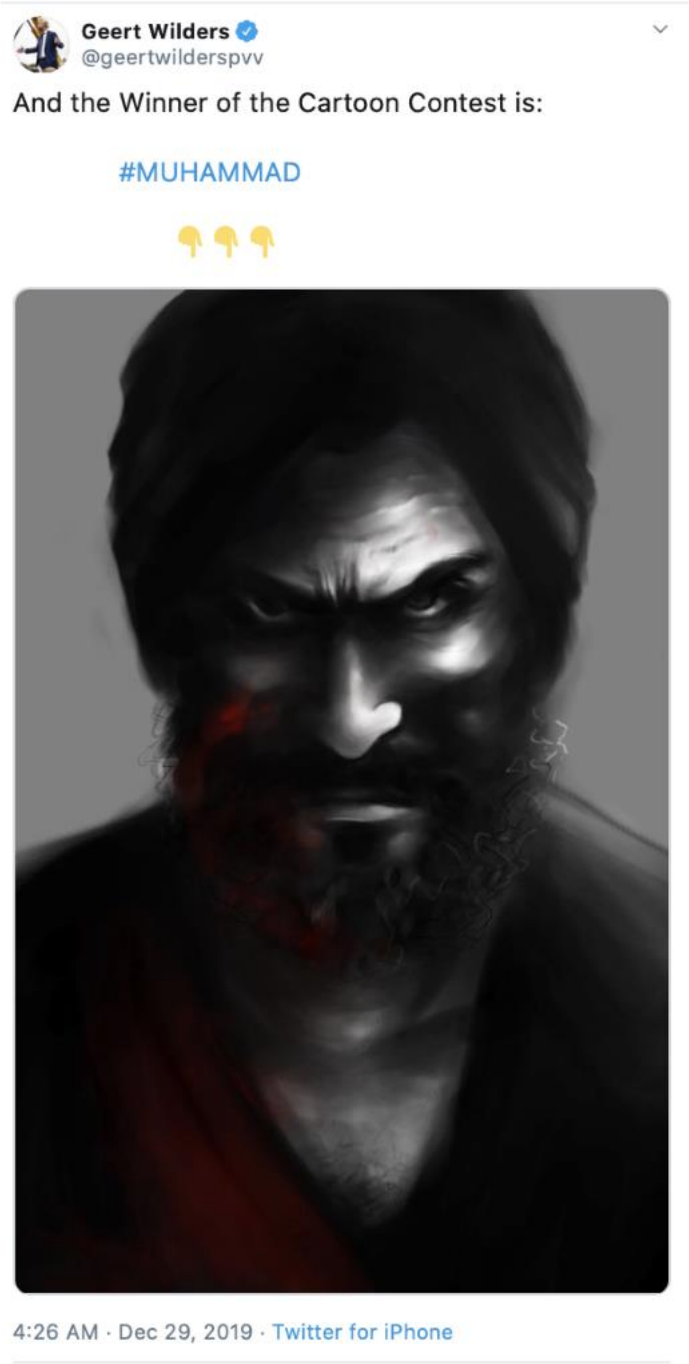
Meanwhile, Russia-based professional trolls have sent over nine hundred tweets in Dutch in the past two years and set up more than six thousand troll Twitter accounts posing as genuine Dutch citizens. These accounts have generated more than thirty thousand messages in English and have a combined following of more than 9.5 million *(DutchNews.nl, 2018)*. Most tweets and retweets focus on conspiracy theories surrounding the MH17 disaster and Wilders. Interestingly, messages in English seem to circulate better than those in Dutch (van der Noordaa & van de Ven, 2018). In early March 2020 the Russian-lead disinformation campaign around the MH17 disaster started picking up again as the Netherlands started prosecuting four suspects of Russian and Ukrainian nationality for murder as they are alleged to have been involved in the collusion that ultimately lead to the attack. Russia continues to deny their involvement with the shootdown (Deutsch & van den Berg, 2020; Fomina, 2020). Russia apparently also offered to try three of the suspects, which are Russian nationals, in Russia, which the Dutch Minister of Justice refused in October of last year (van den Berg, 2020).

The Dutch intelligence services - mainly the General Intelligence and Security Services (AIVD) - are also reacting to the growing threat of digital espionage and foreign trolling. The budget received by Dutch intelligence increases year-on-year, and The National Cyber Security Centrum highlights espionage and sabotage threats originating from China, Iran or Russia as primary concerns in their 2019 cyber security assessment report (CSAN 2019, 2019).

Table 3: Cyber Troop Capacity in the Netherlands

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
		Temporary (both Russian and Dutch activities in NL)		

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.



Geert Wilders
@geertwilderspvv

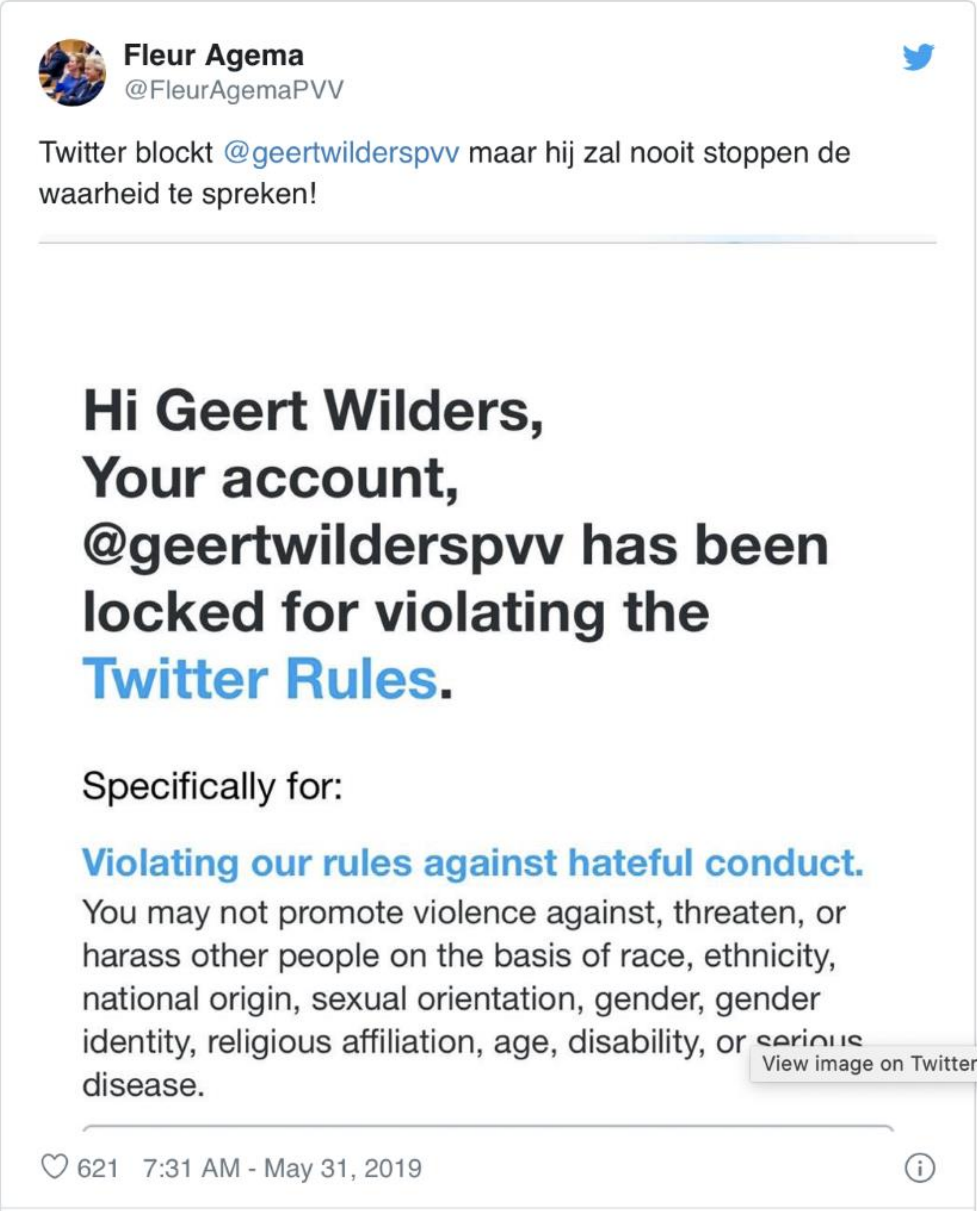
And the Winner of the Cartoon Contest is:

#MUHAMMAD

👇👇👇

4:26 AM · Dec 29, 2019 · Twitter for iPhone

Figure 1: Winner of the Prophet Mohammed cartoon contest held by Geert Wilders in December 2019 (source: https://twitter.com/geertwilderspvv/status/1211141394309533697)



Fleur Agema
@FleurAgemaPVV

Twitter blockt @geertwilderspvv maar hij zal nooit stoppen de waarheid te spreken!

Hi Geert Wilders,
Your account, @geertwilderspvv has been locked for violating the Twitter Rules.

Specifically for:

Violating our rules against hateful conduct.
You may not promote violence against, threaten, or harass other people on the basis of race, ethnicity, national origin, sexual orientation, gender, gender identity, religious affiliation, age, disability, or serious disease.

View image on Twitter

♡ 621 7:31 AM - May 31, 2019

Figure 2: Party colleague Fleur Agema criticising Twitter for suspending Wilders' account (source: https://www.dw.com/en/dutch-populist-geert-wilders-blocked-by-twitter/a-48989709)

References

Bakker, C. (2019, December 2). *Kandidaat Statenlid op Twitter: "Hoezo vluchtelingen? Verkrachters en haatzaaiers."* https://www.dvhn.nl/groningen/Kandidaat-Statenlid-op-Twitter-Hoezo-vluchtelingen-Verkrachters-en-haatzaaiers-24172956.html

Behind the Dutch Terror Threat Video: The St. Petersburg "Troll Factory" Connection. (2016, March 4). *Bellingcat*. https://www.bellingcat.com/news/uk-and-europe/2016/04/03/azov-video/

Bostom, A. G. (2020, February 19). Only Wilders decries the Islam fueling Western European Jew-hatred—Israel National News. *Arutz Sheva 7*. http://www.israelnationalnews.com/Articles/Article.aspx/25221

Cyber Security Assessment Netherlands. (2019). Dutch Ministry of Justice and Security.

Debate in Dutch Parliament about antisemitism on the rise in The Netherlands. (2020, February 18). https://www.youtube.com/watch?v=8aK4mxIKqiE&feature=youtu.be

Deutsch, A., & van den Berg, S. (2020, March 6). Dutch MH17 trial to start without Russian, Ukrainian suspects. *Reuters*. https://www.reuters.com/article/us-ukraine-crisis-mh17-idUSKBN20T0WZ

FOMINA, K. (2020, March 2). As Flight MH17 trial begins, Russia, unlike Iran, refuses to admit guilt. *Coda Story*. https://codastory.com/disinformation/flight-mh17-trial-disinformation/

Mosques seek Twitter ban on Dutch populist Geert Wilders. (2018, May 11). *France 24*. https://www.france24.com/en/20181105-mosques-seek-twitter-ban-dutch-populist-geert-wilders

Freedom House (2020). *Netherlands | Freedom House*. Retrieved March 5, 2020, from https://freedomhouse.org/country/netherlands

Osborne, S. (2018, August 31). Dutch anti-Islam politician Geert Wilders cancels Prophet Muhammad cartoon competition. *The Independent*. https://www.independent.co.uk/news/world/europe/muhammad-cartoon-competition-cancelled-geert-wilders-netherlands-a8515801.html

Pieters, J. (2018a, November 5). *Mosques want populist politician Wilders banned from Twitter*. NL Times. https://nltimes.nl/2018/11/05/mosques-want-populist-politician-wilders-banned-twitter

Pieters, J. (2018b, December 13). Dutch government to launch anti-fake news campaign. *NL Times*. https://nltimes.nl/2018/12/13/dutch-government-launch-anti-fake-news-campaign

Reuters. (2020, December 29). Dutch anti-Islam lawmaker nixes controversial prophet Mohammad cartoon contest—World News—Haaretz.com. *Haaretz*. https://www.haaretz.com/world-news/dutch-anti-islam-lawmaker-nixes-controversial-prophet-mohammad-cartoon-contest-1.8327092

Robert van der Noordaa, & Coen van de Ven. (n.d.). Van vaccineren tot MH17: Russische trollen beïnvloeden ons online. *De Groene Amsterdammer*. https://www.groene.nl/artikel/hoe-russische-trollen-inspelen-op-westerse-angsten

Russian trolls fail to replicate "Trump effect" in Dutch Twittersphere. (2018, July 16). DutchNews.Nl. https://www.dutchnews.nl/news/2018/07/russian-trolls-fail-to-replicate-trump-effect-in-dutch-twittersphere/

Schumacher, E. (2019, May 31). Dutch populist Geert Wilders blocked by Twitter | News | DW | 31.05.2019. *Deutsche Welle*. https://www.dw.com/en/dutch-populist-geert-wilders-blocked-by-twitter/a-48989709

van den Berg, S. (2020, February 12). Dutch refused Moscow request to try MH17 Russian suspects there: Minister. *Reuters*. https://www.reuters.com/article/us-ukraine-crisis-mh17-idUSKBN2062VE

NIGERIA

Introduction

Nigeria is considered partly free by Freedom House, which has observed the country to be making progress in improving fair and democratic elections, though corruption and police brutality remain concerning. Additionally, Sharia statues are imposed in twelve states that include penalties for alleged press offenses (Freedom House, 2019a). A major threat to Nigerian national security is the Islamist terrorist group Boko Haram, which has recently been regaining influence and ground (France-Presse, 2020). In early 2018 the UN reported that a total of 60,000 people have been displaced in the North East of Nigeria due to ongoing hostilities (United Nations News, 2018). The response by military and law enforcement has been violent, including extrajudicial killings and torture (Freedom House, 2019a). There is a growing concern that these military activities are getting out of control, after an incident in October 2018 where soldiers responded to rock throwing protestors by shooting into the group and killing at least forty-five, with the actions subsequently defended by the military and the president (Freedom House, 2019a). This also serves as an example of how governmental institutions respond to public outrage: usually by furthering polarisation through social media, particularly Twitter (Searcey & Akinwotu, 2018).

Internet penetration in the country remains within the 20-30% range, with most access due to mobile phones rather than broadband connection. Moreover, power-cuts remain a threat to connectivity (Freedom House, 2019b). Nigeria's general election held in February 2019 was overshadowed by online manipulations and increased violence, harassment and prosecutions of journalists (Freedom House, 2019b). The two main candidates in the election were President Muhammadu Buhari of the All Progressives Congress (APC) and opposition candidate Atiku Abubakar from the People's Democratic Party (PDP). Ultimately, incumbent president Buhari won his re-election bid. In relation to the 2019 election season local journalists flagged the intense use of misinformation and fake news (BBC Reality Check, 2019; Busari, 2019). Additionally, an article published by Freedom House suggests that both candidates have likely been engaged in corrupt practices and bribery in the past (Brandt, 2018).

Concerning the outbreak of COVID-19, in contrast to other countries Nigeria has not been making many headlines with virus conspiracies, though they certainly exist. Rather, the pandemic highlighted the level of poverty in the country with many families being just as afraid of losing their job and having no food or water as they are of the virus (Akinwotu, 2020; BBC News, 2020; Mbah, 2020).

An Overview of Cyber Troop Activity in Nigeria

Organizational Form

While freedom of expression and the press is constitutionally guaranteed, in practice these freedoms are limited through the law and intimidation efforts such as arresting journalists. Moreover, Internet Service Providers block websites and take down content on request (Freedom House, 2019a, 2019b). Thus, there is a sense of direct control of information flow through the government, though governmental inferences with internet connectivity, or attempts at filtering and censorship are increasingly unusual. However, self-censorship has been increasing due to intimidation tactics, such as arrests under the 2015 Cybercrime Act (Freedom House, 2019b). At the same time Nigeria is no stranger to private contractors working to influence domestic audiences. In the aftermaths of the Cambridge Analytica scandal, it was revealed that the company was involved in Nigeria, where they were hired by a Nigerian billionaire to run a campaign to support Goodluck Jonathan (Cadwalladr, 2018). More recently in 2020, Facebook removed accounts from their platforms that engaged in coordinated inauthentic behaviour and seem to be linked to companies as well (Facebook, 2020).

In December 2017, the Digital Rights and Freedom Bill was passed by the House of Representatives. It has been celebrated as the first of its kind in Africa specifically intended to protect data privacy, free speech, press freedom and outline lawful interception and surveillance (Alabi, 2019b; Chiefe, 2019). However, in March 2018 the Senate proposed a broadly worded Bill on Hate Speech as well as an Internet Falsehood Manipulation Bill, which would seek to establish an independent National Commission for Hate Speech, which also stipulates death by hanging or life-imprisonment for those found guilty of any form of hate speech that led to the death of another person. The International Press Centre and NGOs have been raising concerns that these bills are a serious threat to the freedom of the press and safety of journalists (Abdulrauf, 2019; Amnesty International, 2019; Ijediogor, 2018). After the election, the president declined to sign the Digital Rights and Freedom Bill into law in March 2019, and the bill was subsequently revised and reintroduced to the House in July 2019 to address concerns of Buhari and subsequently passed on the first reading (Chiefe, 2019; Ojekunle, 2019; Olasupo, 2019; Sahara Reporters, 2019). The bills on hate speech and media manipulation remain controversial, with an overwhelming majority of Nigerians asking the Senate to strike them down. Interestingly, the Minister of Information recently denied any knowledge about these bills in international media (Abuja, 2020). It appears that the direction the Nigerian government wants to take in relation to internet freedom and privacy rights remains quite uncertain, at the time of writing (June 2020) none of the bills have passed into law.

With regards to Boko Haram, reports, which are scarce, say the military continues to follow a strong and scientific psychological approach in their propaganda fight with Boko Haram although they have still not publicly admitted to or explained any psychological operations they may be undertaking. The army's obsession with information control started back in 2013 when they offered battlefield tours to media outlets and influencing newspapers on which stories they publish (Grover, 2018). According to the 2019 Freedom in the World profile on Nigeria by the Freedom House, the government and military are also continuously increasing their online surveillance capabilities (Freedom House, 2019b). At the same time, different ethnic groups as well as extremist groups such as Boko Haram use social media and cyber troop methods to attack opponents and recruit followers (Hassan & Hitchen, 2020).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Nigeria

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
		X	X		X

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Fake news was deployed extensively by both main parties during last year's election season to attack their opponents (BBC Reality Check, 2019). For example, Lauretta Onochie, a personal assistant for social media to the president, repeatedly shared a story on social media accusing the PDP of keeping Nigerians in poverty and then giving them food and money at election rallies. The picture she posted with these accusations turned out to be of an unrelated charity event, but her accusations were nonetheless picked up by international news agencies (Busari, 2019). In lesser-known instances, she reportedly accused Atiku of "shopping" for terrorists in the Middle East (Ajulo, 2019) and claimed he was on the watchlist of security operatives in the United Arab Emirates (Tribune Online, 2019).

Meanwhile, local news agencies have reported on specific trolling efforts by campaigns whereby young people were recruited to set-up news accounts to spread information, test certain tactics and engage in other trolling activity on an everyday basis. While there are no official numbers in relation to the presidential campaigns, candidates running for governor or senator pay as much as 60,000 Naira ($165) monthly to people to handle their social media campaigns. Usually, small teams of about twelve people can run over 600 Twitter accounts (The New Times, 2019), with about 19.5% of accounts showing signs of automation, according to research done by the Centre for Democracy and Development (CDD) West Africa (CDD West Africa, 2019). Information on these activities remains scarce, though it is assumed that both the main candidates in last year's election engaged in such tactics. A major reason for sponsoring trolls, according to informants working as trolls or influencers for hire in Nigeria, is that information tweeted by the candidates themselves is perceived as biased, so they hire people with accounts viewed as more neutral. Thus, these accounts sometimes sit dormant until they are needed to spread certain (mis)information (Adepoju, 2019).

In light of the 2019 election the military established a situation room to monitor election violence. Together with the Cyber Warfare Command, which was activated on 4 February 2019 to disrupt terrorist propaganda, the situation room is engaged with monitoring, identifying and countering various forms of fake news and propaganda being put out by terrorists and other "subversive elements" (Alabi, 2019a; Buratai, 2019; Mutum, 2019). Meanwhile opposition parties have urged the army to stay away from the election after the president told them to be "ruthless" with those found interfering with the voting process (Muhumuza, 2019). However, it appears that fears of foreign inferences in the election in particular were not unfounded. In May 2019 the DFRLab found a set of 265 Facebook and Instagram assents which were taken down by Facebook to be linked to an Israeli political marketing firm called Archimedes Group that had ran influence campaigns around the world, including in Nigeria during election season. For the most part, activities seem to have supported President Buhari's bid for re-election whilst attacking his main competitor Atiku (Bandeira et al., 2019).

Nigeria also seems to be evolving as a welcoming location for building troll networks, as Twitter announced it had taken down seventy-one accounts, while Facebook took down forty-nine profiles and eighty-five Instagram accounts all based in either Nigeria or Ghana, which had been attempting to polarise online discourse by engaging in conversations about social issues and spreading conspiracies about COVID-19 around the world, including in the UK and US. According to Twitter and Facebook all these accounts were working on behalf of Russia, many having connections to the Internet Research Agency. They also noted that the network seemed to have still been in its early stages when it was detected (Dickey, 2020; Hern & Harding, 2020).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Nigeria

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms

Human Bots	Support Attack Opposition Driving Divisions	Disinformation Trolls Data Driven Strategies	Facebook Twitter

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

In general, cyber troop activity in Nigeria appears temporary in nature, focusing on particular political situations and campaigns. With regards to trolls for hire it is unclear whether these are active and open for business, and if so, whether political actors employ them outside of election cycles. Either way, in terms of coordination these trolls are not organized by the government or politicians themselves, but rather by whomever offers their services in the first place.

At present it appears that the government's main focus is on further defining the legal limits and rights that come with online spaces while simultaneously expanding the surveillance capabilities of both law enforcement and the military.

Table 3: Cyber Troop Capacity in Nigeria

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
		Temporary	Limited	

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

References

Abuja, J. A. (2020, February 5). Hate speech, social media bills fail to get support of Nigerians at town hall meeting. *The Guardian Nigeria News*. https://guardian.ng/news/hate-speech-social-media-bills-fail-to-get-support-of-nigerians-at-town-hall-meeting/

Adepoju, P. (2019, February 7). Social media trolls and influencers are set for a bitter battle in Nigeria's elections. *Quartz Africa*. https://qz.com/africa/1545067/social-media-trolls-and-influencers-are-set-for-a-bitter-battle-in-nigerias-elections/

Ajulo, L. (n.d.). *Alleged Defamation: Atiku demands public apology from Buhari's aide*. Retrieved May 28, 2019, from https://www.worldstagegroup.com/alleged-defamation-atiku-demands-public-apology-from-buharis-aide/

Akinwotu, E. (2020, May 15). "People are more scared of hunger": Coronavirus is just one more threat in Nigeria. *The Guardian*. https://www.theguardian.com/global-development/2020/may/15/people-are-more-scared-of-hunger-coronavirus-is-just-one-more-threat-in-nigeria

Alabi, S. (2019a, February 20). Election: Buratai inaugurates "situation room", issues emergency numbers. *Premium Times Nigeria*. https://www.premiumtimesng.com/news/more-news/312618-election-buratai-inaugurates-situation-room-issues-emergency-numbers.html

Alabi, S. (2019b, February 20). Mr President, It's time to sign the Digital Rights Bill. *The Guardian Nigeria News - Nigeria and World News*. https://guardian.ng/technology/mr-president-its-time-to-sign-the-digital-rights-bill/

As Nigerians vote, false information spreads. (2019, February 14). https://www.bbc.com/news/world-africa-47226397

Bandeira, L., Carvin, A., Karan, K., Kaul, A., Nimmo, B., & Sheldon, M. (2019). *Inauthentic Insreali Facebook Assets Target the World*. DFRLab. https://medium.com/dfrlab/inauthentic-israeli-facebook-assets-target-the-world-281ad7254264

BBC News. (2020, May 16). Child beggars at the centre of Nigeria's virus outbreak. *BBC News*. https://www.bbc.com/news/world-africa-52617551

Brandt, C. (2018). *Nigeria Heads for Elections in February, but Governance Is the Real Challenge*. https://freedomhouse.org/blog/nigeria-heads-elections-february-governance-real-challenge

Buratai, T. (2019). Nigerian Army Activates Cyber Warfare Command to disrupt terrorists propaganda- Gen. Buratai. https://prnigeria.com/2019/02/04/army-activates-cyber-warfare/

Busari, S. (2019, February 15). How fake news was weaponized in Nigeria's elections. *CNN*. https://www.cnn.com/2019/02/15/africa/fake-news-nigeria-elections-intl/index.html

Cadwalladr, C. (2018, April 4). Revealed: Graphic video used by Cambridge Analytica to influence Nigerian election. *The Guardian*. https://www.theguardian.com/uk-news/2018/apr/04/cambridge-analytica-used-violent-video-to-try-to-influence-nigerian-election

CDD West Africa. (2019). *Nigeria's "fake news" eco-system* (pp. 1–7). Centre for Democracy & Development West Africa. https://www.cddwestafrica.org/wp-content/uploads/2019/03/Nigerias-fake-News-Ecosystem-1.pdf

Chiefe, U. (2019, December 3). Your online freedom is at risk; the new Digital Rights and Freedoms Bill may just save it. *Techpoint.Africa*. https://techpoint.africa/2019/12/03/digital-rights-freedoms-bill/

Defamation: Atiku demands apology, retraction, N500m as damages from Buhari's Aide. (2019, May 19). *Tribune Online*. https://tribuneonlineng.com/212888/

Dickey, P. O. J. |Christopher. (2020, May 5). Russians Are Using African Troll Factories—And Encrypted Messaging—To Attack the U.S. *The Daily Beast*. https://www.thedailybeast.com/russians-are-using-african-troll-factories-to-attack-the-us

Facebook. (2020, October 8). Removing Coordinated Inauthentic Behavior. *About Facebook*. https://about.fb.com/news/2020/10/removing-coordinated-inauthentic-behavior-september-report/

France-Presse, A. (2020, May 17). Report: Jihadist Influence Growing in Northwest Nigeria | Voice of America - English. *Voa News*. https://www.voanews.com/africa/report-jihadist-influence-growing-northwest-nigeria

Freedom House | Nigeria. (2019). Freedom House. https://freedomhouse.org/country/nigeria/freedom-world/2019

Freedom on the Net | Nigeria. (2019). Freedom House. https://freedomhouse.org/country/nigeria/freedom-net/2019

Grover, E. (2018). *Nigerian army deploys "secretive tactics" in propaganda war with Boko Haram*. https://www.city.ac.uk/news/2018/january/boko-haram-propaganda-nigerian-army

Hassan, I., & Hitchen, J. (2020, October 6). Nigeria's Disinformation Landscape. *Items: Insights from the Social Sciences*. https://items.ssrc.org/disinformation-democracy-and-conflict-prevention/nigerias-disinformation-landscape/

Hern, A., & Harding, L. (2020, March 13). Russian-led troll network based in west Africa uncovered. *The Guardian*. http://www.theguardian.com/technology/2020/mar/13/facebook-uncovers-russian-led-troll-network-based-in-west-africa

Mbah, F. (2020, May 4). Businesses reopen as Nigeria eases coronavirus lockdown. *Al Jazeera*. https://www.aljazeera.com/news/2020/05/businesses-reopen-nigeria-eases-coronavirus-lockdown-200504094440082.html

Muhumuza, R. (2019, February 19). Nigeria's opposition urges military to stay away from vote. *Miami Herald*. https://www.miamiherald.com/news/nation-world/article226454575.html

Mutum, R. (2019, February 13). *Nigerian Army inaugurates situation room for 2019 elections*. Daily Trust. https://www.dailytrust.com.ng/nigerian-army-inaugurates-situation-room-for-2019-elections.html

Ojekunle, A. (2019, March 21). Buhari rejects digital rights bill, a bill seeking to protect the rights of internet users in Nigeria from infringement. *Business Insider by Pulse*. https://www.pulse.ng/bi/politics/buhari-rejects-digital-rights-bill-a-bill-seeking-to-protect-the-rights-of-internet/zztwxz1

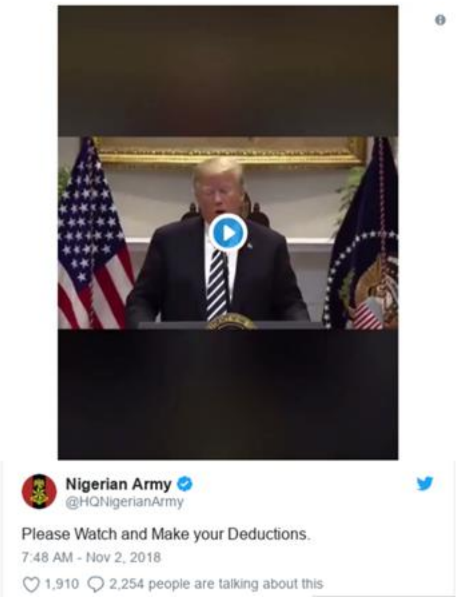
Olasupo, A. (2019, July 29). Revised digital rights bill passes first reading. *The Guardian Nigeria News*. https://guardian.ng/news/nigeria/national/revised-digital-rights-bill-passes-first-reading/

Sahara Reporters. (2019, July 26). Bill To Protect Rights Of Internet Users In Nigeria Passes First Reading In Parliament. *Sahara Reporters*. http://saharareporters.com/2019/07/26/bill-protect-rights-internet-users-nigeria-passes-first-reading-parliament

Searcey, D., & Akinwotu, E. (2018, November 3). Nigerian Army Uses Trump's Words to Justify Fatal Shooting of Rock-Throwing Protesters. *The New York Times*. https://www.nytimes.com/2018/11/02/world/africa/nigeria-trump-rocks.html

Social media trolls, influencers set for a fight in Nigeria's elections. (2019, September 2). *The New Times | Rwanda*. https://www.newtimes.co.rw/africa/social-media-trolls-influencers-set-fight-nigerias-elections

United Nations News. (2018). UN allocates $9 million to help thousands of people displaced in north-east Nigeria. https://news.un.org/en/story/2018/03/1006071



Nigerian Army
@HQNigerianArmy

Please Watch and Make your Deductions.

7:48 AM - Nov 2, 2018

♡ 1,910 2,254 people are talking about this

Figure 1: Video published on Twitter reacting to military shooting in October 2018[1]

NORTH KOREA

Introduction

As a one-party, dynastic totalitarian dictatorship, North Korea is plagued by pervasive surveillance, arbitrary arrests, punishments for political offenses and human rights violations. All domestic media is run by the state, and while several foreign news agencies have established offices in Pyongyang, they are only active sporadically, and other foreign media have their visits strictly managed. Foreign media based in South Korea (e.g. BBC, Radio Free Asia, Voice of America) broadcast Korean-language radio programs into North Korea, though the government jams most of them (*North Korea | Freedom House*, 2020). Additionally, there is no connection to international internet, and platforms such as Facebook, Twitter and YouTube are blocked. There is hardly any domestic online opinion for the administration to try and influence (Benedictus, 2016).

In the early summer of 2020 North Korea decided to cut all ties of communication with the South which had been established after a historic 2018 summit between the two countries. A liaison office built on Northern territory with South Korean money was blown up by North Korea, an event broadcast on North Korean television (BBC News, 2020). Analysts assume that the North is attempting to manufacture a crisis after peace talks have failed and activists and defectors in the South have continued to send leaflets with anti-North Korean propaganda into the North (Berlinger & Kwon, 2020). North Korea vowed to send millions of propaganda leaflets into the South (Choe, 2020), and the military planned to move activity into the border region and start re-installing loudspeakers at the border to broadcast propaganda. However, as quickly as these plans were rolled out, they were taken back and the loudspeakers were taken down again (McCurry, 2020; Park, 2020). At present North Korea's next steps remain unclear.

An Overview of Cyber Troop Activity North Korea

Organizational Form

Given the nature of the state as a totalitarian dictatorship, any influence operations are run directly by government agencies. Domestically, state-run media broadcast the information and narratives approved by the administration and, given that foreign information sources are either heavily restricted or banned altogether, state-owned media are more or less the only source of information for North Korean citizens. Additionally, most forms of private communication are monitored through a network of informants (*North Korea | Freedom House*, 2020). It appears that North Korea may be developing their social media platforms. In 2016 a Facebook clone briefly appeared on the North Korean internet that was also accessible from abroad, though experts believe the North Korean administration had not intended that it would be accessible externally (BBC News, 2016).

Meanwhile, North Korea is waging an information war against foreign narratives that are critical of the country, focusing most of their efforts on South Korea. Reportedly, North Korean agents posted about 41,373 pieces of propaganda in 2012 alone (Benedictus, 2016), and the country continues to grow its network of cyber specialists and intelligence agents (Strategy Page, 2019). In addition, a range of organizations linked to North Korea, but not officially affiliated with them, run disinformation campaigns on international online platforms.

Table 1: Organizational Form and Prevalence of Social Media Manipulation in North Korea

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
	x			x	

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

When it comes to North Korea's strategy towards foreign information operations targeting their Southern neighbor, most of their activity seems to focus on driving divisions and potentially eliciting support in areas still debated in the South. An estimated 200 troll troops focus on disrupting discussion about topics including whether the Southern ban on pro-North Korean narratives is necessary (Benedictus, 2016). Domestically, North Korea continuously runs pro-government propaganda that includes praise for the Supreme Leader Kim Jong-un that has religious fervor (Szilak, 2017).

North Korean hackers also continuously attempt to plant malware and steal data from South Korea. About 200 hacker cells are believed to have been active in 2018 and 2019, mainly operating outside of North Korea due to the bad domestic internet connection (mainly China, Russia and Southeast Asian countries). These hackers reportedly have made around USD $100 million for the North Korean dictatorship with their activities (Strategy Page, 2019). During the recent COIVD-19 outbreak it appears that North Korea seemed to turn towards disinformation attacks once again. A report posted in March 2020 Google's Threat Analysis Group noted that North Korean hackers persistently attack news outlets to spread disinformation (FDD, 2020; Gidwani, 2020).

The country's foreign disinformation operations have not gone unnoticed. In early 2020 Facebook began placing warning notes about editorial dependence on the pages, posts and advertisements of several organizations that they believed to backed by North Korea (Min, 2020). Over the past decade, the country seems to have realized the benefits of having a social presence on international (Western) social media. As early as 2010 the government opened profiles on Facebook, after their Twitter accounts were blocked by South Korea under their security laws (Roberts, 2010). More recently (2020), North Korea seems to have joined YouTube to employ it as new tool of propaganda, posting a video featuring an English-speaking woman taking viewers on a virtual tour across the nation (Yonhap, 2020).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in North Korea

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Human Hacked/Stolen accounts	Support Attacking Opposition Driving Divisions	Disinformation Trolls	Facebook Twitter YouTube Own Websites

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

Generally, there are very little sources on North Korean activities available, making it difficult to judge their capacity. According to the blog StrategyPage, which provides quick and easy access to military affairs worldwide, North Korea runs a "Mangyongdae Revolutionary Academy" (Agence France-Presse, 2018; The Straits Times, 2018) that is intended to train selected members of elite families in several fields that include computer science in order to develop foreign agents in 'enemy' countries, particularly South Korea. Moreover, they state that the North Korean hacker force consists of about 7,000 people, with about 300 specializing in online opinion rigging, operating more than 160 propaganda pages (Kang, 2018). Each individual hacker returns about USD $100,000 in yearly revenue (Strategy Page, 2019). There is very little known about how much these activities cost the North Korean state, or how they finance their activities.

Table 3: Cyber Troop Capacity in North Korea

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
7,000		Permanent	Training/Coordinated	Medium

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

References

Agence France-Presse. (2018, July 26). The school that trains the next generation of North Korean leaders. *South China Morning Post*. https://www.scmp.com/news/asia/east-asia/article/2157045/inside-mangyongdae-revolutionary-school-where-north-korea

BBC News. (2016, May 31). Facebook copy created in North Korea. *BBC News*. https://www.bbc.com/news/technology-36416970

BBC News. (2020, June 16). N Korea blows up joint liaison office with South. *BBC News*. https://www.bbc.com/news/world-asia-53060620

Benedictus, L. (2016, November 6). *Invasion of the troll armies: 'Social media where the war goes on.'* Guardian. https://www.theguardian.com/media/2016/nov/06/troll-armies-social-media-trump-russian

Berlinger, J., & Kwon, J. (2020, June 10). North Korea isn't talking to the South anymore. Experts say it could be trying to manufacture a crisis. *CNN*. https://www.cnn.com/2020/06/09/asia/north-korea-south-korea-communications-intl-hnk/index.html

Choe, S.-H. (2020, June 22). North Korea vows to shower millions of propaganda leaflets on South. *The Irish Times*. https://www.irishtimes.com/news/world/asia-pacific/north-korea-vows-to-shower-millions-of-propaganda-leaflets-on-south-1.4285247

FDD. (2020, April 1). FDD | North Korea Turns to Cyber Disinformation Attacks Amid Global Coronavirus Outbreak. *Fouondation for Defense of Democracies*. https://www.fdd.org/analysis/2020/04/01/north-korea-turns-to-cyber-disinformation-attacks-amid-global-coronavirus-outbreak

Gidwani, T. (2020). *Identifying vulnerabilities and protecting you from phishing* (Threat Analysis Group). https://blog.google/threat-analysis-group/identifying-vulnerabilities-and-protecting-you-phishing/

Kang, T. (2018, July 25). North Korea's Influence Operations, Revealed. *The Diplomat*. https://thediplomat.com/2018/07/north-koreas-influence-operations-revealed/

McCurry, J. (2020, June 24). North Korea suspends plan to increase military pressure on South. *The Guardian*. http://www.theguardian.com/world/2020/jun/24/north-korea-suspends-plan-to-increase-military-pressure-on-south

Min, C. C. (2020, June 5). Facebook issues new warnings on North Korean propaganda pages | NK News. *NK News - North Korea News*. https://www.nknews.org/2020/06/facebook-issues-new-warnings-on-north-korean-propaganda-pages/

North Korea | Freedom House. (2020). Freedom House. https://freedomhouse.org/country/north-korea/freedom-world/2020

Park, J. (2020, June 24). N.Korea Suspends "Military Action Plans" Takes Down Loudspeakers. *KBS World Radio News*. http://world.kbs.co.kr/service/news_view.htm?lang=e&Seq_Code=154367

Roberts, L. (2010, August 21). *North Korea joins Facebook*. https://www.telegraph.co.uk/technology/facebook/7957222/North-Korea-joins-Facebook.html

Strategy Page. (2019, February 24). Information Warfare: North Korean Sith Incentives. *Strategy Page*. https://www.strategypage.com/htmw/htiw/articles/20190224.aspx

Szilak, I. (2017, December 6). Meeting, Everywhere, The Rulers Of North Korea. *HuffPost*. https://www.huffpost.com/entry/rulers-of-north-korea-travel_b_1718186

The Straits Times. (2018, July 26). At this school in North Korea, classrooms are equipped with tanks, grenade launchers. *The Straits Times*. https://www.straitstimes.com/asia/east-asia/at-this-school-in-north-korea-classrooms-are-equipped-with-tanks-grenade-launchers

Yonhap. (2020, June 4). N. Korea embraces YouTube as new tool for propaganda aimed at wider audience. *The Korea Herald*. http://www.koreaherald.com/view.php?ud=20200604000892

OMAN

Introduction

As a hereditary monarch, Oman is currently considered "not free" by the Freedom House organization. The governmental power is concentrated on the sultan, and citizens have little to no political rights or civil liberties. Criticizing or dissenting from the state will lead to criminal charges and the regime continues to harass activists and critics that comment on Omani policy making. Freedom of the press and media is limited, and while there are private outlets run in Oman, next to those run by the state, they still typically accept government subsidies and self-censor to avoid legal repercussions[1].

In January 2020 Oman went through a shift in power after Sultan Qaboos bin Said died, and a new Sultan, Haitham bin Tariq al-Said, took power. He has since reshuffled large parts of the government and its ministries amongst other things he announced a new foreign and finance minister. Geopolitically, Oman has maintained a neutral position and has often acted as an intermediary between Iran and the West, working as a facilitator of communication, brokering deals between the different parties active in the Middle East, as well as the West[2].

An Overview of Cyber Troop Activity Oman

Organizational Form

At the moment, there is not much evidence available of the Omani government running any kind of influence campaign via cyber troops. Since the administration essentially controls most information flows in the country through their penal code and harassment of critics and dissidents, leading to self-censorship within those media outlets not run by the state itself, there may be little incentive to engage in such activities. Rather, the government continuously warns the public about trusting un-affiliated news sources or getting their news from social media, saying these sources attempt to endanger Oman, sometimes even connecting such accounts to terrorism. Instead citizens are urged to receive their news from official media institutions and state bodies[3].

The Sultanate seems to focus their effort on curbing any unwanted online activity through law rather than counter-activity: they block access, detain critics and pass laws specifically designed to criminalize the use of social media to express oppositional views, and in light of COVID-19 a new law penalizing the spreading of fake news with up to 3 years in prison was passed as well[4]. However, there are a few reports that accuse the administration of using bots and online surveillance to harass activists not just offline, but online as well[5]. In the end, any cyber troop activity the country may be engaging in is likely organized through government agencies.

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Oman

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
	X				

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Oman has a Government Communication Centre, which is usually the body to respond to any rumors, while many of the laws governing online information space are enforced through the Information Technology Authority[6]. There are some that have accused the Omani regime of running their own influence or rather smear campaigns against their opponents, as one article notes that “although the Sultanate of Oman tries to promote the image of the neutral state, it has spared no effort to harm opponents via bots”[7]. Given the general repressive nature of the state, it is almost impossible to find concrete proof of such cyber troop activities specifically, and reports are long and far in between.

Due to its neutrality status within the region and in international politics, Oman has been the target of foreign smear campaigns. For example, Oman facilitated the secret negotiations that lead to the Iran nuclear deal. As a reaction Oman faced an intense campaign by US far-right circles, such as the Washington-based Foundation for Defense of Democracy, which accused Oman of smuggling Iranian weapons to Houthis in Yemen, which would clearly go against Oman’s stance to bring peace and stability to the Middle East[8]. In addition, several papers have observed fake accounts spreading rumors and conspiracies in Oman to “shatter national unity”, particularly on Twitter. These accounts appear to be posing as Omani nationals, but most domestic observers seem convinced that they are not and are another symptom of foreign forces trying to ruin Oman[9].

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Oman

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Human Fake Bots	Pro-government support Attack Opposition Suppression	Disinformation Data-driven strategies (constant monitoring)	Twitter Facebook

Source: Authors’ evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

For the most part it appears that conspiracies and rumors are circulated in Oman during specific events and particular (sensitive) occasions. As such it appears that activities are temporary, and, domestically, liminal in organization, though foreign led influence or smear campaigns against Oman are much more organized[10].

Table 3: Cyber Troop Capacity in Oman

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
		Temporary[1]	Liminal[1]	

[1] The observed monitoring and punishing of dissidents and critics is permanent and coordinated Source: Authors’ evaluations based on data collected. Blank spaces indicate no evidence was found.

References

Al-Meqbali, T. (2019, August 27). متخصصون: الحسابات الإخبارية على وسائل التواصل الاجتماعي تفتقر للمهنية.. وضرورة تكاتف جهود التصدي لـ&;المزيفة&;. https://alroya.om/post/244907/-متخصصون-الحسابات-الإخبارية-على-وسائل-التواصل-الاجتماعي-تفتقر-للمهنية-وضرورة-تكاتف-جهود-التصدي-لـ-المزيفة

Al-Shabiba. (2016, October 22). تصريح من المدعي العام .. هل تطال العقوبات المجموعات الواتسابية في جرائم تقنية المعلومات؟. *Shabiba*. http://www.shabiba.com/article/160976

Al-Shabiba. (2019, July 30). السلطنة تواجه “الشائعات” عبر الإنترنت بعقوبات صارمة. *Al-Shabiba*. http://www.shabiba.com/article/231595

Ayman, ي. (2020, January 31). الادعاء العام يحذر من إرسال أو إعادة إرسال الأخبار الكاذبة ويوضح العقوبة.. https://www.atheer.om/archives/515917/الادعاء-العام-يحذر-من-إرسال-أو-إعادة-إر/

Bahajjaj, Dr. A. (2018, September 25). جريدة الرؤية العمانية الذباب الإلكتروني.. https://alroya.om/post/222895/الذباب-الإلكتروني

Barrington, L. (2020, August 27). Pompeo meets Oman’s Sultan on last leg of Mideast tour. *Reuters*. https://www.reuters.com/article/us-usa-oman-pompeo-idUSKBN25N0NY

Oman | Freedom House. (2019). Freedom House. https://freedomhouse.org/country/oman/freedom-world/2020

Owtram, F. (2020, January 24). Oman After Qaboos: Continuities, Challenges and Choices. *Middle East Centre*. https://blogs.lse.ac.uk/mec/2020/01/24/oman-after-qaboos-continuities-challenges-and-choices/

Times of Israel. (2020, August 18). Oman names new foreign minister, day after rare call with Israel | The Times of Israel. *The Times of Israel*. https://www.timesofisrael.com/oman-names-new-foreign-minister-day-after-rare-call-with-israel/

Watan Yogharid Khairj-al-Serb. (2019, May 26). السلطنة هدف لحملات تشويه وتشكيك .. لهذه الأسباب يشن اليمين الأميركي حملة على عُمان.. https://www.watanserb.com/2019/05/26/السلطنة-هدف-لحملات-تشويه-وتشكيك-لهذه/

الجنوبي, خ. (2018, January 5). الذباب الإلكتروني.. حرب مفتوحة بدون سلاح. https://muwatin.net/archives/4720

تحذير للعُمانيين ... ما حقيقة إعلان حالة الطوارئ في السلطنة؟. (2020, January 10). https://www.watanserb.com/2020/01/10/تحذير-للعُمانيين-ما-حقيقة-إعلان-حالة/

Pakistan

Introduction

Pakistan has experienced an increase in the use of computational propaganda during the past year. With seeds in the 2018 elections, coordinated inauthentic online behavior sponsored by the government, various political parties, and the military public relations department, has become rampant, and the online landscape in Pakistan has shifted considerably. Additionally, the government has been strengthening its control over content published online by shutting down internet services during protests and introducing laws that disregard online privacy.

An Overview of Cyber Troop Activity in Pakistan

Organizational Form

In the build-up to the national elections in 2018, various news sources reported that all of the leading political parties were discussing the creation and use of fake social media profiles with their social media strategy teams (Sohail, 2018). According to *The Diplomat*, an anonymous social media executive of the Pakistan Muslim League (N) reported that almost "everyone is running fake Facebook accounts and Twitter bots" in order to keep "pace with what others are doing" (Sohail, 2018). Social media managers from the PML-N, Pakistan Tehreek-e-Insaf and the Pakistan People's Party (PPP) have declared, off the record, that the "creation of fake Facebook and Twitter accounts to propagate their narratives was the official policy of each party" (Shahid, 2018).

The creation of cyber agencies within the Pakistani government have also been reported. In March 2020, Prime Minister Khan approved the establishment of a digital media office charged with responding to criticism and opposition to the policies of the PTI government (Digital Rights Monitor 2020). In February 2019, former Information Minister Fawad Chaudhry stated that the government had "prepared a mechanism" to control hate speech on social media. It was also stated that the government would be introducing a new authority, the Pakistan Media Regulatory Authority, to enforce regulations for digital, print and electronic media (Geo News, 2019). Despite these announcements, the project remains stalled due to multiple ministerial changes. However, the existing Pakistan Electronic Media Regulatory Authority (an independent body that regulates electronic media) is now looking to regulate the top content services and Web TV channels. In this regard, a white paper was published on their website in January. Despite concerns raised by parliamentarians and human rights groups that PEMRA would not have a legal mandate to regulate on these matters, PERMA has continued to seek comments from all the key stakeholders (Raza 2020).

Furthermore, the government proposed a set of online harms rules, dubbed the Citizen Protection (Against Online Harm) Rules 2020 (Rules, 2020), that called for social media companies to flag fake news and remove the accounts spreading the content, including the accounts of Pakistanis living abroad (Raza 2020). Under these rules platforms would be compelled to block accounts and remove content that "violates or affects the religious, cultural, ethnic or national security sensitivities of Pakistan" and is "involved in [the] spreading of fake news or defamation" (*The Express Tribune*, 2019). The Rules also proposed creating the post of National Coordinator that would have the power to determine fake news in online spaces. The Rules have received widespread criticism from civil society organizations and online social media companies who have threatened to shut down their services in the country. Due to these criticisms the Rules have remained suspended and the government is currently consulting with key stakeholders to further refine them (Raza 2020).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Pakistan

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
	Pakistan Media Regulatory Authority, Inter-Service Public Relations (ISPR) unit of the Pakistani military.	PML-N, PTI, PPP, Information Minister Fawad Chaudhry, Prime Minister Imran Khan			

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Bots and fake accounts: According to research by the Atlantic Council's Digital Forensic Research Lab (2018), parties across the political spectrum have been using bots and fake accounts to amplify messages ahead of the 2018 elections. One PML-N candidate running for the NA-142 constituency, Chaudry Riaz-ul-Haq, used the hashtag #NA142RIAZKA on Twitter, gathering 3,144 mentions in two days. These mentions originated from 22 accounts, 17 of which were created in June 2018, with an average of 142 mentions per account, strongly suggesting automated activity. Similarly, the Pak Sarzameen Party's campaign, using the hashtag #VoteForDolphin, reached 11.2 million users, but with an average of 21 posts per user, also signaling potential bot activity. Democracy Reporting International found that 52% of #PMLN accounts and 46% of #PTI accounts were likely bots (Mirbahar & Serrato 2018). Moreover, Digital Rights Monitor Pakistan (2018) monitored trending hashtags during the election period and found that, out of the 800,000 tweets, retweets, and replies for the 37 tracked hashtags, "almost all of them had high human-bot activity" and that "some human-bot accounts were also found directly engaged in incitement to violence against political rivals" (Ibid).

Alongside bots, fake accounts emerged such as @PakistansPoll, which claimed to be the official poll of Pakistan Twitter. From 2015 until June 2018, approximately 30% of the retweets it posted were from the PTI and its leader, Imran Khan. Asad Baig, Executive Director of Media Matters for Democracy, noted that "bot platforms" were created to automate contributions to hashtags for higher activity; as platforms such as TweetDeck were being used to automatically send a high volume of tweets (Digital Rights Monitor Pakistan 2018).

Misleading and manipulated content: According to the Center for International Media Assistance, a large majority of the disinformation spread online during the 2018 elections comprised of videos and images of real events captioned with incorrect information and circulated on platforms including Facebook and Twitter. These images were subsequently posted and shared by politicians. In one example, PPP politician Ghinwa Bhutto contributed to the spread of a conspiracy theory about the prime minister's ex-wife Jemima Goldsmith was a "Jewish agent", working against Islam and Pakistan. She did this by posting an old photo of Imran Khan's children and ex-wife on vacation in Mexico wearing ponchos that had resurfaced on Twitter. Captions were included that suggested that the photo was taken in a Jewish prayer house and that the ponchos were traditional Jewish attire. She pointed to this picture as so-called evidence that the conspiracy theory was correct (Raza 2019).

Media manipulation has not been limited to purely political enterprises in Pakistan. Aggressive campaigns have also targeted journalists, and particularly female journalists. One research found that organized campaigns against female journalists are often sexualized and incite violence (Digital Rights Monitor 2018). Moreover, Amnesty International uncovered an extensive network of fake social media profiles that were being used to infiltrate civil society organizations. For example, a prolonged campaign was launched against Diep Saeeda, a human rights defender. These networks were used to infiltrate activist communities, luring them into giving away their Facebook or Google log-in credentials and to download malicious spyware (Amnesty International, 2018).

Coordinated online behavior and amplification of content: In addition to bots, Pakistan's online landscape is also highly influenced by coordinated networks of humans who see themselves as political cyber-troop activists and strive to impact and shift online discourse to suit their agenda. These networks often operate openly and organize under team names, such as "Team Pak Zindabad" and "IK Warriors". This helps them to attract members and improve their efficiency for organizing around a particular goal. A common tactic of such groups is to aggressively tweet and engage with a particular issue, often accompanied by a hashtag, which then forces the issue into the "trending" panel. Research found that "almost 95% of the trending political campaigns in Pakistan are boosted artificially to mislead the public, giving a false impression that there is genuine grass-roots support or opposition for a particular group or narrative" (Jahangir & Poplzaj, 2019). Alternatively, these networks also mass-report tweets that oppose their agenda as spam, which automatically causes the Twitter algorithm to block that issue's access to the "trending" panel (Ibid).

Disinformation: A common strategy in Pakistan is the use of disinformation to discredit political actors online, often by coordinated campaigns accusing politicians of blasphemy, a criminal offence which carries the death penalty (Freedom House, 2017). Complaints of blasphemy are frequently used to limit free speech online. *The Diplomat* (2018) has reported a case of a journalism student, named Mashal Khan, who was lynched in April 2017 by a mob that suspected that he had uploaded blasphemous content to Facebook. This phenomenon is supplemented by other similar cases. Two Christian brothers were sentenced to death for allegedly sharing "disrespectful material" about the prophet Mohammad on their website, and there are other cases of individuals being were arrested for similar activity on social media (Freedom house, 2019).

Mass reporting and restriction of content: Pakistan has been rated as a country with some of the most restrictive approaches to content on social media platforms. According to Facebook's transparency report, Pakistan restricted 2,200 posts between January and June, 2018; 4,200 between July and December, 2018; and 5,700 between January and June, 2019, indicating more than a twofold increase in one year (Facebook Transparency Report, 2019). Similarly, on Twitter, there have been thousands of accounts reported and a 45% increase between July-December 2018 and January-June 2019 in official government requests to remove accounts**.** However, Twitter maintained a 0% compliance rate with these requests during both periods (Twitter Transparency Report, 2019). The current proposed online harms Rules, 2020 are aimed at addressing this by making it compulsory for social media companies to comply with the government's takedown requests (Raza 2020).

In January 2019, a number of journalists, activists, and lawyers received notice from Twitter that content they had published was in violation of Pakistani law, a claim allegedly stemming from correspondence with government or security forces (Freedom House 2019). The government has also steadily increased its requests of content removal from Google, with 2,323 items requested for removal between January and June, 2018, and 3,299 between January and June, 2019 – a 42% increase (Google Transparency Report).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Pakistan

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Bots, Fake accounts, Human	Incitement to violence; Misleading messages; Smear campaigns; Suppressing participation; Manipulating online conversations; Counter critical narratives; Weakening protest movements on social media; Drive particular agendas.	Mass reporting; Amplification of content; Disinformation, harassment	Facebook, Twitter

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

Political parties take advantage of their volunteers and members, and often actively train them in "social media electioneering". Social media teams of the big parties, such as PTI and PML-N have over 1,000 members each, but their strength is significantly amplified by volunteers. Leading up to the 2018 elections, for example, many parties conducted official training events and social media conventions, some attracting over 10,000 people, who were trained in how to be effective on social media (Jahangir, 2018).

Social media platforms are clamping down on these activities. Facebook removed 103 pages, groups and accounts for engaging in coordinated inauthentic behavior on Facebook and Instagram relating to one particular network originating in Pakistan in April, 2019. These pages posted content relating to Pakistani military, Pakistani interests, Kashmir communities, and current affairs. They also engaged in political news, including topics related to the Indian government, it leaders, and its military. A Facebook report linked these accounts to employees of the Inter-Service Public Relations Unit (ISPR) of the Pakistani military. The report alleged that the campaign spent US$1,100 on ads from May 2015 until December 2018, with 2.8 million accounts following one or more of these pages (Facebook, 2019).

Reports have shown that the new digital media office established by Prime Minister Khan in March 2020, charged with responding to criticism and opposition to the policies of the PTI government, has allocated 42 million rupees (around $250,000) to establish the office, which will comprise of 27 individuals, with a view to defend state policies online (Digital Monitor, 2020).

Table 3: Cyber Troop Capacity in Pakistan

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
Parties have attracted over 10,000 people to media events; PML-N and PTI have around 1000 members on their social media teams; The new digital media office established by Prime Minister Khan will comprise of 27 individuals.	Inter-Service Public Relations Unit (ISPR) spent $1,100 on inauthentic online campaign; The government has allocated $250,000 to establish a new digital media office under Prime Minister Khan.			

Surveillance and censorship: Online surveillance is becoming increasingly sophisticated in Pakistan. The cybersecurity firm Lookout identified custom Android and iOS surveillance ware named Stealth Mango and Tangelo that were being utilized by a highly targeted intelligence-gathering campaign, which they believe to be operated by members of the Pakistani military (Lookout, 2018).

The current online harms rules that have been proposed reveal an attempt by the Pakistani government to strengthen its ability to surveil online activity via legal means. The 2013 Fair Trial act and PECA provide a legal basis for conducting surveillance with judicial oversight (Raza, 2020). However, the new regulations that have been proposed defy the parent law and propose the forcing of social media companies to open up data centers in Pakistan and register an office in Islamabad. Most importantly, social media companies are obliged to allow law enforcement agencies to access data and to moderate content (Al Jazeera 2019). These rules remain suspended and are under consultation.

Pakistani authorities have also participated in the curbing of political discourse online by censoring, blocking, and disturbing internet and mobile communication infrastructure. According to the Pakistan Telecommunication Authority, there are over 831,000 blocked websites in the country, with reasons ranging from pornography and blasphemy to anti-state, sectarian content, and defamation (Freedom house 2019). In June, 2017, the Berkman-Klein's Internet Monitor reported that Pakistan "blocks news and human rights websites and content critical of the faith of Islam", such as nudity and sexual content (Freedom House, 2017).

Social media content has also been restricted during religious and national holidays. In November, 2017, social media platforms were suspended nationwide for two days in the wake of protests that turned violent (Freedom House, 2018). In April, 2018, news website NayaDaur was blocked for more than one week, before the Pakistan Telecommunication Authority (PTA) unblocked it. No explicit reason for the blocking was given, but the action followed the publication of an article sympathetic to the Pashtun human rights' movement (Freedom House, 2018). In June, 2018, during the run-up to the general election, individuals trying to access a website operated by the Awami Workers Party were told that the website was not accessible as it "contains content that is prohibited for viewership from within Pakistan" (Jahangir, 2018). The party later challenged this in the Islamabad High Court and in September, 2019, the High

Court directed the PTA to frame the rules it was implementing and specify a more transparent process for blocking websites. This has contributed to the PTA's attempts to devise the Citizen Protection (Against Online Harm) Rules, 2020, despite the Rules not specifying a clear transparent process for blocking websites (Raza, 2020).

References

Al Jazeera. 2019. Pakistan government's new social media rules draw criticism. *Al Jazeera.* https://www.aljazeera.com/news/2020/02/pakistan-government-social-media-rules-draws-criticism-200214060043837.html

DFRLab. 2019. Pakistan Army's Covert Social Network. *Medium*. https://medium.com/dfrlab/pakistan- armys-covert-social-network-23ce90feb0d0.

Digital Rights Monitor. 2018. Investigative study finds custom made 'bot platforms' contributing to trending political hashtags in Pakistan. *Digital Rights Monitor.* http://digitalrightsmonitor.pk/investigative-study-finds-custom-made-bot-platforms-contributing-to-trending-political-hashtags-in-pakistan/

Digital Rights Monitor. 2020. PTI government ready to setup digital media wing to regulate criticism on the internet. *Digital Rights Monitor.* http://digitalrightsmonitor.pk/pti-government-ready-to- setup-digital-media-wing-to-regulate-criticism-on-the-internet/

Facebook. 2019. Removing Coordinated Inauthentic Behavior and Spam from India and Pakistan. *Facebook.* https://about.fb.com/news/2019/04/cib-and-spam-from-india-pakistan/

Facebook Transparency Report. 2019. Content Restrictions Pakistan. *Facebook.* https://transparency.facebook.com/content-restrictions/country/PK

Freedom in the World. 2017. Pakistan. *Freedom House.* https://freedomhouse.org/country/pakistan/freedom-world/2017.

Freedom in the World. 2018. Pakistan. *Freedom House.* https://freedomhouse.org/country/pakistan/freedom-world/2018.

Freedom on the Net. 2019. Pakistan. Freedom House. https://freedomhouse.org/country/pakistan/freedom-net/2019#footnote1_syqdfhr

Geo News. 2019. Govt to launch crackdown against hate speech on social media: Chaudhry. *Geo News.* https://www.geo.tv/latest/228041-govt-prepares-mechanism-to-control-hate-speech-on-social- media-massive-crackdown-next-week.

Google Transparency Report. 2019. Government requests to remove content. *Google.* https://transparencyreport.google.com/government-removals/by-country/PK?hl=en

Mirbahar, H. S., & Serrato, R. 2018. Social Media and Elections. *Democracy Reporting International.*

Jahangir, R. 2018. Pakistan's online clampdown. *Dawn*. https://www.dawn.com/news/1441927.

Jahangir. R. 2018. How political parties manipulate cyberspace for electioneering. *Herald.* https://herald.dawn.com/news/1398599

Jahangir, R., & Popalzaj, S. 2019. While Twitter trends may be artificial, hashtag merchants are real people. Dawn News. https://www.dawn.com/news/1518967

Lookout. Security Research Report: Stealth Mango & Tangelo. *Lookout.* https://info.lookout.com/rs/051- ESQ-475/images/lookout-stealth-mango-srr-us.pdf.

Raza, T. 2019. Mapping Digital Disinformation around Elections: A Case Study of Pakistan's 2018 General Elections. *Center for International Media Assistance*. https://www.cima.ned.org/publication/mapping-online-disinformation-around-pakistans-2018- general-elections/

Raza, T. 2020. Email interview.

Saleemi, U. 2018. Politico-religious hate speech steers social media ahead of polls. *Pakistan Today*. https://www.pakistantoday.com.pk/2018/07/21/politico-religious-hate-speech-steers-social- media- ahead-of-polls/

Shahid, K. K. 2018. Could Facebook Data Leaks Impact Pakistan's Elections? *The Diplomat.* https://thediplomat.com/2018/05/could-facebook-data-leaks-impact-pakistans-elections/.

The Express Tribune. 2019. Facebook, Twitter, Google may suspend services in Pakistan after new social media rules. *The Express Tribune.* https://tribune.com.pk/story/2166612/8-facebook-twitter- google-may-suspend-services-pakistan-new-social-media-rules/

Twitter Transparency Report. 2019. Pakistan. *Twitter.* https://transparency.twitter.com/en/countries/pk.html

Philippines

Introduction

The Philippines is considered “partly free” according to Freedom House’s Freedom of the World index (Freedom House, 2020a). Internet freedom has also been on decline in the Philippines (Freedom House, 2020b). This is largely due to the erosion of political and civil rights under the Duterte administration (Freedom House, 2020b). In particular, freedom of speech and freedom of the press have been under increasing threat in the Philippines, with legal cases taken against independent media websites like Rappler, alongside intimidation, harassment and trolling against news organizations and civil society groups (Freedom House, 2020b). The COVID-19 pandemic has also led to a clamp down of freedom of speech online, with certain forms of speech made via social media about the pandemic being criminalized (Freedom House, 2020b).

When it comes to Internet access, the Philippines has a large Facebook userbase, with roughly 69 million Filipinos on the platform in 2017 (Swearingen, 2018). Part of this growth came from the introduction of the Free Basics program, which subsidizes data charges incurred by users so that they may use basic services and access certain platforms for free, including Facebook. Since 2015, there was an increase in Internet penetration as a result of Free Basics, and in many cases, Facebook is the Internet to many citizens who cannot afford data plans to access content not offered through Free Basics (Mihm, Oulamine, Singer, 2019). The combination of high-Internet penetration via Facebook and mobile devices with the shrinking space for online speech and freedom of the press creates a unique environment for computational propaganda and social media manipulation in the Philippines to thrive. Indeed, the Philippines has been described by Facebook public policy director, Katie Harbath as “patient zero in the global disinformation epidemic” (Bengali and Halper, 2019).

An Overview of Cyber Troop Activity in the Philippines

Organizational Form

In the Philippines, we found examples of many types of organizations conducting social media manipulation. In this overview, we focus specifically on government and political party activities in this domain. There is an emerging body of academic and journalistic inquiries into the troll farms that have emerged within the Philippines (see for example, Ong & Cabanes 2019; Mahtani and Cabato, 2019). It is important to acknowledge the growth of this industry, however, the review below focuses on cyber troop activity – or government and political parties who are using social media to manipulate public opinion. We discuss some examples where industry, influencers and trolls intersect with cyber troop actors, but like all cases, we do not provide detailed overviews of how these actor-networks operate outside of the scope of cyber troop activity.

Cyber Troop activity in the Philippines is infamous for their work on the 2016 elections that brought Duterte to the Presidential office (see Alba 2018). During his campaign, Duterte’s campaign worked with social media influencers, bloggers, and paid trolls to spread and amplify his campaign messages (Alba, 2018; Ong & Cabanes 2019). Many of these networks are still active today, with platforms acting against accounts they identify. For example, in March 2019 Facebook removed Facebook and Instagram pages, groups and accounts that were linked to a network organized by Nic Gabunada, who also worked with President Duterte during his 2016 campaign (Gleicher, 2019). As social media manipulation has become a prominent characteristic of Filipino social media pages and groups, other political parties and oppositional candidates have also adopted similar techniques (Silverman 2019).

In addition to political parties, there is also evidence of government-led cyber troops operating in the Philippines, though there is less public-facing information available on their activities. In September 2020, Facebook removed a network of accounts on Facebook and Instagram that was linked to the Philippine military and police force (Gleicher 2020). As described in more detail below, these fake accounts were distributing local news about military and law enforcement activities in the country.

Table 1: Organizational Form and Prevalence of Social Media Manipulation in the Philippines

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
	Evidence Found	Evidence Found	Evidence Found	Evidence Found	Evidence Found

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

A wide range of strategies, tools, and techniques of computational propaganda and social media manipulation have been observed in the Philippines. In the Philippines, there has been evidence of both human and automated fake accounts. One recent example from 2020 includes the use of fake accounts by the Filipino military and police forces to discus local news about the military and law enforcement activities, such as the anti-terrorism bill (Gleicher, 2020). There have also been examples of automated accounts in the Philippines. For example, after Duterte's election there were more than 30,000 tweets that mentioned the President in a two-hour period, which, according to Rappler, was more tweets than those associated with any other Presidential candidate in the past month (Ressa, 2016).

While President Duterte was campaigning for the Presidential office, cyber troops made use of fake accounts to spread disinformation. For example, Rappler identified a network of accounts that used fake photos, had few friends, and all followed each other (Hofilena, 2016). Despite being a small network (approximately 26 accounts), they managed to generate more than 50,000 shares and reach more than 12 million users (Hofilena, 2016; Mihm, Oulamine, Singer, 2019). Experts describe how the weaponization of the Internet, and of Facebook in particular, represented many of the tactics that were being used during Brexit and the 2016 Election campaign of former US President Donald Trump (Silverman 2019).

Fake accounts being operated by cyber troops in the country spread disinformation are still active (Gleicher, 2019). For example, in 2019, Facebook took down a network of fake accounts operated by Nic Gabunada, covering topics such as local news and politics, while supporting the current administration and attacking opponents or discussing controversial events (Gleicher, 2019). These accounts also had significant impact, with more than 3.6 million followers before they were taken down by Facebook (Gleicher 2019). Some academic research has highlighted how disinformation and misleading memes, data-driven strategies and other kinds of social media manipulation techniques have become more widespread now than in 2016 (Ong, Tapsell and Curato, 2019).

Cyber troops in the Philippines also use trolling and harassment strategies to suppress political participation and freedom of the press. One prominent example is the attacks Maria Ressa—a highly accomplished Filipino journalist—received after her news organization Rappler published a transcript of a telephone conversation between President Donald Trump and President Rodrigo Duterte of the Philippines (Etter, 2017). Here, a coordinated network of bots and fake accounts flooded social media with the hashtag #ArrestMariaRessa, while she received a consistent flow of hate messages and threats, including a call for her to be "raped repeatedly until she died" (Monaco et al., 2018). Maria has continued to face online trolling and harassment, as well as pending criminal cases instigated by the government (Buan, 2019). In June 2020, Maria along with former Rappler researcher Reynaldo Santos Jr. were found guilty of cyber libel, which they have appealed at the time of writing. Since February 2019, several social media campaigns have helped draw attention to the attacks on freedom of the press in the Philippines and to bolster support for Maria Ressa and Rappler (Freedom House, 2020b).

The online trolling attacks are a widespread phenomenon in the Philippines. However, they do not just have online impacts for freedom of the press and freedom of speech. In some instances, online trolling has turned into offline violence: for example, in 2020 two human rights defenders in the Philippines who were repeatedly trolled online were killed within a week of each other (BBC News, 2020).

The increased domestic demand for trolling and other techniques of social media manipulation have led to the professionalization of these services. With a large English-speaking workforce, individuals who might find jobs in call centres or as content moderators are also finding contract work as professional trolls (Silverman, 2019; Mahtani and Cabato, 2019). In domestic campaigns, trolls-for-hire will work "round-the-clock" shifts on platforms such as Facebook and Twitter on astroturf campaigns designed to support certain politicians, while debating and attacking political opponents (Mahtani and Cabato, 2019). They are also starting to grow internationally, with some firms being offered contracts in the UK while others are looking to expand regionally (Silverman, 2019; Mahtani and Cabato, 2019).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in the Philippines

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Human, Automated	Pro-government Support, Oppositional Attacks, Suppressing, Polarization	Disinformation, Data-Driven Strategies, Trolling, Amplification	Facebook, Instagram, Twitter

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

Research on cyber troop capacity in the Philippines suggests permanent levels of activity, with networks associated with President Duterte, PR firms, influencers and the government continually being identified by platforms, activists, journalists, and academic researchers. In previous reports, we have found some evidence of spending by cyber troops in the Philippines. This includes funding towards a troll farm being operated by Nic Gabunada, Duterte's social media director, for a contract valued at $200,000. As described above, cyber troops have also spent money on Facebook advertising to push disinformation on the platform, including 59,000 USD spent by Nic Gabunada and 1,300 USD spent by a network originating from the military and law enforcement (Gleicher 2019, 2020).

Table 3: Cyber Troop Capacity in the Philippines

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
	Evidence Found	Permanent	Coordinated / Centralized	High

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

References

Bengali, Shashank and Evan Halper. (2019). Troll Armies, A Growth Industry in the Philippines, May Soon Be Coming to an Election Near You. https://www.latimes.com/politics/story/2019-11-19/troll-armies-routine-in-philippine-politics-coming-here-next

Buan, Lian. (2019). LIST: Cases vs. Maria Ressa, Rappler Directors, Staff, since 2018. https://www.rappler.com/nation/list-cases-filed-against-maria-ressa-rappler-reporters

Gleicher, Nathaniel (2019). Removing Coordinated Inauthentic Behaviour from the Philippines. https://about.fb.com/news/2019/03/cib-from-the-philippines/

Gleicher, Nathaniel (2020). Removing Coordinated Inauthentic Behaviour. https://about.fb.com/news/2020/09/removing-coordinated-inauthentic-behavior-china-philippines/

Hofilena, Chay F. (2016). Fake Accounts, Manufactured Reality on Social Media. https://www.rappler.com/newsbreak/investigative/fake-accounts-manufactured-reality-social-media

Mahtani and Cabato (2019). Why Crafty Internet Trolls in the Philippines May Be Coming to a Website Near You. https://www.washingtonpost.com/world/asia_pacific/why-crafty-internet-trolls-in-the-philippines-may-be-coming-to-a-website-near-you/2019/07/25/c5d42ee2-5c53-11e9-98d4-844088d135f2_story.html

Mihm, Henry, Ines Oulamine and Fiona Singer. (2019). The Philippines Deserves More from Facebook. https://www.lawfareblog.com/philippines-deserves-more-facebook

Ong, Jonathan Corpus & Jason Vincent A. Cabanes. (2019). When Disinformation Studies Meets Production Studies: Social Identities and Moral Justifications in the Political Trolling Industry. *International Journal of Communication, 13(2019). https://ijoc.org/index.php/ijoc/article/view/11417*

Ong, Jonathan Corpus, Ross Tapsell & Nicole Curato. (2019). Tracking Digital Disinformation in the 2019 Philippine Midterm Election. https://www.newmandala.org/wp-content/uploads/2019/08/Digital-Disinformation-2019-Midterms.pdf

Ressa, Maria. (2016). Propaganda War: Weaponizing the Internet. https://www.rappler.com/nation/propaganda-war-weaponizing-internet

Silverman, Craig. (2019). The Philippines Was a Test of Facebook's New Approach to Countering Disinformation. Things Got Worse. https://www.buzzfeednews.com/article/craigsilverman/2020-philippines-disinformation

Swearingen, Jake. (2018). Facebook Used the Philippines to Test Free Internet. Then a Dictator was Elected. https://nymag.com/intelligencer/2018/09/how-facebooks-free-internet-helped-elect-a-dictator.html

Poland

Introduction

Since the political party Prawo i Sprawiedliwośc (PiS) won the federal elections in 2015, the political climate in Poland has been in turmoil. In 2020, the country held its two-round presidential election. President Andrej Duda of the PiS—the ruling party that lost its majority in the Senate in October 2019—disputed the re-election on 28 June 2020 with Rafał Trzaskowski of the centrist Platforma Obywatelska (PO), Władysław Kosiniak-Kamysz Polskie Stronnictwo Ludowe (PSL), Robert Biedroń of left-wing Spring, Krzysztof Bosak of the Konfederacja far-right coalition, and independent Szymon Hołownia. A few weeks later, he won the runoff with 51.03% of votes.

The government has restructured the judicial system, giving it less independence. At the same time, judges and prosecutors have been subjected to smear campaigns by the government and state-backed media. The government also passed laws that increased control over the media. Beyond the direct implications of these measures, they also "triggered a series of highly publicized mass protests on multiple political and social issues" (Gorwa, 2017). In addition to the PiS's Euroskepticism and Poland's weight at NATO in Central and Eastern Europe (Bush & Kurzynski, 2020), these developments have raised concerns with the European Union and the United States.

The increasing polarization of the political sphere and "the general lack of neutral online platforms for debate on Polish politics" (Gorwa, 2017) have created a fertile ground for trolling. Online attacks target those who oppose the governments or have spoken out against their stance on gender issues, the Polish-Jewish past, and immigration, among other things. Hate speech has also increased. For instance, in 2019, the United Nations Committee Against Racial Discrimination called on Poland to act on the growing homophobic speech in the media, which was bolstered by cities and provinces declaring LGBT-free-zones.

It is worth noting that while in 2011 Internet penetration was close to 59% and Facebook users in Poland accounted for 5.5 million, by 2016 these figures had risen to 80% and 22.6 million, respectively, which has led to increased interest in the internet and social media as a political marketing medium (Gorwa, 2017).

An Overview of Cyber Troop Activity in Poland

Organizational Form

The ruling PiS has been accused of manipulating social media and news portals through fake accounts that spread hate speech and amplify content (Gorwa, 2017). As Gorwa states, although there is little evidence, it is believed that Paweł Szefernaker, a Secretary of State in the Chancellery of the Polish Prime Minster, managed several of these operations.

The government has also been found to coordinate online smear campaigns against a group of judges. Łukasz Piebiak, Deputy Justice Minister, was behind these operations and was forced to resign in August 2019 after his involvement was uncovered (Bush & Kurzynski, 2020). The main activities were followed by an online hatter contracted by Piebiak known as Emilia. She "was associated with one of the employees of the National Council of the Judiciary, who had previously worked at the Ministry of Justice" (Mierzyńska, 2019d). The question remains as for whether Zbigniew Ziobro, the Justice Minister, was also involved in the campaign. Whilst Piebiak's communications with Emilia indicated that "his boss was being informed", this is not in itself sufficient evidence (Applebaum, 2020). However, there are signs indicating the existence of a broader network that helped coordinate the dissemination of the smear campaign on Twitter. The judges Jarosław Dudzicz, Konrad Wytrykowski, and Maciej Nawacki also disseminated hate content across the social media platform. Additionally, the news portal Wirtualna Polska received a sum of money to promote the policies of the Ministry of Justice (Applebaum, 2020).

In the course of the 2020 general election campaigns, according to Bush et al. (2020) the Polish far right Konfederacja, whose candidate is Krzysztof Bosak, was using "highly coordinated tactics" and being more aggressive than its counterparts. Already in the European Parliament elections in 2019, Mierzyńska (2019b) identified an unnatural increase in Konfederacja's followers, some of which had empty profiles. Also, Janusz Korwin-Mikke, co-founder of the party and candidate for deputy of the Polish Parliament, was linked to a network of Facebook pages that used automation techniques to boost their content (Bush & Kurzynski, 2020). And a network of sites that are currently being used by the far-right shows that some of the sites are managed by activists and organizations. That is the case of Jacek Międlar and the nationalist group Roty Niepodległości (Legions of Independence) (Bush et al., 2020).

Other actors across parties, such as far-right candidate Dariusz Matecki (Mierzyńska, 2019a), were linked to disinformation and hate speech content dissemination. However, some of these activities might simply be personal projects and not state-backed operations (Gorwa, 2017). In the case of Matecki, he had employment contracts of PLN 4008 (almost 1000 dollars) gross per month with the Ministry of Justice between June 2017 and August 2018, and between December 2018 and March 2019 (Mierzyńska, 2019a). Although it is not clear the nature of these contracts, he promotes content about Ziobra, the Ministry of Justice, and the party Solidarity Poland, with the use of automation techniques (Mierzyńska, 2019d).

Additionally, in 2016 Dominik Tarczyński, member of the European Parliament and member of PiS, created a group of Twitter trolls called #drugazmiana. They coordinate hate campaigns against the opposition. With the assumption that they are soldiers of a cursed internet and they must defend the rule of the PiS, they justify personal attacks and use military references (Mierzyńska, 2019d).

On the other hand, there is evidence of a private contractor's involvement in the creation of "more than 40 thousand unique identities" that were used by politicians and political parties" (Gorwa, 2017). One of these companies is Cat@Net, which worked for both left and right-wing clients. The agency worked to create content that favoured the public broadcaster TVP. However, the contract was signed by an external PR company (AM Art-Media PR) and there is no evidence that the broadcaster knew about the operations (Davies, 2019). One other beneficiary of the company's operations was Andrzej Szejna, deputy head of the Democratic Left Alliance (SLD), during his campaign as candidate for European Parliament. Whilst he denies contracting Cat@Net, he states that his Twitter account was managed for free by a "former president of a powerful arms factory": Krzysztof Krystowski. Krystowski co-controlled Cat@Net and since 2015 works as vice president for the helicopter division of arms company Leonardo, for which the agency also developed online campaigns (Pruszkiewicz et al., 2019). It is also worth noting, that the company hired people with disabilities for remote working and, as a result, received government subsidies.

Cat@Net is also linked to a media network, which consists of portals and their associated social network accounts (e.g. nczas.com), and a video production agency (SDM Pictures), among others. It has also been revealed that France Libre 24 (FL24), an anti-immigrant and anti-Muslim disinformation portal targeting France, belongs to this network. The website of Janusz Korwin-Mikke and nczas.com were among the top four distributors of FL24 content. The portal is registered in Poland by 6S Media and uses the same IP address as portals run by another company within the network, 5S Media. The partners of 6S Media are Adam Gwiazda, Adam Wojtasiewicz (one of the owners of Cat@Net), Tomasz Sommer, and Krzysztof Szczawiński, who are both partners at 3S Media and 5S Media. Wojtasiewicz, Sommer, and Szczawiński are also part of the board of Fundacji „Najwyższy Czas", a far-right weekly news magazine linked to Janusz Korwin-Mikk and Konfederacją that dissemiantes anti-EU, anti-immigrant, and anti-Semitic content. (Mierzyńska, 2020).

Finally, as regards foreign operations in Poland, there are several indications of Russian disinformation campaigns in the country. As Gorwa (2017) exposes, it is rumoured that Russia sponsored nationalist groups and spread online propaganda. These incidents have been more widely addressed by scholars than domestic interference. Operations involve anti-Polish disinformation campaign by Russian actors.

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Poland

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
2015	Evidence found	Parties: PiS, Konfederacja Politicians: Paweł Szefernaker (Secretary of State in the Chancellery of the Polish Prime Minster) Łukasz Piebiak (Deputy Justice Minister) Janusz Korwin-Mikke (Co-founder of the Konfederacja party and candidate for deputy of the Polish Parliament) Dominik Tarczyński (Member of the European Parliament, PiS)	Cat@Net AM Art-Media PR Krzysztof Krystowski (Linked with Cat@Net and vice president for the helicopter division of arms company Leonardo) News portal Wirtualna Polska Adam Gwiazda (partner at 6S Media), Adam Wojtasiewicz (partner at 6S Media and owner of Cat@Net), and Tomasz Sommer and Krzysztof Szczawiński (partners at 3S Media, 5S Media, and 6S Media).	Roty Niepodległości	Dariusz Matecki

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

As has been described by Gorwa (2017), there have been records of mass flagging reporting against far-right Facebook groups and pages by anti-fascist Facebook groups since 2014.

However, trolling, disinformation, and amplification are the most frequent strategies of political online social media manipulation.

Whilst online news outlets, such as the popular news websites ONET and Virtual Poland, became fields for trolling behaviour, it is often said that political parties used services of paid users to comment on news sites, such as Gazeta Wyborcza. As a result, some media outlets "have been modified to make it more difficult for users to reply to each other" (Gorwa, 2017). Similar techniques have been deployed on social media. According to Gorwa (2017), paid employees at troll farms use up to fifteen accounts and procure unique content to post in order to target opinion leaders and infiltrate Facebook groups and pages, while maintain the appearance of authenticity. Bots are used, instead, for spamming and hate campaigns.

With the increasing use of social media as a source of political information, disinformation has also been on the rise in Poland, both by the ruling party and state-backed media, and its opponents, such as the PO. The main narratives that are contended are related to LGBT issues, feminism and women's rights, immigration, corruption, energy policy, pan-Slavism, judicial independence, issues about the Second World War and the Holocaust, and the relations between Poland and the United States, Ukraine, and Russia (Bush & Kurzynski, 2020).

Manipulation campaigns are undertaking using both human and bot-like accounts. According to Gorwa (2017), automated accounts by the right-wing in Twitter are twice as prevalent than left-wing accounts. On Facebook, research by Avaaz shows that there are simultaneous activities on multiple pages with the same stories, indicating inauthentic behaviour (Bush & Kurzynski, 2020).

As has already been mentioned, the company Cat@Net developed a campaign to promote the highly partisan state broadcaster TVP. The employees, who managed fake accounts, were asked to post credible positive comments on "the government's subsidy for TVP and the television licence fee" and attack accounts which criticized TVP. An analysis of the campaign's influence shows that these accounts created 10,000 posts and probably reached around 15 million views (Davies, 2019). The pro-Szejna campaign, was similarly aimed at amplifying positive content related to his candidacy to the European Parliament with the use of at least ninety social media accounts (Davies, 2019).

Additional incidents can be found in recent years in Poland. Since 2018, a group of judges that expressed their disagreement with policies issued by the government have been subjected to threats against their careers and criminal investigations. This was accompanied by coordinated online attacks against them. The attacks originated from a Twitter account which created fake content and defamatory information, and trolled the targeted judges (Applebaum, 2020). As Applebaum (2020) states, the campaign also targeted a foreign audience, in order to convince people "that Polish judges are Communists left over from the bad old days, and that they therefore deserve to be purged".

According to Marchal et al. (2019), during the run-up to the 2019 European Parliament Elections, around 21% of the content Polish internet users were exposed to on Twitter consisted of junk messages (Mierzyńska, 2019c) and users "shared more 'junk news' than legitimate news" on this platform (Marchal et al., 2019). The Institute for Strategic Dialogue (2019) identified at least 803 fake human and bot accounts that were active during this period and disseminated disinformation with anti-Semitic and pro-Russian narratives. It has also identified a network of Facebook groups, pages, and accounts that promoted the right-wing party Konfederacja, and pro-government accounts that massively posted content that linked to "anti-Semitic youth-oriented sites" (ibid.).

The far-right network on Facebook was coordinating its amplification strategies as part of the campaign for the presidential elections that took place in 2020. They did so by promoting not only "Islamophobic, anti-US, anti-immigrant, and anti-Semitic content", but also pro-Bosak content and attacks on PiS and PO. The content was often created on websites with party-related petition ads, such as Wprawo.pl, Pantarhei24.com, Magnapolonia.org, and Dzienniknarodowy.pl, and was then disseminated in Facebook pages and groups with up to 260,000 followers (Bush et al., 2020).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Poland

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Bots and Human. Fake and Real.	Pro-government, pro-party Attacks on opposition, Trolling	Disinformation, Trolls, Amplification strategies	Twitter, Facebook Minor evidence: Instagram, YouTube

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

Whilst there is no evidence on contracts for social media manipulation by public actors, a recent investigation has led light on the structure of private contractors. The company Cat@Net, by November 2019, had fourteen employees who ran in total at least 179 accounts (seventy on Facebook, ninety-four on Twitter, eleven on Instagram, and three on YouTube) (Pruszkiewicz et al., 2019). The company often seeks out university students or graduates to work as freelancers. Most of them are disabled, enabling the company to receive 1.5 million zloty (around 350,000 dollars) over four years in public subsidies from Poland's National Disabled Rehabilitation Fund (Davies, 2019). After a trial period in which employees create their avatars and sufficient convincing content to establish trust within the network, they can join the private Cat@Net Slack channel. Two managers give indications on the content, as well as targeted posts and accounts, and topics to follow. The chat also is used for employees to receive feedback on their content from colleagues and as a place on to post achievements. Employees are also asked to complete an Excel file with their comments and name of avatar and managers are then asked to unify all comments and send daily, weekly, and monthly reports to their supervisors (Pruszkiewicz et al., 2019).

Table 3: Cyber Troop Capacity in Poland

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
		Temporary	Decentralised	Medium

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

References

Applebaum, A. (2020, January 28). The Disturbing Campaign Against Poland's Judges. *The Atlantic*. https://www.theatlantic.com/ideas/archive/2020/01/disturbing-campaign-against-polish-judges/605623/

Bush, D., Gielewska, A., & Kurzynski, M. (2020, March 10). *Polish Presidential Election 2020: Two Months Out*. https://cyber.fsi.stanford.edu/io/news/polish-elections-2-months-out

Bush, D., & Kurzynski, M. (2020, January 28). *Poland: Presidential Election 2020 Scene-Setter* [Standford Internet Observatory]. https://cyber.fsi.stanford.edu/io/news/poland-scene-setter

Davies, C. (2019, November 1). Undercover reporter reveals life in a Polish troll farm. *The Guardian*. https://www.theguardian.com/world/2019/nov/01/undercover-reporter-reveals-life-in-a-polish-troll-farm

Gorwa, R. (2017). Computational Propaganda in Poland: False Amplifiers and the Digital Public Sphere. *Computational Propaganda Project Working Paper Series*. http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Comprop-Poland.pdf

Institute for Strategic Dialogue. (2019). *2019 EU Elections Information Operations Analysis: Interim Briefing*. Institute for Strategic Dialogue. https://www.isdglobal.org/isd-publications/interim-briefing-propaganda-and-digital-campaigning-in-the-eu-elections/

Marchal, N., Kollanyi, B., Neudert, L.-M., & Howard, P. N. (2019). Junk News During the EU Parliamentary Elections: Lessons from a Seven-Language Study of Twitter and Facebook. 6.

Mierzyńska, A. (2019a, February 26). Skrajnie prawicowy spamer promuje Ziobrę, płaci mu ministerstwo. Jak „dobra zmiana" robi internety. *Oko.Press*. https://oko.press/skrajnie-prawicowy-spamer-promuje-ziobre-placi-mu-ministerstwo-jak-dobra-zmiana-robi-internety/

Mierzynska, A. (2019b, June 1). *Obalamy mity! W sieci to Koalicja miała program, PiS tylko straszył, a Konfederację uwielbiali fejkowi użytkownicy*. https://oko.press/obalamy-mity-w-sieci-to-koalicja-miala-program-pis-tylko-straszyl-a-konfederacje-uwielbiali-fejkowi-uzytkownicy/

Mierzyńska, A. (2019c, June 24). Miliardy fake'owych kont, boty na polskich portalach. Analiza kampanii do PE w sieci. *Oko.Press*. https://oko.press/miliardy-fakeowych-kont-i-boty-na-polskich-portalach-analiza-kampanii-do-pe-w-sieci/

Mierzyńska, A. (2019d, August 20). *Afera Piebiaka, macki Ziobry. Ujawniamy, kto jeszcze uczestniczył w akcji hejtowania sędziów*. https://oko.press/afera-piebiaka-zaangazowane-wiecej-osob-powiazanych-z-resortem-ziobry/

Mierzyńska, A. (2020, January 22). *Polska skrajna prawica ruszyła na „podbój" Francji. W Polsce jej portale mają milionowe zasięgi*. https://oko.press/polska-skrajna-prawica-ruszyla-na-podboj-francji-w-polsce-jej-portale-maja-milionowe-zasiegi/

Pruszkiewicz, K., Ciesla, W., & Szczygiel, K. (2019, November 1). Undercover at a Troll Farm. *Investigate Europe*. https://www.investigate-europe.eu/undercover-at-a-troll-farm/

QATAR

Introduction

Qatar is consistently ranked not free in Freedom House's annual ranking of Internet freedoms and classified as repressed by the CIVICUS Monitor (CIVICUS, 2019). The hereditary Emir Sheikh Tamim bin Hamad Al Thani holds all executive, legislative, and judicial authority. Four fifths of the population are non-citizens with no political rights, few civil liberties and limited access to economic opportunities (Freedom House, 2020). Qatar amended its penal code in 2020 to include criminal penalties for spreading "fake news" online. This imposes up to five years imprisonment for "whoever broadcasts or publishes or republishes rumours or statements or false or malicious news or propaganda, inside or outside the state, whenever it is intended to harm national interests or incite public opinion or disturb the social or public order of the state" (Article 136) (Human Rights Watch, 2020).

Computational propaganda originating from Qatar is not well-documented. Reporting focuses on the ongoing diplomatic dispute between Qatar and the 'Quartet' of Gulf states (Saudi Arabia, United Arab Emirates, Bahrain, Egypt). On 23 May 2017, the state-run Qatar News Agency (QNA) posted controversial statements allegedly made by Qatari Emir Sheikh Tamim Bin Hamad Al Thani. The comments affirmed good relations with Iran, the Muslim Brotherhood, Hezbollah, and Hamas. Qatari officials quickly denied that Thani had made these comments, claiming that QNA and associated social media accounts had been hacked. Nonetheless, Saudi Arabia and the UAE media dismissed the hacking story and accused Qatar of supporting terrorism (Owen Jones, 2017). This caused the Quartet to sever diplomatic ties with Qatar. An added layer of complexity arose when US investigators found that it was Russian hackers that had breached QNA and planted the false news report that triggered the crisis, allegedly orchestrated by the UAE (Perez & Prokupecz, 2017). This dispute has been the subject of consistent computational propaganda in the region. Reuters reported that "online attacks against the small Gulf state surged" following the diplomatic boycott of Qatar in June 2017 (Knecht, 2018).

Reports of computational propaganda cannot all be taken at face value due to the nature of this dispute. The News of Bahrain claimed that "thousands of fake social media accounts are being used by the Qatari regime every day to defame Bahrain" (Zafran, 2018). And Al Arabiya (2018) reports that the Interior Ministry of Bahrain issued a statement that Qatar was seeking to influence public opinion through fake social media accounts. While no evidence has been provided to support these claims, in combination with more verifiable reports that Qatar is engaging in a degree of computational propaganda suggests that it has developed its capabilities in the context of this online information battle.

An Overview of Cyber Troop Activity in Qatar

Organizational Form

Freedom House (2020) note that security forces monitor personal communications, and that social media users can face prosecution for posting politically sensitive content. Journalists practice self-censorship and face prosecution for defamation and other press offences.

The Qatari national cybercrime law of 2014, entitled 'On suppression of electronic crimes', provides a legal framework for the prosecution of ICT-related crimes (Qatari Legislation, 2014). The second section of the law on 'Criminal Content' details the prosecution for different types of content posted online. It criminalises the creation and administration of terrorist groups' platforms and communication (Article 5), the creation and administration of a website that spreads fake news that compromises national security or public order (Article 6), and content that infringes upon moral values (Article 8)—with a maximum of three years in prison and a fine of 100,000QAR (US$27,464). Anti-terrorism legislation is used to target human rights activists using accusations of inciting hatred, working against national security, and spreading fake news.

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Qatar

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
2017	Evidence Found		Commercial botnets		

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Automation

The most documented technique is the use of automated fake Twitter accounts. There is evidence of automated activity supporting Qatar in the Gulf diplomatic crisis:

- Ben Nimmo states that Twitter bots were deployed to boost messaging on both sides of the diplomatic dispute between Saudi Arabia and Qatar, and that some of these appeared to be commercial as well as locally focused botnets (Nimmo, 2018).
- The BBC reported that tweets containing the hashtags 'Tamim the Glorious' and 'Qatar is Not Alone' were pushed by fake accounts, and even appeared on Twitter's trending homepage.
- On #Tamim_the_Glorious, one account (@sabaqksa) had 201 retweets in the space of a couple of seconds, which Nimmo said was "not a normal pattern of behavior" (Pinnell, 2018). Another surge of traffic on this hashtag saw one hundred accounts posting 1,410 times in a five-hour period, which Nimmo called "utterly implausible" that humans could have operated.
- On the hashtag 'Qatar is not alone' (#قطرليستوحدها) a scan of tweets highlights two significant spikes in activity in the initial hours of 24 May 2017, following the diplomatic incident. Traffic more than doubled in a single minute, suggesting possible botnet involvement (Nimmo, 2018). There also appeared to have been foreign involvement, as a network of bots "whose primary language and focus appears as Turkish" drove spikes in hashtags. Nimmo concluded that the focus of these Arabic-language hashtags was clearly local and regional rather than international; an attempt at messaging to the domestic population rather than the non-Arab world (Nimmo, 2018).
- BBC Monitoring (2018) found evidence of automated activity on both sides of the dispute between Qatar and Gulf states, finding that "a noticeable number of their followers were fake, and their sole purpose appeared to be boosting the credibility of larger accounts".
-

Disinformation

Coronavirus mis- and disinformation has been disseminated throughout the Gulf and has been leveraged to exacerbate existing rivalries. A trending Arabic hashtag, #Qatar_is_Corona (#قطر_هي_كورونا) links to multiple anti-Qatar conspiracy theories. The most recent case of disinformation targeting Qatar were false reports of an attempted coup in May 2020. This resulted in 'coup in Qatar'—which allegedly originated from Saudi Arabia—trending in Qatar and Saudi Arabia. Doctored video alleged to show gunfire in Doha, which was covered by Saudi-sponsored media outlets (Tarawnah, 2020). This disinformation was boosted by bot accounts ahead of the anniversary of the diplomatic feud (Walton & Levasseur, 2020).

Judicial Harassment

Qatari poet Mohamed Al-Ajami was subjected to fifteen years in prison for poem recitals that were posted online in 2011. The poems were "critical of the ruling family" and other rulers in the Gulf Cooperation Council. Blogger and human rights defender Sultan Al-Khalaifi was held incommunicado on 2 March 2011 after expressing criticism of Qatar's censorship of books in his blog. In response to arguments made by Al Khalaifi's lawyer, the cybercrime legislation was strengthened (Gulf Center for Human Rights, 2016).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Qatar

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Fake, Automated	Pro-government messages, attacking the opposition	Creation of disinformation	Facebook, Twitter, Instagram

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

Table 3: Cyber Troop Capacity in Qatar

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
		Liminal		Low/Medium

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Qatar has repeatedly been the target of computational propaganda campaigns. Marc Owen Jones (2019) details the "huge social media propaganda campaign" that followed the diplomatic crisis. News outlets have reported that the rift between the Saudi government and Qatar is "frequently bot-ridden" (Collins & Wodinsky, 2018) and that 17% of a random sample of Arabic tweets mentioning Qatar in a sample from 2017 were sent by automated accounts (Jones & Abrahams, 2018). In August 2017, Saudi Arabia's 'king of disinformation' Saud al-Qahtani said that the hashtag #LeaveTamim was trending in Qatar, reflecting how Qataris wanted to oust their ruler. However, this hashtag was mostly generated by anti-Qatar bots, signaling that Qatari Twitter trends are subject to international manipulation (Jones & Abrahams, 2018). Targeting was further evidenced by Twitter's suspension of 5,350 accounts linked to Saudi Arabia, Egypt, and the UAE, which included messaging that criticized Qatar (Borger, 2020).

Anti-Qatar propaganda has continued in recent years—between May 2017 and May 2020, accounts "encourage coup d'états, manipulate trends, smear Qatar as a belligerent actor in the Middle East, and muddy the waters of truth around the Gulf crisis". Most recently, this has taken the form of fake accounts accusing Qatar of spreading coronavirus to Argentina, and the conspiracy theory that Qatar helped fund China's development of coronavirus to harm Gulf economies (Owen Jones, 2020).

References

Al Arabiya. (2018, July 21). Bahrain detects 'fake accounts run by Qatar to harm its interests'. *Al Arabiya English*. https://english.alarabiya.net/en/News/gulf/2018/07/21/Bahrain-detects-fictitious-accounts-managed-by-Qatar-to-harm-its-interest.html

BBC Monitoring. (2018, August 31). Online trolls and fakery rises in Arab world. *BBC News*. https://www.bbc.com/news/technology-45372272

Borger, J. (2020, April 2). Twitter deletes 20,000 fake accounts linked to Saudi, Serbian and Egyptian governments. *The Guardian*. https://www.theguardian.com/technology/2020/apr/02/twitter-accounts-deleted-linked-saudi-arabia-serbia-egypt-governments

CIVICUS. (2019). *Qatar CIVICUS - Tracking conditions for citizen action*. https://monitor.civicus.org/country/qatar/

Collins, B., & Wodinsky, S. (2018, October 18). Twitter pulls down bot network that pushed pro-Saudi talking points about disappeared journalist. *NBC News*. https://www.nbcnews.com/tech/tech-news/exclusive-twitter-pulls-down-bot-network-pushing-pro-saudi-talking-n921871

Freedom House. (2020). *Freedom House | Qatar*. https://freedomhouse.org/country/qatar/freedom-world/2020

Gulf Center for Human Rights. (2016). Qatar, civil society and human rights: Lack of civil society space hinders work of human rights defenders (Mission Report). Gulf Center for Human Rights.

Human Rights Watch. (2020, January 22). *Qatar: 5-Year Prison Sentence Set for 'Fake News'*. Human Rights Watch. https://www.hrw.org/news/2020/01/22/qatar-5-year-prison-sentence-set-fake-news

Jones, M., & Abrahams, A. (2018, June 5). Analysis | A plague of Twitter bots is roiling the Middle East. *Washington Post*. https://www.washingtonpost.com/news/monkey-cage/wp/2018/06/05/fighting-the-weaponization-of-social-media-in-the-middle-east/

Knecht, E. (2018, November 14). Qatar welcomes Twitter crackdown on bots used to attack country online. *Reuters*. https://uk.reuters.com/article/uk-gulf-qatar-twitter-idUKKCN1NJ2UE

Nimmo, B. (2018, September 19). *Robot Wars: How Bots Joined Battle in the Gulf*. Journal of International Affairs. https://jia.sipa.columbia.edu/robot-wars-how-bots-joined-battle-gulf

Owen Jones, M. (2017, June 7). Analysis | Hacking, bots and information wars in the Qatar spat. *Washington Post*. https://www.washingtonpost.com/news/monkey-cage/wp/2017/06/07/hacking-bots-and-information-wars-in-the-qatar-spat/

Owen Jones, M. (2019). Propaganda, Fake News, and Fake Trends: The Weaponization of Twitter Bots in the Gulf Crisis. *International Journal of Communication, 13*, 1389–1415.

Owen Jones, M. (2020, June 2). Qatar blockade: Saudi-led disinformation war is the tip of the iceberg. *Middle East Eye*. http://www.middleeasteye.net/opinion/qatar-blockade-saudi-led-disinformation-war-just-tip-iceberg

Perez, E., & Prokupecz, S. (2017, June 7). CNN Exclusive: US suspects Russian hackers planted fake news behind Qatar crisis. *CNN*.

https://edition.cnn.com/2017/06/06/politics/russian-hackers-planted-fake-news-qatar-crisis/index.html

Pinnell, O. (2018, June 3). The online war between Qatar and Saudi Arabia. *BBC News*. https://www.bbc.com/news/blogs-trending-44294826

Qatari Legislation. (2014). *Cybercrime Prevention Law of Qarar*. http://www.ilo.org/dyn/natlex/docs/ELECTRONIC/100242/120183/F1232109237/100242.pdf

Tarawnah, N. (2020, June 7). MENA region battles the infodemic: From fake news to hashtag-washing in the region’s ongoing information wars. *IFEX*. https://ifex.org/mena-region-battles-the-infodemic-from-fake-news-to-hashtag-washing-in-the-regions-ongoing-information-wars/

Walton, G., & Levasseur, A. (2020, June 2). *Disinformation at heart of Gulf feud*. AFP Fact Check. https://factcheck.afp.com/disinformation-heart-gulf-feud

Zafran, M. (2018, July 24). Qatar creates half a million fake accounts to target Bahrain. *News of Bahrain*. https://www.newsofbahrain.com/epaper/24-07-2018/single/page-03.pdf

REPUBLIC OF NORTH MACEDONIA

Introduction

The Republic of North Macedonia, formerly the Former Yugoslavian Republic of Macedonia, has been described as a "partly free" parliamentary republic, with a highly polarised media landscape and a history of intimidation and attacks against journalists (though in recent years the intimidation and attacks on journalists have become less common) (*Freedom House | North Macedonia*, 2020). From 2006 to 2017, North Macedonia's politics were tense, with the nationalistic VMRO DPMNE party in power, and with a strong grip on government and media institutions. As recently as 2016, the European Commission considered North Macedonia a 'captured state' (SWD(2016) 362 final, 2016), and it was only under the newly elected coalition government in 2016, led by the Social Democratic Union of Macedonia party that a naming dispute with Greece was settled, enabling significant steps towards integrating within the community of democratic Euro-Atlantic countries (Gjuzelov & Hadjievska, 2020), a process that the Russian Federation is attempting to prevent (Tsalov, 2020).

North Macedonia attracted international attention in 2017 when it was revealed that teenagers in Veles, a small North Macedonian town, had run a large-scale fake news campaign during the US Presidential Election, with over 100 pro-Trump websites and Facebook pages (Subramanian, 2017). Ahead of the 2019 European Elections, the Republic of North Macedonia was one of the key countries on Facebook's watchlist of countries that had conducted "coordinated inauthentic behavior" in foreign elections ("40 Lidí, 24 Jazyků. Facebook Vytvořil Tým, Který Blokuje Falešné Zprávy o Evropských Volbách v Dublinu," 2019; "Česko Je Rejdištěm Dezinterpretací a Dezinformací, Říká Rektor. O Unii Chce Šířit Objektivní Informace," 2019). Recently, the North Macedonian government drafted a proposal to fight fake news, for instance with a strategy of investing in media literacy programs, predominantly aimed at teenagers, that explain the consequences of disinformation. The aim was to prevent the events of 2016 from being repeated, and to stop the Republic of North Macedonia being known as a 'fake news land' (Marusic, 2019; Tardáguila, 2019). However, thus far this fight has mainly been fought by private and non-profit organizations, such as the Citizens Association, with little support from the government (Vasilevski, 2020).

Domestically, while television remains the primary source of news for the majority of the adult population, studies show that North Macedonian youth are increasingly looking to social media networks for information. According to a survey of 1,015 respondents by the Institute for Communication Studies, more than one third of respondents report spending one to three hours per day on Facebook. Some 71% of youth between 15 and 24 agree with the statement that "it is important for me to share the opinion of public figures that I follow on social networks". An equal amount believes that online activism is more important than offline activism. Meanwhile, 49% of the respondents reported that they follow political news and parties, 39% follow entertainment news, and 33% follow news about economics (Kalinski, 2018); (Western Balkans Democracy Initiative, 2019).

An Overview of Cyber Troop Activity Republic of North Macedonia

Organizational Form

The media landscape in the Republic of North Macedonia is highly polarized with many outlets having ties to particular political parties (Apostolov, 2020; *Freedom House | North Macedonia*, 2020). Thus, one of the ways that political actors can share their viewpoints and narratives is through news outlets that they have connections with. Recently, researchers at the DFRLab of the Atlantic Council discovered that dozens of Facebook pages with links to at least 10 Macedonian news outlets appeared to exhibit behavior pointing towards coordinated activity. While it does not appear that the news outlets were directly managing these activities, their existence potentially implicates these political actors in having access to sophisticated cyber troop techniques. Moreover, it appears that Facebook pages added to political polarization ahead of 2020's parliamentary election, with some of the newspapers benefitting from the pages' activities being known as supporters of particular politicians. Interestingly it appeared that some of the pages were not managed from the Republic of North Macedonia, but the US (Nikolic, 2020).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in the Republic of North Macedonia

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
		x			x[1]

[1] The connection between political actors and citizens organising e.g. troll farms are alleged and appear indirect Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

The increasing reliance on news from social media has alarmed commentators who are concerned that online news as well as mis- and disinformation, which are prevalent in the Republic of North Macedonia's media ecosystem, are becoming increasingly popular with its citizens. The country's citizens ranked last out of 35 European countries in a study of resilience to fake news that was conducted by the Open Society Institute. According to the study, North Macedonia's position was due to limited media freedoms and poor media literacy (Veselinovic, 2018). An investigative journalist, Sashka Cvetkovska, commented that "every day we face the overproduction of fake news", with citizens having limited trust in the media (Civil Media, 2018). For instance, in April 2019 the presidential elections were marked by substantial disinformation on social media, spread by presidential candidates, political parties and online news sites (Crithink, 2019). Similarly, a large disinformation campaign accompanied the country's joining of NATO on the 27th of March 2020. Directing public attention away from this event, content focused on conspiracies about 5G technology as the reason for the spread of COVID-19 (F2N2, 2020).

Additionally, Russian influence is a concern. When the referendum for replacing the name of The former Yugoslav Republic of Macedonia to the Republic of North Macedonia took place in September 2018, the vote was accompanied by a heavy disinformation campaign. It was assumed that this largely originated from the Russian state, because the rhetoric of the social media content was strongly pro-Russian. The hashtag #boycott was widely used on Facebook and Twitter, and according to analysis by the German Marshall Fund, about 40 Facebook accounts were created every day in the weeks leading up to the referendum, with the sole purpose of amplifying content that promoted the boycotting of the vote (Metodieva, 2019). On Twitter, #boycott was mentioned more than 24,000 times and was tweeted more than 20,000 times. A significant portion of the accounts that shared this hashtag, analysis found, had been created in August 2018 and shared the same features: a local (Macedonian) name and a random string of numbers as usernames (Metodieva, 2019). Both Russian and Hungarian-backed Media Groups have been observed as consistent influences upon the North Macedonian public over the past few years, including during the 2020 parliamentary election ("Balkans Watch Briefing: March 2020," 2020; F2N2, 2020b).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in the Republic of North Macedonia

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Human Bots	Support Attack Opposition Driving Divisions	Disinformation Trolls Amplifying content	Facebook Twitter

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

While fake news and troll farms remain at an all-time high, for the most part they do not seem to have any links to the government of the Republic of North Macedonia. In relation to the pro-Trump campaign ran from the North Macedonia in 2016, investigations have uncovered links between North Macedonian, Russian, and US citizens. It appears that US and foreign partners of the Trump campaign may have been aware of the Macedonian efforts, though nothing concrete has been evidenced (Cvetkovska et al., 2018). Moreover, the 2018 campaign to boycott the vote on changing the name of the country to the Republic of North Macedonia was largely led by ultranationalist, private citizens who did not appear to have any evidential links with the government or other domestic political actors (Zafeiropoulos, 2019).

Thus, while political actors may have indirect access to news outlets and associated amplification strategies, the country has very little official capacity, and influence campaigns organized by domestic state actors focusing on national politics seem to be a temporary phenomenon that accompany particular political events. However, given the general amount of fake news regularly produced by actors with no association to the national government, it is difficult to examine the origins of influence and disinformation campaign. In addition, a pledge to ban political advertising in electronic media outside of election campaigns by the government did not come to fruition. Thus, as things stand there is no legal framework in North Macedonia that prevents online influence campaigns from taking place outside of election cycles, and there are examples of parties carrying out media campaigns on TV stations outside of campaign time (Apostolov, 2020).

Table 3: Cyber Troop Capacity in the Republic of North Macedonia

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
		Temporary	Decentralised	Low

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

In light of the recent COVID-19 pandemic, it appears that the country's efforts to limit the activity of troll farms and the spread of fake news has not been successful. Recently, Facebook revealed that it had banned a far-right conspiracy theory and fake news website called Natural News from their network as it had hired troll farms from North Macedonia (and the Philippines) to spread conspiracy theories about the virus (Collins & Zadrozny, 2020). In response, NATO announced that it would assist the Republic in combatting fake news in relation to COVID-19

(Marusic, 2020). Finally, analysts have found that Macedonian troll farms and disinformation campaigns on Facebook and Twitter were involved in targeting Australia’s 2019 federal election (Murphy, 2020; Taylor, 2020).

References

40 lidí, 24 jazyků. Facebook vytvořil tým, který blokuje falešné zprávy o evropských volbách v Dublinu. (2019, July 5). *IROZHLAS*. https://www.irozhlas.cz/volby/facebook-fake-news-volby-do-evropskeho-parlamentu-2019_1905070650_haf

Apostolov, V. (2020, June 23). Switched off: North Macedonia’s Media Reforms Fade Away. *Balkan Insight*. https://balkaninsight.com/2020/06/23/switched-off-north-macedonias-media-reforms-fade-away/

Balkans Watch Briefing: March 2020. (2020, March). *Balkans Watch*. https://preview.mailerlite.com/p3j5y7

Česko je rejdištěm dezinterpretací a dezinformací, říká rektor. O unii chce šířit objektivní informace. (2019, May 4). *IROZHLAS*. https://www.irozhlas.cz/zpravy-domov/euforka-univerzita-palackeho-olomouc-fake-news-dezinformace-evropska-unie_1904051740_och

Civil Media. (2018, July 5). Лажните вести предизвик на традиционалните медиуми. *Civil Media*. https://civilmedia.mk/lazhnit-vsti-prdizvik-na-tradizionalnit-mdiumi/

Collins, B., & Zadrozny, B. (2020, May 29). Troll farms from North Macedonia and the Philippines pushed coronavirus disinformation on Facebook. *NBC News*. https://www.nbcnews.com/tech/tech-news/troll-farms-macedonia-philippines-pushed-coronavirus-disinformation-facebook-n1218376

Crithink. (2019, June 5). Топ-5 дезинформации за претседателските избори. *Crithink*. http://crithink.mk/top-5-dezinformacii-za-pretsedatelskite-izbori/

Cvetkovska, S., Belford, A., Silverman, C., & Feder, J. L. (2018). *The Secret Players Behind Macedonia’s Fake News Sites*. Organized Crime and Corruption Reporting Project. https://www.occrp.org/en/spooksandspin/the-secret-players-behind-macedonias-fake-news-sites

F2N2. (2020a, April 24). HOW DID THE EPIDEMIC OF LIES REGARDING 5G TECHNOLOGY SPREAD. *F2N2*. https://f2n2.mk/en/how-did-the-epidemic-of-lies-regarding-5g-technology-spread/

F2N2. (2020b, July 12). KREMLIN CALLED – MEDDLING INTO NORTH MACEDONIA’S PARLIAMENTARY ELECTIONS 2020. *F2N2*. https://f2n2.mk/en/kremlin-called-meddling-into-north-macedonias-parliamentary-elections-2020/

Freedom House | North Macedonia. (2020). Freedom House. https://freedomhouse.org/country/north-macedonia/freedom-world/2020

Gjuzelov, B., & Hadjievska, M. I. (2020). Institutional and symbolic aspects of illiberal politics: The case of North Macedonia (2006–2017). *Southeast European and Black Sea Studies*, *20*(1), 41–60.

Kalinski, V. (2018, December 29). Таблоидирани медиуми за ширење лажни вести. *Радио Слободна Европа*. https://www.slobodnaevropa.mk/a/29677879.html

Marusic, S. J. (2019, August 15). North Macedonia’s War on ‘Fake News’ Meets Suspicion. *Balkan Insight*. https://balkaninsight.com/2019/08/15/north-macedonias-war-on-fake-news-meets-suspicion/

Marusic, S. J. (2020, April 15). NATO to Help North Macedonia Combat Fake News About Virus. *Balkan Insight*. https://balkaninsight.com/2020/04/15/nato-to-help-north-macedonia-combat-fake-news-about-virus/

Metodieva, A. (2019). *Russian Narrative Proxies in the Western Balkans*. The German Marshall Fund of the United States. http://www.gmfus.org/sites/default/files/publications/pdf/Russian%20Narrative%20Proxies%20in%20Balkans.pdf

Murphy, K. (2020, June 21). *Foreign actors targeted Facebook users during Australian 2019 election, thinktank finds*. The Guardian. http://www.theguardian.com/australia-news/2020/jun/22/foreign-actors-targeted-facebook-users-during-australian-2019-election-thinktank-finds

Nikolic, I. (2020, June 25). North Macedonia: Facebook Pages Target Users with 'Identical Content.' *Balkan Insight*. https://balkaninsight.com/2020/06/25/north-macedonia-facebook-pages-target-users-with-identical-content/

Subramanian, S. (2017, February 15). Meet the Macedonian Teens Who Mastered Fake News and Corrupted the US Election. *Wired*. https://www.wired.com/2017/02/veles-macedonia-fake-news/

SWD(2016) 362 final. (2016). *Commission Staff Working Document: The former Yugoslav Republic of Macedonia 2016 Report*. European Commission. https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/pdf/key_documents/2016/20161109_report_the_former_yugoslav_republic_of_macedonia.pdf

Tardáguila, C. (2019, November 4). Macedonia has a plan to quit being known as "fake news land." *Poynter*. https://www.poynter.org/fact-checking/2019/macedonia-has-a-plan-to-quit-being-known-as-fake-news-land/

Taylor, A. (2020, June 23). Western Balkan Disinformation Campaigns Found Interfering in Australian Elections. *Exit - Explaining Albania*. https://exit.al/en/2020/06/23/western-balkan-disinformation-campaigns-found-interfering-in-australian-elections/

Tsalov, Y. (2020, July 4). Russian interference in North Macedonia: A View Before the Elections. *Bellingcat*. https://www.bellingcat.com/news/uk-and-europe/2020/07/04/russian-interference-in-north-macedonia-a-view-before-the-elections/

Vasilevski, A. (2020, April 27). URGENT MEASURES ARE NEEDED TO PREVENT FAKE NEWS. *F2N2*. https://f2n2.mk/en/urgent-measures-are-needed-to-prevent-fake-news/

Veselinovic, M. (2018, September 30). Macedonia sees low turnout in name change referendum amid disinformation campaign. *CNN*. https://edition.cnn.com/2018/09/29/europe/macedonia-name-referendum-nato-intl/index.html

Violence erupts as protesters storm Macedonia parliament. (2017, April 28). *Www.Euractiv.Com*. https://www.euractiv.com/section/enlargement/news/violence-erupts-as-protesters-storm-macedonia-parliament/

Western Balkans Democracy Initiative. (2019). *Socio-Political Participation of Youth in North Macedonia: Apathy, Optimism or Disappointment?* Westminster Foundation for Democracy, North Macedonia. https://www.wfd.org/wp-content/uploads/2019/12/WFD-Youth-NMK.pdf

Zafeiropoulos, K. (2019, December 18). Alexander the Bot: The Twitter War for the Macedonian Soul. *Balkan Insight*. https://balkaninsight.com/2019/12/18/alexander-the-bot-the-twitter-war-for-the-macedonian-soul/

RUSSIA

Introduction

Reports of Russian computational propaganda have dominated the international news cycle since 2016. Actors operating on behalf of the Federation of Russia are often cited as the most sophisticated and pioneering actors to engage in the manipulation of social media. Many other countries, both targets and allies, have begun to imitate Russia's computational propaganda techniques—and media sources often claim that their 'playbook' has been globally adopted (Frenkel et al., 2019).

These policies need to be understood in the context of the Russian presidency's consolidation of power and the broader historical background. President Vladimir Putin has been the dominant figure in Russia's political landscape since his election in 2000. Putin was re-elected for a third term in March 2018, and constitutional amendments that were approved in a nationwide vote in 2020 mean that Putin can seek two more terms as president, allowing him to stay in power until 2036 if re-elected (Reuters, 2020). Throughout his presidency, Putin has restricted the independence of various state institutions and the media, which has been accompanied by increasing nationalism and hostility to the West.

As the world grappled with COVID-19 in 2020, disinformation campaigns which sought to capitalise on the pandemic for propagandistic purposes have been attributed to Russian actors. Declassified US intelligence revealed that websites linked to disinformation and propaganda propagated by the Main Intelligence Directorate (GRU), such as the conspiracy theory that the virus was created by the US military (Barnes & Sanger, 2020). The European Union has also claimed that Russia had unleashed a "significant disinformation campaign" pushing false narratives in English, Spanish, Italian, German and French (Emmott, 2020). Russia's COVID-19 disinformation follows the well-established pattern for disseminating malicious information: relying on state TV, proxy websites, and thousands of false social media personas to push pro-Kremlin and anti-Western narratives on Twitter, Facebook and Instagram (Glenza, 2020). According to a report by the US Global Engagement Center, the same fake accounts have previously been identified as propagating messages about the civil war in Syria, the Gilets Jaunes in France, and Chile's mass demonstrations.

The scale and sophistication of Russia's ongoing computational propaganda is exemplified by a campaign exposed by Graphika in June 2020 (Nimmo, Francois, Eib, Ronzaud, Ferreira, et al., 2020). Dubbed 'Secondary Infektion', researchers uncovered a Russia-linked campaign active from January 2014 to early 2020 which posted 2,500 pieces of content. This was discovered across three hundred platforms, including Facebook, Twitter, YouTube, Reddit, Medium, Quora, LiveJournal, blogspot, and niche discussion forums. It posted in seven languages (English, Russian, German, Spanish, Ukrainian, French, and Swedish), and targeted Ukraine, US, Poland, Germany, UK, EU, Russia, Sweden, Turkey, Lithuania, International Organisations, Georgia, Latvia, France, and Moldova.

Whilst Russian computational propaganda is a global threat that has gained increased media, government and academic attention, the topic is also subject to misinformation, inaccurate and hyperbolic reporting. Commentators often blame Russian trolls for negative outcomes or exaggerate their sophistication (Ingram, 2018). Aric Toler, researcher at Bellingcat, warned of the lack of context and nuance in reporting on Russian disinformation, citing the example of an inaccurate New York Times article on Russian health disinformation which was even shared by former president Barack Obama on Twitter (Toler, 2020). The danger of sensationalist reporting on Russian bots and trolls is that this may amplify otherwise fringe narratives and exaggerate the impact of their activities.

An Overview of Cyber Troop Activity in Russia

Organizational Form

Cyber troop activity exists within the government apparatus of loyalist security forces, a subservient judiciary, a repressive media environment, and a legislature with minimal opposition (Freedom House, 2019). Manipulation is reported to originate in part from state institutions: authorities in the Karachay-Cherkess Republic put out a public tender seeking to employ individuals to manipulate social media, and the city of Moscow is reported to employ pro-government troll farms. State employees in Moscow were instructed to like the social media posts of public officials, municipal workers in Krasnoyarsk ordered to leave positive comments to promote a 2019 winter youth sports competition, and the Moscow mayor's office has a team of pro-government activists to undertake online campaigns to praise the mayor (RuNet Echo, 2019). Emails hacked by Anonymous in 2012 alleged to show that the youth group Nashi was involved in pro-Putin blogs and comments; with some activists paid as much as 600,000 roubles (£12,694) to leave hundreds of comments on negative press articles (Elder, 2012).

Internet Research Agency

The Internet Research Agency (IRA) is one of the principal cyber troop organisations. It is run by Yevgeny Prigozhin, a Russian oligarch closely connected to Putin, often referred to as 'Putin's chef'. The activities of the IRA were first reported by Novaya Gazeta which claimed it was formed in September 2013 (Гармажапова, 2013). It first came to Western media attention following Adrien Chen's 2015 article 'The Agency' in The New York Times (Chen, 2015). The troll farm was located in St. Petersburg's Lakhta-Olgino neighbourhood (Graff, 2018b). It hired hundreds of employees to set up fake accounts and post pro-Putin, anti-Western content online, with a particular focus on targeting Ukraine and other Eastern European countries (Elliott, 2014). It was run similarly to any other marketing agency, with departments focused on graphics, data analysis, and search engine optimization, as well as IT and financing (Barrett, 2018). Estimates of its total staff differ widely, from four hundred to one thousand (Graff, 2018a). Initially, the IRA was used as a tool of domestic political manipulation, but it increasingly turned to foreign interference operations—first in Ukraine and later around the world (Bellingcat, 2020).

GRU

The Main Intelligence Directorate (GRU), Russia's military intelligence agency, has been attributed to computational propaganda campaigns. The Stanford Internet Observatory reported on the GRU's activities from 2014-19, noting the prominent use of narrative laundering and hack and leak operations (DiResta & Grossman, 2019). The report released by Special Counsel Robert Mueller (2019) following 2016 US presidential election interference attributed operations to GRU Unit 26165 and Unit 74455. US intelligence officials have also linked campaigns to the GRU's propaganda unit, known as Unit 54777 or the 72nd Special Service Center (Barnes & Sanger, 2020). The indictment issued by the Mueller investigation stated that the GRU had hacked emails from Democratic Party staff and allies, before publishing them online and promoting them through a network of fictitious social media personas. This operation combined hackers with a "fake grassroots campaign, fake social media accounts, non-existent journalists, and a dedicated website" (Nimmo, 2018c). The

GRU’s 2016 presidential election interference operation was smaller than that of the IRA, focusing mainly on mobilizing African American opinions (utilizing ‘#BlacksAgainstHillary’), supporting Russian military operations in Syria, and working closely with hacking units. The GRU has been connected to a blogging campaign from 2016-20 which used false personas to post anti-Western and pro-Kremlin messages in blogs which were amplified on social media platforms such as Facebook and Twitter (Nimmo, Francois, Eib, & Tamora, 2020).

Media

Russian media is dominated by channels that are either run directly by the state or owned by companies closely linked to the Kremlin, such as Russia Today (rebranded as ‘RT’) and Sputnik. RT’s parent company, TV-Novosti, is registered as a state-owned Autonomous Non-commercial Organization with the Russian Ministry of Justice and is almost entirely funded by the state budget (99.5%–99.9%) (Nimmo, 2018d). RT’s editor-in-chief has even gone as far as describing RT as an “information weapon” used in “critical moments” (Nimmo, 2018a). To this end, RT “subordinates journalism to one-sided reporting and selective interviewing to support the Russian government’s narratives and ‘conduct the information war’” (Nimmo, 2018a).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Russia

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
2012	GRU (Units 26165, 74455. 54777), RT, Sputnik, Public Sector workers	President Vladimir Putin	Internet Research Agency (Yevgeny Prigozhin)	Nashi	Evidence Found

Source: Authors’ evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Full Spectrum Propaganda

Computational propaganda follows the strategy of “dismiss, distort, distract, dismay” (Nimmo, 2018b). To achieve this, Russian computational propaganda relies on a combination of state and fringe media sites alongside social media operations. This has led to what Ben Nimmo (2018a) calls ‘Full Spectrum Propaganda’, resulting in a blend of attributed and non-attributed elements which allows a scale of complexity and plausible deniability. Full spectrum of propaganda is used for ‘narrative laundering’: a story is created or planted in fringe online communities, then legitimised through repeated citation across multiple media entities and amplified by fictitious social media users.

Russian propaganda has been discovered on almost every major media, social media, and technology platform. Ukrainian soldiers have been targeted with propaganda by SMS text messages on their mobile phones (@DFRLab, 2017). NATO’s Strategic Communications Centre uncovered extensive inauthentic activity on Russian service VK (VKontakte) among Russian-speaking populations in Estonia, Latvia, Lithuania and Poland (NATO StratCom, 2019). Reports indicate that alongside the major social media platforms, Instagram, Vine, Pinterest, SoundCloud, Pokémon Go, Tumblr, Reddit, Google (Google+, Gmail, Voice, Ads), Meetup, Medium, Gab and PayPal were all used to some extent in the 2016 presidential election operation (DiResta et al., 2018).

Hack and Leak

Russia considers itself to be engaged in 'full-scale information warfare' (Giles, 2016). Russia's approach to the information sphere encompasses both offensive cyber capabilities and information and content strategies—an approach that distinguishes Russia's IW (information warfare) tactics from the West. Russia's computational propaganda strategy involves the hacking of sensitive information which is subsequently leaked and amplified across traditional media and social media channels. For example, the Mueller indictment reported that the GRU hacked emails from the Democratic Party, which were published on the website DCLeaks and subsequently amplified using fictitious American personas' social media accounts (Mueller, 2019). The GRU was also implicated in targeting the World Anti-Doping Agency (WADA) in October 2018, with the arrest of four GRU hackers for leaks which were amplified by government outlets, Russian media and Internet trolls (Nimmo, 2018c). During the 2019 UK general election, UK-US trade negotiation documents were leaked and then amplified by the Labour Party in their campaign. The UK government has said that Russia sought to spread online the illegally obtained, leaked documents (BBC, 2019). In what appears to be an evolution of this tactic, Russian actors have now been found to fabricate and forge leaked documents and amplify them on fringe sites such as BuzzFeed Community, Reddit, Medium and Quora (Nimmo, 2019).

Foreign Influence Operations

Russian computational propaganda efforts have global reach. Campaigns have been conducted in Russian, English, Arabic, French, Czech, Georgian among many other languages (Helmus et al., 2018). Information operations have been uncovered in some form in a large number of European states, Canada, the US, Australia, Africa, Central Asia, and many other countries are beginning to investigate the extent of Russian interference (Dorell, 2017; Jensen & Sear, 2018).

Europe

Snegovaya (2017) has detailed a sophisticated campaign to target the Russian minority in the 2017 German elections. In December 2018, Russian accounts were implicated in using the hashtag #giletsjaunes, the French name for the Yellow Vest protest movement (Blakely, 2018). The DFR Lab (2018b) had previously uncovered extensive Russian information operations in France related to President Emmanuel Macron and attributed to the IRA. There is also evidence of Russian information operations in the Baltics, which is monitored by NATO's Strategic Communications Centre of Excellence, located in Riga, Latvia (NATO StratCom, 2019).

United States

The IRA is best-known for its interference in the 2016 US presidential election. As early as April 2014, the IRA expanded its activities to target the US population through YouTube, Facebook and Twitter, with the stated goal to "spread distrust toward the candidates and the political system in general" as part of the 'Translator Project' (Graff, 2018a). IRA employees even travelled to the US to collect intelligence for their interference operations. The IRA used stolen social security numbers and fake and stolen identity documents to establish 'sock puppets' or fake identities. They used fraudulent bank accounts to purchase political advertisements—taking advantage of the capacity of many online platforms for micro-targeted messaging. The team harnessed bots to amplify hashtags like #Trump2016, #TrumpTrain,

#MAGA, and #Hillary4Prison. The hashtags, advertisements and images that were shared predominantly opposed presidential candidate Hillary Clinton and supported Donald Trump (Shane & Goel, 2017). During the election, more than 99% of all engagement came from just twenty Facebook pages controlled by the IRA—including 'Being Patriotic', 'Heart of Texas', 'Blacktivist' and 'Army of Jesus' (Timberg & Romm, 2018). IRA instructions stated: "use any opportunity to criticize Hillary and the rest (except Sanders and Trump—we support them)" (Graff, 2018a). The IRA team even organised real-life political rallies, such as in New York and Washington DC.

Reports presented to the US Senate Intelligence Committee in December 2018 have further illustrated the impacts of Russia's interference in the 2016 presidential election. Researchers at the Oxford Internet Institute found that Russian interference began as early as 2012, continued after the election ended, and sought to divide American voters along lines such as race, ethnicity and identity (Howard et al., 2018). New Knowledge found that the IRA reached 126 million on Facebook, 20 million on Instagram, 1.4 million on Twitter, and uploaded 1,000 videos to YouTube (DiResta et al., 2018).

Despite the global outrage at Russian interference activities, the manipulation of US political discourse has continued. Secretary of Defense James Mattis confirmed that Russia attempted to interfere in the US midterm elections in 2018 (Seligman, 2018). There is evidence of IRA interference ahead of the 2020 US presidential elections. US intelligence officials made their first public assessment that the Kremlin was attempting to interfere in the 2020 campaign in support of President Trump (Barnes, 2020). In a campaign dubbed IRACopyPasta by Graphika, fifty Instagram accounts that posted about US social and political issues were exposed (Francois et al., 2019). Posts aligned with the strategic messaging of 2016: expressing support for Donald Trump and Bernie Sanders while attacking other candidates. A notable development is that activities uncovered ahead of the 2020 election show a marked change in tactics. Accounts copied and pasted text to avoid errors, used less text and fewer hashtags, hid accounts better, removed watermarks for original content, and used local people and media to post (Alba, 2020).

United Kingdom

The poisoning of Sergei Skripal, a former Russian intelligence operative, in Salisbury in March 2018, was followed by a wave of online propaganda and disinformation. UK government analysis claimed that they uncovered a 4,000% increase in the spread of propaganda from Russia-based accounts since the attack, many of which were identified as automated accounts (Stewart, 2018). Official Twitter accounts were even involved: the Russian Foreign Ministry's official account mocked the British government with tweets accusing them of blaming Russia for everything, even the weather, in what the DFRLab (2018a) labelled 'Troll Diplomacy'.

A report by the UK's Intelligence and Security Committee of Parliament, released in July 2020, found that the British government failed to conduct an assessment of Russian attempts to interfere in the 2016 Brexit referendum (Sabbagh et al., 2020). Rather than failing to uncover interference, the report claims the government actively avoided seeking evidence of Russia meddling—in contrast to the US response to 2016 election interference. Open source reporting found that Russian-linked social media accounts tweeted thousands of pro-Leave messages on the day of the Brexit referendum (Field & Wright, 2018). A Guardian investigation found that in the UK, tweets from IRA troll accounts were quoted more than eighty times across British-read media outlets (Hern et al., 2017).

Syria

Russia has used computational propaganda alongside its military intervention in Syria and in support of its regional ally, Bashar al-Assad. In April 2017, Russian bot activity increased following the chemical attack in Khan Sheikhoun, Syria, which UN investigators concluded was perpetrated by the Syrian government. The hashtag #SyriaHoax was the number one trending topic on Twitter, boosted by an army of inauthentic accounts attempting to discredit the international condemnation of the use of chemical weapons (The Syria Campaign, 2017). The Syrian volunteer rescue organisation, the White Helmets, have been the continual target of conspiracy theories and disinformation that has been disseminated and amplified by trolls linked to the Russian government since 2015 (Solon, 2017).

Africa

Foreign influence operations linked to Russia have been exposed in Africa. The Stanford Internet Observatory reported on the presence of campaigns linked to Yevgeny Prigozhin and the private military contractor Wagner Group on the continent.

Operations on Facebook and Instagram targeted the Central African Republic, the Democratic Republic of Congo, Libya, Madagascar, Mozambique, and Sudan (Grossman et al., 2019).

In a change of operational tactics, an IRA operation run from within Ghana and Nigeria was exposed in March 2020. This campaign, located in Africa but targeting Black communities in the US, operated from June 2019 to March 2020 on Facebook, Instagram, and Twitter. Graphika dubbed this operation ‘Double Deceit’ as it used unwitting, authentic activists and users under the cover of a human rights NGO to propagate their messages covertly (Nimmo, Francois, Eib, Ronzaud, Smith, et al., 2020).

Ukraine

The IRA’s initial foreign target was Ukraine, alongside other European democracies. A NATO publication suggested that Russian IW has been utilised from the onset of the Euromaidan demonstrations, to the annexation of Crimea, to the ongoing military operations in Eastern Ukraine (Jaitner, 2018). Russia’s disinformation apparatus was utilised heavily during the downing of Malaysian Airways flight MH17 over Eastern Ukraine. The IRA posted 71,000 tweets aimed at communicating a pro-Russia version of events (Bellingcat, 2020). Researchers found that Russian accounts promoted inconsistent alternative theories for the incident, such as suggesting Ukraine downed the plane with an air-to-air missile as well as the theory that Ukraine shot it down with a ground-to-air missile (Vesselkov et al., 2020).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Russia

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Automation, Human, Fake, Real, Impersonation	Pro-government, attacks on opposition, distracting messages, polarisation, trolling	Creation of disinformation, trolls, data driven strategies, amplification strategies	Facebook, Instagram, Twitter, YouTube, Reddit, Medium, Quora, LiveJournal, Blogspot, Vine, Pinterest,

			SoundCloud, Pokémon Go, Tumblr, Google (Google+, Gmail, Voice, Ads), Meetup, Gab, PayPal, VKontakte, Buzzfeed Community

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

The scale and complexity of Russia's computational propaganda operations, as well as the number of actors involved, makes determining the capacity and resources a difficult task. In February 2018, the US special counsel investigation into Russia's interference in the 2016 US election, led by Robert Mueller, indicted thirteen Russian nationals and three organizations for "conspiracy" to illegally influence the US presidential campaign (Mueller, 2019). The 2018 indictment offers the best insight into the organizational capacity of the operations. Although news stories have largely focused on the IRA, the Mueller indictment also revealed details about a network of affiliates which funded the IRA, many of which were connected to Yevgeny Prigozhin (Graff, 2018a). It is claimed the IRA operated with a monthly budget of as much as US$1.25 million and spent thousands of dollars a month buying political advertising (Lee, 2018). The IRA attracted young professionals looking for "simple, well-paid work" by paying higher than average salaries, 40,000 rubles a month (US$700), according to former workers who have been interviewed (Graff, 2018a). From 2014-15, the IRA was reportedly 300-400 staff, according to a former employee (Troianovski, 2018). The operation to inflame US political debates, dubbed 'Project Lakhta', had a budget that totalled more than US$35 million during the period January 2016 and June 2018 (Graff, 2018b).

Table 3: Cyber Troop Capacity in Russia

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
Multiple teams, IRA (300-1,000)	$35 million for Project Lakhta	High	High	High

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Timeline of platform suspensions attributed to Russia:

In response to ongoing Russian activities, social media platforms have continually suspended accounts for violating platform policies on foreign interference and coordinated inauthentic behavior. These takedowns offer an insight into the scale and breadth of Russian-attributed operations:

- Twitter first removed 3,841 accounts affiliated with the IRA in October 2018 (Gadde & Roth, 2018). This was followed by a further 418 accounts attributed to Russia which mirrored the earlier IRA activity, removed in January 2019 (Roth, 2019a), and an additional 4 accounts in June 2019 (Roth, 2019b).
- Facebook removed two networks of Russian accounts in January 2019. The first network operated in the Baltics, Central Asia, the Caucasus, and Central and Eastern

European countries. The 364 suspended pages and accounts were linked to employees of Sputnik, which spent US$135,000 on ads from October 2013 to January 2019. The second network operated in Ukraine and had similar characteristics to IRA activity. The network comprised 26 pages, 77 accounts and 41 Instagram accounts, which spent US$25,000 in 2018 (Gleicher, 2019a).

- In March 2019, 1,907 pages, groups and accounts were suspended for coordinated inauthentic behavior and linked to Russia (Gleicher, 2019b).
- In May 2019, a network of 97 accounts, pages and groups that focused on Ukraine was removed, alongside a network of 21 accounts, pages and Instagram accounts that targeted Austria, the Baltics, Germany, Spain, Ukraine and the UK (Gleicher, 2019c).
- In October 2019, three networks of accounts, pages and groups tied to Yevgeny Prigozhin were suspended, which targeted Madagascar, Central African Republic, Mozambique, Democratic Republic of the Congo, Côte d'Ivoire, Cameroon, Sudan, and Libya. The networks posted in Arabic and English and amplified RT and Sputnik stories (Gleicher, 2019e).
- In October 2019, 50 Instagram accounts and 1 Facebook account that targeted the US and showed links to the IRA were suspended (Gleicher, 2019d).
- In February 2020, 78 accounts, 11 pages, 29 groups and 4 Instagram accounts were removed by Facebook for violating policies on foreign interference. The activity targeted Ukraine and neighbouring countries, posting in Russian, English and Ukrainian, and was attributed by Facebook to Russian military intelligence services (Gleicher, 2020a).
- In April 2020, 46 pages, 91 Facebook accounts, 2 groups and 1 Instagram account were removed for foreign interference originating from Russia, the Donbass region in Ukraine and the Crimean Peninsula. This network posted in Russian, English, German, Spanish, French, Hungarian, Serbian, Georgian, Indonesian, and Farsi. The activity was also linked to media organisations NewsFront and SouthFront (Gleicher, 2020b).

References

Alba, D. (2020, March 29). How Russia's Troll Farm Is Changing Tactics Before the Fall Election—The New York Times. *The New York Times*. https://www.nytimes.com/2020/03/29/technology/russia-troll-farm-election.html?auth=login-email&login=email

Barnes, J. E. (2020, August 7). Russia Continues Interfering in Election to Try to Help Trump, U.S. Intelligence Says. *The New York Times*. https://www.nytimes.com/2020/08/07/us/politics/russia-china-trump-biden-election-interference.html

Barnes, J. E., & Sanger, D. E. (2020, July 28). Russian Intelligence Agencies Push Disinformation on Pandemic. *The New York Times*. https://www.nytimes.com/2020/07/28/us/politics/russia-disinformation-coronavirus.html

Barrett, B. (2018, February 17). Mueller Indictment Shows Russia's Internet Research Agency Inner Workings. *Wired*. https://www.wired.com/story/mueller-indictment-internet-research-agency/

BBC. (2019, December 7). PM: We must find source of UK-US trade document leak. *BBC News*. https://www.bbc.com/news/uk-50699168

Bellingcat. (2020, August 14). *Putin Chef's Kisses of Death: Russia's Shadow Army's State-Run Structure Exposed—Bellingcat*. Bellingcat. https://www.bellingcat.com/news/uk-and-europe/2020/08/14/pmc-structure-exposed/

Blakely, R. (2018, December 8). *Russian accounts fuel French outrage online*. https://www.thetimes.co.uk/article/russian-accounts-fuel-protesters-outrage-online-xx2f2g8th

Chen, A. (2015, June 1). The Agency. *The New York Times*. https://www.nytimes.com/interactive/2020/admin/100000003715857.embedded.html?

@DFRLab. (2017, May 22). *Electronic Warfare by Drone and SMS*. Medium. https://medium.com/dfrlab/electronic-warfare-by-drone-and-sms-7fec6aa7d696

@DFRLab. (2018a, March 18). *#PutinAtWar: Russia's Troll Diplomacy*. Medium. https://medium.com/dfrlab/putinatwar-russias-troll-diplomacy-7ad04e1a26b9

@DFRLab. (2018b, November 28). *#TrollTracker: Glimpse Into a French Operation*. Medium. https://medium.com/dfrlab/trolltracker-glimpse-into-a-french-operation-f78dcae78924

DiResta, R., & Grossman, S. (2019). *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014-2019*. Standford Internet Observatory. https://cyber.fsi.stanford.edu/io/publication/potemkin-think-tanks

DiResta, R., Shaffer, K., Ruppel, B., Sullivan, D., Matney, R., Fox, R., Albright, J., & Johnson, B. (2018). *The Tactics & Tropes of the Internet Research Agency*. New Knowledge. https://disinformationreport.blob.core.windows.net/disinformation-report/NewKnowledge-Disinformation-Report-Whitepaper.pdf

Dorell, O. (2017, January 9). Russia engineered election hacks and meddling in Europe. *Usatoday*. https://www.usatoday.com/story/news/world/2017/01/09/russia-engineered-election-hacks-europe/96216556/

Elliott, C. (2014, May 4). The readers' editor on… the pro-Russia trolls below the line on Ukraine stories | Chris Elliott. *The Guardian*. https://www.theguardian.com/commentisfree/2014/may/04/pro-russia-trolls-ukraine-guardian-online

Elder, M. (2012, February 7). *Polishing Putin: Hacked emails suggest dirty tricks by Russian youth group*. The Guardian. http://www.theguardian.com/world/2012/feb/07/putin-hacked-emails-russian-nashi

Emmott, R. (2020, March 18). Russia deploying coronavirus disinformation to sow panic in West, EU document says. *Reuters*. https://www.reuters.com/article/us-health-coronavirus-disinformation-idUSKBN21518F

Field, M., & Wright, M. (2018, October 17). Russian trolls sent thousands of pro-Leave messages on day of Brexit referendum, Twitter data reveals. *The Telegraph*. https://www.telegraph.co.uk/technology/2018/10/17/russian-iranian-twitter-trolls-sent-10-million-tweets-fake-news/

Francois, C., Nimmo, B., & Eib, C. S. (2019). *The IRA CopyPasta Campaign* (Graphika Reports). https://graphika.com/reports/copypasta/

Freedom House. (2019). *Russia | Freedom House*. https://freedomhouse.org/country/russia/freedom-net/2019

Frenkel, S., Conger, K., & Roose, K. (2019, February 1). Russia's Playbook for Social Media Disinformation Has Gone Global. *The New York Times*. https://www.nytimes.com/2019/01/31/technology/twitter-disinformation-united-states-russia.html

Gadde, V., & Roth, Y. (2018, October 17). *Enabling further research of information operations on Twitter*. https://blog.twitter.com/en_us/topics/company/2018/enabling-further-research-of-information-operations-on-twitter.html

Giles, K. (2016). *Handbook of Russian Information Warfare* (Fellowship Monograph). NATO. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/NDC%20fm_9.pdf

Gleicher, N. (2019a, January 17). Removing Coordinated Inauthentic Behavior from Russia. *About Facebook*. https://about.fb.com/news/2019/01/removing-cib-from-russia/

Gleicher, N. (2019b, March 26). Removing Coordinated Inauthentic Behavior from Iran, Russia, Macedonia and Kosovo. *About Facebook*. https://about.fb.com/news/2019/03/cib-iran-russia-macedonia-kosovo/

Gleicher, N. (2019c, May 6). Removing More Coordinated Inauthentic Behavior From Russia. *About Facebook*. https://about.fb.com/news/2019/05/more-cib-from-russia/

Gleicher, N. (2019d, October 21). Removing More Coordinated Inauthentic Behavior From Iran and Russia. *About Facebook*. https://about.fb.com/news/2019/10/removing-more-coordinated-inauthentic-behavior-from-iran-and-russia/

Gleicher, N. (2019e, October 30). Removing More Coordinated Inauthentic Behavior From Russia. *About Facebook*. https://about.fb.com/news/2019/10/removing-more-coordinated-inauthentic-behavior-from-russia/

Gleicher, N. (2020a, February 12). Removing Coordinated Inauthentic Behavior From Russia, Iran, Vietnam and Myanmar. *About Facebook*. https://about.fb.com/news/2020/02/removing-coordinated-inauthentic-behavior/

Gleicher, N. (2020b, May 5). April 2020 Coordinated Inauthentic Behavior Report. *About Facebook*. https://about.fb.com/news/2020/05/april-cib-report/

Glenza, J. (2020, February 22). Coronavirus: US says Russia behind disinformation campaign. *The Guardian*. https://www.theguardian.com/world/2020/feb/22/coronavirus-russia-disinformation-campaign-us-officials

Graff, G. (2018a, February 20). Inside the Mueller Indictment: A Russian Novel of Intrigue. *Wired*. https://www.wired.com/story/inside-the-mueller-indictment-a-russian-novel-of-intrigue/

Graff, G. (2018b, October 19). Russian Trolls Are Still Playing Both Sides—Even With the Mueller Probe. *Wired*. https://www.wired.com/story/russia-indictment-twitter-facebook-play-both-sides/

Grossman, S., Bush, D., & DiResta, R. (2019). *Evidence of Russia-Linked Influence Operations in Africa* (Stanford Internet Observatory). https://cyber.fsi.stanford.edu/io/news/prigozhin-africa

Helmus, T. C., Bodine-Baron, E., Radin, A., Magnuson, M., Mendelsohn, J., Marcellino, W., Bega, A., & Winkelman, Z. (2018). *Russian Social Media Influence* [Product Page]. RAND. https://www.rand.org/pubs/research_reports/RR2237.html

Hern, A., Duncan, P., & Bengtsson, H. (2017, November 20). Russian ‘troll army’ tweets cited more than 80 times in UK media. *The Guardian*. https://www.theguardian.com/media/2017/nov/20/russian-troll-army-tweets-cited-more-than-80-times-in-uk-media

Howard, P. N., Ganesh, B., Liotsiou, D., Kelly, J., & Francois, C. (2018). *The IRA, Social Media and Political Polarization in the United States, 2012-2018* (Project on Computational Propaganda). https://comprop.oii.ox.ac.uk/research/ira-political-polarization/

Ingram, M. (2018, February 21). *The media today: Are Russian trolls behind everything?* Columbia Journalism Review. https://www.cjr.org/the_media_today/russian-trolls.php

Jaitner, M. (2018). Russian Information Warfare: Lessons from Ukraine. CCDCOE.

Jensen, M., & Sear, T. (2018, August 22). Russian trolls targeted Australian voters on Twitter via #auspol and #MH17. *The Conversation*. http://theconversation.com/russian-trolls-targeted-australian-voters-on-twitter-via-auspol-and-mh17-101386

Lee, D. (2018, February 16). The tactics of a Russian troll farm. *BBC News*. https://www.bbc.com/news/technology-43093390

Mueller, R. (2019). *Report on the Investigation Into Russian Interference in the 2016 Presidential Election* (U.S. Department of Justice). https://www.justice.gov/storage/report.pdf

NATO StratCom. (2019). *Robotrolling* (No. 1/2019).

Nimmo, B. (2018a, January 23). Russia's Full Spectrum Propaganda. *DFRLab*. https://medium.com/dfrlab/russias-full-spectrum-propaganda-9436a246e970

Nimmo, B. (2018b, April 2). #TrollTracker: Kremlin Supporters Strike Back. *DFRLab*. https://medium.com/dfrlab/trolltracker-kremlin-supporters-strike-back-d994f001d743

Nimmo, B. (2018c, August 2). #TrollTracker: Russia's Other Troll Team. *DFRLab*. https://medium.com/dfrlab/trolltracker-russias-other-troll-team-4efd2f73f9b5

Nimmo, B. (2018d, November 23). Question That: RT's Military Mission. *DFRLab*. https://medium.com/dfrlab/question-that-rts-military-mission-4c4bd9f72c88

Nimmo, B. (2019). *UK Trade Leaks & Secondary Infektion* (Graphika Reports). https://graphika.com/reports/uk-leaks-and-secondary-infektion/

Nimmo, B., Francois, C., Eib, C. S., Ronzaud, L., Ferreira, R., Hernon, C., & Kostelancik, T. (2020). *Secondary Infektion* (Graphika Reports). https://graphika.com/reports/exposing-secondary-infektion/

Nimmo, B., Francois, C., Eib, C. S., Ronzaud, L., Smith, M., Lederer, T., Carter, J., & McAweeney, E. (2020). *IRA in Ghana: Double Deceit* (Graphika Reports). https://graphika.com/reports/ira-in-ghana-double-deceit/

Nimmo, B., Francois, C., Eib, C. S., & Tamora, L. (2020). *From Russia with Blogs* (Graphika Reports). https://graphika.com/reports/from-russia-with-blogs/

Roth, Y. (2019a, January 31). *Empowering further research of potential information operations*. https://blog.twitter.com/en_us/topics/company/2019/further_research_information_operations.html

Roth, Y. (2019a, January 31). *Empowering further research of potential information operations*. https://blog.twitter.com/en_us/topics/company/2019/further_research_information_operations.html

Roth, Y. (2019b, June 13). Information operations on Twitter: Principles, process, and disclosure. *Twitter*. https://blog.twitter.com/en_us/topics/company/2019/information-ops-on-twitter.html

RuNet Echo. (2019, February 17). Russian public sector workers ordered to 'like' social media posts promoting the 2019 Winter Universiade · Global Voices. *Global Voices*. https://globalvoices.org/2019/02/17/russian-public-sector-workers-ordered-to-like-social-media-posts-promoting-the-2019-winter-universiade/

Sabbagh, D., Harding, L., & Roth, and A. (2020, July 21). Russia report reveals UK government failed to investigate Kremlin interference. *The Guardian*. https://www.theguardian.com/world/2020/jul/21/russia-report-reveals-uk-government-failed-to-address-kremlin-interference-scottish-referendum-brexit

Seligman, L. (2018, December 1). Mattis Confirms Russia Interfered in U.S. Midterm Elections. *Foreign Policy*. https://foreignpolicy.com/2018/12/01/mattis-confirms-russia-interfered-in-us-midterm-elections-putin-trump/

Shane, S., & Goel, V. (2017, September 6). Fake Russian Facebook Accounts Bought $100,000 in Political Ads. *The New York Times*. https://www.nytimes.com/2017/09/06/technology/facebook-russian-political-ads.html

Snegovaya, M. (2017, October 17). Russian Propaganda In Germany: More Effective Than You Think. *The American Interest*. https://www.the-american-interest.com/2017/10/17/russian-propaganda-germany-effective-think/

Solon, O. (2017, December 18). How Syria's White Helmets became victims of an online propaganda machine. *The Guardian*. https://www.theguardian.com/world/2017/dec/18/syria-white-helmets-conspiracy-theories

Stewart, H. (2018, April 19). Russia spread fake news via Twitter bots after Salisbury poisoning – analysis. *The Guardian*. https://www.theguardian.com/world/2018/apr/19/russia-fake-news-salisbury-poisoning-twitter-bots-uk

The Syria Campaign. (2017). *Killing the Truth*. https://thesyriacampaign.org/wp-content/uploads/2017/12/KillingtheTruth.pdf

Timberg, C., & Romm, T. (2018, December 17). New report on Russian disinformation, prepared for the Senate, shows the operation's scale and sweep. *Washington Post*. https://www.washingtonpost.com/technology/2018/12/16/new-report-russian-disinformation-prepared-senate-shows-operations-scale-sweep/

Toler, A. (2020, April 15). *How (Not) To Report On Russian Disinformation*. Bellingcat. https://www.bellingcat.com/resources/how-tos/2020/04/15/how-not-to-report-on-russian-disinformation/

Troianovski, A. (2018, February 18). A former Russian troll speaks: 'It was like being in Orwell's world'. *Washington Post*. https://www.washingtonpost.com/news/worldviews/wp/2018/02/17/a-former-russian-troll-speaks-it-was-like-being-in-orwells-world/

Vesselkov, A., Finley, B., & Vankka, J. (2020). Russian trolls speaking Russian: Regional Twitter operations and MH17. *WebSci 20: 12th ACM Conference on Web Science*. https://www.researchgate.net/publication/342399881_Russian_trolls_speaking_Russian_Regional_Twitter_operations_and_MH17

Гармажапова, А. (2013, July 9). *Где живут тролли. И кто их кормит*. Новая газета - Novayagazeta.ru. https://novayagazeta.ru/articles/2013/09/07/56253-gde-zhivut-trolli-i-kto-ih-kormit

RWANDA

Introduction

Rwanda is considered a “not free” country with a score of 22/100 on the Freedom House index. While the country has experienced increased stability and economic growth, the state is repressively governed by the Rwandan Patriotic Front (RPF) led by President Paul Kagame since 1994. Constitutional changes passed in 2015 have in essence guaranteed Kagame’s rule until 2034; while the country does hold elections, they are tainted by fraud, unfair registration processes and political intimidation and smear campaigns against oppositional candidates (Freedom House, 2019a). Similarly, the government also limits freedom of expression online and Freedom House has been observing a decline in internet freedom in their 2019 report. The internet penetration rate has been reported at between 44% to 52%, though the government states that 90% of the population has broadband network access. Only about 4.9% of the population are active on social media, and the main apps, such as YouTube, Facebook, Twitter or WhatsApp are freely available (Freedom House, 2019b).

An Overview of Cyber Troop Activity Rwanda

Organizational Form

Given the general control the governing RPF has on the state’s agencies and institutions, most cyber troop or restriction activity goes through official channels. Blocking and restrictive cybersecurity laws are amongst the most common tools to limit online freedom (Freedom House, 2019b). At the same time, the political intimidation tactics of the administration, which include imprisonment and assassinations (Freedom House, 2019a), lead to a great deal of self-censorship, particularly during politically sensitive times.

The government also maintains an Office of the Government Spokesperson, which is essentially an official propaganda entity that has administrative access to websites of formally independent newspapers (Freedom House, 2019b). The office started operations in late 2011 and has the official job of facilitating communication between the government, its citizens, and global audiences and to provide information regarding the country that Rwandans have been missing (“Office of the Government Spokesperson to Open Soon,” 2011). In addition, the state maintains control over most newspapers by being their main financier, paying for approximately 85-90% of the advertisements displayed in the papers which finance the outlets (Rhodes, 2014a).

Finally, local experts have observed that Rwanda has been running online disinformation campaigns for a long time, relying on a variety of actors, including exchange students and PR firms: the RPF has reportedly been working with American and British PR firms, such as the London company Racepoint, since 2009 (Booth, 2010; Thomson, 2014).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Rwanda

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
	X	X	X		X

Source: Authors’ evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

As many journalists have taken to work in exile, the government has been particularly active in blocking access to news websites based abroad. These blocking efforts focus on local language content so most international news sources remain accessible. Additionally, the President and his administration regularly threatens people who speak out against the government online. Given the country's track record with targeting dissidents, these threats are taken seriously and lead to a great deal of self-censorship online (Freedom House, 2019a).

While the Rwandan administration usually does not provide any explanation for particular content removal or blocking online, in May 2019 it announced its intentions to protect citizens from misinformation and the societally disruptive forces of social media by regulating content on these platforms (Ntirenganya, 2019). At the time of writing no concrete steps or laws have been drafted. There are suggestions that drafting such regulations is particularly tricky for the administration because state agents are amongst the biggest spreaders of misinformation relating to Rwanda, both domestically and abroad (CGTN Africa, 2019; Freedom House, 2019b). The government had tried to introduce social media regulation aiming at supressing oppositional opinions before in 2017, during campaigning time for the presidential election, when the Electoral Commission attempted to regulate posts by opposition parties, taking up to 48 hours to approve campaign messages before they could be posted online. The commission refrained from such regulation after receiving strong criticism from international media (Sawyer, 2017).

In addition to editorial influences the government also manipulates online information through coordinated social media campaigns. Security and other government officials will interfere with the publication of stories on certain topics and debate and harass individuals who post comments considered critical of the government. These activities seem to take place on Twitter and Facebook. Fake Twitter accounts have been found to counter Rwandan critics and spreading and amplifying disinformation and pro-government narratives, some of these state-sponsored accounts even posed as Rwandan news websites (Freedom House, 2019b; Rhodes, 2014b). Much evidence of a 2014 incident dubbed Rwanda's "Twitter-Gate", points towards these activities being organised by staff in close proximity to the President, likely his communication department (Taylor, 2014).

Prominent oppositional politician Diane Shima Rwigara outlined the harassment and threats critics of the government face in a press conference she conducted ahead of the 2017 election in which she intended to run as an independent candidate: those supporting her cause were physically threatened and, in some cases, arrested. Citizens who intended to sign with her to support her bid for president were refused and told by local authorities that they were betraying the country and its leader. Rwigara herself was accused of forging the signatures to enter the election as a candidate and eventually arrested alongside her mother after the election, only to be acquitted in December 2018. When she had originally announced her run for presidency in March 2017, nude photos of her were circulated within 48 hours of her statement. She has accused the RPF government of fabricating and disseminating the images (Rwigara, 2017).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Rwanda

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Human Fake	Support Attack Opposition Suppression	Disinformation Trolls Amplifying Content	Twitter Facebook

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

In general, while there is ample evidence of the government running disinformation and trolling campaigns online, there is very little known about the capacity and resources of these activities. At most, the "Twitter-Gate" incident of 2014 showcased how close the President is to these activities, as Kagame's official Twitter account stepped into a tweet battle between several journalists, activists and a prominent Rwandan trolling account: It appears that someone with access to the President's Twitter account was behind the troll and accidentally tweeted from the wrong account. Kagame's office quickly attempted to bury the scandal by stating that the troll account had been run by an employee in the Presidency without authorization (Taylor, 2014).

Table 3: Cyber Troop Capacity in Rwanda

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
		Permanent	Coordinated	

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

References

Booth, R. (2010, August 3). Does this picture make you think of Rwanda? *The Guardian*. https://www.theguardian.com/media/2010/aug/03/london-pr-rwanda-saudi-arabia

CGTN Africa. (2019, May 18). Rwanda mulling more restrictions on social media. *CGTN Africa*. https://africa.cgtn.com/2019/05/18/rwanda-mulling-more-restrictions-on-social-media/

Freedom House. (2019a). *Freedom House | Rwanda*. https://freedomhouse.org/country/rwanda/freedom-world/2020

Freedom House. (2019b). *Freedom on the Net | Rwanda*. https://freedomhouse.org/country/rwanda/freedom-net/2019

Ntirenganya, E. (2019, May 12). Govt moves to regulate social media content amid misinformation. *The New Times | Rwanda*. https://www.newtimes.co.rw/news/govt-moves-regulate-social-media-content-amid-misinformation

Office of the Government Spokesperson to open soon. (2011, September 28). *The New Times | Rwanda*. https://www.newtimes.co.rw/section/read/35416

Rhodes, T. (2014a, February 19). Advertising and censorship in East Africa's press. *Pambazuka News*. https://www.pambazuka.org/governance/advertising-and-censorship-east-africas-press

Rhodes, T. (2014b, March 24). Twitter war shines light on how Rwanda intimidates press. *Committee to Protect Journalists*. https://cpj.org/2014/03/twitter-war-shines-light-on-how-rwanda-intimidates/

Rwigara, D. S. (2017, June 19). Diane Shima Rwigara asobanura amafoto yamwitiriwe n’imbogamizi yahuye nazo mu gusinyisha. https://www.youtube.com/watch?v=hoEE4erZc20

Sawyer, I. (2017, June 1). Dwindling Options for Opposition Candidates in Rwanda. *Human Rights Watch*. https://www.hrw.org/news/2017/06/01/dwindling-options-opposition-candidates-rwanda

Taylor, A. (2014, March 7). A stray tweet may have exposed Paul Kagame’s Twitter ghostwriter, and maybe much more. *Washington Post*. https://www.washingtonpost.com/news/worldviews/wp/2014/03/07/a-stray-tweet-may-have-exposed-paul-kagames-twitter-ghostwriter-and-maybe-much-more/

Thomson, S. (2014, March 17). Rwanda’s Twitter-Gate: The Disinformation Campaign of Africa’s Digital President. *African Arguments*. https://africanarguments.org/2014/03/17/rwandas-twitter-gate-the-disinformation-campaign-of-africas-digital-president-by-susan-thomson/

SAUDI ARABIA

Introduction

The Kingdom of Saudi Arabia reportedly employs an ‘electronic army’ that posts pro-government messages, inflames sectarian tensions, targets foreign states, and trolls Saudi critics. Saudi-attributed accounts were suspended for platform manipulation on Facebook and Instagram in August 2019, and on Twitter in September and December 2019. Much of the computational propaganda activity occurs on Twitter, which plays a central role in Saudi politics and discourse. With 9.9 million active users, it is the fourth largest Twittersphere in the world (Hubbard, 2019). Saudi activist Omar Abdulaziz claims that with the rise of Crown Prince Mohammed Bin Salman (MBS), “Saudi Twitter gradually morphed into a propaganda platform” (Abdulaziz, 2019). Saudi Arabia’s propaganda apparatus has been described by Iyad el-Baghdadi, a writer and activist, as having “ruthless sophistication” (el-Baghdadi, 2019).

Allegedly, the murder of Jamal Khashoggi in October 2018 can also be linked to Saudi computational propaganda. *The Independent* reported that Khashoggi was at the heart of an ‘online army’ of Saudi activists fighting a ‘misinformation cyberwar’ (Trew, 2018). Khashoggi was a prominent Saudi dissident who had been writing articles critical of Saudi Arabia for *The Washington Post*. Khashoggi had been attempting to combat online abuse, was involved in Disinformation Monitor, and had wired USD $5,000 to Omar Abdulaziz, who was creating a volunteer army known as the ‘Electronic Bees’ to combat Saudi government Twitter trolls (Benner et al., 2018). On 2 October, Khashoggi was assassinated by Saudi intelligence officials in Riyadh’s consulate in Istanbul, Turkey. A United Nations human rights investigation into the assassination found evidence that it was a premeditated killing, planned and perpetrated by officials of Saudi Arabia (Chapelle, 2018). There is also evidence of Saud al-Qahtani’s involvement in the Khashoggi murder, a close adviser to MBS, from the Center for Studies and Media Affairs in Riyadh. *Reuters* reported that according to a high-ranking source, al-Qahtani was video-called via Skype in the room in the Saudi consulate prior to Khashoggi’s murder (Galloni & Robinson, 2018).

An Overview of Cyber Troop Activity in Saudi Arabia

Organizational Form

Al-Qahtani reportedly leads online government trolling and bot networks in Saudi Arabia (Applebaum, 2018). It is alleged that in the 2000s, al-Qahtani was tasked with building an ‘electronic media army’, a network of surveillance, and tools of social media manipulation to advance the Crown Prince’s agenda and suppress his critics. This initiative was further given impetus by the events of the Arab Spring. Al-Qahtani developed a so-called “army of flies” and was labelled by activists as the ‘troll master’; ‘Saudi Arabia’s Steve Bannon,’ and ‘minister of disinformation’. Twitter announced in 2019 that it had permanently suspended the account of Saud al-Qahtani for violating platform manipulation policies (Twitter Safety, 2019a). Qahtani is just one of such accounts that is run by a well-known personality, often verified by Twitter, yet is a “dedicated propaganda mouthpiece of the government” (el-Baghdadi, 2019).

Saudi Arabia has been accused of using computational propaganda to project messages abroad. In November 2017, the government faced allegations of using Twitter bots to disseminate pro-Saudi narratives about the war in Yemen (Freedom House, 2019). Facebook removed a network of accounts with links to individuals associated with the government of Saudi Arabia that had created fictitious personas, disseminated pro-Saudi content, and drove people to off-platform domains (Facebook, 2019). This content focused primarily on the Middle East and

North Africa, including Qatar, Saudi Arabia, UAE, Bahrain, Egypt, Morocco, Palestine, Lebanon, and Jordan. In the December 2019 suspension of Twitter accounts, the majority of the network produced Arabic content, however some content related to events relevant to Western audiences including the amplification of discussions around sanctions in Iran (Twitter Safety, 2019b). Following an incident in which a member of the Royal Saudi Air Force, shot and killed three United States military personnel while undertaking training in Florida, December 2019, a network of accounts linked to the news channel Saudi 24 manipulated the #floridashooting hashtag in order to generate support for Saudi Arabia's counter-terror initiatives (Owen Jones, 2020).

According to *The Guardian*, lobbying firm CTF Partners had built a network of unbranded media pages on Facebook for dozens of clients, including the Saudi government. The report alleges that the company had received "millions of pounds" from the Saudi Arabian government in 2018 to "burnish the reputation of crown prince Mohammed bin Salman" (Waterson, 2019).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Saudi Arabia

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
2012	'Electronic Army', Center for Studies and Media Affairs	Mohammed bin Salman, Saud al-Qahtani, Khaled al-Tuaqaijri	Smaat, NSO Group, Hacking Team, CTF Partners		Evidence Found

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Trolling and harassment

Trolling and harassment are a part of the government's strategy to silence critics and dissidents. Khashoggi tweeted in December 2017 that "Saudi government trolls have a devastating effect on the national public opinion" (Abdulaziz, 2019). Omar Abdulaziz states that the trolling and pressuring of influencers to amplify government messages are central to the Kingdom's Twitter strategy, often targeting Saudis with tribal and racist attacks. Trolling originates from both bot and human accounts, including the accounts of Saudi politicians. Ghada Oueiss, an Al Jazeera journalist, was referred to as a "prostitute" by an account with 338,000 followers – which was verified as Minister Abdullatif al-Shaikh (Roberts, 2018). According to Freedom House, trolls are tasked with suppressing online expressions of dissent and smearing opponents. Trolls are given lists of names and daily quotas to target dissidents on platforms such as Twitter, WhatsApp and Telegram (Freedom House, 2019).

Following an economic boycott against Qatar in June 2017, al-Qahtani encouraged Twitter users to use the hashtag #TheBlackList (#القائمة_السوداء) to identity Saudi citizens who sympathized with Qatar. Al-Qhatani vowed to follow every name that was reported to him. Saudi writer Turki al-Ruqi accused al-Qahtani of acting like an Internet troll when he launched social media campaigns to intimidate dissidents (The New Arab, 2018). Bot networks changed their location to Qatar and propelled anti-government hashtags to the top of Qatari Twitter trends with the aim of leading foreign Twitter users to conclude that Qataris were demanding a change of leadership (Chapelle, 2018). Research at Columbia University discovered that, on both sides of the row, automated networks of Twitter accounts amplified their messages and boosted hashtags. The research suggested that some of these botnets may have been commercial and hired from abroad, while others were made to appear as locally based in both Saudi Arabia and Qatar (Mezzofiore & Burke, 2018).

Automation

There is a large volume of bots on Twitter in Saudi Arabia. Marc Owen Jones, an Assistant Professor in Middle East Studies and Digital Humanities at Hamad bin Khalifa University, Doha, has suggested that half of the active Twitter users in the Kingdom may in fact be bots (Chapelle, 2018). Owen Jones' analysis has found that bots in the Kingdom focus on hashtags relating to domestic issues, such as #Saudi, #Riyadh and #AlQatif, often in support of Saudi government or foreign policy, but also international targets, with hashtags such as #Bahrain and #Yemen, and also with the propagation of sectarian rhetoric (2018). Owen Jones alleges that the scale of this operation is enormous, with dormant Twitter accounts used as 'fake followers', including "potentially up to a million of these accounts". According to his data, 70–80% of Arabic-language tweets containing the word 'Saudi' in a four-month period were posted by bots (Groll, 2018). Automation is commonly achieved through third-party automated tools, as was the case in the amplification of content by Saudi social media marketing firm Smaat (Twitter Safety, 2019b).

Automated bots flooded social media to cast doubt on allegations that Saudi Arabia was involved in the murder of Jamal Khashoggi (Reuters, 2018b). The hashtag announcing Khashoggi's 'kidnapping' disappeared from the list of top trends in Saudi Arabia after a few hours, suggesting that an army of accounts had worked to deliberately bury it (Trew, 2018). The hashtag #UnfollowEnemiesOfTheNation was mentioned 103,000 times in the days following the murder (Applebaum, 2018), and analysis determined that there were hundreds of postings per second (Coleman & Bell, 2018). Ben Nimmo found that 96.3% of the uses of these hashtags were retweets, suggesting a coordinated effort from bots or a retweet farm. On 14 October, Arabic hashtags topped the global trends; 'we all have trust in Mohammed bin Salman' was featured in 250,000 tweets, and 'we have to stand by our leader' in 60,000 tweets. Some of these networks have been spreading propaganda since 2012, whereas others appear commercial and were rented during the specific timeframe (Mezzofiore & Burke, 2018). *NBC News* identified a high volume of Twitter accounts created in quick succession on 16-17 November 2017 and being utilized to spread pro-Saudi messages (Collins & Wodinsky, 2018). Some of these accounts avoided being posted in high volumes, thus evading Twitter's detection mechanisms. However, hundreds of these pro-Saudi accounts were deleted by Twitter in October 2018. Twitter claimed that these pro-government bots had been part of an online propaganda campaign since 2016 (Trew, 2018).

According to Marc Owen Jones, there is a network dubbed 'Diavolo' that promotes content of the conservative news station Saudi 24 and its associated channels, "responsible for spreading sectarian hate speech, antisemitism and conspiracy theories". This network has been active since 2016, with an estimated 3,700 accounts, and focusses on issues related to Iran, Turkey and Qatar (Owen Jones, 2020).

Real accounts

Alongside government employees and automated fake accounts, genuine Twitter accounts are also used to spread propaganda. Twitter accounts of deceased celebrities have been used to spread pro-Saudi propaganda. The hacked Twitter account of David Schwartz, a weather channel meteorologist who died in 2016, had his Twitter handle used to post pro-Saudi messages – possibly because the Twitter account was verified but no longer being used (Owen Jones, 2019) . Similarly, Saudi influencers are often co-opted into spreading propaganda for the government. Over 30 influencers have reported that the Saudi government was blackmailing them with material obtained by hacking their phones. Influencers were then presented with the options of Tweeting favourable propaganda or having private content leaked (Abdulaziz, 2019).

Political hashtags often originate from one real Twitter user and then boosted by a mix of human accounts and bots (Brewster, 2020). In response to allegations that a WhatsApp message from MBS led to the hacking of the iPhone of Jeff Bezos, CEO of Amazon, an army of pro-Saudi Twitter trolls issued calls to boycott Amazon. The hashtag #BoycottAmazonProducts (#قاطعوا_منتجات_امازون) originated from the pro-government account @mbs_mbsksa, with 60,000 followers. Ben Nimmo, director of investigations at Graphika, said that this was a similar strategy to anti-Qatar Twitter traffic in 2017.

Disinformation

Saudi Arabia has been accused of utilising accounts that masquerade as local independent journalist outlets when disseminating pro-Saudi content. Facebook pages were suspended in 2019 on the basis of the accusation that they were masquerading as local news organisations, and six Twitter accounts were removed for masquerading as independent journalists (Twitter Safety, 2019a).

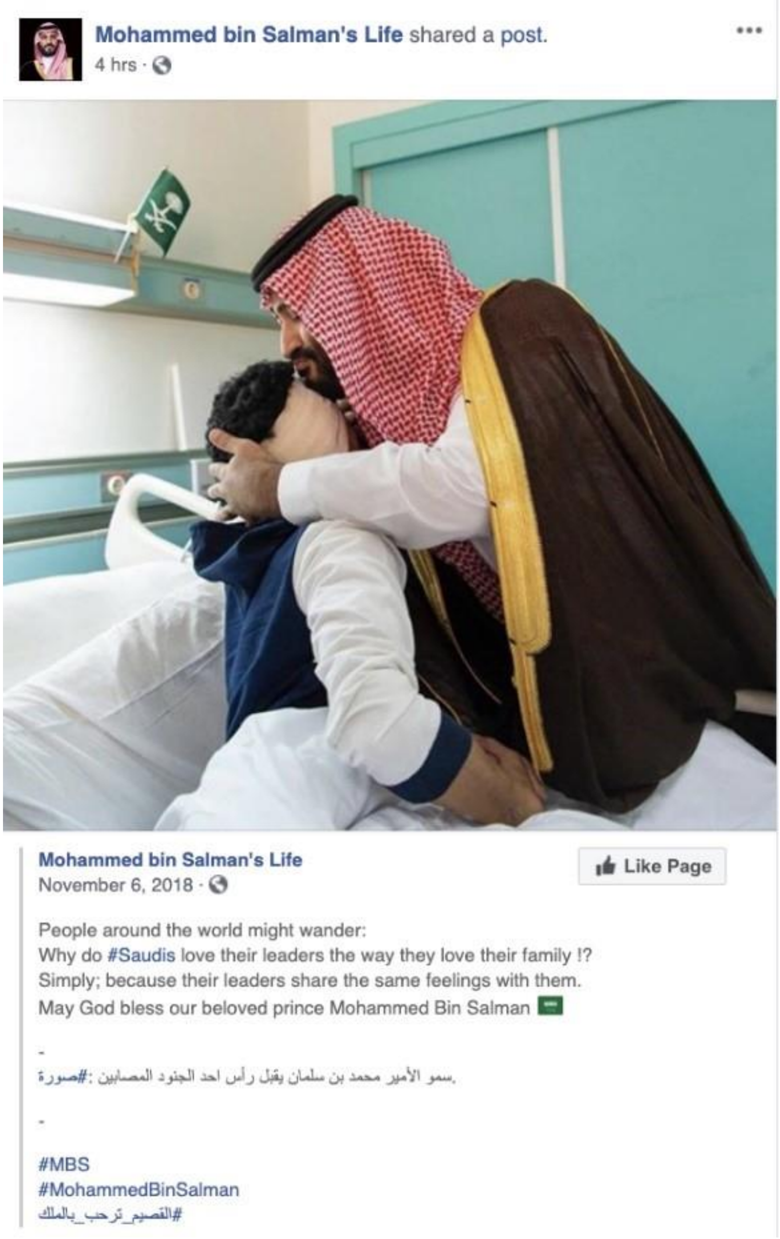
Disinformation was prolific following Khashoggi's murder. At least 53 websites, including alawatanews.com, were part of a network that posed as authentic Arabic-language media outlets to spread disinformation about the Saudi involvement in Khashoggi's murder (Stubbs et al., 2018). The extent of disinformation even led to Reuters falling for a fake news article about the firing of a Saudi general consul, leading to the retraction of an article (Funke, 2018). A fake fact-checking Twitter account called 'Middle East Guardians' was created in September 2018. This is part of a growing trend of malicious fact-checking organisations. The account published a photo that it claimed had been doctored to include Khashoggi's Turkish fiancée, suggesting that she had not been present before his murder and has in fact no relationship to Khashoggi at all. The claim of 'Middle East Guardians' has led to her becoming a target for people who claimed that the whole incident was a set up to make Saudi Arabia look bad. However, the photo was debunked, and fact-checking Twitter account suspended (Funke, 2018).

Espionage

A sophisticated tactic is the use of agents to gain access to confidential information at Twitter. In 2019, the United States Justice Department charged two former Twitter employees for spying on behalf of the Saudi government, by accessing information on dissidents using the platform. Ali Alzabarah, a Saudi citizen, was accused of accessing personal information on 6,000 Twitter accounts on behalf of the government (Nakashima & Bensinger, 2019). This tactic demonstrates the lengths to which the Saudi Arabia goes in its information operations.

Although the official Saudi government line was to deny involvement, many glorified the actions of the spies on Saudi Twitter.

Figure 1: Pro-MBS content removed by Facebook for platform manipulation (Facebook, 2019)



Mohammed bin Salman's Life shared a post.
4 hrs · 🌐

Mohammed bin Salman's Life
November 6, 2018 · 🌐

People around the world might wander:
Why do #Saudis love their leaders the way they love their family !?
Simply; because their leaders share the same feelings with them.
May God bless our beloved prince Mohammed Bin Salman 🇸🇦

-

سمو الأمير محمد بن سلمان يقبل رأس احد الجنود المصابين :#صورة.

-

#MBS
#MohammedBinSalman
#القصيم_ترحب_بالملك

Hacking

Saudi Arabia integrates its propaganda campaigns with its hacking capabilities. One tactic is to hack the phones of dissidents and distribute the compromised information using their Twitter networks. For example, journalist Ghada Ouiess had private personal photos stolen from her phone and posted on Twitter alongside offensive, misogynistic and false claims -- which were subsequently tweeted more than 40,000 times. The accounts frequently displayed the Saudi flag and pictures of MBS. Saudi public figures, such as Naif Al-Asaker of the Saudi Ministry of Islamic Affairs, amplified these posts and contributed to the trending of the hashtag #Ghada_Jacuzzi (Oueiss, 2020).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Saudi Arabia

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Bots, Human, Hacked Accounts	Pro-government messaging, Attacking Opposition (trolling, harassment), Polarising, Suppressing (e.g. hashtag poisoning)	Disinformation (fake journalistic outlets), distraction, artificially amplifying content, trolling and harassment	Twitter, Facebook, Instagram, WhatsApp, Telegram

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

There is evidence of outsourcing capabilities. A BBC investigation found that companies in Saudi Arabia were offering to artificially boost the popularity of hashtags on Twitter, quoting the equivalent of GBP £150 to make a hashtag trend for several hours (BBC, 2018). In the takedown of Facebook and Instagram accounts, it was reported that USD $108,000 had been spent on ads (Facebook, 2019). Amplification of pro-Saudi messaging was uncovered in December 2019 by Twitter, which suspended 88,000 accounts for violating Twitter's platform manipulation rules. These accounts were linked to the Saudi-based social media marketing firm Smaat, which works for high-profile individuals and several government departments in Saudi Arabia (France-Presse, 2019).

Table 3: Cyber Troop Capacity in Saudi Arabia

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
	$108,000 in Facebook and Instagram Ads			

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

References

Abdulaziz, O. (2019, November 14). Opinion | Saudi spies hacked my phone and tried to stop my activism. I won't stop fighting. *Washington Post*. https://www.washingtonpost.com/opinions/2019/11/14/saudi-spies-hacked-my-phone-tried-stop-my-activism-i-wont-stop-fighting/

Applebaum, A. (2018, October 17). Opinion | Saudi Arabia's information war to bury news of Jamal Khashoggi. *Washington Post*. https://www.washingtonpost.com/opinions/global-opinions/saudi-arabias-information-war-to-bury-news-of-jamal-khashoggi/2018/10/17/e4825a5a-d227-11e8-b2d2-f397227b43f0_story.html

BBC. (2018, March 2). How much to fake a Twitter trend? About £150. *BBC News*. https://www.bbc.com/news/blogs-trending-43218939

Benner, K., Mazzetti, M., Hubbard, B., & Isaac, M. (2018, November 1). Saudis' Image Makers: A Troll Army and a Twitter Insider. *The New York Times*. https://www.nytimes.com/2018/10/20/us/politics/saudi-image-campaign-twitter.html

Brewster, T. (2020, January 23). 8,500 Tweets And Counting—Saudi Trolls Demand Amazon Boycott After Bezos Hack. *Forbes*.

https://www.forbes.com/sites/thomasbrewster/2020/01/23/8500-tweets-and-counting--saudi-trolls-demand-amazon-boycott-after-bezos-hack/

Chapelle, A. (2018, June 4). Twitter bots, fake news and propaganda in the Qatar crisis. *Al Jazeera*. https://www.aljazeera.com/news/2018/06/twitter-bots-fake-news-propaganda-qatar-crisis-180604134035342.html

Coleman, A., & Bell, C. (2018, October 18). Bot campaign follows Khashoggi disappearance. *BBC News*. https://www.bbc.com/news/blogs-trending-45901584

Collins, B., & Wodinsky, S. (2018, October 18). Twitter pulls down bot network that pushed pro-Saudi talking points about disappeared journalist. *NBC News*. https://www.nbcnews.com/tech/tech-news/exclusive-twitter-pulls-down-bot-network-pushing-pro-saudi-talking-n921871

el-Baghdadi, I. (2019, September 29). Opinion | Saudi Arabia is suffocating the Arabic public sphere. We must fight back. *Washington Post*. https://www.washingtonpost.com/opinions/2019/09/30/saudi-arabia-is-suffocating-arabic-public-sphere-we-must-fight-back/

Facebook. (2019, August 1). *Removing Coordinated Inauthentic Behavior in UAE, Egypt and Saudi Arabia* [Facebook]. https://about.fb.com/news/2019/08/cib-uae-egypt-saudi-arabia/

France-Presse, A. (2019, December 20). Twitter blocks accounts linked to Saudi 'state-backed' manipulation effort. *The Guardian*. https://www.theguardian.com/technology/2019/dec/20/twitter-blocks-accounts-saudi-arabia-manipulation-effort

Freedom House. (2019). *Saudi Arabia | Freedom House*. Freedom House. https://freedomhouse.org/country/saudi-arabia/freedom-net/2019

Funke, D. (2018, October 18). Khashoggi misinformation highlights a growing number of fake fact-checkers. *Poynter*. https://www.poynter.org/fact-checking/2018/khashoggi-misinformation-highlights-a-growing-number-of-fake-fact-checkers/

Galloni, A., & Robinson, S. (2018, October 23). How the man behind Khashoggi murder ran the killing via Skype. *Reuters*. https://www.reuters.com/article/us-saudi-khashoggi-adviser-insight-idUSKCN1MW2HA

Groll, E. (2018). *The Kingdom's Hackers and Bots*. https://foreignpolicy.com/2018/10/19/the-kingdoms-hackers-and-bots-saudi-dissident-khashoggi/

Hubbard, B. (2019, November 7). Why Spy on Twitter? For Saudi Arabia, It's the Town Square. *The New York Times*. https://www.nytimes.com/2019/11/07/world/middleeast/saudi-arabia-twitter-arrests.html

Mezzofiore, G., & Burke, S. (2018, October 19). Twitter shuts down bots pushing pro-Saudi message. *CNN*. https://www.cnn.com/2018/10/19/tech/twitter-suspends-spam-khashoggi-accounts-intl/index.html

Nakashima, E., & Bensinger, G. (2019, November 6). Former Twitter employees charged with spying for Saudi Arabia by digging into the accounts of kingdom critics. *Washington Post*. https://www.washingtonpost.com/national-security/former-twitter-employees-charged-with-spying-for-saudi-arabia-by-digging-into-the-accounts-of-kingdom-critics/2019/11/06/2e9593da-00a0-11ea-8bab-0fc209e065a8_story.html

Oueiss, G. (2020, July 8). Opinion | I'm a female journalist in the Middle East. I won't be silenced by online attacks. *Washington Post*. https://www.washingtonpost.com/opinions/2020/07/08/im-female-journalist-middle-east-i-wont-be-silenced-by-online-attacks/

Owen Jones, M. (2018, January 14). *Automated sectarianism and pro-Saudi propaganda on Twitter | Exposing the Invisible*. http://exposingtheinvisible.org/resources/automated-sectarianism

Owen Jones, M. (2019, February 25). Saudi trolls hijacking dead people's Twitter accounts to amplify Riyadh Propaganda. *Al Araby*. https://english.alaraby.co.uk/english/indepth/2019/2/25/saudi-trolls-hacking-dead-peoples-twitter-to-spread-propaganda

Owen Jones, M. (2020, January 20). Saudi Arabia's bot army flourishes as Twitter fails to tame the beast. *Middle East Eye*. http://www.middleeasteye.net/opinion/despite-twitter-culls-riyadhs-disinformation-network-still-going-strong

Roberts, M. (2018, October 19). Opinion | Saudi ministers are harassing critics on Twitter. *Washington Post*. https://www.washingtonpost.com/blogs/post-partisan/wp/2018/10/19/saudi-ministers-are-harassing-critics-on-twitter/

Stubbs, J., Paul, K., & Khalid, T. (2018, November 1). Fake news network vs bots: The online war around Khashoggi killing. *Reuters*. https://uk.reuters.com/article/uk-saudi-khashoggi-disinformation-idUKKCN1N63R0

The New Arab. (2018, October 13). *Saud al-Qahtani, MbS' 'media enforcer', in fresh spotlight amid Khashoggi affair*. Alaraby; The New Arab. https://english.alaraby.co.uk/english/indepth/2018/10/13/spotlight-on-mbs-enforcer-saud-al-qahtani-amid-khashoggi-affair

Trew, B. (2018, October 20). Bee stung: Was Jamal Khashoggi the first casualty in a Saudi cyberwar? | The Independent. *Independent*. https://www.independent.co.uk/news/world/middle-east/jamal-khashoggi-saudi-arabia-cyberwar-trolls-bee-army-missing-journalist-turkey-us-a8591051.html

Twitter Safety. (2019a). *Disclosing new data to our archive of information operations*. https://blog.twitter.com/en_us/topics/company/2019/info-ops-disclosure-data-september-2019.html

Twitter Safety. (2019b, December 20). *New disclosures to our archive of state-backed information operations*. https://blog.twitter.com/en_us/topics/company/2019/new-disclosures-to-our-archive-of-state-backed-information-operations.html

Waterson, J. (2019, August 1). Revealed: Johnson ally's firm secretly ran Facebook propaganda network. *The Guardian*. https://www.theguardian.com/politics/2019/aug/01/revealed-johnson-allys-firm-secretly-ran-facebook-propaganda-network

Serbia

Introduction

Despite Serbia's status as a parliamentary democracy, Serbian citizens have experienced a slow but steady erosion of their freedoms ever since the Serbia Progressive Party (SNS) gained power. In 2019 Freedom House has amended the country's status from "free" to "partly free" due to the "deterioration in the conduct of elections, continued attempts by the government and allied media outlets to undermine independent journalists through legal harassment and smear campaigns, and President Aleksandar Vučić's de facto accumulation of executive powers that conflict with his constitutional role" (*Freedom House Report 2019: Serbia*). In line with these observations, most efforts around computational propaganda in Serbia originate or are related to and supporting the SNS and President Vučić.

Press freedoms and the conditions for journalists in the country have continued to decline since Vučić come to power, initially as Prime Minister, in 2014. Before becoming Prime Minister, Vučić was the Minister of Information from 1998 to 2000 and was the main force behind the introduction of legislation intended to fine journalists for criticizing the government, as well as the banning of foreign TV networks (Albert, 2020), (Hajdari, 2019). The undermining of the freedom of information appears to be a trend in the Balkan region more broadly; Croatia and Montenegro have also targeted the freedom of information and reinforced state secrecy. "Right to know" legislation, introduced in several Balkan countries in the mid 2000s, is increasingly being either infringed upon or simply ignored (Pavlovic, 2019).

On June 21st of June this year Serbia held parliamentary elections. The SNS won with 63.5% of the votes (Dragojlo, 2020). Before the elections the Organization for Security and Co-operation in Europe (OSCE) raised concerns that Serbian legislation does not comprehensively cover all the fundamental aspects of the electoral process, recommending changes "pertaining to election administration, campaign regulations and monitoring, media regulations and oversight, dispute resolution and observers [which] have not been addressed". Additionally, the OSCE noted that many oppositional politicians complained about biased media coverage, potential pressure on voters and possible misuse of state resources (Organization for Security and Co-operation in Europe, 2019). The election was overshadowed by large protests by Serbians, who claimed that the election was being run in an unfair manner, and accused the government of under-reporting the cases of COVID-19 (Jovanovic, 2020).

An Overview of Cyber Troop Activity in Serbia

Organizational Form

According to a report by Deutsche Welle from 2017, the SNS has recruited a team of trolls with contingents in every town. Working under a veil of secrecy, cyber troops were hired as civil servants (with a monthly salary of EUR €370, according to a Deutsche Welle informant) (Rujevic, 2017).

Additionally, governmental control, and thus control by the SNS, over social media and other news media is tight. The country generally has an underdeveloped media landscape with fairly little unbiased and accurate news coverage. Most outlets simply copy and paste government statements, and reports by Kremlin-backed media such as Sputnik are widely quoted by Serbian mainstream media. Moreover, a network of online influencers and other anonymous and semi-anonymous outlets share Sputnik content, giving the outlet a broad reach (Stefano & Nardelli, 2018). However, whether these influencers and outlets are connected to either the Serbian or Russian government, or both, remains hard to evidence.

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Serbia

Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
	SNS, Ivica Dacic (former PM), Vučić (current president)			Civil servants Influencers

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Generally, state-sponsored or party-owned tabloids are responsible for spreading right-wing discourses in Serbia that promote hate and violence. Most domestic news stories are black and white, either praising Russia and condemn the West, or stories that are more pro-West but have virtually no explicit links to Serbian issues (Stefano & Nardelli, 2018). Moreover, the 2019 Freedom House report on Serbia cited above observed that opposition parties are increasingly being discredited and attacked by state-owned and sponsored media, which is significantly decreasing their means of gaining support (Dragojlo, 2020), (Amnesty International, 2018).

In recent years Serbia has also been developing its bilateral relations with China. The recent COVID-19 outbreak has been used by both countries to develop these relations. Former prime minister Ivica Dacic said that the representation of the virus in the West was "part of a special war against China" (Djurdevic & Heil, 2020). At the same time, China has been providing support to Serbia to fight the pandemic while also increasing their influence in the country. For example, China's ambassador to Serbia, Chen Bo, opened a Twitter account on the 20th of March to report on Chinese efforts in supporting Serbia as well as the apparent mutual love and support between Chinese and Serbian citizens (figure 1) (Albert, 2020). Meanwhile, Vučić has attacked the European Union on several occasions for not providing support to Serbia, labelling notions of European solidarity a fairytale, even though the EU has been supporting the medical infrastructure in Serbia for the past two decades and is including the country in European COVID-19 relief efforts (Ruge & Oertel, 2020).

Some reporters have even claimed that Serbia's attack on the EU and appreciation of Chinese help against the virus as a "much-needed propaganda boost for Beijing", and "an opportunity to start reframing its [China's] role from that of the country that accelerated the virus's spread through cover-ups, to that of the magnanimous global power offering leadership at a time of panic" (Lockett & Kynge, 2020). As such, Serbia, whether knowingly or not, seems to be involved in both China's foreign and domestic influence operations portraying China as a 'savior' in the Corona Crisis.

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Serbia

Account Types	Messaging and Valence	Communication Strategies	Platforms
Human Fake/Stolen accounts	Pro-government Attack on opposition/EU	Disinformation Trolls	Twitter

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

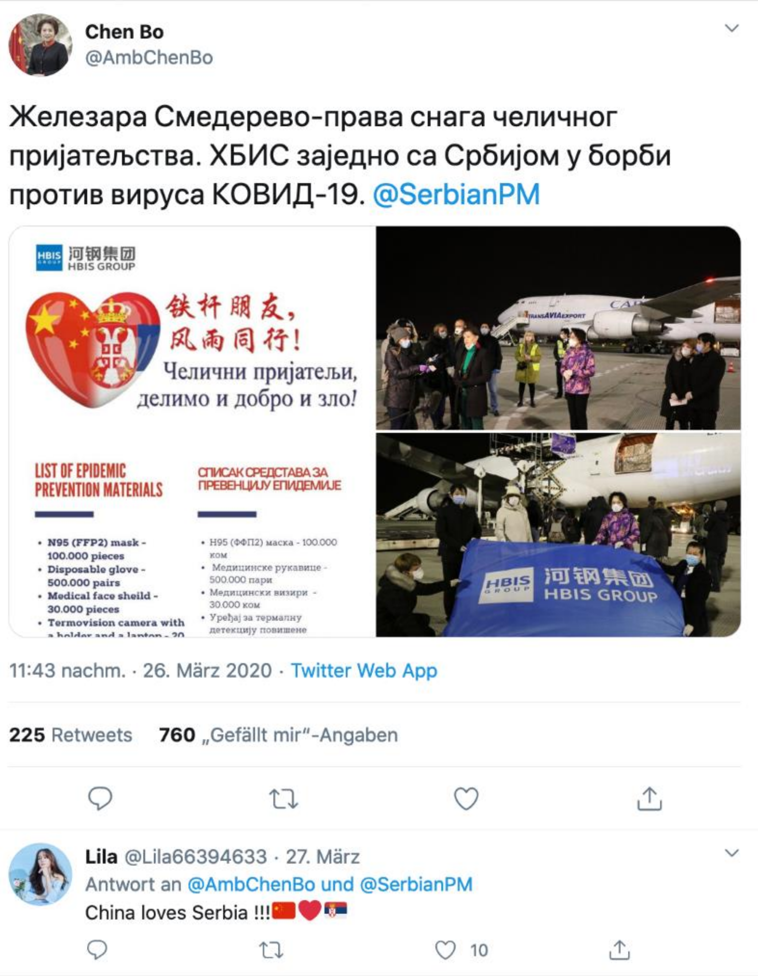
Organizational Capacity and Resources

The trolling team hired by the SNS reportedly consists of roughly 100 individuals who manage thousands of identities that comment on online news articles. In so doing they work to stifle opposition campaigns by either linking them to Western operatives or praising the Serbian government (Rujevic, 2017). However, there are no more recent updates on the trolling teams as the government and SNS continue to spread their propaganda through human-operated channels.

Table 3: Cyber Troop Capacity in Serbia

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
100	Monthly salary for each team member is about $408	Permanent	Coordinated by the SNS/government, level of coordination hard to determine	

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.



Chen Bo
@AmbChenBo

Железара Смедерево-права снага челичног пријатељства. ХБИС заједно са Србијом у борби против вируса КОВИД-19. @SerbianPM

HBIS 河钢集团 HBIS GROUP
铁杆朋友，
风雨同行！
Челични пријатељи,
делимо и добро и зло!
LIST OF EPIDEMIC PREVENTION MATERIALS
• N95 (FFP2) mask - 100.000 pieces
• Disposable glove - 500.000 pairs
• Medical face sheild - 30.000 pieces
• Termovision camera with
СПИСАК СРЕДСТАВА ЗА ПРЕВЕНЦИЈУ ЕПИДЕМИЈЕ
• Н95 (ФФП2) маска - 100.000 ком
• Медицинске рукавице - 500.000 пари
• Медицински визири - 30.000 ком
• Уређај за термалну детекцију повишене
HBIS 河钢集团 HBIS GROUP

11:43 nachm. · 26. März 2020 · Twitter Web App

225 Retweets 760 „Gefällt mir"-Angaben

Lila @Lila66394633 · 27. März
Antwort an @AmbChenBo und @SerbianPM
China loves Serbia !!!🇨🇳❤️🇷🇸

10

Figure 1: China's ambassador to Serbia reporting on the support China is providing to Serbia during the COVID-19 crisis (***source:*** *https://twitter.com/AmbChenBo/status/1243307674944647170*, ***note:*** *the account @Lila66394633 seems to be fake based on its activity*)

References

Albert, E. (2020, March 27). How a Pandemic Drew China and Serbia Closer. *The Diplomat*. https://thediplomat.com/2020/03/how-a-pandemic-drew-china-and-serbia-closer/

Amnesty International. (2018). *Serbia 2017/2018*. Amnesty International. https://www.amnesty.org/en/countries/europe-and-central-asia/serbia/report-serbia/

Djurdevic, M., & Heil, A. (2020, March 5). No Joke! Serbian President Makes Light Of Coronavirus As One More Reason To Hit The Bottle. *RadioFreeEurope/RadioLiberty*. https://www.rferl.org/a/serbian-president-makes-light-of-coronavirus-as-one-more-reason-to-hit-the-bottle/30468925.html

Dragojlo, S. (2020, June 21). Serbia President's Party Scores Landslide in Election Boycotted by Opposition. *Balkan Insight*. https://balkaninsight.com/2020/06/21/serbia-presidents-party-scores-landslide-in-election-boycotted-by-opposition/

Freedom House Report 2019: Serbia. (2019). Freedom House. https://freedomhouse.org/country/serbia/freedom-world/2019

Hajdari, U. (2019, January 2). Serbian Journalists Are Under Attack. Does the International Community Care? *The New Republic*. https://newrepublic.com/article/153011/stop-ignoring-happening-serbia

Jovanovic, N. (2020, June 22). Serbia Under-Reported COVID-19 Deaths and Infections, Data Shows. *Balkan Insight*. https://balkaninsight.com/2020/06/22/serbia-under-reported-covid-19-deaths-and-infections-data-shows/

Lockett, H., & Kynge, J. (2020, March 24). From cover-up to global donor: China's soft power play. *Financial Times*. https://www.ft.com/content/efdec278-6d01-11ea-9bca-bf503995cd6f

Pavlovic, D. (2019, May 2). Right to Know: A Beginner's Guide to State Secrecy. *Balkan Insight*. https://balkaninsight.com/2019/03/05/right-to-know-a-beginners-guide-to-state-secrecy/

Ruge, M., & Oertel, J. (2020). *Serbia's coronavirus diplomacy unmasked*. European Council on Foreign Relations. https://www.ecfr.eu/article/commentary_serbias_coronavirus_diplomacy_unmasked

Rujevic, N. (2017, January 5). Serbian government trolls in the battle for the internet. *Deutsche Welle*. https://www.dw.com/en/serbian-government-trolls-in-the-battle-for-the-internet/a-37026533

Serbia, Parliamentary Elections 2020: Needs Assessment Mission Report. (2019). Organization for Security and Co-operation in Europe. https://www.osce.org/odihr/elections/serbia/442735

Serbia protests: President Vucic the target of Belgrade rally. (2019, March 17). *BBC*. https://www.bbc.co.uk/news/world-europe-47602362

Stefano, M. D., & Nardelli, A. (2018, November 24). The BBC Is Fighting Against Russian Disinformation With A News Service In Serbia. *BuzzFeed*. https://www.buzzfeed.com/albertonardelli/bbc-serbian-russian-disinformation-fake-news-battle

SOUTH AFRICA

Introduction

Generally, South Africa is considered a free country with a free online space which has established itself as a platform for political mobilisation and debate[1]. Internet penetration is spreading quickly across the country, though high costs and disparities between urban and rural in terms of access remain an issue[2]. In May 2019 the country held a general election, which the ruling party African National Congress (NAC) won, though they lost votes compared to previous elections[3]. During the campaign time self-censorship, online harassment and online manipulation were increasing, leading to a decrease in internet freedom according to the Freedom House's *Freedom on the Net* report.

The South African government is generally not involved in controlling access or censoring content online. The 5 major undersea cables connecting the country to international internet are all operated by private companies[4]. In recent years, however, several governmental officials have pronounced an intention to regulate social media, on the pretext that it is increasingly used to spread false information. There are two major bills which could affect governmental censorship and surveillance rights. The first is the Film and Publications Amendment Bill, which was ratified on October 2, 2019[5]. The bill is supposed to protect children from adult content, but it could be abused to censor content online by, for example, regulating content uploaded on platforms such as YouTube and blocking websites[6]. The second is the Cybercrimes and Cyber Security Bill, which spiked controversy as critics pointed out how it would empower the state's ability to surveille citizens. After several revisions which included the omission of questionable sections, the bill passed in 2018[7].

In relation to the COVID-19 pandemic, South Africa has become significant in two very distinct ways. On the one hand, research by the Atlantic Council's DFRLab found a set of Facebook pages and profiles created by a South African marketing company that spread conspiracies around the virus internationally, primarily to sell face masks[8]. At the same time the country was praised for its COVID-19 reporting and fight against fake news, making South Africa rank second in the world for the most reliable news on the pandemic[9].

An Overview of Cyber Troop Activity in South Africa

Organizational Form

One of the biggest examples of an online influence operation in South Africa was paid for by the Gupta brothers, who had quite the political influence under ex-president Zuma (he resigned in 2018). To distract from their power, they reportedly paid several PR and marketing companies, including Bell Pottinger, to stir public attention towards other topics. Their campaign allegedly ran from 2013 to 2017[10]. Whether there was any governmental or presidential support or knowledge of these operations remains unclear.

There are, however, other examples of the government trying to control narratives directly, most prominently through the state-owned broadcaster SABC[11]. Several board members of the company are part of the governing ANC. According to some critical writers this entanglement has led to the downfall of the broadcaster, calling their program ANC propaganda[12]. Past elections also saw the use of online influencers and seemingly neutral websites pushing ANC narratives[13]. It appears that the latest general election in May 2019 was accompanied by opposing parties, mainly the Economic Freedom Fighters (EFF) and ANC, heavily engaging in fighting each other's narratives in digital space as well[14]. Moreover, there were accusations made towards Russia for attempting to influence the vote, though the Russian embassy to South Africa quickly denied the allegations[15]. Nevertheless, articles reporting on the accusation were quick to point out that the ruling ANC has had good relations with Moscow for decades[16].

Self-censorship appears to have primarily increased during the election due to the EFF leading several well-orchestrated attacks against journalists online to deter them from criticising the party[17]. In spite of these activities many journalists and ordinary citizens continued reporting on and discussing politically sensitive issues.

Table 1: Organizational Form and Prevalence of Social Media Manipulation in South Africa

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
	State-owned broadcaster SABC	ANC EFF	Weak Evidence Found		Paid influencers

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

From what is known, the Gupta brothers paid companies to harass critical journalists and push other stories online to distract primarily through sockpuppet and automated accounts on Twitter, many of which appear to have originated from India[18]. Investigations of the bots and sockpuppet accounts found that for the most part they were not successful, but rather ridiculed and dubbed as 'Guptabots'. Their detection was also made easy because they only tweeted in English and used a style foreign to most South Africans[19].

The strategies employed by the EFF to intimidate journalists ranged from old-fashioned phone calls to cyberbullying predominantly through Twitter[20]. In general, manipulation of online space through political actors seems to be an increasing issue in South Africa. The country has seen a rise in fake social media profiles and bots[21]. While the ruling ANC also occasionally make use of the SABC, as mentioned earlier, local newspapers have observed "an army of trolls" working for the EFF leading up to the election in May 2019 to attack and "not leave the enemy to chance". Around the same time the ANC had opened a 'social media attack room'[22]. It appears these two parties were the most engaged in cyber troop activity.

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in South Africa

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Human Bots Hacked/stolen (fake) accounts	Attack Opposition Support Distraction Suppression (intimidation)	Disinformation Trolling Amplification	Twitter, Facebook

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

Generally, cyber troop activity seems sporadic and focused on election seasons. However, when these come around, the governing party is willing to spend quite some money. During

2016 local elections the ANC allegedly spent $2.75 million on a “black ops room” or “war room” to run misinformation campaigns against their opponents, with SABC being one of the main channels to reach millions of rural voters[23]. Reportedly, the room never went into full operations due to mismanagement and lack of funding and the ANC has tried its best to not be directly connected to it.

With regards to the cyber troop activities of the EFF and ANC during election season last year, there is little to no information about the amount of resources spent on them.

Table 3: Cyber Troop Capacity in South Africa

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
	$2,750,000	Temporary	Coordinated within parties (not across government)	

Source: Authors’ evaluations based on data collected. Blank spaces indicate no evidence was found.

References

ANCIR. (2017, September 4). The Guptas, Bell Pottinger and the fake news propaganda machine. *TimesLIVE*. https://www.timeslive.co.za/news/south-africa/2017-09-04-the-guptas-bell-pottinger-and-the-fake-news-propaganda-machine/

Bateman, C. (2017, November 21). Flooding viewers with ANC propaganda: SABC then and now - Ed Herbst. *BizNews.Com*. https://www.biznews.com/thought-leaders/2017/11/21/flooding-viewers-anc-propaganda-sabc

Burke, J., & Harding, L. (2019, May 8). Documents suggest Russian plan to sway South Africa election. *The Guardian*. http://www.theguardian.com/world/2019/may/08/documents-suggest-russian-plan-to-sway-south-africa-election

BusinessTech.co.za. (2019a, February 14). *South African ISPs and networks will have to report you for piracy under new law*. https://businesstech.co.za/news/technology/299646/south-african-isps-and-networks-will-have-to-report-you-for-piracy-under-new-law/

BusinessTech.co.za. (2019b, May 11). South African national election 2019 final results. *Business Tech*. https://businesstech.co.za/news/government/316134/south-african-national-election-2019-final-results/

BusinessTech.co.za. (2019c, November 7). How South Africa’s new controversial ‘internet censorship’ laws will impact you. *Business Tech*. https://businesstech.co.za/news/internet/351857/how-south-africas-new-controversial-internet-censorship-laws-will-impact-you/

BusinessTech.co.za. (2020, April 15). New ‘high-tech’ government tool will take down fake news in South Africa. *Business Tech*. https://businesstech.co.za/news/it-services/389903/new-high-tech-government-tool-will-take-down-fake-news-in-south-africa/

Comrie, S. (2017, January 24). EXCLUSIVE: The ANC’s R50m election “black ops.” *News24*. https://www.news24.com/SouthAfrica/News/exclusive-the-ancs-r50m-election-black-ops-20170124

COVID19 Infodemics Observatory. (2020, May 8). http://covid19obs.fbk.eu

Crymble, L. (2020, April 14). South Africa ranks 2nd as country with most reliable Covid-19 news. *BizCommunity*. https://www.bizcommunity.com/Article/196/15/202731.html

Daily Maverick. (2019, May 17). LETTER TO THE EDITOR: Report implicating Russia in bid to influence elections 'nothing more than clickbait.' *Daily Maverick*. https://www.dailymaverick.co.za/article/2019-05-17-report-implicating-russia-in-bid-to-influence-elections-nothing-more-than-clickbait/

Fraser, A. (2017, September 5). TechCentral: We go inside the Guptabot fake news network. *Daily Maverick*. https://www.dailymaverick.co.za/article/2017-09-05-techcentral-we-go-inside-the-guptabot-fake-news-network/

Freedom House. (2019). *Freedom on the Net | South Africa*. Freedom House. https://freedomhouse.org/country/south-africa/freedom-net/2019

Haffajee, F. (2019a, March 7). EFF's Republic of Impunity (Part Three): EFF leads the information war with its cyber army. *Daily Maverick*. https://www.dailymaverick.co.za/article/2019-03-07-eff-leads-the-information-war-with-its-cyber-army/

Haffajee, F. (2019b, March 7). The EFF's Republic of Impunity (Part One): An army of trolls marches on in mindless violence – and nobody is stopping them. *Daily Maverick*. https://www.dailymaverick.co.za/article/2019-03-07-an-army-of-trolls-marches-on-in-mindless-violence-and-nobody-is-stopping-them/

IOL. (2020, April 15). Government steps up campaign against fake news with hi-tech solution. *IOL*. https://www.iol.co.za/news/south-africa/government-steps-up-campaign-against-fake-news-with-hi-tech-solution-46747740

Kekana, M. (2019, June 13). New app developed to detect Twitter bots—In any language. *The Mail & Guardian*. https://mg.co.za/article/2019-06-13-new-app-developed-to-detect-twitter-bots-in-any-language/

le Roux, J. (2018, November 2). The history of WMC | News24. *News24*. https://www.news24.com/Analysis/the-history-of-wmc-20181101

le Roux, J., & Knight, T. (2020). *South Africa-based Facebook groups stoked coronavirus fears to sell face masks*. https://medium.com/dfrlab/south-africa-based-facebook-groups-stoked-coronavirus-fears-to-sell-face-masks-11212f9846cb

McKaiser, E. (2019, March 7). What the EFF, Malema? What about democracy? *The Mail & Guardian*. https://mg.co.za/article/2019-03-07-what-the-eff-malema-what-about-democracy/

Parliament has passed the 'internet censorship' bill – here's what it means for you. (2018, August 3). https://businesstech.co.za/news/media/229911/parliament-has-passed-the-internet-censorship-bill-heres-what-it-means-for-you/

Plaut, M. (2019, February 3). Elections 2019: How South Africa will track fake news and bots. *The South African*. https://www.thesouthafrican.com/elections-2019-how-south-africa-will-track-fake-news-and-bots/

Ryklief, S. (2020, April 17). South Africa ranks second in the world for reliable Covid-19 news. *IOL*. https://www.iol.co.za/news/south-africa/south-africa-ranks-second-in-the-world-for-reliable-covid-19-news-46850429

Wentzel, W. (2019, November 11). Get ready for the Films and Publications Amendment Act. *Screen Africa*. https://www.screenafrica.com/2019/11/11/uncategorized/get-ready-for-the-films-and-publications-amendment-act/

South Korea

Introduction

South Korea is a country with a robust democracy and with political pluralism that mainly covers conservative and liberal views. Personal freedoms are largely respected, and the media landscape of the country is relatively diverse. However, internet freedom, freedom of expression and political corruption remain issues: pro-North Korean activities or expressions of support are legally banned and the state still struggles with the aftermath of former President Park Geun-hye's corruption scandal, leading to her impeachment in 2016 (*Freedom House | South Korea*, 2017; *Freedom House | South Korea*, 2020). In early 2017 South Korea's Constitutional Court formally removed President Park from power and an ensuing snap election in May 2017 brought Moon Jae-in of the liberal Minjoo Party into office (*Freedom House | South Korea*, 2018).

Corruption cases between major South Korean companies such as Samsung and high-ranking government officials continue in the aftermath of Park's presidency. Meanwhile the new administration has renewed a campaign against 'fake news', a campaign that some have suggested has been used to pressure journalists that are critical of the government, and new online tracking and filtering systems are being used that provide for more closely monitoring the activities of citizens (Choe, 2018; Freedom House | South Korea, 2020; Freedom on the Net | South Korea, 2019).

An Overview of Cyber Troop Activity in South Korea

Organizational Form

Generally, cyber troop activity that works to spread particular political narratives originates from either governmental agencies which influence public opinion on the state and administration as a whole, from politicians and parties, and from hired third parties such as bloggers. Given the rushed nature of the last election in South Korea, happening less than two months after Park's impeachment, there was little time to develop election campaigns utilising cyber troop techniques and tools. Nonetheless, previous elections have seen a range of cyber troop activities. Notably, Park had been accused of utilising intelligence and military services to aid her election victory in 2012. Park repeatedly denied these accusations (Choe, 2013a; *Freedom on the Net | South Korea*, 2019; Harlan, 2013), but in 2017 the High Court sentenced the former director of South Korea's National Intelligence Service (NIS) to four years in prison for domestic political interference campaigns committed between 2009 and 2013 (Choe, 2013b). The new administration has since vowed to reform the NIS so that it focuses its activities on intelligence collection and analysis in relation to foreign affairs and North Korea, stepping away from domestic political events (M. Yoon, 2017).

In South Korea there are two regulatory/oversight bodies when it comes to broadcasting and telecommunication: the KCC (Korea Communications Commission) and the KCSC (Korea Communications Standards Commission). Both ultimately answer to the president and are the government's main agencies through which online content is regulated. At present, observers express concern that the current Korean government may try to limit the freedom of expression online with their declared war on 'Fake News' (Choe, 2018; Freedom on the Net | South Korea, 2019).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in South Korea

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
	x	x			x

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

South Korea has one of the fastest internet networks in the world, and in general the government does not restrict connectivity or access. Rather, the government focuses on censoring online content. The KCSC is responsible for monitoring and evaluating online content to determine whether or not to censor and it also assesses applications for censorship from other agencies and individuals. While the KCSC does not publish lists of blocked websites, they do report the number of pages which cannot be accessed: the latest available report from 2018 lists a total of 187,980 websites that were blocked and 41,000 websites that were deleted (*2018 Internet Communications Content Review Status Report*, 2019). In February 2019 the KCSC introduced a new filtering tool which allows them to block what they deem to be illegal content from HTTPS sites (Netizen Report Team, 2019). Several laws provide a broad administrative framework enabling these content restriction activities. Additionally, these laws and corresponding fines have motivated journalists and activists to self-censor to avoid the quite common charge of defamation (*Freedom on the Net | South Korea*, 2019).

According to the investigations into the NIS's interventions on domestic political opinion, the agency operated up to 30 "extra-departmental teams", teams which often include internet-savvy civilians. Days before the 2012 presidential election, agents of the NIS's anti-North Korea psychological warfare team flooded the internet with comments that were generally supportive of Park's bid for the presidency and accusing the then main opposition candidate Moon of being pro-North Korean (M. Yoon, 2017). It appears that the psychological warfare team have produced more than 5,000 posts online in their campaign against North Korea since 2009 and that they built upon this established campaign to attack opposition parties and their candidates ahead of the 2012 election.

Additionally, other teams of the NIS published over 1,700 posts that directly address South Korean domestic politics, attacking labour activists, opposition politicians and other critics as 'Leftist followers of North Korea'. The agency has authorised the posting of about 1.2 million tweets (Choe, 2013a; *Freedom on the Net | South Korea*, 2019). Furthermore, former Defence Minister Kim Kwan-jin also utilised the Ministry's Cyber Command Unit to launch a smear campaign against Park's opposition. Kim mobilised all members of the unit from March 12 to April 11, 2012. The unit ran its own internet news outlet called Point News from 2012 to 2015. 470 members of the unit also created online accounts to attack liberal politicians (Ser, 2017). Furthermore, Moon's 2017 campaign was not without cyber troop activity. A governor by the name of Kim Kyoung-soo has been convicted of manipulating the order of online comments under 80,000 news articles with the help of online bloggers. Kim allegedly also utilised automated software that could amplify content online and produced over 99.7 million "likes" and "dislikes" (Lee, 2019).

Nonetheless, the effectiveness of these campaigns and other disinformation remains unclear, and increasing public awareness is starting to limit domestic political influencing attempts (Corcoran et al., 2019).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in South Korea

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Human Bots	Support Attack Opposition Distracting Driving Divisions	Disinformation Data-driven Strategies Trolls Amplifying Content	Twitter Local Platforms News articles (comment section)

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

While there is not a great amount of detail known about the current resources available to cyber troop activity and influence campaigns in South Korea, some data does exist. For example, the Cyber Command of the Ministry of Defense used a budget of about 342 million won (USD $314,570) to run their internet news outlet Point News (Ser, 2017). The investigation following the impeachment of former President Park also found that both Park's administration as well as that of the previous President, Lee Myung-bak, were involved in persistent online opinion manipulation activities outside of election cycles. For instance, activities included 'blacklisting' critical artists and writers which were defunded and often subject to systematic online harassment (Al Jazeera, 2017; S. Yoon, 2017). Whether current President Moon's administration maintains any form of cyber troop activity to influence domestic opinion is unclear, though the accusations around Moon's 2017 campaign would indicate that his team does not shy away from such activity.

In relation to South Korea's psychological warfare operation against the North, reports suggest that during the Park administration the NIS maintained at least 658 Twitter identities and nine dedicated cyber troops (Benedictus, 2016). Most of these attacks and influence campaigns remain domestic: given the low internet penetration rate of North Korea, cyber troop activities against the North make little sense. Rather, more traditional methods such as sending leaflets on balloons over the border to the North are employed, and these remain largely undertaken by activists (Choe, 2020).

The South Korean government has been running an anti-North Korean propaganda broadcast for decades, through radio, loudspeakers, billboards and leaflets sent towards the North. The practice was stopped in 2004 to reduce tension, but after two South Korean soldiers patrolling the border stepped on North Korean mines in 2015, South Korea started recommenced these activities (LA Times, 2015; A. I. Park, 2015). In 2018, South Korea stopped once again after the North and South Korean summit, but in June 2020 North Korea closed down all communication with the South and subsequently blew up the Korean liaison office built on Northern territory with Southern money (BBC News, 2020). The North re-installed loudspeakers at the border, before suspending their military (and loudspeaker) plans again (Berlinger & Kwon, 2020; J. Park, 2020). To date, the South Korean response has been cautious with no specific counter-steps being announced (Kim, 2020).

Table 3: Cyber Troop Capacity in South Korea

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
		Permanent	Coordinated	

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

References

2018 Internet Communications Content Review Status Report (p. 6). (2019). Korea Communications Standards Commission. http://www.kocsc.or.kr/eng/cop/bbs/selectBoardArticle.do#LINK

Al Jazeera. (2017, January 21). South Korea: Minister arrested over "artist blacklist." *Al Jazeera*. https://www.aljazeera.com/news/2017/01/south-korea-minister-arrested-artist-blacklist-170121043536391.html

BBC News. (2020, June 16). N Korea blows up joint liaison office with South. *BBC News*. https://www.bbc.com/news/world-asia-53060620

Benedictus, L. (2016, November 6). Invasion of the troll armies: 'Social media where the war goes on.' *The Guardian*. https://www.theguardian.com/media/2016/nov/06/troll-armies-social-media-trump-russian

Berlinger, J., & Kwon, J. (2020, June 10). North Korea isn't talking to the South anymore. Experts say it could be trying to manufacture a crisis. *CNN*. https://www.cnn.com/2020/06/09/asia/north-korea-south-korea-communications-intl-hnk/index.html

Choe, S.-H. (2013a, June 14). South Korean Intelligence Agents Accused of Tarring Opposition Online Before Election. *The New York Times*. https://www.nytimes.com/2013/06/15/world/asia/south-korean-agents-accused-of-tarring-opposition-before-election.html

Choe, S.-H. (2013b, November 21). Prosecutors Detail Attempt to Sway South Korean Election. *The New York Times*. https://www.nytimes.com/2013/11/22/world/asia/prosecutors-detail-bid-to-sway-south-korean-election.html

Choe, S.-H. (2018, October 2). South Korea Declares War on 'Fake News,' Worrying Government Critics. *The New York Times*. https://www.nytimes.com/2018/10/02/world/asia/south-korea-fake-news.html

Choe, S.-H. (2020, June 11). As Floating Propaganda Irks North Korea, the South Isn't Happy Either. *The New York Times*. https://www.nytimes.com/2020/06/11/world/asia/north-korea-balloons-propaganda.html

Corcoran, C., Crowley, B. J., & Davis, R. (2019). *Disiinformatiioin Threat Watch: The Disinformation Landscape iin East Asiia nd Implications for US Policy* [Student Report]. Belfer Center for Science and International Affairs. https://www.belfercenter.org/sites/default/files/2019-06/PAE/DisinfoWatch%20-%202.pdf

Freedom House | South Korea. (2017). Freedom House. https://freedomhouse.org/country/south-korea/freedom-world/2017

Freedom House | South Korea. (2018). Freedom House. https://freedomhouse.org/country/south-korea/freedom-world/2018

Freedom House | South Korea. (2020). Freedom House. https://freedomhouse.org/country/south-korea/freedom-world/2020

Freedom on the Net | South Korea. (2019). Freedom House. https://freedomhouse.org/country/south-korea/freedom-net/2019

Harlan, C. (2013, July 6). In South Korea's latest controversies, spy agency takes a leading role—The Washington Post. *The Washington Post*. https://www.washingtonpost.com/world/asia_pacific/in-south-koreas-latest-controversies-spy-agency-takes-a-leading-role/2013/07/06/8b610c74-e3ca-11e2-aef3-339619eab080_story.html

Kim, B. (2020, June 23). S. Korea Cautious on How to Respond to N. Korea's DMZ Loudspeakers. *KBS World Radio News*. http://world.kbs.co.kr/service/news_view.htm?lang=e&Seq_Code=154342

LA Times. (2015, August 10). South Korea resumes anti-North Korea broadcasts after land mine explosions. *Los Angeles Times*. https://www.latimes.com/world/asia/la-fg-korea-land-mines-broadcast-20150810-story.html

Lee, S. (2019, January 30). Governor Kim Kyoung-soo sentenced to 2 years for online opinion-rigging. *The Korea Times*. http://www.koreatimes.co.kr/www/nation/2020/06/251_262961.html

Netizen Report Team. (2019, February 22). Netizen Report: Both Bangladesh and South Korea are waging a 'war on porn' — and paving the way for political censorship. *Global Voices Advocacy*. https://advox.globalvoices.org/2019/02/22/netizen-report-both-bangladesh-and-south-korea-are-waging-a-war-on-porn-and-paving-the-way-for-political-censorship/

Park, A. I. (2015, October 28). Using PSYOP against North Korea. *Council on Foreign Relations*. https://www.cfr.org/blog/using-psyop-against-north-korea

Park, J. (2020, June 24). N.Korea Suspends "Military Action Plans" Takes Down Loudspeakers. *KBS World Radio News*. http://world.kbs.co.kr/service/news_view.htm?lang=e&Seq_Code=154367

Ser, M. (2017, November 30). Ex-defense head approved smear campaign. *Korea JoongAng Daily*. https://koreajoongangdaily.joins.com/2017/11/30/politics/Exdefense-head-approved-smear-campaign/3041460.html

Yoon, M. (2017, August 3). State spy agency's election smear campaign confirmed via internal probe. *The Korea Herald*. http://www.koreaherald.com/view.php?ud=20170803000834

Yoon, S. (2017, September 29). 10 years later, an internet post haunts actress: Despite a decade and a name change, she says people still ask her, 'aren't you dead yet?' *Korea JoongAng Daily*. https://koreajoongangdaily.joins.com/2017/09/29/etc/10-years-later-an-internet-post-haunts-actress-Despite-a-decade-and-a-name-change-she-says-people-still-ask-her-arent-you-dead-yet/3039063.html

Spain

Introduction

Spain is considered a free and stable democracy. In general the government does not engage in limiting Internet access by blocking or censoring content. The country has a free and independent media, although most outlets, radio and TV stations are part of bigger corporations.

Spain is experiencing a new diversity in its political landscape. Traditionally, the country has consisted of a two-party democracy, however, with the general election of April 2019 this dynamic changed. The general election was called by Prime Minister Pedro Sánchez of the Partido Socialista Obrero Español (PSOE) after right-wing and Catalan separatist parties rejected the 2019 budget proposed by his minority coalition. Observers expected that right-wing parties would profit significantly from the election, and extreme right party Vox did take seats for the first time, but the PSOE received 28.7% of the votes, ahead of the conservative Partido Popular (16.7%) and the liberal Ciudadanos party (15.9%). However, because of the failure of investiture voting and the lack of agreement between parties, new general elections were held on November 2019 which resulted in a governing coalition with Unidas Podemos.
Political parties have been actively using computational propaganda during critical events, mostly to amplify content and disseminate disinformation. According to Gelado-Marcos and Puebla-Martinez (2019), more than half of the Spanish population are vulnerable to disinformation. The results of their study show that vulnerability is greater among certain population segments, such as "the youth and the elderly", people who are economically inactive or unemployed, and people who "spend more than three hours a day consuming contents in the internet" (Gelado-Marcos and Puebla-Martinez, 2019).

An Overview of Cyber Troop Activity in Spain

Organizational Form

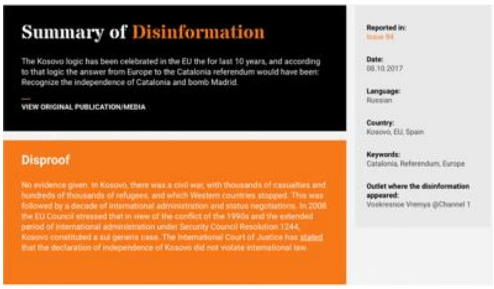
Whilst there is no evidence of the government's involvement in social media manipulation campaigns, political parties have been actively using computational propaganda during critical events, such as the 2017 Catalan independence referendum. For instance, the pro-Catalan independence party, Esquerra Republicana de Catalunya, was linked to inauthentic Twitter accounts behavior (DFRLab, 2019).

General elections play a crucial role in boosting computational propaganda operations. In 2019, Partido Popular used bots to amplify their content on Twitter (Robinson & Sardarizadeh, 2019), Facebook, and Instagram (Gleicher, 2019). Podemos, on the other hand, sent automated mass messages to their supporters via WhatsApp and Facebook to reach its audience (Stone, 2019). In the case of Vox, it frequently uses Instagram to share memes and mock other parties. Lastly, far-right activist Javier Capdevila Grau managed one of the main Facebook groups identified by Avaaz as sharing fake content (Colomé, 2019).

With regards to private contractors, both Illuminati Lab and I3 Ventures were involved in different campaigns. While the former managed an anti-secessionism campaign between 2014 and 2015 (Andrino & Colomé, 2020), the latter is said to be behind the campaign of attacks against soccer players and opponents of FC Barcelona in 2020 (Andrino & Colomé, 2020). Analysis of the first campaign indicates a strong association with Societat Civil Catalana (Catalonian Civil Society), however, its former president denies its involvement.

Finally, it is worth noting that the Spanish central government accused Russia of meddling with the Catalan referendum through their own groups and news outlets, such as Sputnik and RT. In November 2017, the Spanish government announced that their intelligence services were of the opinion that Russian-based groups had used social media to spread misinformation. Russia stated that Spain's accusations were typical of Western Russophobia, while Catalans mocked the central government, stating that they hardly needed to be reminded of their grievances by Russia (Palmer, 2017). Moreover, Spain's Foreign Minister has subsequently stated that there is no concrete evidence that Russia has been involved. Nevertheless, the EU's fact- checking task force found evidence of Russian-backed media spreading disinformation about the Catalan situation (Figure 1). Half of the stories shared by RT a day before the referendum were about police violence, with headlines including "Powerful videos: the brutal police repression against voters in the Catalan Referendum" (Alandete, 2017). In addition, Javier Lesaca, a researcher at Washington State University, analysed more than 5 million social media messages sent from 29 September to 5 October 2017 by Sputnik and RT and found an "entire army of zombie accounts that are perfectly coordinated" (Alandete, 2017). Lesaca too found that part of the networks used were previously employed in Venezuela (Figure 2). The Madrid-based think tank Royal Elcano Institute called these activities part of the Russian information "war" in Catalonia (Palmer, 2017). Other experts, such as Klaus-Jürgen Nagel from the University of Barcelona (Universitat Pompeu Fabra), have said that such a claim is an exaggeration and that Russia simply provides information from their geopolitical perspective (Palmer, 2017).

Figure 1: Example of disinformation by Russia, uncovered by the EU disinformation task force



Summary of Disinformation

The Kosovo logic has been celebrated in the EU the for last 10 years, and according to that logic the answer from Europe to the Catalonia referendum would have been: Recognize the independence of Catalonia and bomb Madrid.

VIEW ORIGINAL PUBLICATION/MEDIA

Disproof

No evidence given. In Kosovo, there was a civil war, with thousands of casualties and hundreds of thousands of refugees, and which Western countries stopped. This was followed by a decade of international administration and status negotiations. In 2008 the EU Council stressed that in view of the conflict of the 1990s and the extended period of international administration under Security Council Resolution 1244, Kosovo constituted a sui generis case. The International Court of Justice has stated that the declaration of independence of Kosovo did not violate international law.

Reported in:
Issue 94

Date:
08.10.2017

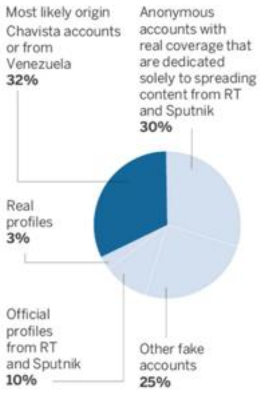
Language:
Russian

Country:
Kosovo, EU, Spain

Keywords:
Catalonia, Referendum, Europe

Outlet where the disinformation appeared:
Voskresnoe Vremya @Channel 1

Source:https://euvsdisinfo.eu/report/the-logical-answer-from-europe-to-the-catalonia-referendum-would-have-been-recognize-the-independence-of-catalonia-and-bomb-madrid/ Figure 2: Types of accounts used to spread misinformation during the Catalan referendum as analysed by Lesaca



Source: https://elpais.com/elpais/2017/11/11/inenglish/1510395422_468026.html

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Spain

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
2014		Evidence found (among them, Esquerra Republicana de Catalunya (ERC), Vox, Podemos, and Partido Popular)	2014-2015: Illuminati Lab 2020: I3 Ventures		Far-right activist Javier Capdevila

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Twelve days before the 2014 Catalan self-determination referendum, campaigns against Catalan self-determination started on Twitter. Automated fake accounts were used to amplify content against the independence movement, and particularly the anti-independence group Societat Civil Catalana. Although the president of the association denied its involvement, the operations were coordinated by the agency Illuminati Lab, a subsidiary of Nicestream, which has operated in other Spanish-speaking countries (Andrino & Colomé, 2020).

The event that the greatest influence on misinformation and disinformation activities was the 2017 Catalan independence referendum. The situation leading up to and following the vote became chaotic with disinformation and fake stories flooding the debate from both sides. The national public broadcaster RTVE was criticized by its own journalists and its news council (overseeing the broadcaster's impartiality) for biased coverage during this period. Additionally, the Spanish judicial authorities issued orders to close websites linked to the organisation of the referendum, something that the courts had ruled as unconstitutional and illegal (2017).

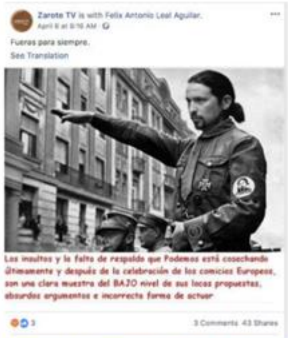
It is most likely that the considerable amounts of fake stories and hate speech circulating during the period was due to the sensitive nature of the subject of the referendum (Erickson, 2017). Fake tweets from politicians were shared as well as stories claiming Spanish tanks had been deployed to Catalonia. The use of WhatsApp was also hugely problematic because fake stories circulated freely in private chats, where it was extremely difficult for fact-checkers to examine and debunk false claims.

In early 2019, the trial of 12 Catalan separatists began in Madrid. The government launched an EU-wide campaign to counter the narrative of the trial as politically-motivated. The Spanish ambassador to London stated that the pro-independence regional government of Catalonia had launched a "massive campaign of disinformation", with "the principal underlying message […] that Spain is not a democracy", and the aim of delegitimizing the trial and the Spanish central government (Wintour, 2019). According to the ambassador, Spain intended to fight back with transparency (they livestreamed the trial for example) and its own campaign called 'This is the real Spain' to advertise the country's diversity in opinion and inclusiveness.

That same year, Spain had two general elections, in April and November. In order to counter disinformation during the electoral campaigns, Maldita.es and First Draft, along with sixteen media outlets launched Comprobado (Gelado-Marcos and Puebla-Martinez, 2019).

However, days before the April elections, Facebook quietly took down three far-right networks for fake and duplicated accounts, which ran about 30 Facebook pages reaching over 1.7 million Spaniards (Graham-Harrison & Jones, 2019). Amongst the content shared were fake stories and doctored pictures of politicians (Figure 3). The Unidad Nacional Española page that was removed had by far the biggest reach, with roughly 700,000 followers. Facebook took action against these networks after the activist group Avaaz uncovered them and presented their evidence to the company on 12 April 2019 (Graham-Harrison & Jones, 2019). Avaaz's campaign director Christoph Schott stated that Facebook had done a great job in acting swiftly to take down the pages. However, Schott also stated that what Avaaz had uncovered was "likely just the tip of the disinformation iceberg". As for the actors behind these networks, Avaaz could only identify one individual, Javier Capdevila Grau, a far-right activist (Colomé, 2019).

Figure 3: Doctored images of Podemos leader doing the Hitler Salute



Zarote TV is with Felix Antonio Leal Aguilar.
April 8 at 8:16 AM

Fueras para siempre.
See Translation

Los insultos y la falta de respaldo que Podemos está cosechando últimamente y después de la celebración de los comicios Europeos, son una clara muestra del BAJO nivel de sus locas propuestas, absurdos argumentos e incorrecta forma de actuar

3

3 Comments 43 Shares

Doctored images of Podemos leader Pablo Iglesias doing the Hitler Salute

Caption:"the insults and the lack of support that Podemos is gaining lately and after the celebration of the European elections, are the clear evidence of the LOW level of their crazy proposals, absurd arguments and wrongful conduct"

Source: https://avaazimages.avaaz.org/SpainSummary.pdf

In another investigation, Avaaz discovered that around 9.6 million registered Spanish WhatsApp users had received hateful memes and disinformation on the platform in relation to the upcoming election (O'Brien, 2019). This figure is apparently higher than the disinformation reach of any other platform, as roughly 89% of Spaniards use WhatsApp (O'Brien, 2019). Most of the content that has been disseminated seems to have originated from right-wing extremist groups. Meanwhile, WhatsApp took action against Podemos, which had been using WhatsApp as a channel to reach tens of thousands of followers to deliver campaign messages. WhatsApp took the channel offline in the week before the election, stating that Podemos was breaking the terms of usage by sending automated mass messages (Stone, 2019). Podemos said that they were indeed doing exactly that but felt singled out as they are not the only party employing the social media platform in that way. As it has been highlighted by journalist Desiree Garcia, disinformation is often initiated in WhatsApp and then disseminated on Twitter (Smith, 2019).

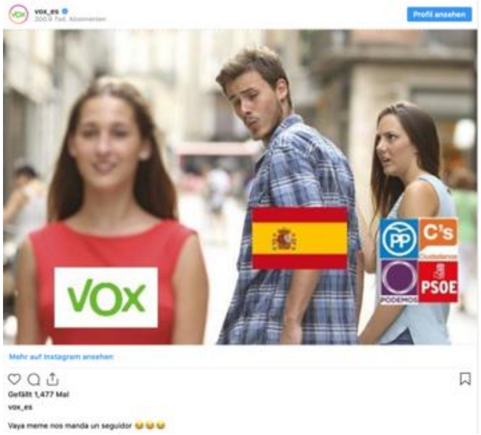
Analyses show that whilst the left wing party Podemos has a larger pool of followers on Twitter, supporters of the right wing Vox party were more involved and engaged at a higher frequency (Smith, 2019). In September 2019, Twitter released information on 256 suspicious accounts that were created in the run-up to the first general election of the year and removed in April. They were linked to the Partido Popular and boosted pro-party content, as well as attacks against opposition parties (Robinson & Sardarizadeh, 2019). It is also worth noting that according to the Institute for Strategic Dialogue, at least around 3,000 Twitter automated accounts originating in Venezuela were used in Venezuela by Venezuelan opposition parties and were also part of a pro-Vox and anti-Islam network (Smith, 2019).

In June 2019, Twitter announced that it had suspended 130 fake accounts which, according to the social media platform, were linked to Esquerra Republicana de Cataluyna and promoted pro-Catalan independence content (Roth, 2019). DFRLab analysed the accounts that were suspended and found that these included accounts that were operated from abroad, and had multiple posts in Spanish, Portuguese, and Russian. The content included references to promoting a pro-independence march and the release of two Catalan pro-independence leaders (DFRLab, 2019)

In September 2019, Facebook removed 65 Facebook accounts and 35 Instagram accounts associated with the Partido Popular. According to the company, these accounts spent $1,275 on ads (Gleicher, 2019). The party was linked to other 259 accounts on Twitter that were removed on the basis that they were manipulative. Specifically, they were fake accounts that amplified specific content.

It is worth noting that, generally, Spanish politicians, parties and the government have learned to utilize the Internet and, in particular, social media platforms. Among the most widely used are Facebook, Instagram, WhatsApp and Twitter (Oelsner, 2019). Most parties use these platforms to advertise their presence and their programmes, and if the party is in power, the government and their policies. The right-wing extremist party Vox is by far the most successful on Instagram, where they regularly share memes and mock other parties (Figure 4), while the left wing party Podemos fares the best on Facebook, with over a million likes. Interestingly, Twitter is less influential in Spain. Podemos has the largest following on the platform.

Figure 4: Example Instagram post by right-wing extremist party Vox



Gefällt 1,477 Mal

vox_es

Vaya meme nos manda un seguidor 😂😂😂

Source: https://www.euronews.com/2019/04/26/weekend-long-read-social-media-use-in-spain-s-election-campaign-the-good-the-bad-and-the-u

In 2020, a campaign against soccer players and opponents of FC Barcelona was uncovered. The agency I3 Ventures, which is related to people behind Illuminati Lab, was uncovered as the private contractor, managing six fake Facebook accounts for EUR €1 million. Whilst it has been evidenced that the company presented a social media analysis report to the club in June 2019, both parties deny the existence of a contract for trolling and cyber-attacks (Plaza, 2020). Lastly, during the first months of the coronavirus crisis in Spain, a network of false Facebook accounts with inauthentic behaviour promoted the government's content. The Spanish Ministry of Health denies it has promoted those activities and the incident is under investigation (Holroyd, 2020).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Spain

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Bots and Human. Fake accounts.	Pro-party Attacks on opposition Driving division	Disinformation Amplification strategies	Twitter, WhatsApp, Instagram, Facebook

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

Organizational capacity is low and, as it has been previously stated, social media manipulation is most often active during crucial events, such as general elections, and around specific topics, such as Catalan independence.

Table 3: Cyber Troop Capacity in Spain

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
		Temporary		Low

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

References

Alandete, D. (2017, November 11). Russian network used Venezuelan accounts to deepen Catalan crisis. *El País*. https://elpais.com/elpais/2017/11/11/inenglish/1510395422_468026.html

Andrino, B., & Colomé, J. P. (2020, February 26). 900 cuentas falsas de la misma empresa que contrató el Barça hicieron campaña contra el secesionismo. *El País*. https://elpais.com/tecnologia/2020/02/25/actualidad/1582654196_700802.html

Colomé, J. P. (2019, April 24). Facebook removes three far-right networks ahead of Spanish election. *EL PAÍS*. https://english.elpais.com/elpais/2019/04/24/inenglish/1556089608_414749.html

DFRLab. (2019, August 9). Catalonia Twitter Takedown: Inorganic Campaign Pushed Pro-Independence Content. *Medium*. https://medium.com/dfrlab/catalonia-twitter-takedown-inorganic-campaign-pushed-pro-independence-content-fe9ee0e44f3c

Equipo Nizkor and Derechos Human Rights (2017, septiembre 13). Auto mandando deshabilitar 2 webs sobre el referéndum catalán e identificar los medios que hayan publicado publicidad institucional sobre la convocatoria del referendum. http://www.derechos.org/nizkor/espana/doc/cat1550.html

Erickson, A. (2017, October 19). How fake news helped shape the Catalonia independence vote. *Washington Post*. https://www.washingtonpost.com/news/worldviews/wp/2017/10/19/how-fake-news-helped-shape-the-catalonia-independence-vote/

Gelado-Marcos, R. & Puebla-Martínez, B. (2019). "Estudio de los factores condicionantes de la desinformación y propuesta de soluciones contra su impacto en función de los grados de vulnerabilidad de los grupos analizados". Research project funded by Facebook and the Fundación Luca de Tena, available at: https://laboratoriodeperiodismo.org/estudio-sobre-la-desinformacion/

Gleicher, N. (2019, September 20). Removing Coordinated Inauthentic Behavior in Spain. *About Facebook*. https://about.fb.com/news/2019/09/removing-coordinated-inauthentic-behavior-in-spain/

Graham-Harrison, E., & Jones, S. (2019, April 25). Facebook takes down far-right groups days before Spanish election. *The Guardian*. https://www.theguardian.com/world/2019/apr/25/facebook-takes-down-far-right-groups-days-before-spanish-election

Holroyd, M. (2020, April 24). Facebook investigates fake accounts sharing Spanish government content. *Euronews*. https://www.euronews.com/2020/04/24/facebook-investigates-fake-accounts-sharing-spanish-government-content-thecube

O'Brien, C. (2019, April 26). Spanish WhatsApp users reportedly flooded with 'disinformation and hate' ahead of elections. *VentureBeat*. https://venturebeat.com/2019/04/26/spanish-whatsapp-users-reportedly-flooded-with-disinformation-and-hate-ahead-of-elections/

Oelsner, N. (2019, April 26). Spain's election and the battle for control of social media. *Euronews*. https://www.euronews.com/2019/04/26/weekend-long-read-social-media-use-in-spain-s-election-campaign-the-good-the-bad-and-the-u

Palmer, E. (2017, November 18). *Did Russian «fake news» stir things up in Catalonia?* https://www.bbc.com/news/world-europe-41981539

Plaza, P. (2020, February 23). *'Barçagate': Así actúan los ejércitos de bots maliciosos*. La Vanguardia. https://www.lavanguardia.com/deportes/20200223/473679658708/i3-ventures-cuentas-falsas-barcelona-bartomeu-bots-redes-sociales-twitter.html

Robinson, O., & Sardarizadeh, S. (2019, September 20). Twitter suspends former MBS adviser and Chinese «fake» accounts – BBC Monitoring. *BBC Monitoring*. https://monitoring.bbc.co.uk/product/c2013o03

Roth, Y. (2019, June 13). Information operations on Twitter: Principles, process, and disclosure. *Twitter*. https://blog.twitter.com/en_us/topics/company/2019/information-ops-on-twitter.html

Smith, R. (2019, May 21). *Venezuelan bots, WhatsApp and disinformation in Spain*. First Draft. https://firstdraftnews.org:443/latest/venezuelan-bots-whatsapp-and-disinformation-in-spain/

Stone, Jon (2019, April 25). *WhatsApp suspends communication channel of Spanish left-wing party Podemos days before election.* https://www.independent.co.uk/news/world/europe/spain-elections-whatsapp-podemos-channel-close-left-ing-de-olmo-a8886481.html

Wintour, P. (2019, February 12). Spain says 'disinformation' surrounds Catalan separatists' trial. *The Guardian*. https://www.theguardian.com/world/2019/feb/12/spain-disinformation-surrounds-catalan-separatists-trial

Sri Lanka

Introduction

After twenty-six years of civil war between Tamil rebels and the government (1983-2009), Sri Lanka is still recovering from the violent conflict (Freedom House, 2019). Although some improvements have been made and the country has moved beyond the turbulent and repressive first years of the aftermath, historical socio-political tensions persist (Hattotuwa, 2018).

Critical speech is condemned, and journalists are being intimidated. Episodes of violence (e.g. clashes between Muslims and Buddhists in Ampara and Kandy in 2018 and bombings on churches and hotels on Easter Sunday 2019) have recently agitated the country. After these episodes, the government pre-emptively blocked social media and instant messaging applications, such as Facebook, WhatsApp, Viber, and Instagram (Freedom House, 2019; Sigal, 2019). Environmental issues have also been used as a means to target racist and extremist speech against Muslims (Hattotuwa, 2019) and, according to CIVICUS (2019), the candidacy and then electoral success of Gotabaya Rajapkasa in 2019, triggered the awakening of racist and Sinhalese ethnonationalists groups.

In January 2020, Amnesty International, the Committee to Protect Journalists, and Reporters Without Borders issued a letter to President Rajapaksa and called for safer and more supportive conditions for journalists. This came as a reaction against the intimidation and harassment to which journalists are subject. As the letter states, moreover, "State and private broadcast and print media are carrying out smear campaigns on journalists critical of the Government, and these are mirrored on their social media channels, where those journalists are further demonized" (Sri Lanka: Joint Letter to President Rajapaksa on the Harassment and Intimidation of Journalists, 2020).

Additionally, both individual users and government officials have been increasingly spreading disinformation (Freedom House, 2019). Although in 2019 a bill that aimed to criminalize "fake news" failed to pass, several arrests have occurred, often targeting people critical to the government. On the other hand, institutions that support the government are not subject to such scrutiny (Chandimal & Fernando, 2020). What is more, on 1 April 2020, the police announced it would arrest people who were disseminating false information or expressing criticism to public officials involved in the COVID-19 response (Gunatilleke, 2020). During the pandemic, the President himself published a statement "condemning the spread of fake news on social media platforms with various false messages claiming to be from him" («Gotabaya Rajapaksa condemns fake news during a crackdown on social media», 2020).

An Overview of Cyber Troop Activity in Sri Lanka

Organizational Form

Facebook and Twitter have been used as mediums for manipulating public opinion since at least 2014 and 2015, respectively (Hattotuwa, 2018). As Hattotuwa et al. (2018) stated, whilst in the early years Facebook was the main media for dissemination of information, Twitter still "escaped scrutiny at the time".

Whilst there is no evidence of state-led cyber troops, the government has recently been involved in blocking social media and instant messaging (e.g. WhatsApp, YouTube, Facebook, Instagram, Viber, Snapchat and Messenger) in attempts to stop hate speech and the dissemination of false information online in the aftermaths of violent incidents, such as in

Kandy in 2018 and the Easter attacks in 2019 (Sigal, 2019; NetBlocks, 2019). It has also engaged in the arrest of people who spread "fake news" in the context of COVID-19. However, there are also incidents of the state-owned media outlet Sunday Observer, the President of the Public Health Inspectors association, a candidate for Parliament, and other politicians disseminating disinformation without further consequences (Chandimal & Fernando, 2020).

On the other hand, in late 2017 several accounts trolled Groundviews on Twitter. Analysis of the incident indicated that these fake accounts, which were created "on some sort of quota system" were promoting and amplifying content of Namal Rajapaksa—a member of Parliament, son of the former President and nephew of the current President (Hattotuwa & Wijeratne, 2018).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Sri Lanka

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
		Evidence found			

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

By the run-up to the general elections of 2015, disinformation and misinformation, with pro-party and polarizing content, was disseminated over Facebook (Hattotuwa & Wijeratne, 2018). Recent violent incidents have been accompanied by the spread of disinformation. During violence in Ampara and Kandy in March 2018, for instance, several fake Twitter accounts were identified to be amplifying the reach of anti-Muslim narratives that promoted false or misleading content (Hattotuwa et al., 2018)

Similarly, after the bombings claimed by the Islamic State on Easter 2019, content targeting Muslims and rumours were widely spread. These included rumours about poisoned water supply in Hunupitiya and the criminalization of VPN usage, among others. One of the Facebook pages behind disinformation activities impersonated the police (Freedom House, 2019). Another post on Facebook that was widely shared used a video from an attack over a debt issue in 2018 to spread the rumour that a man "dressed in a burqa" was arrested after he claimed he was involved in the attacks (AFP, 2019). However, political authorities were also sources of disinformation. For instance, a member of the Sri Lanka's Podujana Peramuna party shared photos that corresponded to an event in Iraq in 2016, claiming that these were taken during the preparations of the attacks (Freedom House, 2019).

In the run-up to the elections of November 2019, supporters of the candidates disseminated racist posts and disinformation on social media, especially on Facebook, WhatsApp, and Twitter (Srinivasan, 2019), in what might have been the highest levels of dissemination of online propaganda during an election in Sri Lanka (S. Hottotuwa, personal communication, July 11, 2020; Hattotuwa, s. f.). Although this does not indicate coordinated activity, long before the presidential election concerns had been raised over "Facebook's decision to allow politicians to promote content already rated false by fact-checkers" (Wong, 2019). In fact, as it has been highlighted by researcher Sanjana Hottotuwa, an official Facebook page related to Gotabaya Rajapaksa, candidate of the Sri Lanka People's Front and current president, promoted previously-debunked content (Ibid.). However, the volune of online propaganda in the November 2019 elections was unprecedented in the country.

As suggested by Hattotuwa, mis-and-disinformation during coronavirus lockdown was not only worrisome, but some widely spread content showed signs of coordinated inauthentic behaviour. For instance, the promotion of militarization one day after the 2020 general election announcement was spread with identical posts on Facebook, reaching more than 12,600 likes and 4,000 shares within 24 hours (Hattotuwa, 2020). Similarly, identical pro-Gotabaya Rajapkasa content by pro-SLPP and Rajapkasa Facebook pages that amplified militarization was posted almost simultaneously (Ibid.). Moreover, the criminalization of spreading disinformation took new dimensions, as the government explicitly said it would take legal actions. On 29 May the Police had already been investigating around four hundred cases and had arrested sixteen people, one of them a man who was "part of the media team of a minister in the previous government" (BBC Monitoring, 2020a, 2020b).

Attacks and hate speech are also part of the social media environment in Sri Lanka. Already in the context of violence in Aluthgama in 2014, Bandula Jayasekara—former editor in Chief of the Daily News and Presidential spokesperson—promoted hate speech via Twitter against journalists and activists; and Champika Ranawaka—Minister of Power and Energy—tagged both local and foreign journalists as promoters of fake news (Groundviews, 2017).

However, over the years socio-political tensions have increasingly manifested on social media (Hattotuwa, 2018; CIVICUS, 2019). As highlighted by Freedom House (2019), hate speech has been amplified on Facebook and other social media platforms, mostly with anti-Muslim content.

Hate and harassment has also been used to target specific individuals. For instance, Sandya Ekneligoda, a human rights activist whose husband was abducted in 2010, was subjected to a smear and attacks campaign that labelled her a traitor (CIVICUS, 2019). The attacks included aggressive and abusive content and also targeted her sons. She assigns the organization of the attacks to the Rajapaksa clan and other attacks to nationalistic Buddhist monks (Ibid.).

Finally, it is worth noting that in 2018, Groundviews identified a network of fake and automated accounts that overwhelmingly followed public figures. Although these accounts were inactive, they showed a worrisome possibility: "at some point in the future, to activate these bots in a way that through multi-nodal, multi-lingual, multi-media content production, dissemination and echoing, at scale, overwhelms the discussion of specific issues or actors, and overall, serves to strategically confuse, misdirect, misinform and undermine trust in Twitter as a whole" (Hattotuwa et al., 2018).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Sri Lanka

Account Types	Messaging and Valence	Communication Strategies	Platforms
Bots, Human Fake, Real	Support, attacks on opposition, Driving division, Suppressing speech	Disinformation, Trolls, Amplifying content	Twitter, YouTube, Facebook, WhatsApp

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

There are no details about how cyber troops in Sri Lanka are organized nor the resources allocated for their activities.

Table 3: Cyber Troop Capacity in Sri Lanka

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
		Permanent and temporary		Medium

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

References

AFP. (2019, May 22). Fake news rampant after Sri Lanka attacks despite social media ban. *Bangkok Post*. https://www.bangkokpost.com/world/1682004/fake-news-rampant-after-sri-lanka-attacks-despite-social-media-ban

BBC Monitoring. (2020a, March 31). *Highlights from Sri Lanka's Sinhala, Tamil-language press, websites 31 Mar 20*. BBC Monitoring. https://monitoring.bbc.co.uk/product/f201ky27

BBC Monitoring. (2020b, May 29). *Highlights from Sri Lanka's Sinhala, Tamil-language press, websites 29 May 20*. BBC Monitoring. https://monitoring.bbc.co.uk/product/f201rdd8

Chandimal, D., & Fernando, R. (2020, May 3). Freedom of Expression vs. Hate Speech, Fake and Misleading News. *Groundviews*. https://groundviews.org/2020/05/03/freedom-of-expression-vs-hate-speech-fake-and-misleading-news/

CIVICUS. (2019, October 31). *Sri Lanka: 'Trolls accusing people of being traitors are organised and political'*. CIVICUS. https://www.civicus.org/index.php/media-resources/news/interviews/4145-sri-lanka-trolls-accusing-people-of-being-traitors-are-organised-and-political

Freedom House. (2019). *Freedom of the Net 2019: Sri Lanka*. Freedom House. https://freedomhouse.org/country/sri-lanka/freedom-net/2019

Gotabaya Rajapaksa condemns fake news during a crackdown on social media. (2020, April 4). *Tamil Guardian*. https://www.tamilguardian.com/content/gotabaya-rajapaksa-condemns-fake-news-during-crackdown-social-media

Groundviews. (2017, April 7). *Disinformation in Sri Lanka: An overview* [Groundviews]. https://groundviews.org/2017/07/04/disinformation-in-sri-lanka-an-overview/

Gunatilleke, G. (2020, April 16). *Covid-19 in Sri Lanka: Is Free Speech the next Victim?* OHRH. https://ohrh.law.ox.ac.uk/covid-19-in-sri-lanka-is-free-speech-the-next-victim/

Hattotuwa, S. (s. f.). Presidential Election 2019 Framing content on Twitter, Facebook, YouTube and Instagram anchored to 2019's presidential election campaign. https://docs.google.com/document/d/1aJ84sTLgGeJ3VhToQDyFEyqn9fUnd-0al2UBUH5jNe4/edit

Hattotuwa, S. (2018). *Digital Blooms: Social Media and Violence in Sri Lanka* (Policy Brief N.º 28; p. 12). Toda Peace Institute and Alliance for Peacebuilding.

Hattotuwa, S. (2019, March 25). The ecology of an issue: 'Save Wilpattu' on Facebook and Twitter. *Groundviews*. https://groundviews.org/2019/03/25/the-ecology-of-an-issue-save-wilpattu-on-facebook-and-twitter/

Hattotuwa, S. (2020). *Mis/mal/disinformation & information ecologies during Coronavirus pandemic in Sri Lanka*.

https://docs.google.com/document/d/1pr26ADx3UX3iS2mlWosJyVYAA_TKlplenUJPTr92lNk/edit

Hattotuwa, S., & Wijeratne, Y. (2018, January 24). Namal Rajapaksa, bots and trolls: New contours of digital propaganda and online discourse in Sri Lanka. *Groundviews*. https://groundviews.org/2018/01/24/namal-rajapaksa-bots-and-trolls-new-contours-of-digital-propaganda-and-online-discourse-in-sri-lanka/

Hattotuwa, S., Wijeratne, Y., & Serrato, R. (2018). Weaponising 280 characters. What 200,000 tweets and 4,000 bots tell us about state of Twitter in Sri Lanka.

International Media Support. (2020, febrero 27). *The Truth Square—Trapping Disinformation*. International Media Support. https://www.mediasupport.org/the-truth-square-trapping-disinformation/

NetBlocks. (2019, April 21). Social media blocked in Sri Lanka following church and hotel bombings. *NetBlocks*. https://netblocks.org/reports/social-media-blocked-in-sri-lanka-following-church-and-hotel-bombings-XaAwlQBM

Sigal, I. (2019, April 23). Government actions in Sri Lanka Easter bombings raise the question: Is social media helping or hurting? *Global Voices Advocacy*. https://advox.globalvoices.org/2019/04/23/government-actions-in-sri-lanka-easter-bombings-raise-the-question-is-social-media-helping-or-hurting/

Sri Lanka: Joint letter to president Rajapaksa on the harassment and intimidation of journalists. (2020, February 25). Amnesty International. https://www.amnesty.org/en/documents/document/?indexNumber=asa37%2f1860%2f2020&language=en

Srinivasan, M. (2019, November 13). Concerns over fake news, disinformation ahead of Sri Lanka polls. *The Hindu*. https://www.thehindu.com/news/international/concerns-over-fake-news-disinformation-ahead-of-sri-lanka-polls/article29965462.ece

Wong, J. C. (2019, November 12). Sri Lankans fear violence over Facebook fake news ahead of election. *The Guardian*. https://www.theguardian.com/world/2019/nov/11/facebook-sri-lanka-election-fake-news

SUDAN

Introduction

Sudan is currently considered not free. In 2019 a coup of military and civil protestors ousted the repressive regime of Omar al-Bashir and his National Congress Party (NCP), and hopes are that in 2022 the country will elect a new government, replacing the current transitional administration. While civic spaces are slowly opening up to allow for more individual freedom and political pluralism, the shadow of the old regime looms large, and the protection of individual rights and political freedoms remains unclear. Still, the combination of military and civil representatives in the interim administration is cause for hope, as the military had attempted to take control by themselves when removing al-Bashir from office in April 2019, but ultimately gave in to civil demands of representation when protests did not cease[1].

The interim constitution agreed on in August 2019 technically guarantees freedom of the press, however, hostility towards journalists has a long history in Sudan. During the protests leading to the downfall of al-Bashir's regime national and local bureaus of international newspapers, most notably Al-Jazeera, were repeatedly closed and journalists were detained without charge. The transitional government has lifted some of the most severe restrictions, though journalists continue to be targets[2]. Additionally, internet freedom suffered greatly during the mass protests with al-Bashir's regime regularly blocking social media, and the military causing one of the longest internet shutdowns in history (June 3rd to July 9th, 2019)[3]. At the same time internet penetration in Sudan is low: of its 40 million population, 13 million use the Internet but more than 28 million own a mobile phone[4].

An Overview of Cyber Troop Activity Sudan

Organizational Form

The previous NCP regime was quite aware of the threat that social media could bring to its power as citizens in repressed countries started to organize themselves in the wake of the Arab Spring. As a reaction, the regime created the Cyber Jihad Unit within its National Intelligence Security Service (NISS). The BBC reported that the NCP warned that its "cyber-jihadists" will "crush" Internet-based dissent[5]. Moreover, the NISS was said to control digital media use through "blocking, controlling, jamming and slowing down certain websites, and hacking private accounts" under the old regime[6]. NetBlocks, a digital rights organization, said it had found evidence of "an extensive internet censorship regime"[7]. Citizen Lab ascertained through leaked documents that Hacking Team, an Italian offensive cyber weapons company, had at one point sold sophisticated computer spyware to Sudan's regime[8].

At present, it appears that the transitional government is easing off such harsh, direct measure of control and influence. Nevertheless, the situation remains fragile and lacks a legal framework to appeal current laws allowing for the jailing of people for allegedly spreading false news[9]. As Sudan struggles with a harsh economic crisis[10], the new administration failed to show leadership in the recent Coronavirus crisis and reverted back to old ways: parts of the country experienced temporary internet or social media shutdowns, which appeared to be enforced in order to avoid increasing local political and ethnic tensions caused by the virus[11].

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Sudan

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
	NISS	NCP			x

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

The Cyber Jihad Unit appears to focus on combatting domestic dissent. It disseminated misinformation to thwart protesters – for example, claiming that protests are a deliberate ploy to destabilize Sudan – and spread propaganda about the government's handling of the economy[12]. The unit proactively monitors content on "blogs, Facebook, Twitter, and news and public forums like Sudanese online, Sudan for All, Hurryat and Elrakoba"[13]. In the lead-up to protests in January 2011, supporters of the NCP posted on activist Facebook pages to warn them against joining protests [14].

The unit also regularly spread fake news to influence public debate and infiltrated online discussions to collect information on dissidents[15]. At the same time, the old regime used disinformation as an excuse to clamp down on opposition: In March 2014, the government declared certain websites would be banned for spreading false information about government activities. In April 2017, during Sudan's fuel crisis, the finance minister stated that he held WhatsApp responsible for spreading false information and creating the fuel crisis, and in 2018 the regime passed a law making the spread of false news online illegal as a response[16].

Next to these local strategies, evidence suggests that Russian influence operations have found their way into Sudan as well. Russia has been benefitting from Sudan's diamond and gold deposits for a while now and is known to have trained local military forces[17]. The Stanford Internet Observatory documented Russian internet activity targeting Sudanese politics starting in mid-2018, which stayed persistent throughout the coup removing al-Bashir and the NCP from power. Websites posing as news outlets and Facebook pages posing as official political parties and news pages for the transitional government, shared mildly positive content about whomever was in power and occasional critiqued protestors[18]. Facebook took down these troll accounts in October 2019[19]. In addition, the former Sudanese regime coordinated with a Russian company called M-invest to spread rumors and disinformation about the anti-government protests. Documents suggest the company had a thought-out plan and detailed fabricated stories such as a social media campaign claiming that Israel supported the protestors[20].

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Sudan

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Human	Support Attack Opposition Suppression	Disinformation Trolls	Facebook Twitter WhatsApp

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

Reportedly, the Cyber Jihad Unit had received training in Malaysia and India and is alleged to have 200 full-time employees[21]. There is very little information available on the unit's activities or general existence after the regime change. However, the unit did appear on the 2020 top 20 press freedom's digital predators list of Reporters Without Borders[22], thus it appears they are still active.

Table 3: Cyber Troop Capacity in Sudan

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
		Unclear at the moment	Coordinated	

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

In light of the recent COVID-19 pandemic Sudan struggles to contain the virus, as the media is flooded with misinformation and denial of the virus's existence[23]. Sudan has one of the highest numbers of COVID-19 cases in Africa and was struggling with poverty and insufficient medical supply before the pandemic already. The government initially attempted to contain the virus, leading to confusion, stigma and panic[24]. Some medical workers even reported being attacked by police forces who were trying to enforce the lockdown[25].

References

AFP. (2020, April 9). Sudan still in crisis a year after Bashir's ouster. *NST Online*. https://www.nst.com.my/world/world/2020/04/582773/sudan-still-crisis-year-after-bashirs-ouster

BBC. (2011, March 23). Sudan to unleash cyber jihadists—BBC News. *BBC News*. https://www.bbc.co.uk/news/technology-12829808

BBC News. (2020, May 25). Coronavirus in Sudan exposes new leaders. *BBC News*. https://www.bbc.com/news/world-africa-52735520

Eljaili Abubkr, L. (2014, April 11). *Online surveillance and censorship in Sudan | Association for Progressive Communications*. Assocation for Progressive Communications. https://www.apc.org/en/blog/online-surveillance-and-censorship-sudan

Freedom House | Sudan. (2018). Freedom House. https://freedomhouse.org/country/sudan/freedom-world/2018

Freedom House | Sudan. (2020). Freedom House. https://freedomhouse.org/country/sudan/freedom-world/2020

Freedom on the Net | Sudan. (2019). Freedom House. https://freedomhouse.org/country/sudan/freedom-net/2019

Grossman, S., Bush, D., & DiResta, R. (2019). *Evidence of Russia-Linked Influence Operations in Africa*. Stanford Internet Observatory. https://fsi.stanford.edu/news/prigozhin-africa

Harding, L. (2019, October 30). Facebook removes Africa accounts linked to Russian troll factory. *The Guardian*. http://www.theguardian.com/technology/2019/oct/30/facebook-removes-africa-accounts-linked-russian-troll-factory-yevgeny-prigozhin

Lamoureaux, S., & Sureau, T. (2019). Knowledge and legitimacy: The fragility of digital mobilisation in Sudan. *Journal of Eastern African Studies*, *13*(1), 35–53. https://doi.org/10.1080/17531055.2018.1547249

Lister, T., Shukla, S., & Elbagir, N. (2019, April 25). A Russian company's secret plan to quell protests in Sudan. *CNN*. https://www.cnn.com/2019/04/25/africa/russia-sudan-minvest-plan-to-quell-protests-intl/index.html

Marczak, B. (2014, February 17). *Mapping Hacking Team's "Untraceable" Spyware*. Citizen Lab. https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/

Morgan, H. (2020, April 7). COVID-19: Sudan struggles with denial and misinformation. *Al Jazeera*. https://www.aljazeera.com/news/2020/04/covid-19-sudan-struggles-denial-misinformation-200407154437389.html

Reynolds, N. (2019). *Putin's Not-So-Secret Mercenaries: Patronage, Geopolitics, and the Wagner Group*. Carnegie: Endowment for International Peace. https://carnegieendowment.org/2019/07/08/putin-s-not-so-secret-mercenaries-patronage-geopolitics-and-wagner-group-pub-79442

Ro, C. (2020, June 25). Why Health Workers In Sudan Have Been Leaving Their Posts Amid Covid-19. *Forbes*. https://www.forbes.com/sites/christinero/2020/06/25/why-health-workers-in-sudan-have-been-leaving-their-posts-amid-covid-19/

RSF. (2020, March 10). RSF unveils 20/2020 list of press freedom's digital predators | Reporters without borders. *Reporters Without Borders*. https://rsf.org/en/news/rsf-unveils-202020-list-press-freedoms-digital-predators

Saba, Y., & Eltahir, N. (2019, January 2). Sudan restricts social media access to counter protest movement—Reuters. *Reuters*. https://www.reuters.com/article/us-sudan-protests-internet/sudan-restricts-social-media-access-to-counter-protest-movement-idUSKCN1OW0Z7

Sudan internet shows signs of recovery after month-long shutdown. (2019, September 7). *NetBlocks.Org*. https://netblocks.org/reports/sudan-internet-recovery-after-month-long-shutdown-98aZpOAo

Suliman, M. (2019a, October 4). As Sudan transitions to democracy, urgent reforms must tackle disinformation. *Global Voices Advocacy*. https://advox.globalvoices.org/2019/10/04/as-sudan-transitions-to-democracy-urgent-reforms-must-tackle-disinformation/

Suliman, M. (2019b, October 4). As Sudan transitions to democracy, urgent reforms must tackle disinformation—Global Voices Advox. *Global Voices Advocacy*. https://advox.globalvoices.org/2019/10/04/as-sudan-transitions-to-democracy-urgent-reforms-must-tackle-disinformation/

SWEDEN

Introduction

Sweden is a parliamentary monarchy with fair and free elections and a multi-party system. The country has one of the most robust freedom of information statutes in the world which is well respected by government authorities. The media are free and independent, mostly privately owned and state subsidized regardless of political affiliation. Additionally, public broadcasters regularly air programs in several minority languages. While threats to journalists have reportedly increased in recent years, such incidents do not seem to impact the news media's work or lead to self-censorship (*Freedom House Report 2019: Sweden*, 2019). In general, as of early 2020 the trust of citizens in the freedom of opinion and the press, as well as trust in the media more generally, remains quite high in international comparison (Powell, 2020).

An Overview of Cyber Troop Activity in Sweden

Organizational Form

Most political parties maintain a social media presence on various major platforms (Twitter, Facebook). It appears that both parties and individual politicians are not engaged in any systematic cyber troop activity. Nevertheless, discussion of domestic and foreign politics online does become more intense at certain times and can intersect with international politics. During the recent US Democrat party Presidential primaries, supporters of Joe Biden disseminated a video showing rival candidate Bernie Sanders praising the Soviet Union in 1988 to undermine his campaign. This video had first been tweeted by former Swedish prime minister Carl Bildt in February 2019 (Savodnik, 2020). Private users and journalists criticized Bildt for his comments under his original Tweet, calling it misinforming and hypocritical (figure 1). Other incidences show that Swedish politicians are not as experienced with online trolling and fake accounts: On 22nd March 2020, Social Democrat MEP Marita Ulvskog retweeted a message from a fake Trump account, assuming it was Trump's official account (figure 2).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Sweden

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
		x			

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

During the 2018 Swedish general election fake news, trolls and bots flooded Swedish internet spaces, as has become common during most recent elections held in European countries. Research by the Swedish Defence Research Agency found that the number of Twitter bots increased significantly in the weeks leading up to the elections. Moreover, these bots were 40% more likely than human Twitter users to support the anti-immigrant Sweden Democrats party. Troll attacks spreading disinformation have also become a common sight online, most of which stem from right-wing extremists that specifically hold immigrants accountable for crime in Sweden. Twitter bots in particular have pushed this anti-immigrant viewpoint in recent years, while the debate has been going since 2015. The far-right party Sweden Democrats that profits the most from this narrative were able to increase their vote share from 4.6% to 17.5% (the Social Democrats received the largest share of the vote, with 28%) (Meaker, 2018; Swedish Defence Research Agency, 2018). It appears, however, that these computational and bot activities are not tied directly to the Sweden Democrats, but instead have their roots in American far-right groups and potentially Russian groups, though these connections remain difficult to trace and confirm (Becker, 2019).

In addition to the Sweden Democrats, several hyper-partisan news pages such as Samhällsnytt, Nyheter Idag, and Fria Tider, are also profiting from bot activities on Twitter. These pages are alternative or partisan news-sources known to share disinformation, with a particular emphasis on linking immigration to a rise in crime, either by manipulation news stories or making them up. Such pages are popular and read by roughly 10% of the Swedish population on a weekly basis (Meaker, 2018). As with the activities on social media, it is not clear where the Twitter bots pushing these alt-right topics originates. Some Swedish governmental officials have speculated on the usual foreign suspect, Russia. However, many academics believe that the bots originate from within Sweden due to their fluency in Swedish (Bershidsky, 2018; Meaker, 2018).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Sweden

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Human Bots	Attack on Opposition Driving Divisions	Disinformation Trolls	Twitter

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

Cyber troop activity in the country tends to be temporary and scarce, at least activity organized by domestic political actors. Politicians and political parties tend to start undertaking more online activity during election seasons or in relation to politically sensitive issues or events, such as the current COVID-19 crisis. Nevertheless, there are rarely any instances of deliberate disinformation or other types of cyber troop activity. Politicians do regularly take to Twitter to criticize each other. For example, Jimmie Åkesson's (leader of the Sweden Democrats') recent visit to Greece, where he handed out flyers saying "we [Sweden] are full", were heavily criticized by government officials, ministers and other opposition parties (Meaker, 2018; SBS News, 2020). These activities, however, do not seem to be part of any larger disinformation or influence campaigns.

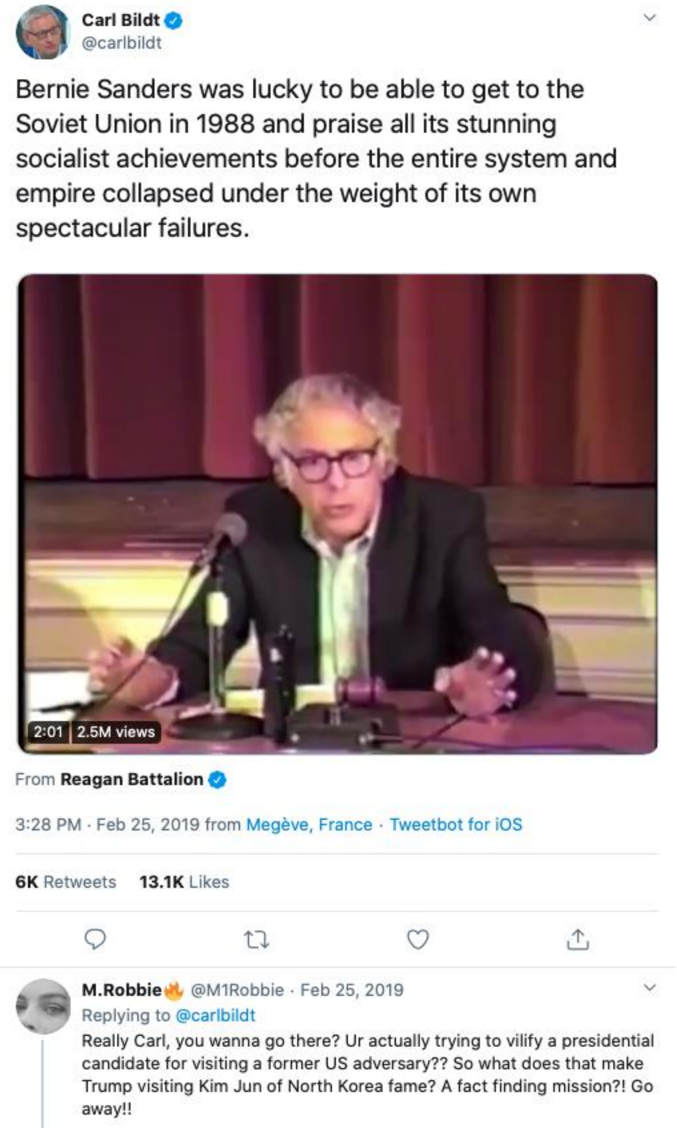
Table 3: Cyber Troop Capacity in Sweden

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
		Temporary		

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

In light of the parliamentary and local elections in September 2018, the Swedish government launched various measures to counter fake news and trolling in relation to the election: (1) a "Facebook hotline" run by the government to allow the quick reporting of forged pages and profiles; (2) measures to counter disinformation, boost resilience against fake news in the Swedish population by preserving an open society, and support the free exchange of knowledge and information; (3) the introduction of "source criticism" courses in middle and high school classes; and (4) the distribution of leaflets with information on how to spot disinformation. It is not clear how successful these measures have been, but they are nonetheless still a quite unique effort to combat fake news amongst European countries (Brattberg & Maurer, 2018; Guerrini, 2018; *The Local Sweden*, 2018). Similar measures were employed for the European Parliamentary elections in 2019 ("Så skyddar MSB EU-valet från desinformation," 2019).

In addition, Swedish citizens have also started their own initiatives. Private citizens have worked to debunk false news on Reddit and Quora, and founded a Facebook group in 2016, with around 75.000 members mainly from Sweden, who under the hashtag #Jagärhär (#Iamhere), defend people attacked online by trolls and try to counter the spread of disinformation in an attempt to rebalance online discussions. While some critics have called #Jagärhär a form of censorship, initiators said they have no agenda and primarily want to spread positivity and love (Eyre & Goillandeau, 2019). They have since acquired NGO-status and have worked with groups around the EU to further an agenda which includes goals such as working for inclusion and counteracting polarization, filter bubbles, propaganda, hatred, and racism (jagärhär.se, 2017).


Carl Bildt
@carlbildt

Bernie Sanders was lucky to be able to get to the Soviet Union in 1988 and praise all its stunning socialist achievements before the entire system and empire collapsed under the weight of its own spectacular failures.

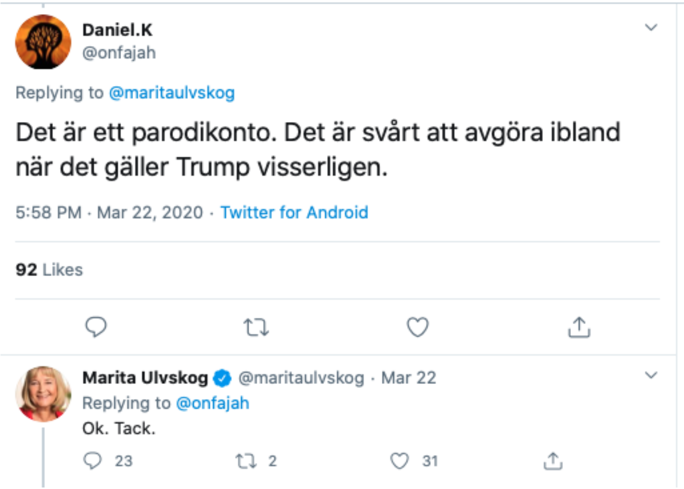
From Reagan Battalion

3:28 PM · Feb 25, 2019 from Megève, France · Tweetbot for iOS

6K Retweets 13.1K Likes

M.Robbie @M1Robbie · Feb 25, 2019
Replying to @carlbildt
Really Carl, you wanna go there? Ur actually trying to vilify a presidential candidate for visiting a former US adversary?? So what does that make Trump visiting Kim Jun of North Korea fame? A fact finding mission?! Go away!!

Figure 1: Former Swedish prime minister tweeting about Sanders in the Soviet Union (source: https://twitter.com/carlbildt/status/1100039769810235393?lang=en)



Daniel.K
@onfajah

Replying to @maritaulvskog

Det är ett parodikonto. Det är svårt att avgöra ibland när det gäller Trump visserligen.

5:58 PM · Mar 22, 2020 · Twitter for Android

92 Likes

Marita Ulvskog @maritaulvskog · Mar 22
Replying to @onfajah
Ok. Tack.

Figure 2: Twitter user replying to Tweet about Trump from Social Democrat Marita Ulvskog saying that the account she referenced was fake (source: https://twitter.com/onfajah/status/1241771131901751305)

References

Becker, J. (2019, August 10). The Global Machine Behind the Rise of Far-Right Nationalism. *The New York Times*. https://www.nytimes.com/2019/08/10/world/europe/sweden-immigration-nationalism.html

Bershidsky, L. (2018, August 30). *Twitter's Trolls Are Coming for Sweden's Election*. https://www.bloomberg.com/opinion/articles/2018-08-30/the-online-twitter-trolls-are-coming-for-sweden

Brattberg, E., & Maurer, T. (2018, May 31). *How Sweden is preparing for Russia to hack its election*. https://www.bbc.com/news/world-44070469

Den ideella föreningen #jagärhär. (2017, April 10). *Jag är här*. https://www.jagarhar.se/uncategorized/den-ideella-foreningen-blir-till/

Eyre, M., & Goillandeau, M. (2019, January 15). Here, here: The Swedish online love army who take on the trolls. *The Guardian*. https://www.theguardian.com/world/2019/jan/15/the-swedish-online-love-army-who-battle-below-the-line-comments

Far-right leader in Sweden criticised for anti-migrant Greece trip. (2020, March 5). *SBS News*. https://www.sbs.com.au/news/far-right-leader-in-sweden-criticised-for-anti-migrant-greece-trip

Freedom House Report 2019: Sweden. (2019). Freedom House. https://freedomhouse.org/country/sweden/freedom-world/2019

Guerrini, F. (2018, August 14). Sweden's 2018 General Election Could Provide A Blueprint For Fake News Countering. *Forbes*. https://www.forbes.com/sites/federicoguerrini/2018/08/14/swedens-2018-general-election-could-provide-a-blueprint-for-fake-news-countering/

Meaker, M. (2018, September 9). Inside the online disinformation war trying to tear Sweden apart. *Wired UK*. https://www.wired.co.uk/article/sweden-election-polls-far-right

Powell, L. (2020, March 25). Is the EU doing enough to fight Fake News? *The New Federalist*. https://www.thenewfederalist.eu/is-the-eu-doing-enough-to-fight-fake-news

Så skyddar MSB EU-valet från desinformation. (2019, May 20). *Myndigheten för samhällsskydd och beredskap*. https://www.msb.se/sv/aktuellt/nyheter/2019/maj/sa-skyddar-msb-eu-valet-fran-desinformation/

Savodnik, P. (2020, February 21). "Canceled Because of a Video You Didn't Even Make": Inside a Bernie-Biden Troll War | Vanity Fair. *Vanity Fair*. https://www.vanityfair.com/news/2020/02/inside-bernie-biden-twitter-troll-war-lyndi-li

Sweden to create new authority tasked with countering disinformation. (2018, January 15). https://www.thelocal.se/20180115/sweden-to-create-new-authority-tasked-with-countering-disinformation

Swedish anti-immigration leader slammed over border stunt. (2020, March 5). *The Local Sweden*. https://www.thelocal.se/20200305/swedish-anti-immigration-leader-slammed-over-border-stunt

Swedish Defence Research Agency. (2018). *The Swedish election and bots on Twitter* [Text]. Swedish Defence Research Agency. https://www.foi.se/en/foi/news-and-pressroom/news/2018-09-12-the-swedish-election-and-bots-on-twitter.html

Syria

Introduction

Computational propaganda in Syria should be viewed against the backdrop of existing domestic repression, tight Internet controls, and the ongoing civil war. The Assad family, members of the Syrian Ba'ath Party, have been in power in Syria since Hafez al-Assad seized power in the 1970 military coup. Although the Ba'ath party is a secular Pan-Arab organization, the minority Alawite elite has come to dominate both the party and the military, and as such, has become increasingly repressive as opposition to their leadership has grown (Economist, 2000). In 2011 the rule of Hafez's son, Bashar al-Assad, was challenged by the Arab Spring protests. The protests led to violent repression by the government and have transformed into a complex and brutal war involving both regional and international actors (BBC, 2018). The civil war in Syria has been described as the "first social media war" and the "the first skirmish in the Information War" (O'Neil, 2013; Diresta, 2018). Syria's Internet infrastructure has been severely damaged and is increasingly subject to significant censorship as the Assad regime has long attempted to assert total control over political communication (Freedom on the Net, 2019).

An Overview of Cyber Troop Activity in Syria.

Organizational Form

One prominent actor behind cyber troop activity in Syria is the Syrian Electronic Army (SEA), a hacker group which is widely considered to be supported by the Syrian government (Harding and Arthur 2013; Stork, 2014). In a 2011 speech in Damascus, Assad linked anonymous online warriors to his frontline troops: "There is the electronic army, which has been a real army in virtual reality" (Harding and Arthur, 2013). The SEA registered its domain in 2011 on servers maintained by the Assad-linked Syrian Computer Society, further suggesting that there are tacit links or government support (Freedom House, 2018).

Two of the SEA's chief operators, Ahmed al Agha and Firas Dardar, have made it onto the FBI's most-wanted list (Brewster, 2018). In May 2018, Open Canada reported that the SEA was re-launching with a new mission as "domestic cyber police", an agenda consistent with the Assad regime's objective to reimpose its sovereignty over the Syrian population (Abas, 2018). Furthermore, Forbes reported that the group is investing resources into developing spyware, having developed malware dubbed 'SilverHawk' to target security and privacy focused communication apps such as WhatsApp and Telegram (Brewster, 2018).

Each side in the civil war has waged its own propaganda campaign: the radical Islamist group the Islamic State (also known as ISIS, ISIL, or Daesh) is widely recognized as a successful innovator in this field (Berger and Morgan, 2015), while regional powers (such as Iran) and global powers (such as the US and Russia) have also been accused of spreading computational propaganda in the conflict (Cockburn, 2016). There is also evidence of co-ordination between regional and global actors, as recent reports have also emphasized the close alignment between Syrian and Russian propaganda (Diresta, 2018). Scott Lucas, Professor of International Studies at the University of Birmingham, has suggested that "although Moscow became militarily involved in the Syrian conflict in 2015, they had a propaganda office at the presidential palace in Damascus since the beginning" (Palma, 2018).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Syria

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
	X		x	Syrian Electronic Army	

Source: Author’s evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Bots and amplification of content

An early report on Syria’s cyber troops claimed that in 2011 the government invested in Twitter bots to overwhelm the revolutionary narrative with pro-government posts (York, 2011). York (2011) noted that the government had outsourced this campaign to a Bahraini company, EGHNA, which successfully flooded the #Syria hashtag in 2011. Another tactic was drowning out protesters’ voices on Twitter with irrelevant information. For example, photography using #Syria from accounts such as @LovelySyria and @SyriaBeauty.

Harassment

Katina Michael (2017) wrote in The Conversation that, in response to Arab Spring activists using hashtags such as #Syria, #Daraa, and #Mar15, government intelligence officers began to threaten online protesters. Syrian blogger Anas Qtiesh wrote that accounts were “believed to be manned by Syrian *mokhbarat* (intelligence)” with “an endless arsenal of bite and insults”.

Cyber-attacks

The SEA combines cyber-attacks and propaganda using various tactics, such as phishing to take over social media accounts of Western news outlets (Harding and Arthur, 2013). In 2013, the SEA hacked the official Associated Press Twitter account and tweeted that Barack Obama had been injured in an explosion, which lead to a momentary panic knocking the stock market value by US$136 billion (Fisher, 2013). Harding and Arthur (2013) argue that high-profile attacks on Western targets serve the double purpose of punishing Western news organizations critical of Syria's regime and spreading Damascus's alternative narrative.

Mass reporting

In 2018 the Facebook pages of dozens of opposition and media groups were suspended, which activists believe is the direct result of the mass-reporting of these pages for violating community guidelines by pro-Assad supporters (Freedom House, 2018). The suspension of media groups’ accounts has had a profound influence on access to information; with more than two hundred media workers having been killed since the start of the revolt, both the Syrian people and international audiences have increasingly come to rely on social media for information (BBC, 2018).

Disinformation

The Syrian Civil Defence, commonly known as the ‘White Helmets’, have been subject to frequent disinformation campaigns. Conspiracies such as the idea that the Syrian chemical attacks are a hoax created by the White Helmets, are often widely shared by Russian state-run media outlets such as RT, and by Western far-right activists. Many of the same accounts which claim that American victims of mass shootings are actually actors in a “staged” tragedy repeat the same allegation about Syrian war victims (Palma, 2018).

Since the White Helmets that documented the chemical attack in Khan Sheikhoun in April 2017, which killed at least eighty-three people, they have been continually discredited by an online network of activists, conspiracy theorists, and Russian government trolls (Solon, 2017). For example, Graphika discovered an online network of 14,000 Twitter users talking about the White Helmets that looked "very similar" and included many known pro-Kremlin troll accounts (Ibid). Moreover, Russia's official channels have posted memes discrediting the organization, and alleging they staged 'hoax' chemical attacks. Investigative journalist agency Bellingcat observed that, from August to November 2018, the Russian and Syrian governments' state-controlled media outlets have repeated these narratives about the White Helmets and their involvement with chemical weapons in the rebel areas of north-western Syria (Bellingcat, 2018).

In 2019 the leader of the white helmets, Raed Salah, claimed that these information attacks and disinformation campaigns against them had continued. This came after the Twitter account of the Russian embassy in Syria was suspended for posting that the rescue group was faking images of bombings (Middle East Eye, 2019). In a recent cross-platform study, Wilson and Starbird (2020) examine both sides of the online discourse about the White Helmets and find that tracing information across platforms shows that anti-White Helmets groups received multi-dimensional support from Russia's state sponsored media, including content production and amplification of certain voices. Their research also highlights how the White Helmets themselves use social media to promote their work and foster solidarity.

In April 2018, there was a surge of disinformation following the chemical attack in Douma. Nearly half of the counternarrative accounts created in the week between the Douma chemical attack and the Western strike against Syria were claimed to be managed by inauthentic actors. Sky News reported that the UK government had documented more than 45,000 posts propagating disinformation in the two weeks following the chemical attack on 7 April 2018 (Bunkall, 2018). According to BBC Trending, in the hours after the attack, 'Syria' was the top trending term on Twitter, but the messages by pro-Assad activists were overwhelmed by reports from news outlets. The hashtag #SyriaHoax was used around 17,000 times a week in April 2017 but failed to make Twitter's list of top trends (BBC, 2018). Following the US-led missile strike on Syrian targets, the Pentagon claimed a 2,000% increase in Russian troll activity on social media. There were found to be part of a campaign to present alternative narratives sowing doubt about the evidence that Assad was responsible for the chemical attack (Guynn, 2018).

These online disinformation wars have proliferated in the more recent military assaults launched by Turkish troops and allied Syrian rebels against the Syrian Kurdish militia, the People's Protection Units (YPG). The Turkish state-funded news organization Anadolu Agency stated that social media accounts close to the YPG have been attempting media manipulation in relation to Turkey's "Operation Peace Spring". In a "fact checking" campaign, launched by Turkish Government officials and pro-government media outlets, a number of examples were listed of "photos taken in different regions and different years during the Syrian civil war that were shared as if they happened during Operation Peace Spring". Turkish Journalist Hakan Celik argued that these Syrian Kurdish groups were trying to create a perception the Turkey is carrying out ethnic cleansing (BBC Monitoring).

Aware that public support in the United States for a military presence in Syria is finite, the government of Bashar al-Assad has developed and encouraged messages which undermine the Operation Inherent Resolve (OIR) anti-ISIS campaign. At the same time, pro-SARG (Syrian Arab Republic Government) social media accounts have boosted the role of the Syrian Arab Army (SAA) in countering ISIS. Overall, pro-SARG social media accounts are promulgating a narrative which depicts the government of Bashar al-Assad as fighting a foreign-backed counterinsurgency which seeks to conquer territory historically of special importance to the Muslim world. This is being conducted by accounts on Twitter such as "Ivan Sidorenko", (@IvanSidorenko1), "Peto Lucem", (@PetoLucem), "PartisanGirl", (@Partisangirl), and "The'Nimr'Tiger", (@TheNimrTiger or @Souria4Syrians) (O'Leary & Heras, 2019).

These narrative contestations are components of a broader, multi-domain proxy war in Syria in an era of peer competition. The social media reverberations into and out of Syria may have implications for the future deployments of cyber troops as proxy conflicts accelerate.

Social media troops are one element of this approach in the Syrian conflict which includes Electronic Warfare (EW), Information Warfare (IW), and a contested multinational airspace (Mcleary, 2018). US Lt. Gen. Paul Funk stated in late 2018 that adversaries such as Russia "want to take us on in the edges, in the information space or in EW" (Mcleary, 2018). Some researchers suggest that this 'edge' might also extend outwards into exploiting vulnerabilities to create discord in domestic civilian social media environments of militaries, no matter the contribution size. This may even extend geographically to populations as far away from Syria as Australia. In a report to the Australian parliament in late 2018, Tom Sear suggested Russian active cyber measures coincided with a possible correlation with Russian state-sponsored IRA sock-puppet activity influencing opinion on issues like 'syria', 'aleppo', 'merkel', 'isis', even 'sports,' in the Australian Twittersphere when assets were in conflict in airspace over Syria in 2017 (Sear, 2018).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Syria

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Bots, Fake, Real	Spreading pro-government propaganda; attacking the opposition, smear campaigns; distracting or diverting conversations or criticism away from important issues; suppressing participation through personal attacks or harassment.	Creation of disinformation or manipulated media; mass-reporting of content or accounts; trolling, and harassment; amplifying content and media online	Facebook, Twitter,

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

Pro-Assad activists linked to the SEA reportedly earn around US$500–US$1,000 for high-profile attacks on Western targets (Harding and Arthur, 2013).

Table 3: Cyber Troop Capacity in Syria

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
	500-1000$	Permanent	Somewhat Centralised	Medium

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

References

Abas, A. 2018. The New Face of the Syrian Electronic Army. *Open Canada.* https://www.opencanada.org/features/new-face-syrian-electronic-army/

BBC Monitoring. 2019. Turkey launches campaign against disinformation on Syria offensive. *BBC.* https://monitoring.bbc.co.uk/product/c2015g9l.

BBC News. 2018. Syria war: The online activists pushing conspiracy theories. *BBC.* https://www.bbc.co.uk/news/blogs-trending-43745629

BBC Trending. 2018. The online activists pushing Syria conspiracy theories. *BBC News.* http://www.bbc.co.uk/news/blogs-trending-43745629e

Bellingcat. 2018. Chemical Weapons and Absurdity: The Disinformation Campaign Against the White Helmets. *Bellingcat.* https://www.bellingcat.com/news/mena/2018/12/18/chemical-weapons-and-absurdity-the-disinformation-campaign-against-the-white-helmets/

Berger, J. M., & Morgan, J. 2015. The Isis Twitter census: Defining and describing the population of ISIS supporters on Twitter. *Brookings.*

Brewster, T. 2018. Syrian Electronic Army Hackers Are Targeting Android Phones with Fake WhatsApp Attacks. *Forbes.* https://www.forbes.com/sites/thomasbrewster/2018/12/05/syrian-electronic-army-hackers-are-targeting-android-phones-with-fake-whatsapp-attacks/

Bunkall, A. 2018. Russian bots behind '4,000% rise' in spread of lies after Salisbury and Syria attacks - Govt analysis. *Sky News. https://news.sky.com/story/russian-bots-behind-4000- rise-in-spread-of-lies-after-salisbury-and-syria-attacks-11338466*

Cockburn, P. 2016. The Explanations behind Russian and US airstrikes in Syria are a lesson in propaganda. *Independent***.** https://www.independent.co.uk/voices/the-explanations-behind-us-and-russian-airstrikes-in-syria-are-a-lesson-in-propaganda-a7325081.html

Diresta, R. 2018. How ISIS and Russia Won Friends and Manufactured Crowds. *Wired.* https://www.wired.com/story/isis-russia-manufacture-crowds/

Ensor, J. 2018. Russian misinformation about 'imminent' White Helmets chemical attack could spell start of Idlib siege. *The Telegraph*. https://www.telegraph.co.uk/news/2018/09/02/russian-disinformation-campaign-syria-threatened-spark-new-war/

Fisher, M. 2013. Syrian hackers claim AP hack that tipped stock market by $136 billion. Is it terrorism? *The Washington Post*. https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/

Freedom House. 2019. Freedom on the Net: Syria. *Freedom House.* https://freedomhouse.org/report/freedom-net

Freedom House. 2018. Freedom in the world: Syria. *Freedom House*. https://freedomhouse.org/country/syria/freedom-world/2018

Guynn, J. 2018. Pentagon claims 2,000% increase in Russian trolls after Syria strikes. What does that mean? *USA today.*

http://www.usatoday.com/story/news/world/2018/04/15/pentagon-claims-2-000-increase-russian-trolls-after-syria-strikes/518665002/

Harding, L. & Arthur, C. 2013. Syrian Electronic Army: Assad’s cyber warriors. *The Guardian*. https://www.theguardian.com/technology/2013/apr/29/hacking-guardian-syria-background

Mcleary, P. 2018. Russia Winning Info & Electronic War In Syria, US & UK Generals Warn. *Breaking Defense*. https://breakingdefense.com/2018/10/russia-winning-information-electronic-war-over-syria-us-uk-generals-warn/

Michael, K. 2017. Bots without borders; how anonymous accounts hijack political debate. *The Conversation*. https://theconversation.com/bots-without-borders-how-anonymous-accounts-hijack-political-debate-70347

Middle East Eye. 2019. Syria War: White Helmets head condemns Russian disinformation campaign. MEE. https://www.middleeasteye.net/news/syria-war-white-helmets-head-condemns-continued-targeting-civilians-and-rescue-volunteers

O’Leary, C.A., & Heras, N.A. 2019. Political Strategy in Unconventional Warfare: Opportunities Lost in Eastern Syria and Preparing for the Future. Joint Special Operations University Report 19-1. https://jsou.libguides.com/ld.php?content_id=48094082.

O’Neil, P.H. 2013. Why the Syrian uprising is the first social media war. *Daily Dot*. https://www.dailydot.com/layer8/syria-civil-social-media-war-youtube/

Palma, B. 2018. Critics Slam Viral Stories Claiming Douma Chemical Attack Victims Died from Dust. *Snopes*. https://www.snopes.com/news/2018/04/20/critics-slam-viral-stories-claiming-douma-chemical-attack-victims-died-dust/.

Solon, O. 2017. How Syria's White Helmets became victims of an online propaganda machine. *The Guardian*. https://www.theguardian.com/world/2017/dec/18/syria-white-helmets- conspiracy-theories

Stork, C. 2014. Syria Uses Electronic Army to Spread Propaganda Online – and These Other Governments Do Too. *Mic*. https://mic.com/articles/79815/syria-uses-electronic-army-to- spread-propaganda-online-and-these-other-governments-do-too

The Economist. 2000. Hafez Assad. *The Economist*. https://www.economist.com/node/82659

White, S. P. 2018. Information Warfare in the Digital Age: A study of #SyriaHoax. *Technology Science*.

Wilson, T., & Starbird, K. 2020. Cross-platform disinformation campaign: lessons learned and next steps. *Misinformation Review*. https://misinforeview.hks.harvard.edu/article/cross- platform-disinformation-campaigns/.

York, J.C. 2011. Syria's Twitter spambots. *The Guardian*. https://www.theguardian.com/commentisfree/2011/apr/21/syria-twitter-spambots-pro-revolution

Taiwan

Introduction

The disinformation landscape in Taiwan is particularly complex. The strategic importance of Taiwan to China makes it a recognized target for China's propaganda and influence efforts. The threat of Beijing's influence was a major media topic during the 2020 Taiwan presidential elections and led Taiwanese authorities to establish various laws and institutions to combat "fake news". While much of Taiwan's disinformation problem originates from its complicated ties with China, the focus on Beijing's influence has often made it difficult to differentiate between foreign coordinated inauthentic behaviour and those that actually originate from domestic actors.

An Overview of Cyber Troop Activity in Taiwan.

Organizational Form

An early report undertaken by Oxford Internet Institute's Computational Propaganda project that examined the distribution of online disinformation in Taiwan noted that the presence of domestic computational propaganda and "cyber armies" can be dated back to at least 2014 (Monaco, 2017). During the 2014 Taipei mayoral election the emergence of a new "netzien" movement played a significant role in the Sunflower Student Movement's support for Ko Wen-je (a medical doctor at the National Taiwan University Hospital) (Lin & Wu, 2019). According to a report by CommonWealth, these netziens were divided into "volunteer online armies" of supporters and "real internet armies" of political PR companies and marketing companies (Ibid). Data explored by Ko and Chen (2015) found that the campaign for Sean Lian, the candidate for the Kuomintang party (KMT) used manual propogandists as a cyber army during the mayoral elections to influence voters. During the same elections the use of data science and bots for "intelligence" purposes was also evident (Monaco, 2017). A member of Ko Wen-je's online campaign has stated that crawler bots were used to collect data from social media in order to understand the kinds of content that they should use to promote Ko's campaign (Ibid).

Despite these early instances of computational propaganda, the country's 2018 midterm elections and 2020 presidential elections saw misinformation intensify (Shu, 2020). Elections have become a well-recognized target for online disinformation campaigns on a global scale, and the importance of the Taiwanese election can be viewed in terms of its strategic importance to Beijing (Stanford Internet Observatory, 2019a). Media coverage during the 2020 presidential elections focused mainly on the role of the Chinese intelligence services and their interest in discrediting Taiwanese President Tsai Ing-wen of the Democratic Progressive Party (DPP), who is seen as an advocate for Taiwanese independence (Aspinwall, 2020). A recent study by the V-Dem Institute at the University of Gothenburg in Sweden has found that Taiwan is among the countries that are exposed to the highest levels of foreign influence through online disinformation dissemination (Shu, 2020).

In response to these developments, Taiwan passed an Anti-Infiltration Law to combat these perceived threats from China. According to Reuters, "the law gives legal teeth to efforts to stop China funding activities on the Island, such as lobbying or election campaigns." Lawmakers of Tai's DPP backed the bill despite criticism from the opposition that the law acts as a "political tool" to gain votes, calling it a threat to Taiwan's democracy (Lee & Hamacher, 2019).

Despite these new efforts in trying to stop Chinese influence, experts have warned that accusing Beijing of being behind every case of online misinformation in Taiwan can be "more counterproductive than helpful" (Aspinwall, 2020). One specific case of this was the tragic event of the viral spread of a fake report regarding the director of Taiwan's representative office in Osaka, Japan, Su Chii-cherng, that ended in him committing suicide. The report claimed that Taiwanese travellers were left stranded at Osaka's Kansai Airport during a typhoon and were eventually saved by buses sent by the Chinese embassy. The story quickly went viral and was circulated by both Taiwanese and Chinese media outlets. Despite the report being quickly proved as false, it led to harsh criticism of Su, who committed suicide a week later (Ibid).

According to Aspinwall (2020), the incident was held up as "symbolic of the threat posed to Taiwan by Chinese influence operations," and was "widely cited by International media, and by Tsai herself." However, a court in Taiwan alleged that the real person behind the post was actually a Taiwanese university student, Slow Yang, a YouTuber and supporter of the Democratic Progressive Party, who apparently hired internet trolls to criticize Su's office (Ibid). Aspinwall argues that this event highlights the "well-known difficulties in determining the actual scope, intent, and efficacy of state influence," and that "while Beijing aggressively attempts to influence Taiwan's democratic institutions, most disinformation circulating through Taiwan's online ecosystem comes not from China but from within the country" (Ibid).

Despite these revelations, anger over Chinese influence led to a protest in June 2019 that called for the government to do more in disciplining so called "red media", and for more legislation requiring greater transparency in media funding and foreign connections (Taiwan Democracy Bulletin, 2019). The DPP has responded by pushing Taiwan's National Communications Commission to fight back against these accounts of fake news. The commission has reacted by imposing fines on individuals and news organization for spreading so called fake news and other security violations and has begun investigations against numerous news outlets (Aspinwall, 2020).

In December 2019, weeks before the presidential elections, viral and politically polarizing stories dominated election coverage: the first being the story of an alleged Chinese defector Wang "William" Liqiang, who gave a 60-minute interview to media outlets in Australia, in which he recounts working on disinformation efforts organized by the Chinese Communist Party. Wang professed to have meddled in the August 2018 elections in Taiwan by creating 200,000 fake social media accounts and 20 internet companies to attack the DPP online. Wand claimed that over 1.5 billion RMB was given to Taiwanese media companies to promote Han Kuo-yu's campaign for Kaohsiung mayor (Stanford Internet Observatory, 2019b). Also of significance in the lead up to the elections was Facebook's taking-down of 118 fan pages, 51 accounts, and 99 groups for inauthentic activity. One of the pages removed was 2020 韓國瑜總統後援會,one of the largest and extremely active pro-Han Kuo-Yu political fan groups (Ibid).

Similar to other countries around the world, Taiwan's media landscape has also been hit by the online spread of disinformation on the issue of COVID-19. Numerous posts on social media platforms (primarily Facebook) have spread false claims with regards for instance to the Taiwanese government's handling of the pandemic and the number of those infected in Taiwan. Due to the rise of misinformation, Taiwan's Special Act on COVID-19 Prevention, Relief, and Restoration passed in February 2020. The act stipulated that individuals who are found to have spread false information about COVID-19 that risks harming the public can face a maximum prison term of three years and a possible fine of 99,000$ USD (Taiwan Democracy Bulletin, 2020).

According to a briefing produced by the Ministry of Justice Investigation Bureau, more than 70% of the cases of disinformation related to COVID-19 since February have originated from China. The report noted that these were most likely spread by angry Chinese netziens who have used fake accounts to promote the narrative that the situation in Taiwan is much worse than stated by the Taiwanese government, with a view to promoting the competence of China (Focus Taiwan, 2020).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Taiwan

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
2014		Han Kuo-yu, Ko Wen-je, Sean Lian, KMT, DPP.	X	X	Kaohsiung Fan Group - 2020 韓國瑜總統後援會

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Cyber armies: A major theme of early computational propaganda in Taiwan is the use of Cyber army tactics: real persons who are hired to post opinions and comment during election campaigns. During the 2014 Taipei mayoral election, competing candidates Sean Lien and Ko Wen-je were both accused of using these tactics. These manual propagandists were mainly used on Taiwan's PTT platform and posted articles promoting a favourable view of Lien and a negative view on his opponent Ko Wen-je (Monaco 2017).

Crawler bots: During the same election, technical experts involved in Ko's campaign mentioned that crawler bots were used to crawl public pages on Facebook and collect data on users, likes, shares etc. This data allowed them to better understand who liked the candidates content and what content was most popular in order to better classify users into interest groups. Using this information, the campaign could then tailor content to each group. The campaign estimated that it was able to gather information on 11-14 million Taiwanese users on Facebook (Monaco, 2017).

Viral misinformation: As mentioned above, the spread of fake news online in Taiwan has become a major issue and is continuously growing (Monaco, 2017). Government officials in Taiwan have also taken part in spreading unverified information, as we have seen in the Kansai airport flooding story. Shortly after the incident, government officials claimed that the post was a malicious Chinese plant and President Tsai herself mentioned the incident in an interview as an example of fake news originating from China (Aspinwall, 2020).

In recent years YouTube has also become an increasingly important platform for the spread of disinformation in Taiwan. According to Wang Li-Jie, chief operating officer of Sola, a public opinion monitoring company that worked with Mayor Ko with his online campaign, "Taiwan has entered the video era in 2018" (Lin & Wu 2019). To increase his exposure, during the mayoral elections Han Kuo-yu, a relatively unknown member of the opposition Kuomintang party appeared on several talk shows and interviews during his campaign. This footage was subsequently used to produce short videos to be uploaded on Facebook fan pages, Line, and YouTube. The videos quickly extended their reach and went viral. A questionnaire distributed to Han Kuo-tu supporters showed that the key resources of information they used came from YouTube. According to Wang Tai-li, a professor in National Taiwan University, the short clips and re-edits of news videos helped present misleading narratives in the run-up to the election (Shu, 2020).

Content farms: Although content farms have been present in Taiwan for many years, their presence in the political realm has only become evident in recent years. According to a report produced by CommonWealth, content farms are "websites that directly use articles from other media or repackage them with sensational headlines to drive hits and leverage the higher traffic to get ads" (Lin & Wu, 2019). Internet analytics site "Page Board" suggests that out of Taiwan's 100 most influential fan pages, 23 were fan pages of content farm websites. According to Puma Shen, assistant professor at the national Taipei University's Graduate School of Criminology, people who manage content farm pages are largely motivated by money, while there are also some pro-China political parties that will also operate their own content farmers in Taiwan while in communication with China (Hioe, 2020). Shen also notes that because it has become more difficult to run content farms on Facebook, other systematic efforts to spread fake news, such as using Line or YouTube, have taken centre stage (Ibid).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Taiwan

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Real, fake	Pro party and anti-opposition, Collection of user data on users to classify users into interest groups and tailor campaign content to each group, Pro China.	Disinformation, Cyber armies, Crawler bots, Content farms	LINE, Facebook, PPT, YouTube

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Experts have noted that Taiwan's high exposure to disinformation has made it highly effective in analysing Chinese propaganda. Taiwanese citizens have become relatively aware of these influence campaigns and can for the most part spot the cultural and linguistic abnormalities in fake posts (Hioe, 2019). Protests against the influence of "red media" show that the Taiwanese public are willing to fight against these types of influence campaigns.

Taiwan's civil society has also been very proactive in efforts to combat disinformation. For example, the Youth Combatting Fake News Front, a coalition of over 100 student organizations, have worked to oppose unchecked facts, biased media, and Chinese disinformation (Taiwan Democracy Bulletin, 2019). One of the Front's campaigns focused around the slogan "take back the tv remote", in which students refused to watch news that disproportionality covered pro-China stories. Other initiatives from various groups and fact checking organizations include: the Fake News Cleaner that tries to break through online echo chambers and bridge generational gaps online by discussing health news rather than politics, using games, and designing messages that are appealing to elders; and Cofacts, a fact checking platform that created a bot that automatically replies to Line users who send suspicious links to it, on whether the article has been checked by the organization (Taiwan Democracy Bulletin, 2019).

References

Monaco, N. J. 2017. Working Paper No. 2017.2 Computational Propaganda in Taiwan: Where Digital Democracy Meets Automated Autocracy. *Computational Propaganda Research Project.* https://blogs.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Comprop-Taiwan.pdf

Lin, R., & Wu, F. 2019. Taiwan Caught in Online Opinion War. *CommonWealth.* https://english.cw.com.tw/article/article.action?id=2375.

Shu, C. 2020. Why the world must pay attention to the fight against disinformation and fake news in Taiwan. *Techcrunch*. https://techcrunch.com/2020/01/07/why-the-world-must-pay-attention-to-the-fight-against-disinformation-and-fake-news-in-taiwan/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAABdqACH90RkF2UeNS5ligE9CLXjRaMld7oaRT5BB6qpBvO9_CkGDTngbgP8b--DRKDGWY2v0LZu6m4xleAjhxwgWD2PtW9uT0XVIpwRWLCs8okM-t138kcZD8QdIMKyRITFeAzEiVViN5fc0eys8U_bmvhkBsN45Sv8L9t7F2PhW.

Stanford Internet Observatory. 2019. Taiwan: Presidential Election 2020 Scene Setter. *Stanford Internet Observatory*. https://cyber.fsi.stanford.edu/io/news/taiwan-presidential-election-2020-scene-setter.

Aspinwall, N. 2020. Taiwan’s War on Fake News Is Hitting the Wrong Targets. *Foreign Policy*. https://foreignpolicy.com/2020/01/10/taiwan-election-tsai-disinformation-china-war-fake-news-hitting-wrong-targets/.

Lee, Y., & Hamacher, F. 2019. Taiwan passes law to combat Chinese influence on politics. *Reuters.* https://www.reuters.com/article/us-taiwan-lawmaking/taiwan-passes-law-to-combat-chinese-influence-on-politics-idUSKBN1YZ0F6,

Taiwan Democracy Bulletin. 2019. TBD Vol. 3 No. 6: Defending Democracy Through Media Literacy. *Taiwan Democracy Bulletin.* https://bulletin.tfd.org.tw/tdb-vol-3-no-6-defending-democracy-through-media-literacy/.

Focus Taiwan. 2020. 70 percent of fake COVID-19 news from China: Investigation Bureau. *Focus Taiwan*. https://focustaiwan.tw/cross-strait/202004080010.

Taiwan Democracy Bulletin. 2o2o. TDB Vol. 4 No. 1: Taiwan’s Battle Against Rampant COVID-19 Disinformation. *Taiwan Democracy Bulletin.* https://bulletin.tfd.org.tw/tdb-vol-4-no-1-taiwans-battle-against-rampant-covid-19-disinformation/.

Stanford Internet Observatory. 2019b. Taiwan Election: The Final Countdown. *Stanford Internet Observatory*. https://cyber.fsi.stanford.edu/io/news/taiwan-election-final-countdown .

Hioe, B. 2020. Fighting fake news and disinformation in Taiwan: An interview with Puma Shen. New Bloom. https://newbloommag.net/2020/01/06/puma-shen-interview/.

TAJIKISTAN

Introduction

The Republic of Tajikistan has one of the most repressive media environments in the world, ranking 161st out of 180 countries in the World Press Freedom Index 2020 (Reporters Without Borders, 2020). This media environment, alongside pressure on opposition parties and electoral fraud, has led to a situation in which there has not yet been an election that has been judged free and fair (Putz, 2020). Parliamentary elections on 1st March 2020 delivered an expected victory to President Emomali Rahmon of the People's Democratic Party. This was the first election since the Supreme Court's decision in 2015 to designate the most prominent opposition group, the Islamic Renaissance Party of Tajikistan (IRPT), as a terrorist organisation (RFE/RL, 2020).

Accusations of social media manipulation are levelled and politicised by both the government and the opposition. The Institute of Economy and Trade of the Tajik State University of Commerce accused opposition groups, including the IRPT, of circulating fake information on social networks. It is claimed that propagandists within IRPT have sought to mislead public opinion, deceive people, and incite social conflicts (*Донишкадаи Иқтисод ва савдои Донишгоҳи давлатии тиҷорати Тоҷикистон*, 2018). In turn, Muhiddin Kabiri, the leader of the IRPT exiled in Europe, has accused the government of circulating fake news, stating that "the state budget is being used for a whole army of propagandists and for creating fake news" (Фергана, 2018b). Pro-government trolls have reported that Kabiri is the main target of harassment campaigns (RFE/RL, 2019). Despite the politicised nature of the allegations, reports do indicate that government-sponsored cyber troop activity persistently takes place, targeting journalists, critics, and activists.

An Overview of Cyber Troop Activity in Tajikistan

Organizational Form

Cyber troop activity is coordinated by government ministries but is carried out by both government agencies and citizens. Justice for Journalists (2020) notes that "law enforcement agencies have set up a troll farm". Reporters Without Borders (2020) state that "authorities…have created 'troll factories' to discredit critics". As early as the November 2013 elections, Abdufattoh Shafiev, a prominent Tajik blogger, said that the authorities had formed "special campaign groups to intimidate bloggers and activists" (Fayz, 2013). The Central Asian Bureau for Analytical Reporting (CABAR) report that anonymous comments in response to criticism of the government originates from 'reply-generating farms' ('fermai chavob') (Khalimov et al., 2019). This is not a completely novel practice in Tajikistan. In the printed media there is a legacy of the government using anonymous authors to produce replies to criticism of the authorities. Reply-generating farms are therefore just the latest tactic in the evolution of the tracking and rebuttal of criticism led by the state.

Unpaid citizens also participate in cyber troop activity. An investigation by Radio Free Liberty's Tajik service found that university students, officials and lecturers were being pressured by the state to serve as online trolls (RFE/RL, 2019). The investigation found that hundreds of people were recruited into "response factories", and subsequently set up multiple fake social media accounts to counter the "smear campaign" that the government claimed was being spread by the opposition. Orders for these response factories come from the Ministry of Education and Science, who in turn receive instruction from law enforcement agencies. Similarly, Justice for Journalists (2020) report that the Ministry of Internal Affairs or the State

Committee for National Security tasks the Ministry of Education and Science, which in turn assigns work to trolls -- typically university professors and teachers -- who initiate coordinated campaigns to discredit opponents. CABAR also alleges that pro-government support on the Internet is forced and unpaid, and often undertaken by students and state employees (Khalimov et al., 2019). Recently, derogatory pictures and memes criticising the government have been posted by fake accounts on Facebook, including personalised insults, calling certain individuals rats, thieves, and murderers. This illustrates that either the opposition is becoming bolder in confronting the government online, or that pro-government accounts are themselves establishing a smear campaign by imitating opposition activists with a view to discrediting them.

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Tajikistan

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
2013	Ministry of Education and Science, law enforcement agencies			Evidence Found (Unpaid university staff & students)	

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

The most prolific cyber troop technique in Tajikistan is the trolling and harassment of government opponents -- targeted towards journalists, critics, opposition politicians and activists. The tactics used to attack government critics depends on whether they live in Tajikistan or abroad. For critics that are in Tajikistan, trolls send direct messages to opponents and their families in an attempt to intimidate them and drive them out of the country. For critics who have left the country, they are trolled publicly as it is harder to intimidate them with physical threats. Much of Tajikistan's independent media has been eliminated, and journalists face harassment, intimidation, and blackmail from the intelligence services on a regular basis (LaHucik, 2019). Justice for Journalists (2020) found that attacks and threats online have become regular experiences for Tajik journalists. RFE/RL's sources have claimed that trolls were instructed to use any means, including bad language and fake photos, to attack government critics and activists. Instructions for harassment come from the government. Ahead of a livestream on Facebook and YouTube by Kabiri, the leader of the IRPT, trolls received a letter that called on individuals to be "active during the interview" and prepare questions and comments (RFE/RL, 2019). Anora Sarkorova, a Tajik journalist, explains that trolls work together by amplifying each other's comments and therefore raising negative messages to the top of comments sections. As a result, ordinary users become involved in the harassment by leaving comments or liking and further amplifying the top posts (ICHRP, 2020).

In February 2018, the Forum for Tajik Freethinkers (FTF) was founded by civil activists, led by Alim Sherzamonov, chief executive and deputy leader of opposition party National Alliance of Tajikistan. In an interview, Sherzamonov stated that websites under the State National Security Committee's control published negative comments about the FTF. The FTF website received a "large scale smear campaign", with attacks on the FTF's leadership coming from religious scholars (Ulema Council) and the government. Sherzamonov states that the FTF leadership “receive[s] threats regularly. For instance, they write to me on social media from fake accounts and threaten to punish my relatives” (Фергана, 2018a).

According to an article by exiled journalist Temur Varqi, critics of the regime are branded as terrorists and extremists -- including Salim Ayubzod, the head of Radio Liberty’s Tajik Service, Mirzo Salimpur, editor of independent news outlet Akhbor.com, and Esfandior Odina, head of the BBC’s bureau in Dushanbe. As such, they become legitimate targets for information attacks by the “trolls and moles of the government” (Ozodandishon, 2019). Varqi also says that there are fake opposition accounts that only mildly criticise the government but harshly condemn the opposition, attempting to divide critics and make the opposition fight amongst themselves. The article further suggests that attacks originate from outside of Tajikistan, which is supported by reports from Mahmuhdjon Saraev, of the Tajik presidential office’s information unit, who suggested that contentious issues were raised by people posting from outside Tajikistan (Rysaliev et al., 2012).

Online harassment has also been accompanied by physical attacks. Abdullo Gurbati, a journalist for independent media outlet Asia-Plus, was assaulted for his reporting on coronavirus. The reporter was required to receive hospital treatment following injuries sustained in the attack which followed an online smear campaign. Gurbati had been the target of a smear campaign by online trolls understood to operate at the behest of the security services. His coverage of coronavirus was followed by accusations that from government-linked online trolls that he is a traitor for receiving support from foreign opposition groups. One video uploaded to YouTube (2020) showed Gurbati’s face edited onto a depiction of coronavirus (Figure 1) (Eurasianet, 2020).

Humayra Bakhtiyar, a Tajik journalist, told the Committee to Protect Journalists that Tajik authorities had harassed and intimidated her family for years as retribution for her critical reporting. She detailed harassment that has included repeated threats made by pro-government trolls on social media and telephone calls (Committee to Protect Journalists, 2019). Content was also created to discredit Bakhtiyar, with photoshopped images, rumours about her family, and rumours of psychological issues all circulated to force her out of journalism (LaHucik, 2019). The campaign of harassment prompted her to move to Europe and seek asylum.

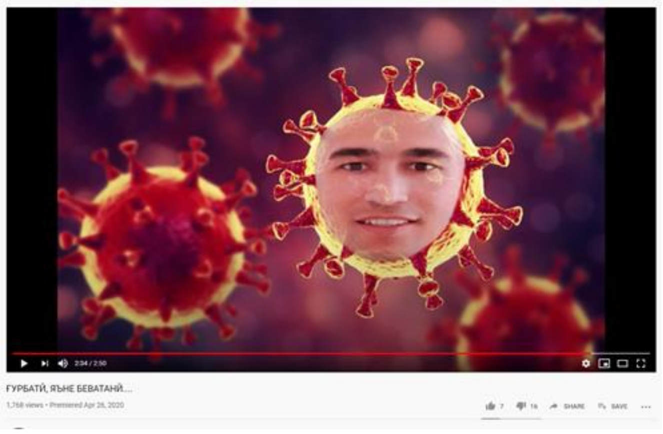

2:34 / 2:50
ҒУРБАТӢ, ЯЪНЕ БЕВАТАНӢ....
1,768 views • Premiered Apr 26, 2020
7
16
SHARE
SAVE

Figure 1: Trolling of a journalist in a video (YouTube, 2020)

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Tajikistan

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Human, Fake	Pro-Government messages, Attacks on Opposition, Trolling	Trolling, creation of disinformation	Facebook

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

The RFE/RL (2019) investigation found that trolls are provided no compensation, but that failure to comply could result in repercussions. It is estimated that there are around 400 such trolls across the country, each operating approximately 10 fake accounts. The recruits are divided into "information-analysis groups" which receives letters and instructions via email.

Table 3: Cyber Troop Capacity in Tajikistan

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
400		Permanent	Centralised	Medium

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

In response to disinformation in Tajikistan, fact-checking website Factcheck.tj debunks misleading and fake articles. The site stated that journalists could receive a stipend for carrying out fact-checks, as part of a project backed by the US embassy in Tajikistan (Gulov, 2018).

References

Asia-Plus. (2014, December 2). Academy of Sciences: IRPT is dangerous to society, like the Taliban and ISIS | Tajikistan News ASIA-Plus. https://asiaplustj.info/ru/news/tajikistan/politics/20141202/199300

Committee to Protect Journalists. (2019, July 18). Tajik authorities harass journalist Humayra Bakhtiyar and family. Committee to Protect Journalists. https://cpj.org/2019/07/tajik-authorities-harass-journalist-humayra-bakhti/

Eurasianet. (2020, May 11). Tajikistan: Reporter for independent newspaper assaulted. https://eurasianet.org/tajikistan-reporter-for-independent-newspaper-assaulted

Fayz, K. (2013, November 6). Tajik polls get social media lift. BBC News. https://www.bbc.com/news/world-asia-24758883

Gulov, R. (2018, September 13). Журналисты Таджикистана могут получить стипендии за проведение фактчекинга—Factcheck.TJ. https://factcheck.tj/ru/2018/09/13/zhurnalisty-tadzhikistana-mogut-poluchit-stipendii-za-provedenie-faktchekinga/

ICHRP. (2020, January). International Ratings of Tajikistan in the field of freedom of expression. Independent Center for the Protection of Human Rights. http://ichrptj.org/ru/blog/obzor-smi-noyabr-dekabr-2019-g-yanvar-2020-g

Justice for Journalists. (2020). Attacks on journalists, bloggers and media workers in Central Asia and Azerbaijan (2017-2019). https://jfj.fund/attacks-on-journalists-bloggers-and-media-workers-in-central-asia-and-azerbaijan-2017-2019/

Khalimov, Y., Dzhamolov, I., Mamadikimzosa, N., Anarbaev, B., & Zamirbekova, A. (2019, November 26). “Reply-generating Farm”, Nur-fans and Trolls. How Bots Work in Central Asian States? CABAR.Asia. https://cabar.asia/en/reply-generating-farm-nur-fans-and-trolls-how-bots-work-in-central-asian-states/

khoruq.tj. (2019). Бобокалони дурӯғгӯён-Мирзо Салимпур (Ҷавоб ба музахрафоти журналисти фирорӣ)—Мақомоти иҷроияи ҳокимияти давлатии шаҳри Хоруғ. http://khoruq.tj/index.php/cokhtori-davlat/muovinoni-rais/77-khabarho/315-bobokaloni-dur-g-jon-mirzo-salimpur-avob-ba-muzakhrafoti-zhurnalisti-firor

LaHucik, K. (2019, June 20). Project Exile: Tajikistan harasses reporter into exile. Global Journalist. https://globaljournalist.org/2019/06/project-exile-tajikistan-harasses-reporter-into-exile/

Ozodandishon. (2019, May 11). ВНИМАНИЕ: Фейковые оппоненты Рахмона в Европе (1). Анҷумани Озодандешони Тоҷик. https://ozodandishon.org/2019/05/11/%d0%b2%d0%bd%d0%b8%d0%bc%d0%b0%d0%bd%d0%b8%d0%b5-%d1%84%d0%b5%d0%b9%d0%ba%d0%be%d0%b2%d1%8b%d0%b5-%d0%be%d0%bf%d0%bf%d0%be%d0%bd%d0%b5%d0%bd%d1%82%d1%8b-%d1%80%d0%b0%d1%85%d0%bc%d0%be%d0%bd%d0%b0/

Putz, C. (2020, March 3). Tajik ‘Election’ Delivers Expected Result. https://thediplomat.com/2020/03/tajik-election-delivers-expected-result/

Reporters Without Borders. (2020). Tajikistan: Praising the “Leader of the Nation”. RSF. https://rsf.org/en/tajikistan

RFE/RL. (2019, May 12). Tajik Students, Educators Claim They’re Pressured To ‘Troll’ Government Critics. RadioFreeEurope/RadioLiberty. https://www.rferl.org/a/tajik-students-educators-claim-they-re-pressured-to-troll-government-critics/29936072.html

RFE/RL. (2020, February 28). No Debate, No Competition, No Surprises: It’s A Tajik Election. RadioFreeEurope/RadioLiberty. https://www.rferl.org/a/no-debate-no-competition-no-surprises--its-a-tajik-election/30460217.html

Rysaliev, A., Tokbaeva, D., & Olimova, L. (2012, February 12). Central Asia’s ‘Troll Wars’. Institute for War and Peace Reporting. https://iwpr.net/global-voices/central-asias-troll-wars

YouTube. (2020, April 26). ҒУРБАТӢ, ЯЪНЕ БЕВАТАНӢ.... https://www.youtube.com/watch?v=U9IuMTDytOQ&feature=youtu.be&fbclid=IwAR32ChPoBrI42IigkItH3lDN5WIRtW6TNPvunRM2SSiOu30YNnqWBalf7Zk&app=desktop

Фергана. (2018a, March 2). Без претензии на власть. Новое объединение таджикских эмигрантов предложило Рахмону сотрудничество. Фергана.Ру. http://www.fergananews.com//articles/9830

Фергана. (2018b, September 18). Мухиддин Кабири: «Таджикистан должен быть светским государством». Фергана.Ру. http://www.fergananews.com//articles/10181

TUNISIA

Introduction

Tunisia is considered the only country to have not returned to authoritarianism or widespread violence following the 2011 Arab Spring. Facebook is claimed to have played a role in mobilising the population to oust autocrat President Ben Ali on 14 January 2011—and it remains the most popular platform in Tunisia—with 66% of the population using Facebook compared to only 3% who use Twitter (Elswah & Howard, 2020).

Social media is used for political communication and engagement by Tunisian politicians, parties, and institutions, but it has also become a platform to spread disinformation and manipulate public opinion (Gibaja, 2019). In 2019, this was particularly prevalent in the context of two rounds of presidential elections (15 September and 13 October) and one round of legislative elections (6 October). Observers noted that mis- and disinformation were prevalent before and during the election period. Further, platform suspensions on Facebook and Instagram in June 2020 revealed a foreign interference campaign originating in Tunisia and targeting Francophone countries in Sub-Saharan Africa (Facebook, 2020).

An Overview of Cyber Troop Activity in Tunisia

Organizational Form

Harassment of activists and censorship of social media were attributed to the state-run Agence Tunisienne d'Internet (ATI) in the context of the 2011 protests. Khaled Koubaa, president of the Internet Society in Tunisia, said that the Tunisian authorities attempted to harass people posting on Facebook prior to the ousting of Ben Ali. As protests began, the head of the ATI said the number of websites blocked by the regime doubled in a few weeks (Reporters Without Borders, 2011). More than one hundred Facebook pages about the protests in Sidi Bouzid were blocked, as well as photo and video sharing sites Flickr, YouTube, Dailymotion, and Vimeo. The Committee to Protect Journalists (CPJ) noted that news websites, critical pages and blogs, and email accounts had been blocked by the ATI (Anderson, 2011). Access to Facebook was allowed; however, Koubaa said that "if they became aware of you on Facebook, they would try to divert your account to a fake login page to steal your password" (Beaumont, 2011). It was reported by the CPJ that this tactic was used to log into activists' Facebook accounts to delete groups, pages, and accounts (Anderson, 2011).

In the context of the 2019 elections, political parties and candidates maintained affiliated Facebook groups and pages to communicate with the electorate, amassing substantial numbers of followers (Advox, 2019). However, it was the unaffiliated pages (without declared ties to parties or candidates) that were most problematic as they were spreading political disinformation and using sponsored content to praise certain parties. It is suggested that there was a degree of coordination or single administrator as there were "patterns of systematic posting of identical political content between pages" (Democracy Reporting International, 2020).

Mona Elswah, a researcher at the Computational Propaganda Project, interviewed civil society organisations in Tunisia and found that "Facebook was used extensively for political campaigning by undeclared political actors" and that this was largely "unmonitored by observation agencies" during the 2019 elections (Elswah & Howard, 2020). Three fact-checking initiatives were created to monitor the elections, but the lack of fact-checking organisations still remained one of the issues facing Tunisia. Initiatives with the capacity to run projects monitoring social media were I Watch, The Tunisian Association for the Integrity and Democracy of Elections (ATIDE) in partnership with Democracy Reporting International, and Mourakiboun (Elswah & Howard, 2020). One organisation, 'Fake News Checking', was run by a group of journalists including Tunisian journalist Moëz Bhar. The Digital Forensic Research Lab noted that despite presenting itself as neutral, Bhar is openly political and in favour of presidential candidate Karoui, raising questions around the true level of neutrality of this organisation (DFRLab, 2019).

In June 2020, Facebook announced it had removed 446 pages, 182 accounts, 96 groups, 60 events and 209 Instagram accounts for 'coordinated inauthentic behaviour' on behalf of a foreign government entity. Fake accounts masqueraded as locals in targeted countries, posting in French about "tourism, diaspora engagement, politics, candidates and elections in countries across Francophone Africa and Tunisia, and…combating the coronavirus pandemic in the region". The accounts accumulated 3.8 million followers on one or more of these pages, and cumulatively spent US$331,000 on ads. Facebook attributed this activity to Tunisian-based PR firm Ureputation (Facebook, 2020).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Tunisia

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
2011	ATI	Evidence Found	Archimedes Group, Ureputation		

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Disinformation

Disinformation was spread throughout the country ahead of the 2019 autumn elections (Freedom House, 2019). This has taken the form of fake polling, forged electoral posters and the spread of unfounded rumours (DFRLab, 2019). For example, on election day in the first round there were fake rumours that one legislative candidate, Olfa Terras, had been arrested while canvassing citizens (Jouini, 2019). This has been exacerbated by the lack of fact-checking expertise and civil society organisations to monitor social media campaigning (Elswah & Howard, 2020).

The most prominent disinformation tactic was the use of Facebook pages that did not have explicit affiliations to candidates or parties. These pages tended to post negative content, disinformation, and polarising content. Democracy Reporting International's (2020) monitoring of social media campaigning with ATIDE during the 2019 elections found that of 291 public Facebook pages identified as having a "high level of political engagement," 40% were not transparent about their affiliation, ownership, or purpose. Unaffiliated pages produced 38.5% of political messaging in the period 15 May to 15 July 2019; with pages that were classified as entertainment or satirical sharing overtly political content (Jouini, 2019). Following the election, part of this campaigning was erased, and some Facebook pages deleted entirely, further suggesting coordinated manipulation (Democracy Reporting International, 2020).

To combat disinformation, the Independent High Authority for Audiovisual Communication (HAICA) developed a digital platform to fight against the proliferation of disinformation in the election period, in addition to training a network of hundreds of journalists in fact-checking (TAP, 2019).

Harassment

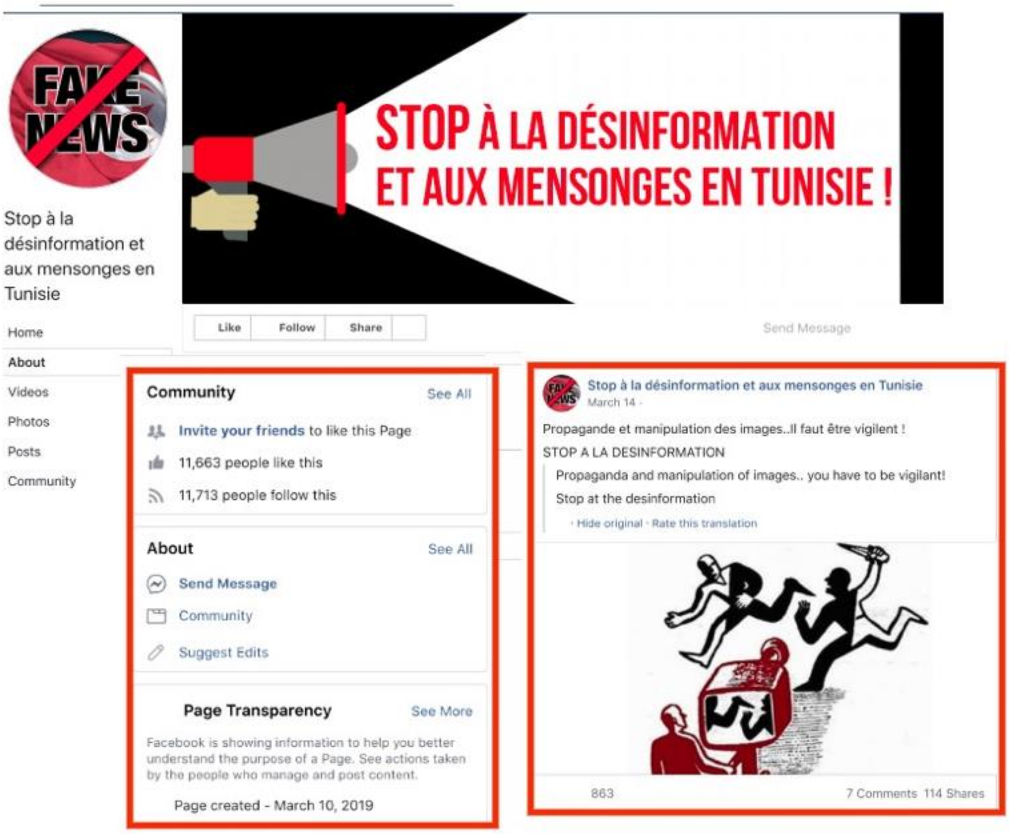
There is evidence of harassment during the build-up to the election, with the presence of "orchestrated campaigns on Facebook to discredit candidates and spread hate speech" (Elswah & Howard, 2020). Unofficial pages ignored electoral regulations, "spreading defamation and disinformation" (Democracy Reporting International, 2020). Meshkal (2019), a Tunisian news website, found that there had not been serious violations of hate speech, but they had seen an increase in "vitriolic language" and regional discrimination (i.e. inter-regional discriminatory comments).

Fake Polling

In May 2019, a fabricated opinion poll circulated claiming that Nabil Karoui was the favoured candidate (Freedom House, 2019). The poll was shared widely on Facebook, Facebook Messenger, and WhatsApp. A legitimate polling company, Sigma, was named on the fake poll—leading to the company's director, Hassen Zargouni, publicly denouncing the poll as fake on Facebook (Jouini, 2019).

Private Contractors

Tunisia was the target of Israeli-based 'coordinated inauthentic behaviour' attributed to the company Archimedes Group by Facebook in May 2019 (Gleicher, 2019b). Archimedes Group is an Israeli cyber influence group operating political campaigns across Africa, and their website claims of 'winning campaigns worldwide' (Bin Hammadi & Al-Khadrawi, 2019). Inkyfada, an investigative website, found that Archimedes Group created eleven pages targeting Tunisia between 17 January and 12 March 2019, accruing 500,000 followers. This campaign both supported and attacked the government, published diverse content targeting multiple parties, and utilised paid advertisements to amplify content (Bin Hammadi & Al-Khadrawi, 2019). Despite being critical of many politicians, the pages did not critique presidential candidate Nabil Karoui, and five pages shared content from Karoui's channel Nessma TV (Jouini, 2019). One suspended page was 'Stop à la désinformation et aux mensonges en Tunisie' which, despite translating to 'Stop disinformation and lies in Tunisia,' propagated disinformation under the guise of fact-checking (*figure 1*) (DFRLab, 2019).



Stop à la désinformation et aux mensonges en Tunisie

Home
About
Videos
Photos
Posts
Community

Like Follow Share

Send Message

Community See All

Invite your friends to like this Page

11,663 people like this

11,713 people follow this

About See All

Send Message

Community

Suggest Edits

Page Transparency See More

Facebook is showing information to help you better understand the purpose of a Page. See actions taken by the people who manage and post content.

Page created - March 10, 2019

Stop à la désinformation et aux mensonges en Tunisie
March 14 ·

Propagande et manipulation des images..Il faut être vigilent !
STOP A LA DESINFORMATION

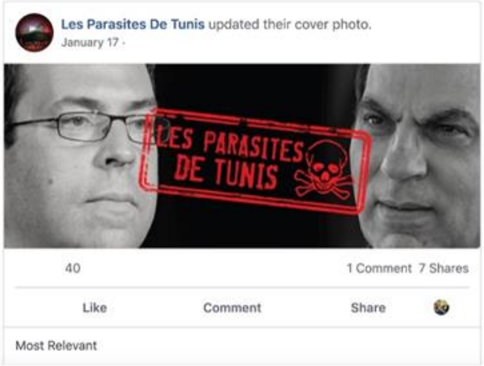
Propaganda and manipulation of images.. you have to be vigilant!
Stop at the desinformation

· Hide original · Rate this translation

863 7 Comments 114 Shares

Figure 1: Fake fact-checking page targeting Tunisia (DFRLab, 2019)

Another suspended page was ‘Les Parasites de Tunis’ (The Parasites of Tunis), which was managed by five administrators in Tunisia and posted content concerning the corruption of government (Bin Hammadi & Al-Khadrawi, 2019). The page’s forty-four posts gained 167,000 interactions (likes, comments, shares). *Figure 2* depicts the page’s cover photo, which shows the current prime minister Youssef El-Shahid and ousted former president Ben Ali.



Les Parasites De Tunis updated their cover photo.
January 17 ·

40 1 Comment 7 Shares

Like Comment Share

Most Relevant

Figure 2: Anti-government Facebook page (Inkyfada, 2019)

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Tunisia

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Fake accounts	Pro-candidate messaging, attacks on opposition candidates, polarising messaging, trolling	Disinformation, Amplifying Content, Trolling, Facebook Ads Expenditure	Facebook, Instagram

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

Civil society organizations have raised concerns about legal and technical obstacles that have obstructed effective social media monitoring. The Tunisian legal system has been critiqued for insufficient data privacy and electoral regulations for a democratic society in the digital age (Elswah & Howard, 2020). And criticisms have been levelled at social media platforms, particularly Facebook, over the lack of transparency regarding political and electoral ads.

Access Now (2019), a digital rights organization, alongside 14 Tunisian civil society organizations wrote an open letter to Facebook requesting that "effective measures for "transparency and accountability" were put in place for users in Tunisia ahead of the election. The letter notes that transparency measures have been implemented in many countries such as the United States and Canada but not globally. As a result, civil society organizations were unable to monitor the amount spent on campaign ads, the demographic targeting of ads, the location and identity of the sponsors of content, or ad metrics (Access Now, 2019).

Table 3: Cyber Troop Capacity in Tunisia

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
	Evidence of Facebook Ads spending, $331,000 by Ureputation	Increase from January-October 2019 (elections)	Somewhat centralised	Low

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

In the context of the global COVID-19 pandemic, *News Tunisia* reported that the Tunisian health ministry had warned of fake Facebook pages that were created to promote rumours and misinformation regarding the crisis (Hana, 2020). A member of parliament, Al-Mabrouk Karsheed, proposed a draft law on 12 March to combat disinformation on the grounds of fighting 'fake news' and controlling social media's impact on national security. Within hours of the announcement there was a wave of criticism on social media, and the MP withdrew the bill (Samaro, 2020).

Facebook's removal of accounts for coordinated inauthentic behaviour has revealed foreign influence campaigns targeting Tunisia. In January 2019, 783 pages, groups and accounts were removed for ties to Iran, targeting multiple countries including Tunisia (Gleicher, 2019a). Likewise, in October 2019, a network of accounts, pages and groups were suspended originated in Egypt, targeting countries across the Middle East and North Africa including Tunisia (Gleicher, 2019c).

References

Access Now. (2019, September 2). Open letter to Facebook on the upcoming Tunisian elections of 2019. *Access Now*. https://www.accessnow.org/open-letter-to-facebook-regarding-the-upcoming-tunisian-elections-of-2019/

Advox. (2019, December 9). *Multiple measures failed to control mis- and disinformation in Tunisia's 2019 elections—Global Voices Advox*. https://advox.globalvoices.org/2019/12/09/multiple-measures-failed-to-control-mis-and-disinformation-in-tunisias-2019-elections/

Anderson, N. (2011, January 15). Tweeting Tyrants Out of Tunisia: Global Internet at Its Best. *Wired*. https://www.wired.com/2011/01/tunisia/

Beaumont, P. (2011, February 25). The truth about Twitter, Facebook and the uprisings in the Arab world. *The Guardian*. https://www.theguardian.com/world/2011/feb/25/twitter-facebook-uprisings-arab-libya

Bin Hammadi, M., & Al-Khadrawi, M. (2019). من المستفيد من مضامين صفحات الفايسبوك التونسية المرتبطة بإسرائيل؟. Inkyfada. https://inkyfada.com/ar/2019/06/19/من-المستفيد-من-مضامين-صفحات-الفايسبوك/

Democracy Reporting International. (2020). *Report: Monitoring Tunisia's election campaigns on social media — what the watchdog did not see*. https://democracy-reporting.org/dri_publications/monitoring-election-campaigns-on-social-media-in-tunisia-what-the-watchdog-did-not-see/

DFRLab. (2019, October 11). *Sorting fact from fiction in Tunisia's presidential election*. Medium. https://medium.com/dfrlab/sorting-fact-from-fiction-in-tunisias-presidential-election-862bcc05bdaf

Elswah, M., & Howard, P. N. (2020). *The Challenges of Monitoring Social Media in the Arab World: The Case of the 2019 Tunisian Elections* (Data Memo 2020.1; The Computational Propaganda Project). https://comprop.oii.ox.ac.uk/research/tunisia-election-memo/

Facebook. (2020, June 5). May 2020 Coordinated Inauthentic Behavior Report. *Facebook Newsroom*. https://about.fb.com/news/2020/06/may-cib-report/

Freedom House. (2019). *Freedom on the Net | Tunisia*. Freedom House. https://freedomhouse.org/country/tunisia/freedom-net/2019

Gibaja, A. F. (2019, May 10). *Protecting Tunisian elections from digital threats | International IDEA*. International IDEA. https://www.idea.int/news-media/news/protecting-tunisian-elections-digital-threats

Gleicher, N. (2019a, January 31). Removing Coordinated Inauthentic Behavior From Iran. *About Facebook*. https://about.fb.com/news/2019/01/removing-cib-iran/

Gleicher, N. (2019b, May 16). Removing Coordinated Inauthentic Behavior From Israel. *About Facebook*. https://about.fb.com/news/2019/05/removing-coordinated-inauthentic-behavior-from-israel/

Gleicher, N. (2019c, October 3). Removing Coordinated Inauthentic Behavior in UAE, Nigeria, Indonesia and Egypt. *About Facebook*. https://about.fb.com/news/2019/10/removing-coordinated-inauthentic-behavior-in-uae-nigeria-indonesia-and-egypt/

Hana, R. (2020, March 29). Tunisia-Health ministry warns of fake news and information. *Tunisia - News in Tunisia and the world*. https://news-tunisia.tunisienumerique.com/tunisia-health-ministry-warns-of-fake-news-and-information/

Jouini, Y. (2019, October 22). Ahead of Tunisia elections, social media was flooded with mis- and disinformation. *Advox Global Voices Advocacy*. https://advox.globalvoices.org/2019/10/22/ahead-of-tunisia-elections-social-media-was-flooded-with-mis-and-disinformation/

Meshkal. (2019, September 5). *Fears over Facebook's Role in Election Campaign*. http://mesh-kal.com/2019/09/05/fears-over-facebooks-role-in-election-campaign/

Reporters Without Borders. (2011, March 11). *Internet Enemies 2011: Countries under surveillance—Tunisia*. Refworld. https://www.refworld.org/docid/4d822684c.html

Samaro, D. (2020, April 1). Tunisia's Parliament on COVID-19: An initiative to fight disinformation or an opportunity to violate fundamental rights? *Access Now*. https://www.accessnow.org/tunisias-parliament-on-covid-19-an-initiative-to-fight-disinformation-or-an-opportunity-to-violate-fundamental-rights/

TAP. (2019, August 3). Digital platform to fight fake news will be tested next week (HAICA). *Agence Tunis Afrique Presse*. http://www.tap.info.tn/en/Portal-Politics/11699752-digital-platform-to

Turkey

Introduction

Turkey continues to experience increasing efforts in computational propaganda. It has been an important year for Turkey, including municipal elections on March 2019; economic turmoil fueled with conspiracy theories; invasion of Northern Syria; cyber clashes with various countries; the emergence of Coronavirus; and intervention in the Libya Civil War with deployment of Turkish ground troops. The country's state of emergency ended in July 2018, which had been in place since an attempted coup in July 2016. The state of emergency resulted in weakened parliamentary and constitutional checks on executive decrees issued by President Erdoğan and his cabinet. One such decree, passed in August 2017, was Decree No.671 which amended the Law on Digital Communications to authorize the government to take "any necessary measure" on the grounds of "national security, public order, prevention of crime" and obliging telecommunications' providers to enforce government orders within 2 hours of receipt (Freedom House, 2018). While this has been applied as a means of repression, it has also been used positively, such as to enable security agencies to crack down on Islamic State communications.

Social media monitoring continues to increase after the July 2016 coup attempt. Turkey's General Directorate of Security, the high command of the country's police, officially asked the public to report any social media account that praised the coup or had a "criminal element," and set up hotlines to deal with citizens' reports of "terror propaganda" (Freedom House, 2018). There has been evidence of particular topics being monitored and banned on social media within the country. For example, evidence has been found that the social media platform TikTok has incorporated Turkey-specific guidelines that explicitly ban content related to Kurdish separatism, and added political figures, such as the president, Recep Tayyip Erdoğan, to the list of people who cannot be criticized or defamed (The Verge 2019). Additionally, in an attempt to control the narrative surrounding the current economic turmoil, it has been reported that over 30 individuals are being tried for social media comments regarding the decline of the Turkish Lira. Various journalists and academics with online presence have been detained as well (Middle East Eye 2019). More recently, the government has reportedly detained over 60 individuals for the spread of "fake and provocative" news about the Coronavirus on social media (Balkan Insight 2020).

An Overview of Cyber Troop Activity in Turkey.

Organizational Form

Turkish computational propaganda efforts have increased following the country's military invasion of Northern Syria, and its intervention in the Libyan Civil war. Following the 'Occupy Gezi Park Protests' in 2013, the ruling AKP government launched a massive project to boost the party's social media presence. In September 2013, the AKP recruited a new social media team, known as the 'New Turkey Digital Office', responsible for converting AKP sentiments into trending hashtags, and engaging in abusive behavior against journalists and civil society movements (Guardian 2016).

Leaked emails of Erdogan's son in law, Treasury and Finance Minister Berat Albayrak in October 2016 revealed government discussion of "a team of professional graphic designers, coders, and former army officials who received training in psychological warfare" to complete tasks related to counter critical narratives and weaken protest movements on social media

(Freedom House, 2019). Additionally, in 2016, the emails revealed a coordinated anti-Western campaign on YouTube to smear critics and fuel anti-Western sentiment in Turkey (Ibid). Berat Albayrak has also been acknowledged as head of heavily influential media group called the Pelican Group who have been considered by various journalists in Turkey as "Erdogans Troll Army", that mostly works on trying to spread disinformation and slander political opponents on social media (Ahval 2020). Erdogan's office has allegedly paid and coordinated an online army of 12,000 Twitter users, financed by a private advertising agency (Nordic Monitor 2019).

Turkey also launched the Directorate of Communications in 2018. Working directly under the presidency. Fahrettin Altun, Communications Director of the Turkish Presidency, announced that the Directorate will be "at the heart of national and global narrative, consensus, insight and interpretation" and stating their main goal is "to expand the framework of effective communication between the nation and the state based on technology" (Altun, 2018).

The AKP is not the only political party in Turkey using online propaganda. In the build-up to the 2018 elections, the *Hürriyet* daily newspaper reported that opposition İYİ ('Good') Party started a Google Ads' campaign for several keywords targeting the AKP. A Google search for 'vacant rooms' took users to the İYİ election vow to open Erdoğan's palace to the public, and 'VPN' led to the phrase "for Internet freedoms, wait until we come to power" (Hurriyet, 2018).

Non-government actors that support government policy are also active in propaganda efforts. A hacking collective called Ayyildiz Tim (the 'Turkish Cyber Army') has increasingly peddled pro-government messages on Twitter through hacking prominent figures' accounts. There are multiple 'Turkish Cyber Army' groups and these are active on social media (Figure 32) (Haberturk, 2017). While there is no immediate evidence that the group is a Turkish government organization, they are strong supporters of the government. The Turkish government launched an official cyber army to defend against cyber threats. In April 2017, the Ministry of Interior and Information Technologies Directorate jointly announced the establishment of a 500-strong cyber army (Haberturk, 2017).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Turkey

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
	X	x	X		x

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Automated coordinated inauthentic behavior:

Bots: In 2017 news sources reported a centralized botnet influencing trending hashtags in two ways: (1) astroturfing (by first boosting a pro-government hashtag), and (2) poisoning (flooding the hashtag with inflammatory content to shade its original message). This was visible in the opposition's hashtag, #DemirtaşıÇokÖzledik ("We missed Demirtaş a lot") campaigning on behalf of the jailed pro-Kurdish Peoples' Democratic Party leader, Selahattin Demirtaş, when bots boosted counter-messages to demoralize his supporters (Sozeri, 2017). Similarly, following the 'Gas for Gold' corruption scandal in late 2013, AKP Trolls adopted 'cyber lynch mob' tactics to silence opposition (Okun, 2017).

There is evidence that some of these Twitter followings have been created organically. Twitter accounts with large follower bases can suddenly be repurposed, such as in the case of the 2015 elections in which "an account with a 'sexy girl profile picture' suddenly changed its name and brand to launch a smear campaign using its 42,000 followers" against the election monitoring group 'Vote and Beyond' (Sozeri, 2015). Similarly, an account under the name 'irem_cevikk' became 'Vote and Fraud'. This fake account used content amplification strategies, using a follower-boosting Twitter application which automated a follow-back system. Another pro-Erdoğan account had 182,000 followers but only nine tweets, and one-month prior had been posting jokes to gain followers (Sozeri, 2015). Bloomberg reported that researchers had found a collection of nearly 18,000 pro-Erdoğan Twitter accounts that used profile pictures taken from pornography sites or public figures such as American actress Megan Fox to gain followers.

Results from the Atlantic Council's Digital Forensic Lad (DFRLab) found that Turkey's invasion of Northern Syria was accompanied by a coordinated social media campaign led by bot-like accounts that promoted pro-government and anti-Kurdish content and hashtags. Some of these accounts tweeted hundreds of tweets within a few hours, and some had alphanumerical handles and no profile pictures, which indicates the use of automation software. Many of these accounts were created in September and October 2019 (the military operation began on October 9th), with large groups of accounts created in the same day. Intrestingly, the most common account creation date was October 10th, a day after the operation began and the day the trending hashtag #BabyKillerPKK (an anti-PKK hashtag) began trending. Many of these accounts almost exclusively tweeted content with that or related hashtags, which indicates that their creation was likely aimed at boosting this particular campaign (Medium 2019).

Disinformation: Leading up to Istanbul's second municipal election in 2019 (after the results of the first were annulled by the government), misleading videos of the opposition candidate began to spread by numerous pro-government accounts, allegedly coordinated by members of the ruling party (Ahval 2019).

Phishing and Hacking: Since summer 2017, the "Turkish Cyber Army" has focused on Twitter phishing to compromise accounts and, upon gaining access, has made pro-Turkish posts, downloaded message history, and sent new phishing attacks. The group has even managed to direct-message US President Donald Trump on Twitter, after having gained access to the Twitter account of the head of the World Economic Forum, Børge Brende, who is followed by Trump. After an account is hacked, its Twitter bio would typically read: "Your account has been hacked by the Turkish cyber army Ayyildiz Tim. Your DM correspondence and important data have been captured!". Chuka Umunna, a British Member of Parliament, was hacked in March 2018, with his compromised Twitter account posting references to the Turkish military operation in Syria (Figure 33) (Evening Standard, 2018). While there is no immediate evidence that the group is a Turkish government organization, they are strong supporters of the government. More recently, cyber-attacks against at least 30 organizations in Europe and the Middle East, involving the intercepting of internet traffic to victim websites, according to British officials and one U.S official, bear the hallmarks of a state backed cyber espionage operation conducted to advance Turkish interests (Stubbs et al. 2020).

Fact-checking organizations have been founded in response to the manipulation of social media, tasked with attempting to combat disinformation. Mehmet Atakan Foca, the editor-in-chief of

Teyit.org (Turkish for 'confirmation') said that the organization receives 25 to 30 reports of suspicious messages, images, and videos every day (Edroos, 2018). A BBC report (2018) found that even fact-checking itself is being used as a tool to sow mistrust and division. One website that claims to be an independent verifier of news but is in fact run by a prominent columnist for Sabah, the main pro-government daily. 'Factcheckingturkey.com' is an English-language fact-checking site that aims to check foreign media coverage of Turkish news (Figure 34). The website was founded under the claim that Turkey was being "represented as yet another dictatorship" in the foreign media (Politico, 2019). This tendency extends outside Turkey too – for example 'factcheckarmenia.com' denies the Armenian Genocide of 1915, and is active in the United States but tied to Turkish government-affiliated organizations. More recently, state funded news agency "Anadolu Agency" has launched a "fact-checking" campaign against "disinformation" regarding Turkey's military offensive into northern Syria (BBC monitor 2019).

Harassment and repression: Online propaganda and repression also support Turkish military policy. In January 2018, there was a wave of arrests in response to the critiques of 'Operation Olive Branch', a Turkish military operation in Afrin, Syria. Turkey asked social media sites, such as Facebook and Twitter, to take down posts that criticized the operation. The Turkish Interior Ministry claimed that they detained 648 people between 20 January and 26 February 2018 over social media posts criticizing the military operation (Human Rights Watch, 2018). People were arrested for "posting information on social media from local sources in Afrin that contained alternative rhetoric to that of the government". Journalist Nedim Turfent, who was reporting on counterterrorism in Turkey's Kurdish region, published a video of soldiers standing over villagers who were face down with their hands bound. Messages seeking Turfent's whereabouts began to appear on his Facebook page and Twitter accounts linked to Turkish counterterror units began to taunt locals with "Where is Nedim Turfent?". Within days, Turfent was detained by the military and charged with membership of a terrorist organization (Bloomberg, 2018).

Online harassment and repression targets Turkish journalists. In 2019, Reporters Without Borders ranked Turkey at 157 out of 180 countries, down from 151 a year earlier, in their Press Freedom Index (reporters without borders 2019). news is prolific, with the Reuters Institute's 2017 report finding that 49% of Turkish people had been exposed to 'fake news' within the previous week, and 38% said they did not trust the news (Reuters Institute, 2017). Individual targeting of journalists often consists of accusations of being a "traitor", a "terrorist", or a "terrorist supporter". 2,000 cases of online abuse, death threats, threats of physical violence, sexual abuse, smear campaigns and hacking have been reported, as part of an AKP campaign to intimidate journalists. Trolling was turned into real lynching in 2016, when the *Hürriyet* newspaper building was attacked by protesters. Female journalists are most often targeted by hundreds of trolls with sexual-related insults, such as the case of Nevsin Mengu, a popular CNN-Turk anchorwoman who was forced out of her job following her coverage of the 2016 coup attempt (Institute for the Future, 2018).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Turkey

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms

Bots, Human, Hacked	Pro government messages, Attacks on Opposition, smear campaigns, suppressing participation, manipulating online conversations, counter critical narratives and weaken protest movements on social media, drive particular agendas.	Manipulated Media, doctored videos, disinformation, hacking, phishing, Amplifying content, harassment	Twitter, YouTube

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

The social media project launched by the government in 2013 hired over 6,000 new employees for its newly formed social media team to counter anti-Erdoğan opinions (Guardian, 2016). The pro-AKP *Star* reported that there would be AKP social media representatives in over 900 districts and 1,000 staff located in Istanbul, 600 in Ankara, and 400 in Izmir (Ibid).

Table 3: Cyber Troop Capacity in Turkey

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
6000, 12,000 Twitter users				

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

References

Ahval News. 2019. CHP's İmamoğlu blasts disinformation campaign against him, refers to Pelican group. *Ahval News*. https://ahvalnews-com.cdn.ampproject.org/c/s/ahvalnews.com/ekrem- imamoglu/chps-imamoglu-blasts-disinformation-campaign-against-him-refers-pelican- group?amp

DFRLab. 2019. Bot-Like Turkish accounts complement military operation in Syria. *Medium.* https://medium.com/dfrlab/bot-like-turkish-accounts-wage-anti-kurdish-hashtag-campaign- 9b1a2908f5b3

Freedom House. Freedom of the Net: Turkey. *Freedom House.* https://freedomhouse.org/country/turkey/freedom-net/2019

Newton, C. 2019. More and more countries are mounting disinformation campaigns online. The Verge. https://www.theverge.com/2019/9/27/20885837/misinformation-state-sponsored-oxford- university-study.

Nordic Monitor. 2019. Turkey undermines NATO cyber-army initiative. *Nordic Monitor*. https://www.nordicmonitor.com/2019/09/turkey-undermines-nato-cyber-army-initiative/

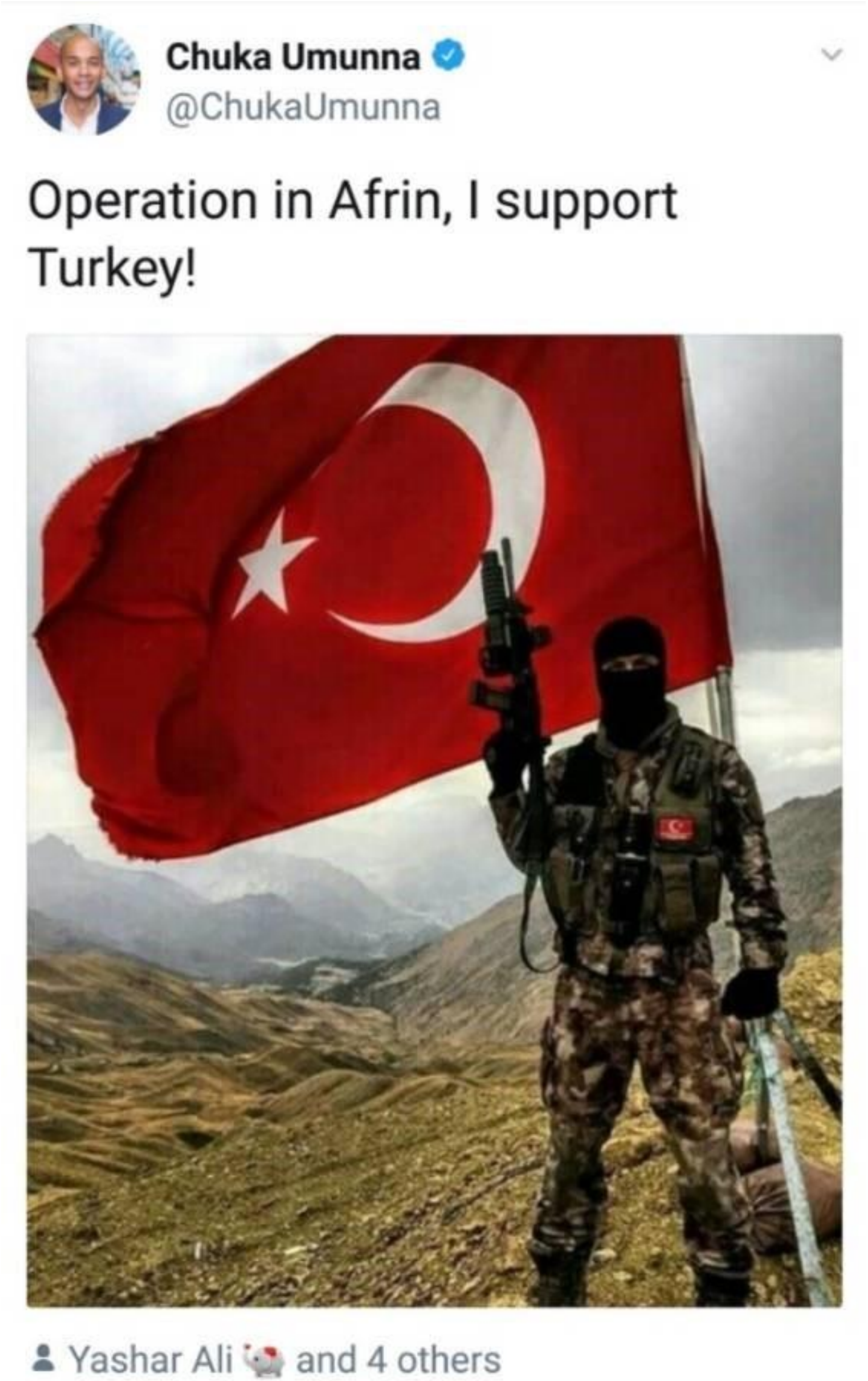
Reporters Without Borders. 2019. World Press Freedom Index. *Reporters Without Borders.* https://rsf.org/en/ranking

Ristic, M., Stojanovic, M., Sirotnikova, M. G., Keller-Alant, A., Firat-Buyuk, H., Vladisavljevic, A., Barberá, M. G., Necsutu, M., & Stojkovski. B. 2020. Europe's other Coronavirus Victim: Information and Data Rights. *Balkan Insights.*

https://balkaninsight.com/2020/03/24/europes-other-coronavirus- victim-information-and-data-rights/

Stubbs, J., Bing, C., & Menn, J. 2020. Exclusive: Hackers acting in Turkey's interest believed to be behind recent cyberattacks – sources. *Reuters.* https://www.reuters.com/article/us-cyber-attack-hijack- exclusive/exclusive-hackers-acting-in-turkeys-interests-believed-to-be-behind-recent- cyberattacks-sources-idUSKBN1ZQ10X

Yildi, M. 2019. Turkey defends official inflation figures as critics pile on condemnation. *Middle East Eye*. https://www.middleeasteye.net/news/turkey-defends-official-inflation-rates-critics-pile- condemnation.

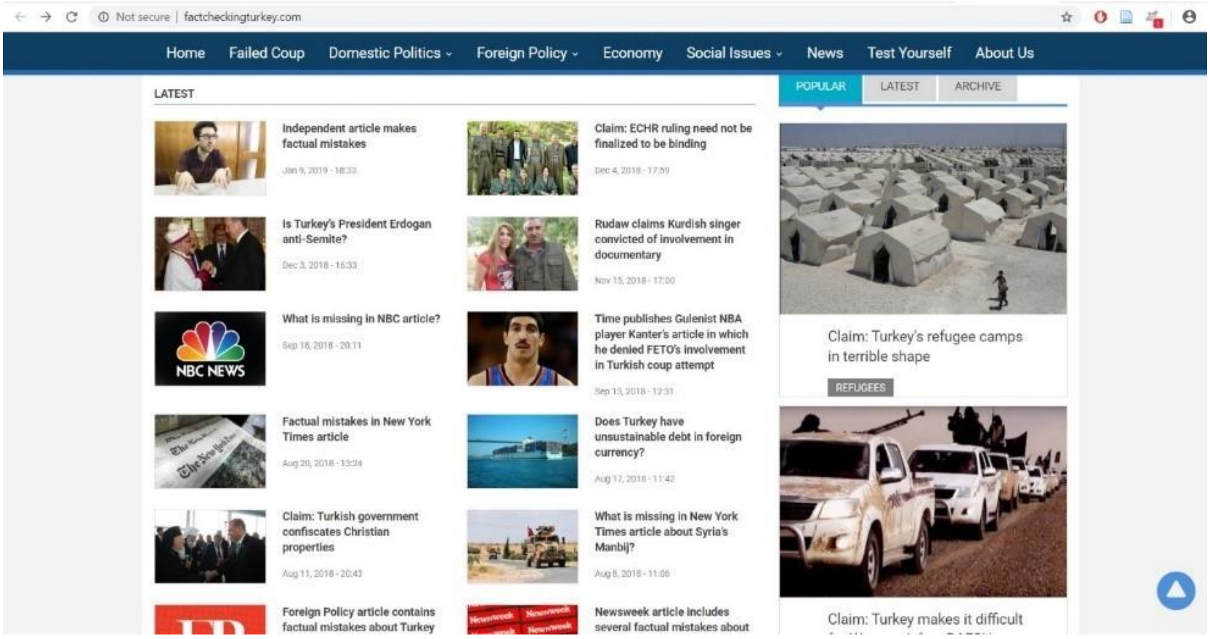


Chuka Umunna
@ChukaUmunna

Operation in Afrin, I support Turkey!

Yashar Ali and 4 others

Figure 1: Chuka Umunna’s hacked Twitter account Source: Evening Standard, 2018



Independent article makes factual mistakes
Jan 9, 2019 - 18:33

Claim: ECHR ruling need not be finalized to be binding
Dec 4, 2018 - 17:59

Is Turkey's President Erdogan anti-Semite?
Dec 3, 2018 - 16:33

Rudaw claims Kurdish singer convicted of involvement in documentary
Nov 15, 2018 - 17:00

What is missing in NBC article?
Sep 18, 2018 - 20:11

Time publishes Gulenist NBA player Kanter's article in which he denied FETO's involvement in Turkish coup attempt
Sep 13, 2018 - 12:31

Factual mistakes in New York Times article
Aug 20, 2018 - 13:24

Does Turkey have unsustainable debt in foreign currency?
Aug 17, 2018 - 11:42

Claim: Turkish government confiscates Christian properties
Aug 11, 2018 - 20:43

What is missing in New York Times article about Syria's Manbij?
Aug 8, 2018 - 11:06

Foreign Policy article contains factual mistakes about Turkey

Newsweek article includes several factual mistakes about

Claim: Turkey's refugee camps in terrible shape

Claim: Turkey makes it difficult

Figure 2: A fake fact-checking portal

UNITED KINGDOM

Introduction

Despite having a substantially free Internet, computational propaganda both originates from and is present within the United Kingdom. Government initiatives have been announced in recent years: a National Security Communications Unit was announced in January 2018, and the consolidation of the British Army's cyber and information warfare capabilities was announced in August 2019. At the political party level, the December 2019 General Election involved "high-level disinformation" and citizen activist groups and individuals contributed to online campaigning in the build up to the election (First Draft, 2019b).

This profile will outline computational propaganda efforts within the UK. However, there is also a wealth of reporting outlining foreign influence operations targeting the UK. Reports have linked foreign interference to the 2014 Scottish Independence Referendum, the 2016 EU Referendum ('Brexit') and the 2017 General Election (Freedom House, 2019). The Intelligence and Security Commission of Parliament Report on Russian interference in UK democratic processes, released in July 2020, found that the government and intelligence agencies failed to conduct a proper assessment of the Kremlin's attempts at interference (Sabbagh et al., 2020).

In response to growing concerns about online harms, the Department for Digital, Culture, Media & Sport (DCMS) and the Home Office in April 2019 released the 'Online Harms White Paper' aiming to create a new regulatory framework to tackle online content (Freedom House, 2019). In addition to this, Parliament's DCMS Committee released its report on disinformation and 'fake news' in February 2019, which explored data targeting, Aggregate IQ, online advertising, and foreign influence campaigns (House of Commons, 2019).

An Overview of Cyber Troop Activity in the United Kingdom

Organizational Form

Government

Military organisations have been established to undertake social media influence activities. In 2015, the British Army set up the 77th Brigade to "challenge the difficulties of modern warfare using non-lethal engagement and legitimate non-military levers as a means to adapt behaviours of opposing forces and adversaries" (British Army, 2020). This unit was a combination of existing units: an existing Media Operations Group, a Military Stabilisation Support Group and a Psychological Operations Group. 77th Brigade staff come from the British armed forces, but it is reported that "half were reservists from civvy street, with full time jobs in marketing or consumer research" (Miller, 2018). Lieutenant General Ivan Jones, Commander Field Army, announced in August 2019 the formation of a cyber warfare unit to fight "above and below the threshold of conventional conflict". It is reported this new unit, 6 Division, will move beyond cyber capabilities into social media information warfare with "an offensive and defensive propaganda remit" (Doffman, 2019).

Government Communications Headquarters (GCHQ), the UK's signals intelligence agency, allegedly conducts covert activities through the Joint Threat Research Intelligence Group (JTRIG) (Clarke, 2019). Leaked documents suggest that online foreign influence operations date back to 2009, citing GCHQ's Operation Quito, intended to shape public opinion in the Falkland Islands (EFF, 2015). It is also reported that during the 2009 Iranian presidential election protests and the 2011 Arab Spring, a “GCHQ unit attempted to shape public opinion through social media” (Clarke, 2019).

Government departments also counter the threat posed by computational propaganda. Former prime minister Theresa May announced in January 2018 that a National Security Communications Unit would be tasked with “combating disinformation by state actors and others” (Bienkov, 2018). The government conducted a public health-style campaign on the risks of disinformation entitled ‘Don’t Feed the Beast’, including a checklist to spot misleading content (Source, Headline, Analyse, Retouched, Error). In light of the disinformation about COVID-19, the government’s Rapid Response Unit identified up to seventy incidents a week, including false narratives, leading to the relaunch of the ‘Don’t Feed the Beast’ campaign (Government Press Release, 2020). In response to an uptick in coronavirus-related disinformation, including content originating from Russia and China, a special cross-Whitehall disinformation unit was set up in March 2020 (Sabbagh, 2020).

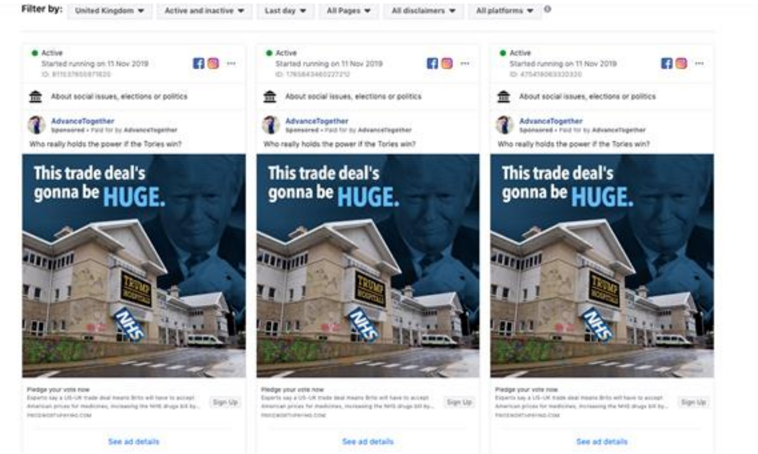
Political Parties

Computational propaganda is a widespread tactic amongst multiple actors in the political system. The extent of this was demonstrated during the General Election in December 2019. The Coalition for Reform in Political Advertising (2019) described political advertising coming from the main parties as “illegal, indecent, dishonest and untruthful”, with advertising that ‘transgressed’ coming from the Conservative Party, Labour Party, Liberal Democrats, and Brexit Party. Analysts reported on the “apparent impunity with which the main parties… employed overt disinformation to secure votes” (Colley et al., 2020). First Draft identified that 90% of the Conservative Party’s Facebook adverts in the first days of December 2019 promoted claims labelled as misleading by Full Fact (Reid & Dotto, 2019).

Digital campaigning also originated from civil society organisations and activists. A pro-Labour party activist group, Momentum, had a team of fifteen people employed to “produce videos, memes and other social media content” (Satariano & Tsang, 2019). First Draft (2019a) also found a number of private individuals were publishing misleading ads on Facebook, including ‘Advance Together’ organised by former Liberal Democrat candidate Annabel Mullin and ‘Campaign Against Corbynism’ run by a Daily Express reporter James Bickerton. Advance Together published unverified claims, and an example of the Facebook content can be seen in Figure 1. Labour activists utilised an automated bot on the dating app Tinder to send anti-Conservative messages to users, for the second election in a row (this technique was also used in the 2017 General Election). Campaigners claimed to have sent out 20,000 individual messages on Tinder during the campaign (Woodford & Darrah, 2019).

Campaigners linked to Indian Prime Minister Narendra Modi’s BJP said they were targeting forty-eight Labour-Conservative marginal seats (Hundal, 2019). The president of the campaign group Overseas Friends of BJP (UK) (OFBJPUK) Kuldeep Singh Shekhawat said they were trying to swing marginal seats towards the Conservative Party (Canton, 2019). WhatsApp messages were circulating among British Hindus, accusing Labour of being ‘anti-India’ (Siddique, 2019). This was the first time the organisation has openly supported a party in a UK general election, and campaigning teams were organised by the OFBJPUK and Friends of India Society International (Canton, 2019). Campaigning was limited to marginal seats, but the extent and impact of these activities was not reported after the election.

Digital communications firms have been hired for political campaigning across the political spectrum and in government communications. During the 2019 election, the Conservative Party hired digital communications firm Topham Guerin following their success in elections in Australia (Satariano & Tsang, 2019). In 2018, data analytics company Cambridge Analytica was implicated in a global scandal concerning data harvesting and electoral interference. Cambridge Analytica worked with Vote Leave as part of the Brexit referendum, and their parent company, SCL Group, is alleged to have worked with governments around the world. Cambridge Analytica is implicated in one of Facebook's largest data breaches: harvesting personal information without authorisation as early as 2014 to profile 50 million US voters and target them with personalised political ads ahead of the 2016 US presidential election (Cadwalladr & Graham-Harrison, 2018). Cambridge Analytica was also implicated in data-driven campaigns around the world: such as helping President Uhuru Kenyatta win campaigns in Kenya in 2013 and 2017, as well as the company's website reporting case studies of operating in Thailand, South Africa, India, Indonesia, and Trinidad and Tobago (Madowo, 2018).



Filter by: United Kingdom ▾ Active and inactive ▾ Last day ▾ All Pages ▾ All disclaimers ▾ All platforms ▾

● Active
Started running on 11 Nov 2019
ID: [illegible]
About social issues, elections or politics
AdvanceTogether
Sponsored • Paid for by AdvanceTogether
Who really holds the power if the Tories win?
Pledge your vote now
Experts say a US-UK trade deal means Brits will have to accept American prices for medicines, increasing the NHS drugs bill by...
PRICEWORTHPAYING.COM
Sign Up
See ad details

● Active
Started running on 11 Nov 2019
ID: [illegible]
About social issues, elections or politics
AdvanceTogether
Sponsored • Paid for by AdvanceTogether
Who really holds the power if the Tories win?
Pledge your vote now
Experts say a US-UK trade deal means Brits will have to accept American prices for medicines, increasing the NHS drugs bill by...
PRICEWORTHPAYING.COM
Sign Up
See ad details

● Active
Started running on 11 Nov 2019
ID: [illegible]
About social issues, elections or politics
AdvanceTogether
Sponsored • Paid for by AdvanceTogether
Who really holds the power if the Tories win?
Pledge your vote now
Experts say a US-UK trade deal means Brits will have to accept American prices for medicines, increasing the NHS drugs bill by...
PRICEWORTHPAYING.COM
Sign Up
See ad details

Figure 1: Advance Together Facebook Ads (First Draft, 2019a)

Table 1: Organizational Form and Prevalence of Social Media Manipulation in the United Kingdom

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
2009	77th Brigade, British Army 6 Division, GCHQ (JTRIG)	Conservative Party, Labour Party, Liberal Democrats, Brexit Party	Evidence Found	Momentum (pro-Labour), OFBJPUK	Evidence Found

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

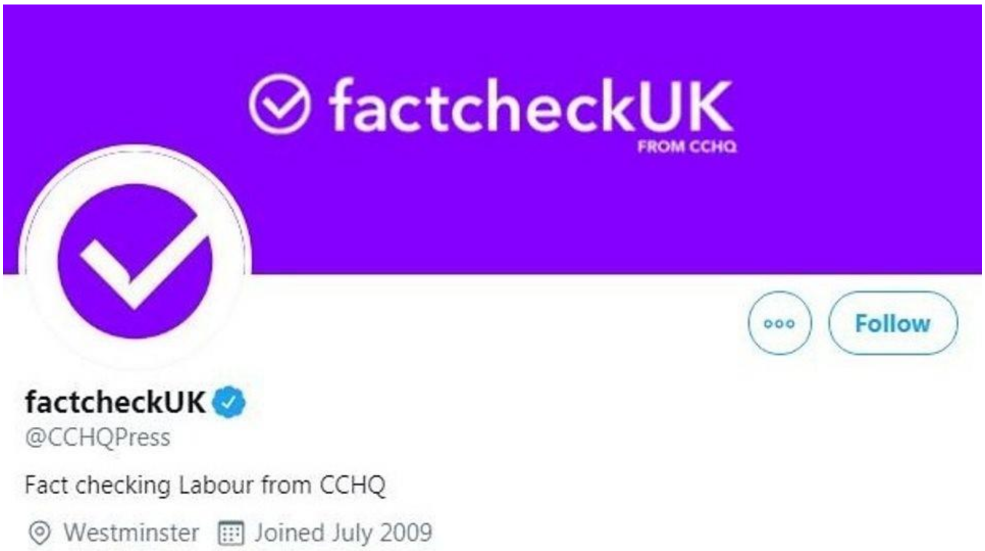
As opposed to the more blatant techniques used in political campaigning, government strategies for manipulation are largely covert. Strategic communications campaigns have been outsourced to third party private companies. For example, a tailor-made social news network called 'This is Woke' ran pages on Facebook and Instagram targeting discussions about news and aspects of the Muslim faith in the UK. It amassed 75,000 followers but was exposed as curated by a UK media firm, Zinc Network, as part of the Home Office's anti-terror strategy (BBC, 2019a). There are also reports of foreign manipulation: Director of GCHQ, Jeremy Fleming, said in April 2018 that the UK had conducted a "major offensive cyber-campaign" against the Islamic State in 2017, making it "almost impossible to spread their hate online, to use their normal channels to spread their rhetoric, or trust their publications" (BBC, 2018).

Previous analysis by the researchers at the Oxford Internet Institute found that during the 2016 UK Brexit referendum "political bots played a small but strategic role shaping Twitter conversations", hashtags associated with the argument for leaving the EU dominated, and less than 1% of sampled accounts generated almost a third of all the messages (Narayanan et al., 2017). Researchers found that junk news accounted for 11.4% of news content shared on Twitter. Conversely, during the 2019 General Election, there was little evidence of widespread social bot activity or junk news. Although voter manipulation and election meddling are still of major concern in the UK, they found very little junk news (less than 2%) circulating over Twitter during their data collection period (Marchal et al., 2019).

The 2019 election saw an increase in party-led disinformation efforts. The Coalition for Reform in Political Advertising said that at least thirty-one campaigns from across the political spectrum had been indecent, dishonest, or untruthful (Tidy & Schraer, 2019). Computational propaganda techniques that have previously featured elsewhere in the world were evident during the election period:

- *Misleading adverts:* First Draft found that 88% (5,952) of the Conservative Party's most widely promoted ads either featured claims which had been flagged by independent fact-checking organisations as not correct or not entirely correct (Tidy & Schraer, 2019).
- *Doctored videos:* The Conservative Party was forced to apologise after spreading an edited video that appeared to show opposition politician Sir Keir Starmer unable to answer a question on Brexit (Murphy, 2019).
- *Fake polling:* First Draft found that hundreds of misleading ads from the Liberal Democrats had featured identical unlabelled graphs, with no indication of the source data (Tidy & Schraer, 2019).
- *Leaked documents*: On 21 October 2019, a reddit user (u/gregoratior) posted a leaked document on UK-US trade negotiations on the r/worldpolitics subreddit. Reddit announced that the documents were uploaded as "part of a campaign that has been reported as originating from Russia" (BBC, 2019b). The leaked documents were further disseminated in Twitter and on conspiracy-heavy website BeforeItsNews.com. Labour used the documents to argue that the NHS would be at risk under a post-Brexit trade deal with the US.
- *Misleading fact-checking:* The Conservative Party Press Office Twitter account (@CCHQPress, 76,000 followers) was renamed 'factcheckUK' to fact-check statements made during a party leadership debate on ITV (Figure 2). Twitter accused the Conservatives of misleading the public and said that 'decisive corrective action' would be taken in the future (Perraudin, 2019).
- *Search Engine Optimisation:* The Conservative Party bought Google Ads so that in searches for Labour's policy manifesto, the top result was a website (labourmanifesto.co.uk) that criticised Labour's proposals (Satariano & Tsang, 2019).

- *Fake accounts:* A fake account was set up to impersonate prospective Brexit Party parliamentary candidate Wayne Bayley, tweeting attacks on Nigel Farage and Boris Johnson, before being suspended by Twitter (First Draft, 2019a).



factcheckUK
@CCHQPress
Fact checking Labour from CCHQ
Westminster Joined July 2009

Figure 2: Conservative Party's 'factcheckUK' on Twitter

- *Harassment:* A report by Demos found that candidates were the target of trolling and abuse by Twitter users. Notably, the type of abuse received by a candidate changed depending on their ethnic background (e.g. Black British candidates were most likely to be insulted for their intelligence), insults were dispersed across the political spectrum, and politicians were insulted for being dishonest. (Smith, 2019).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in the United Kingdom

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Human, automated, fake	Pro-Party Messages, Attacks on Opposition, Polarization Strategies	Facebook & Google Ads, memes, doctored videos, misleading polling, disinformation	Facebook, Twitter, Tinder, Instagram

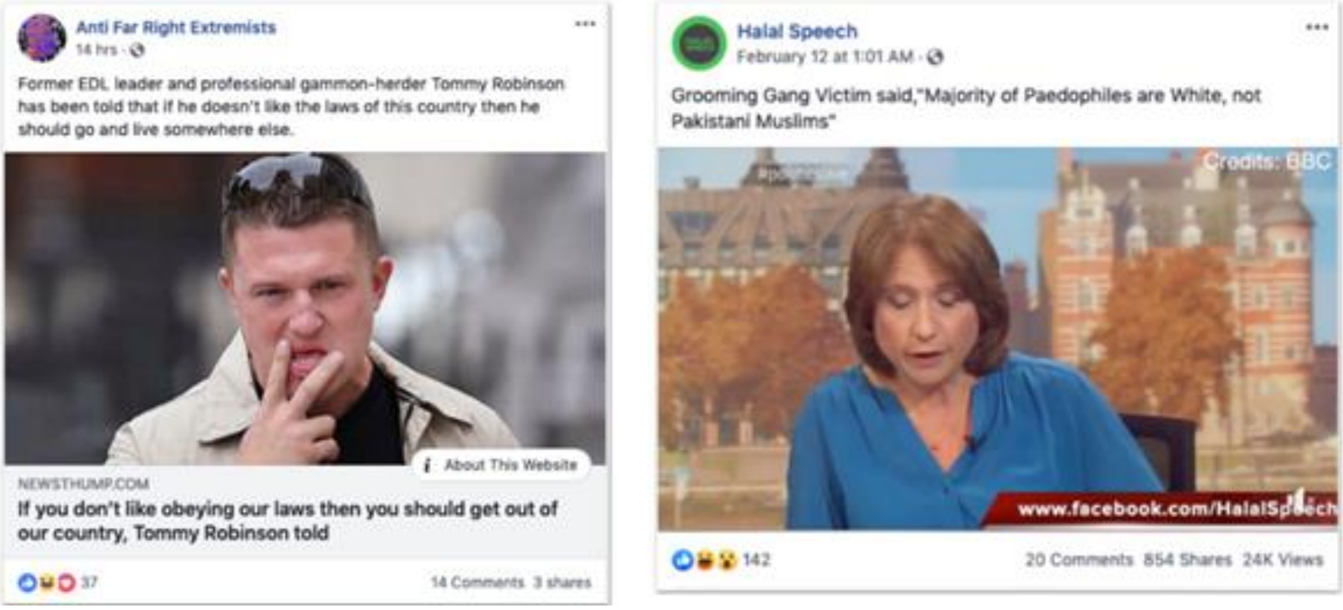
Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

The organizational capacity of the government's computational propaganda activities is unknown. A Freedom of Information request from 2016 indicated that the capacity of the 77th Brigade was 153 Regular and 123 Reserve personnel; however, the letter acknowledges that the number has since increased (Ministry of Defence, 2016). The proportion of personnel directly engaged in computational propaganda is not disclosed.

Leaks connected to the involvement of Cambridge Analytica (as well as Aggregate IQ, or AIQ, and its group holder SLC) in the EU Referendum by whistle-blower Christopher Wylie made public the presence of computational propaganda during the 2016 Brexit campaign. The legitimacy of the Brexit vote has been questioned following revelations around the Leave campaign's out-manoeuvring of spending limits by donating £625,000, US$1 million, to the pro-Brexit student group BeLeave, and the illegality of personal data misuse to target voters. The Guardian reported that £3.5 million was spent on AIQ by four Leave campaign groups (Vote Leave, BeLeave, Veterans for Britain, Northern Ireland's Democratic Unionist Party) for targeted political advertising.

In March 2019, Facebook removed 137 Facebook and Instagram accounts, pages, and groups for engaging in 'coordinated inauthentic behaviour' as part of a domestic-focused network in the UK (Gleicher, 2019). They posted about local and political news, including topics such as "immigration, free speech, racism, LGBT issues, far-right politics" and spent $1,500 on spending for Facebook ads, paid for in US dollars and GB pounds. Attribution of this network has not been made public. Examples of the polarizing content made public by Facebook can be seen in Figure 3. The Digital Forensic Research Lab conducted an analysis of the divisive content and found that the main narratives concerned the role and status of migrants and Muslims in Britain (@DFRLab, 2019).



Anti Far Right Extremists
14 hrs

Former EDL leader and professional gammon-herder Tommy Robinson has been told that if he doesn't like the laws of this country then he should go and live somewhere else.

NEWSTHUMP.COM

If you don't like obeying our laws then you should get out of our country, Tommy Robinson told

Halal Speech
February 12 at 1:01 AM

Grooming Gang Victim said,"Majority of Paedophiles are White, not Pakistani Muslims"

About This Website
37
14 Comments 3 shares
Credits: BBC
www.facebook.com/HalalSpeech
142
20 Comments 854 Shares 24K Views

Figure 3: Divisive Facebook Ads (Facebook, 2019)

Table 3: Cyber Troop Capacity in the United Kingdom

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
Range of sizes: from individuals, teams of 15 to organisations of ~276.		Government activity supports ongoing operations. Political party activity is liminal around elections.	High levels of government coordination. Unknown levels of coordination between political parties, companies and activists.	Medium/High

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

References

BBC. (2018, April 12). UK launched cyber-attack on Islamic State. *BBC News*. https://www.bbc.com/news/technology-43738953

BBC. (2019a, August 16). Home Office role in 'Woke' Muslim social network revealed. *BBC News*. https://www.bbc.co.uk/news/technology-49368872

BBC. (2019b, December 7). PM: We must find source of UK-US trade document leak. *BBC News*. https://www.bbc.com/news/uk-50699168

Bienkov, A. (2018, January 23). Theresa May is setting up a 'fake news' unit to fight Russian propaganda. *Business Insider*. https://www.businessinsider.com/theresa-may-fake-news-national-security-communications-unit-russia-propaganda-putin-2018-1

British Army. (2020). *77th Brigade*. https://www.army.mod.uk/who-we-are/formations-divisions-brigades/6th-united-kingdom-division/77-brigade/

Cadwalladr, C., & Graham-Harrison, E. (2018, March 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Canton, N. (2019, November 5). BJP support group bats for Tories in 48 key UK seats—Times of India. *Times of India*. https://timesofindia.indiatimes.com/world/uk/bjp-supporters-start-campaign-for-tories-in-uk-general-election/articleshow/71911496.cms

Clarke, L. (2019, October 8). Twitter needs to start exposing the UK's murky online propaganda. *Wired UK*. https://www.wired.co.uk/article/uk-disinformation-twitter-facebook

Colley, T., Granelli, F., & Althius, J. (2020). Disinformation's Societal Impact: Britain, Covid, And Beyond. *Defence Strategic Communications, 8*. https://www.stratcomcoe.org/tcolley-fgranelli-and-jalthuis-disinformations-societal-impact-britain-covid-and-beyond

@DFRLab. (2019, March 7). *#TrollTracker: Facebook Takes Down Fake Network in the United Kingdom*. Medium. https://medium.com/dfrlab/exclusive-facebook-takes-down-fake-network-in-the-united-kingdom-58350e0f3401

Doffman, Z. (2019, August 1). Cyber Warfare: Army Deploys 'Social Media Warfare' Division To Fight Russia. *Forbes*. https://www.forbes.com/sites/zakdoffman/2019/08/01/social-media-warfare-new-military-cyber-unit-will-fight-russias-dark-arts/

EFF. (2015, April 9). *GCHQ Operation QUITO to Shape Falklands Public Opinion (Collection)*. Electronic Frontier Foundation. https://www.eff.org/node/85412

First Draft. (2019a, November 15). *UK General Election 2019: Doctored videos, fake accounts and suspicious ads surface in the second week*. First Draft. https://firstdraftnews.org:443/latest/uk-general-election-2019-doctored-videos-fake-accounts-and-suspicious-ads-surface-in-the-second-week/

First Draft. (2019b, December 14). *UK general election 2019: High-level disinformation and false polling reports in the final week*. First Draft. https://firstdraftnews.org:443/latest/uk-general-election-2019-round-up-voting-day/

Freedom House. (2019). *United Kingdom | Freedom House*. https://freedomhouse.org/country/united-kingdom/freedom-net/2019

Gleicher, N. (2019, March 7). Removing Coordinated Inauthentic Behavior From the UK and Romania. *About Facebook*. https://about.fb.com/news/2019/03/removing-cib-uk-and-romania/

Government Press Release. (2020, March 30). *Government cracks down on spread of false coronavirus information online*. GOV.UK.

https://www.gov.uk/government/news/government-cracks-down-on-spread-of-false-coronavirus-information-online

House of Commons. (2019). *Disinformation and 'fake news'* (Eigth Report of Session 2017-19). https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf

Hundal, S. (2019, November 6). *Concerns over 'foreign interference' as India-linked Hindu nationalist group targets Labour candidates*. OpenDemocracy. https://www.opendemocracy.net/en/opendemocracyuk/concerns-over-foreign-interference-as-india-linked-hindu-nationalist-group-targets-labour-candidates/

Madowo, L. (2018, March 21). Opinion | How Cambridge Analytica poisoned Kenya's democracy. *Washington Post*. https://www.washingtonpost.com/news/global-opinions/wp/2018/03/20/how-cambridge-analytica-poisoned-kenyas-democracy/

Marchal, N., Kollanyi, B., Neudert, L.-M., Au, H., & Howard, P. (2019). *Junk News & Information Sharing During the 2019 UK General Election* (Data Memo 2019.4). https://comprop.oii.ox.ac.uk/research/uk-election-memo-2019/

Miller, C. (2018, November 14). Inside the British Army's secret information warfare machine. *Wired UK*. https://www.wired.co.uk/article/inside-the-77th-brigade-britains-information-warfare-military

Ministry of Defence. (2016). *Liability and Strength of 77 Brigade*. Army Secretariat. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/579917/20161214-FOI10962_77961_77X_Manning_Redacted.pdf

Murphy, J. (2019, November 12). *Senior Tory admits doctored video of Sir Keir 'went too far'*. Evening Standard. https://www.standard.co.uk/news/politics/general-election-2019-senior-tory-admits-doctored-video-of-sir-keir-starmer-went-too-far-a4284991.html

Narayanan, V., Howard, P. N., Kollanyi, B., & Elswah, M. (2017). *Russian Involvement and Junk News during Brexit* (Data Memo No. 2017.10). https://comprop.oii.ox.ac.uk/research/working-papers/russia-and-brexit/

Perraudin, F. (2019, November 20). Twitter accuses Tories of misleading public with 'factcheck' foray | Politics | The Guardian. *The Guardian*. https://www.theguardian.com/politics/2019/nov/20/twitter-accuses-tories-of-misleading-public-in-factcheck-row

Reid, A., & Dotto, C. (2019, December 6). *Thousands of misleading Conservative ads side-step scrutiny thanks to Facebook policy*. First Draft. https://firstdraftnews.org:443/latest/thousands-of-misleading-conservative-ads-side-step-scrutiny-thanks-to-facebook-policy/

Sabbagh, D. (2020, March 9). Cross-Whitehall unit set up to counter false coronavirus claims. *The Guardian*. https://www.theguardian.com/world/2020/mar/09/cross-whitehall-unit-coronavirus-disinformation

Sabbagh, D., Harding, L., & Roth, and A. (2020, July 21). Russia report reveals UK government failed to investigate Kremlin interference. *The Guardian*. https://www.theguardian.com/world/2020/jul/21/russia-report-reveals-uk-government-failed-to-address-kremlin-interference-scottish-referendum-brexit

Satariano, A., & Tsang, A. (2019, December 12). Who's Spreading Disinformation in U.K. Election? You Might Be Surprised—The New York Times. *New York Times*. https://www.nytimes.com/2019/12/10/world/europe/elections-disinformation-social-media.html

Siddique, H. (2019, November 11). British Indians warn Hindu nationalist party not to meddle in UK elections. *The Guardian*. https://www.theguardian.com/politics/2019/nov/11/british-indians-warn-hindu-party-not-to-meddle-in-uk-elections

Smith, J. (2019). *The Outrage Election: A CASM Investigation conducted with BBC Click*. Demos. https://demos.co.uk/wp-content/uploads/2019/12/The-Outrage-Election-11.12.19.pdf

The Coalition for Reform in Political Advertising. (2019). *Illegal, Indecent, Dishonest & Untruthful*. https://reformpoliticaladvertising.org/wp-content/uploads/2019/12/Illegal-Indecent-Dishonest-and-Untruthful-The-Coalition-for-Reform-in-Political-Advertising.pdf

Tidy, J., & Schraer, R. (2019, December 17). Election ads: 'Indecent, dishonest and untruthful'. *BBC News*. https://www.bbc.com/news/technology-50726500

Woodford, I., & Darrah, K. (2019, December 12). *Labour activists using Tinder election bots to sway vote*. Sifted. https://sifted.eu/articles/tinder-uk-election/

UKRAINE

Introduction

Ukraine has experienced a number of democratic reforms since the ousting of its former President, Viktor Yanukovych, in 2014. Nevertheless, corruption and attacks on the media and journalists remain an issue, and Russia continues to occupy the autonomous Ukrainian region of Crimea and support separatists in the eastern Donbas area. Ukraine's constitution guarantees the freedom of speech and expression and the media landscape generally allows for political pluralism and critiques of the government. However, many outlets are owned by business magnates who use them as tools to advance their own agenda, and journalists continue to face violence and intimidation. Moreover, Ukraine has prohibited the distribution and transmission of dozens of Russian media outlets, including the major Russian news outlets and television stations, citing the negative consequences of Russian influence on the Ukrainian public as justification (*Ukraine | Freedom House*, 2020).

Generally, Ukraine has an internet penetration rate of about 74%, which has been fairly stable in recent years and is expected to increase to 82% by 2022 (*Ukraine Internet penetration 2012-2022*, 2020). Regions affected conflict, such as Crimea and Donbas, suffer from very poor internet connection. Many Ukrainians access the internet through their mobile phones, and statistics suggest that about 61% of the country's citizens did so in 2019. Ukrainian mobile broadband rates are comparably cheap, with 1GB costing an average of $0.51 (*Freedom on the Net | Ukraine*, 2019). Additionally, social media have become a main source of news for Ukrainians. About 13 million people use Facebook (out of 21.4 million who use the internet in general) (Demchenko, 2019), making it the most popular platform in the country. 74% of Ukrainians who say they use social media as their main source of news say that they use Facebook (Drach, 2020; Kiev International Institute for Sociology, 2019; Ott & Lozovyi, 2019). It appears that social media may be overtaking television as the most important medium for politics.

An Overview of Cyber Troop Activity Ukraine

Organizational Form

Ukraine's government has enforced a strict regime of censorship upon online content originating from Russia. The Ukrainian government has sanctioned several Russian companies, citing a fear of cyberattacks and data collection by Russian authorities (Roth, 2017). As a consequence, this has also put pressure on Ukrainian journalists to self-censor (IREX.org, 2019), presenting stringent controls upon the ways in which Ukraine controls the information that its public consumes, though there is no consensus on the presence of self-censorship amongst journalists is an issue in the country. That said, communications from Russia, and from the Russian government, do still manage to bypass Ukrainian attempts at censorship (Grynko, 2019; Kuzio, 2020).

In addition, investigative reports suggest that Ukrainian politicians have engaged in hiring private contractors, such as public relations companies, and making use of trolling groups and bloggers to polish their image both online and offline. It appears that this largely occurs at the party political level and not through official government agencies, although the working practices and organisation of these contractors remains largely unknown, and most politicians deny any knowledge or association with such online influence campaigns (Freedom on the Net | Ukraine, 2019; Kupfer, 2019; Motorevska et al., 2019). Finally, popular politicians with large social media followings, such as the current President, Volodymyr Zelensky, use their online platforms to communicate more directly with citizens (Motorevska et al., 2019).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Ukraine

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
		x	x		x

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Influence operations initiated by politicians are made up of a mix of automated and human activities that usually aim to spread and amplify narratives that are favorable and which also attack their opposition (*Freedom on the Net | Ukraine*, 2019; Kupfer, 2019). Social media platforms Facebook and Instagram seem to be the prominent stage for these activities. For example, in 2018 a local report noted unusually high, bot-like behavior on the Facebook pages of several politicians, including the page of the former Minister of Information, which looked like an amplification attempt (Скляревская, 2018). Similarly, in the summer of 2019 President Zelensky's Chief of Staff stated that due to the President's highly popular social media accounts his administration had no need to work with journalists to communicate with citizens when they could do so more directly through Facebook, Telegram and Instagram (Grytsenko, 2019). However, according to an investigation by VoxUkraine, Zelensky's Facebook page has the largest number of fake followers amongst Ukrainian politicians, with nearly 28,000 inauthentic accounts (VoxUkraine was careful to point out that they do not claim that these fake accounts or bots are instigated or owned by the politicians). VoxUkraine found 332 Facebook pages of politicians and popular news websites showed inauthentic follower activity (Ott & Lozovyi, 2019).

An exposé published by the Organized Crime and Corruption Reporting Project (OCCRP) in the aftermath of the 2019 parliamentary election found that almost all politicians were engaging in online influence campaigns, even those who publicly spoke out against these tactics. However, the reporters sent to undertake undercover investigations at Ukrainian troll farms were unable to discover the origins of payments for these campaigns, and many politicians either deny any knowledge of influence campaigns on their behalf or refuse to comment (Motorevska et al., 2019).

OCCRP's article outlines that these domestic troll farms pose as PR companies but are not usually registered as official businesses. One reporter that was sent to work undercover was offered a position at the company on the spot, for a monthly salary of 9,000 hryvnia (USD $365), roughly the same amount a cashier would make in Ukraine. The reporter's job consisted of posting comments on Facebook through dozens of fake accounts, producing around 300 comments in one shift. Each shift consisted of about 10 workers. The company appeared to support several individual politicians as well as entire political parties, and the work for political candidates often appeared to be tied to whether it was expected that they had a good chance of being successful in the upcoming election (Motorevska et al., 2019).

In addition to these domestic influence and troll activities, Ukraine is also subject to Russian-based activities. In 2013 a Russian agency was exposed for forming an army of paid online commentators to defended the Russian government and attack its critics in the Ukraine

(Гармажапова, 2013). Some political experts claim that these kinds of Russian activities started as early as 2007 (Motorevska et al., 2019). In the run-up to the 2019 elections observers feared that the flood of fake news coming from Russia could influence the results (Batalov, 2019). In January 2019 Facebook reported the removal of 41 Instagram accounts and 107 Facebook pages 'for engaging in coordinated inauthentic behavior as part of a network that originated in Russia and operated in Ukraine'. In March 2019 Facebook removed another 1,907 pages, groups and accounts seemingly affiliated to Russia and exhibiting inauthentic behavior while spreading disinformation (Facebook Newsroom, 2019a, 2019b). Finally, Russian trolls posing as Ukrainian nationalists have found their way into Ukrainian patriot groups on social media, sometimes even serving as administrators (Romanenko et al., 2016).

At present it appears that both domestic and Russian troll farms are numerous and relentless. There is news about the removals of new accounts due to inauthentic behavior published on average every few months (Radio Free Europe, 2020).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Ukraine

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Human Bot Fake accounts	Support Attack Opposition	Disinformation Trolls Amplifying content	Facebook Instagram Telegram

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

According to the exposé published by the OCCRP, influence campaigns posting around 10,000 comments per month cost between USD $5,000 to $7,000 (Motorevska et al., 2019). How much politicians or parties pay for online influence campaigns remains unclear, particularly because politicians and parties often deny the use of cyber troop operations. Though the nature of the content suggests that it is highly likely that the responsibility for paying for these online activities lies with political actors, investigations have been largely been unable to ascertain this with any certainty. There are some instances where the financiers have been exposed. For instance, Facebook has reported that the agency called Postmen DA was behind a recent set of accounts exhibiting coordinated, inauthentic behavior. This digital agency is known to have worked with former Ukrainian President, Petro Poroshenko, and later the Vakarchuk Party (Drach, 2020; Facebook Newsroom, 2020). Much of the domestic activity appears to focus on specific political events, though activity relating to the current administration of President Zelensky suggests that there have become sustained themes in Ukrainian cyber troop activity.

Table 3: Cyber Troop Capacity in Ukraine

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
		Temporary & Permanent	Coordinated	

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

In recent years there have been several initiatives in Ukraine to educate the public on how to identify disinformation, propaganda and hate speech. The global education organisation IREX (International Research and Exchange Board) started programmes at 50 schools in late 2018 and hopes to bring their program to about 650 schools by 2021 (Cain, 2019; Ingber, 2019). The struggle that Ukraine experiences in relation to fake news and conspiracies has became particularly apparent during the COVID-19 pandemic, as the country scrambles to get a grip on disinformation spread locally and disseminated from outside sources (in particular Russia) (Euractive, 2020; Gumenyuk, 2020).

References

Batalov, N. (2019, March 23). Is Ukraine′s presidential election threatened by fake news? *Deutsche Welle*. https://www.dw.com/cda/en/is-ukraines-presidential-election-threatened-by-fake-news/a-47997358

Cain, G. (2019, March 29). Ukraine's War on Russian Disinformation Is a Lesson for America. *The New Republic*. https://newrepublic.com/article/153415/ukraines-war-russian-disinformation-lesson-america

Demchenko, D. (2019, February 14). Ukraine is the leader in increasing of Facebook popularity and 6 more indicators of the Ukrainian social network audience. *AIN.UA*. https://ain.ua/en/2019/02/14/facebook-audience-ukraine/

Drach, M. (2020). *Journalist Fellowship Paper: How social media shaped Zelenskiy's victory in Ukraine* (pp. 1–50). Reuters Institute for the Study of Journalism. https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2020-08/RISJ_Final%20Report_Maryana%20Drach_2020_Final%202%20%289%29.pdf

Euractive. (2020, March 27). Ukraine struggles to debunk fake virus news. *Www.Euractiv.Com*. https://www.euractiv.com/section/europe-s-east/news/ukraine-struggles-to-debunk-fake-virus-news/

Facebook Newsroom. (2019a, January 17). Removing Coordinated Inauthentic Behavior from Russia. *Facebook Newsroom*. https://about.fb.com/news/2019/01/removing-cib-from-russia/

Facebook Newsroom. (2019b, March 26). Removing Coordinated Inauthentic Behavior from Iran, Russia, Macedonia and Kosovo. *Facebook Newsroom*. https://about.fb.com/news/2019/03/cib-iran-russia-macedonia-kosovo/

Facebook Newsroom. (2020, July 8). Removing Coordinated Inauthentic Behavior. *About Facebook*. https://about.fb.com/news/2020/07/removing-political-coordinated-inauthentic-behavior/

Freedom on the Net | Ukraine. (2019). Freedom House. https://freedomhouse.org/country/ukraine/freedom-net/2019

Grynko, A. (2019, March 29). *Ukrainian outlets Vesti and Strana.ua on Presidential Elections in Ukraine: Fake Narratives, Heroes and Antiheroes | StopFake*. https://www.stopfake.org/en/ukrainian-outlets-vesti-and-strana-ua-on-presidential-elections-in-ukraine-fake-narratives-heroes-and-antiheroes/

Grytsenko, O. (2019, August 4). Chief of Staff Bohdan: 'We don't need journalists to talk to people.' *KyivPost*. https://www.kyivpost.com/ukraine-politics/chief-of-staff-bohdan-we-dont-need-journalists-to-talk-to-people.html

Gumenyuk, N. (2020, June 20). Ukraine's coronavirus cases are surging—Can the media tackle public complacency? *Atlantic Council*. https://www.atlanticcouncil.org/blogs/ukrainealert/ukraines-coronavirus-cases-are-surging-can-the-media-tackle-public-complacency/

Ingber, S. (2019, March 22). In The Wake Of Ukraine's Civil War, Students Learn How To Identify Fake News: NPR. *National Public Radio*. https://www.npr.org/2019/03/22/705809811/students-in-ukraine-learn-how-to-spot-fake-stories-propaganda-and-hate-speech?t=1593773045844

IREX.org. (2019). *Media Sustainability Access* (pp. 1–21). International Research and Exchange Board. https://www.irex.org/sites/default/files/pdf/media-sustainability-index-europe-eurasia-2019-ukraine.pdf

Kiev International Institute for Sociology. (2019). *ДЖЕРЕЛА ІНФОРМАЦІЇ, МЕДІАГРАМОТНІСТЬ І РОСІЙСЬКА ПРОПАГАНДА: РЕЗУЛЬТАТИ ВСЕУКРАЇНСЬКОГО ОПИТУВАННЯ ГРОМАДСЬКОЇ ДУМКИ*. Kiev International Institute of Sociology. https://detector.media/doc/images/news/archive/2016/164308/AReport_Media_Feb2019_v2.pdf

Kupfer, M. (2019, April 12). Disinformation, 'black PR' emerge before April 21 runoff election. *KyivPost*. https://www.kyivpost.com/ukraine-politics/disinformation-black-pr-emerge-before-april-21-runoff-election.html

Kuzio, T. (2020, June 27). Russia is quietly occupying Ukraine's information space. *Atlantic Council*. https://www.atlanticcouncil.org/blogs/ukrainealert/russia-is-quietly-occupying-ukraines-information-space/

Motorevska, Y., Replianchuk, D., & Bidun, V. (2019, September 20). Inside a Ukrainian Troll Farm. *Organized Crime and Corruption Reporting Project*. https://www.occrp.org/en/investigations/inside-a-ukrainian-troll-farm

Ott, M., & Lozovyi, V. (2019, August 7). Erase This If You Can. What Ukrainian Bots Are Doing on Ukrainian Politicians' Pages. *VoxUkraine*. https://voxukraine.org/en/erase-this-if-you-can-what-ukrainian-bots-are-doing-on-ukrainian-politicians-pages/

Radio Free Europe. (2020, May 6). RFE/RL: Facebook removes hundreds of disinformation accounts linked to Russia, Iran, and Georgia. *KyivPost*. https://www.kyivpost.com/world/rfe-rl-facebook-removes-hundreds-of-disinformation-accounts-linked-to-russia-iran-and-georgia.html

Romanenko, N., Mykhyalyshyn, I., Solodko, P., & Zog, O. (2016, October 4). The Troll Network. *ТЕКСТИ.ORG.UA*. http://texty.org.ua/d/fb-trolls/index_eng.html

Roth, A. (2017, May 16). In new sanctions list, Ukraine targets Russian social-media sites. *Washington Post*. https://www.washingtonpost.com/world/in-new-sanctions-list-ukraine-blocks-russian-social-media-sites/2017/05/16/a982ab4e-3a16-11e7-9e48-c4f199710b69_story.html

Ukraine | Freedom House. (2020). Freedom House. https://freedomhouse.org/country/ukraine/freedom-world/2020

Ukraine internet penetration 2012-2022. (2020, June 23). Statista. https://www.statista.com/statistics/1023197/ukraine-internet-penetration/

Гармажапова, А. (2013, September 7). *Где живут тролли. И кто их кормит*. Новая газета - Novayagazeta.ru. https://novayagazeta.ru/articles/2013/09/07/56253-gde-zhivut-trolli-i-kto-ih-kormit

Скляревская, Г. (2018, March 19). Минстець, Арбузов и Ляшко: Что общего у политиков в соцсетях. *detector.media*. https://detector.media/infospace/article/135736/2018-03-19-minstets-arbuzov-i-lyashko-chto-obshchego-u-politikov-v-sotssetyakh/

United Arab Emirates

Introduction

The United Arab Emirates' (UAE) computational propaganda efforts are examined in relation to other initiatives by the Emirati regime: the funding of think tanks and conventional media to disseminate narratives favourable of the regime, and the attempt to promote a narrative differentiating them from Iranian and Qatari expansionism. According to Andreas Krieg, Assistant Professor of Defence Studies at King's College London, these well-orchestrated initiatives to some extent explain why there is very little independent research on political matters inside the country. Moreover, many think tanks researching the Middle East and the Gulf States are directly or indirectly funded by the UAE (Krieg 2018).

The UAE's efforts at computational propaganda form a part of a coordinated military and public diplomacy effort. Efforts are complemented by a range of harsh domestic social media and cybercrime laws that criminalize what it deems to be offences against the state, its rulers and symbols, religion, and 'sympathy for Qatar'. A notable example of this in action is the sentencing of human rights activist Ahmed Mansour to 10 years in prison in May 2018, for "spreading sectarianism and hatred on social media" (Freedom House, 2018).

Social media has been used for surveillance efforts in the UAE from as early as 2013 at least (Bing & Schectman 2019). For example, the Telecommunications Regulatory Authority has been deployed to monitor social media networks, including an automated "alert system that will detect when certain keywords are being used" (Arabian Business, 2015). In February 2016, an official from Dubai's Police stated that authorities monitor users on 42 different social media platforms (Freedom House, 2018).

An Overview of Cyber Troop Activity in United Arab Emirates.

Organizational Form

Emirati computational propaganda began as a complement to a defense strategy of spreading positive messages about the UAE, aimed mainly at a US audience but also to a lesser extent a UK audience. In the context of the 2011 Arab Spring, the UAE deployed a more aggressive strategy including foreign attacks on political Islam (conflating any form of political Islam with Islamic State-type Salafi-jihadism) and against Qatar, Turkey and Iran.

Since 2014, propaganda efforts have expanded to interventions in the West. Campaigns outside the Arab world are generally outsourced to public relations and consulting firms in the US, the UK, Germany, Switzerland, and many others. These public relations and lobbying firms have worked "to sway American public opinion through online and social media campaigns" (Wood, 2018).

According to Krieg, attempts to influence Washington's discourse on the Middle East, and the Trump administration's approach to the region, have mostly played out in person rather than online. Krieg notes that Abu Dhabi has created a powerful web of policymakers, think tanks, and experts in the United States, aligned to neo-con and AIPAC (the American Israel Public Affairs Committee) positions to partake in lobbying (Krieg, 2018).

The UAE currently controls a wide range of traditional news outlets, including their respective social media presences. These include Al-Arabiya (the network is Saudi but operates from the

Emirati capital, Abu Dhabi), which has frequently denounced Iranian and Qatari attempts at computational propaganda, and Sky News Arabic. In its endeavour to create an image of a tolerant Middle Eastern partner that shares US security concerns, the UAE worked with the US to create the Sawab Center in 2015. According to the Emirati Minister of State of Foreign Affairs, the Sawab Center's aim is to "amplify moderate and tolerant voices from across the region" (Vice News 2015). Since then, the Sawab Center has launched a number of social media campaigns including the #deludedfollowers hashtag that focused on the issue of foreign fighters, which in January 2016 earned 163 million impressions on Twitter (European Parliament 2017).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in United Arab Emirates

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
	Telecommunications Regulatory Authority, Sawab Center	X	Charles Communications, DotDev, Newave		X

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Hacking: In May 2017, the Qatar News Agency (QNA) was hacked, and remarks attributed to the Emir of Qatar were published in which he expressed support of Iran, Hezbollah and Hamas, and was critical of Donald Trump. These were also shared by Emirati and Saudi news channels and disseminated via social media. According to James Shires, this operation can be seen as an example of what he has described as "hack-and-leak operations". A hack and leak operation involves "both intrusion into specific digital systems and networks (hack) and an attempt to influence certain audiences through the public release of information obtained through that intrusion (leak)" (Shires, 2020).

A US intelligence investigation claimed that the UAE orchestrated the hacking of the QNA and its social media sites in order to post incendiary and false quotes attributed to the Qatari Emir to spark a divide between Qatar and its neighbours (DeYoung and Nakashima, 2017). Anonymous comments given to a journalist indicated that the meetings in which the hack was orchestrated were in fact conducted by Mohammed bin Zayed, Crown Prince of Abu Dhabi (Shires, 2020). It is claimed that the attack was undertaken by Russian hackers hired by the UAE, though the UAE has denied this. In response to the leaks, Jassim Al Thani, Qatar's Washington-based media attaché, stated that the UAE "weaponized fake news to justify the illegal blockade of Qatar", alongside the use of "cyberespionage, fake news and propaganda" (Collier, 2018).

Coordinated inauthentic behaviour:

In August 2019 Facebook removed 259 accounts, 102 Facebook pages, 5 Facebook groups, 4 Facebook events, and 17 Instagram accounts originating from two marketing firms – New Waves in Egypt and Newave in the UAE. These accounts were partaking in what social media platforms call "coordinated inauthentic behaviour". The network used compromised and fake accounts to disseminate their content and artificially increase engagement. The accounts also hosted events. The pages posted about day to day things but also frequently posted on politics, elections, and topics including alleged support of terrorist groups by Qatar and Turkey, the conflict in Libya, the independence for Somaliland, and more. The companies spend around USD 167,000 on Facebook ads, paid primarily in US dollars and Emirati dirhams (Facebook, 2019).

In October 2019 Twitter took action against a similar network of 271 accounts, also originating from a private marketing firm based in the UAE and Egypt. The accounts were created and manged by DotDev, a private technology firm. These information campaigns were mostly targeted against Qatar and Iran. Another 4248 accounts operating out of the UAE were also suspended when they were found to be employing false accounts while tweeting about regional issues, mainly directed at Qatar and Yemen (Twitter safety, 2019).

Facebook has also found coordinated inauthentic behaviour originating from the UAE-based private marketing firm Charles Communications, with the aim of "artificially increasing engagement" by using fake accounts, and the creation of regional news outlet pages to attract local audience mainly in countries in the Middle East and African region. Many of the pages disseminated messages that were critical of the Qatari government and of the Muslim Brotherhood. The pages run by this firm and two others based in Egypt and Nigeria had around 1.4 million followers on Facebook, 70,000 on Instagram, and around USD 150,000 had been spent on Facebook ads, paid for primarily in US dollars and Emirati dirhams. The pages had clear political objectives, including the promotion of the UAE's image in the targeted regions. These accounts, however, were not proven to be linked to government officials (Sardarizageh, 2019).

In April 2020 Twitter removed 5350 accounts and Facebook removed 55 pages connected to a network of coordinated inauthentic behaviour from UAE, Saudi Arabian and Egyptian datasets. Twitter claimed that multiple social media management firms created this network and found tweets from 2013 that were supportive of Khalifa Haftar, a Libyan strongman who heads the Libyan National Army. This suggests that disinformation operations originating from the UAE targeting Libya were already present in 2013. The accounts discussed domestic politics with an anti-Qatar and anti-Iran narrative. Other prominent narratives included the discrediting of Libyan peace talks, criticism about Iranian influence in Iraq, and criticism of Huthi rebels in Yemen (Stanford Internet Observatory, 2020).

This strategy was also used in the context of the 2017 Gulf Crisis. The advancement of national interests online seemed to have become a more convenient tactic in comparison to other more visible kinetic attacks. Mark Owen Jones' s study on the weaponization of Twitter bots states that bots were used to manipulate Twitter trends and promote narratives "aiming at demonizing Qatar and its government" (Jones, 2019). Jones noted that "in the two months before the Gulf Crisis started, a network of Twitter accounts was set up specifically to have anti-Qatar messages in their bios". These bots attempted to amplify hashtags in order to tempt real people to adopt the hashtags. The source of these accounts remains unclear, however prominent Twitter influencers in the UAE later tweeted about the subject that was then picked up by real accounts (Ritzen, 2019).

According to Ben Nimmo, head of research at the social network analysis firm Graphika, these coordinated networks reveal the scale of pro-Saudi and pro-UAE online operations promoting anti-Qatar and anti-Iran narratives. However, they also reveal the increasing role of marketing PR firms in managing and running disinformation operations on behalf clients. By using PR firms, clients can promote certain political positions while hiding their identities (Sardarizadeh 2019).

Spreading Misinformation: In July 2020 the Daily Beast news website exposed a network consisting of at least 19 fake personas that had successfully placed more than 90 opinion pieces in 46 different publications. The articles promoted narratives praising the United Arab Emirates and criticising Qatar, Turkey, Iran and its proxy groups in Lebanon and Iraq. The personas were given Twitter accounts in March and April 2020, which in turn presented the personas as political consultants and freelance journalists and used fake LinkedIn accounts and fake and stolen avatars. Since the exposure of these personas as fake, the publications involved have removed the articles from their websites and issued apologies, and Twitter has suspended 16 of the accounts (Rawnsley, 2020).

Blocking and censorship: In December 2018, Dubai Police reported that they had blocked 5,000 fake social media accounts in the UAE through an "automated system that monitors this type of account" (Agrarib, 2018). Surveillance is aided by private cybersecurity firm DarkMatter, which acknowledged that 80% of its customers are UAE government agencies. One former DarkMatter operative, also a former US National Security Agency employee, stated that under order from the UAE government they would monitor social media and target people deemed by the UAE's security forces to have insulted the UAE government (Bing and Schectman, 2019).

A report undertaken by Citizen Lab on targeted threats in the UAE found evidence that the UAE government conducts malware attacks against civil society. At least three dissidents, including a journalist and a human rights activist, were targeted in 2012 with Hacking Team spyware. The UAE client had a license from Hacking Team to infect and monitor 1100 devices (Marczak, & Scott-Railton, 2016). In an additional report, Citizen Lab found evidence of the use of Blue Coat products (a California-based provider of network security and optimization products) in the UAE for filtering and monitoring on public networks. According to Citizen Lab, that the UAE has a well-known and pervasive regime of internet content filtering suggests that the presence of Blue Coat filtering products is not surprising (Marquis-Boire et al., 2013).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in United Arab Emirates

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Fake, Real and Hacked	Messages that promote UAE image, anti-Qatar messages, anti-Muslim Brotherhood messages, anti-Iran, anti-Turkey, harassing political dissidents, pro-Saudi, anti-Yemen's southern separatist movement	Use of Trolls and Bots, artificially increasing engagement, the creation of regional news outlets, hacking, misinformation	Twitter, Facebook, Instagram

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

The Huffington Post reported in 2015 that the UAE had spent more than USD 12 million on lobbying and PR from 2014 to 2015, and that some suspect that this has been used to counter online allegations of human rights abuses in the UAE (Ahmed 2015). In 2017, Cambridge Analytica executives created Emerdata, under parent company SCL Social Ltd, which was reportedly awarded a $330,000 contract from the National Media Council of the UAE for social media outreach. The company is recorded as spending USD 60,000 on ads on Facebook, YouTube and Twitter to promote the #BoycottQatar hashtag, and links to articles critical of Qatar alongside disinformation (Siegelman, 2018). The Harbour Group, which has represented the UAE for over 15 years, was allegedly paid more than USD 2.5 million by the UAE for work between October 2016 and March 2017.

Table 3: Cyber Troop Capacity in United Arab Emirates

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
	USD 60,000 on social media ads to promote anti Qatar hashtags and articles, Charles Communication firm spent USD 150,000 on Facebook ads for it coordinated network, Newave spent around USD 167,000 on Facebook ads paid primarily in US dollars and Emirati dirhams.			

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

References

Agrarib, A. 2018. UAE blocks 5,000 fake social media pages. *MSN*.

Ahmed, S. A. 2015. How Wealthy Arab Gulf States Shape the Washington Influence Game. *The Huffington Post*. https://www.huffpost.com/entry/arab-gulf-states washington_n_55e62be5e4b0b7a9633ac659.

Arabian Business. 2015. UAE in crackdown on social media abuse. *Arabian Business*. https://www.arabianbusiness.com/uae-in-crackdown-on-social-media-abuse-585044.html.

Bing, C. and Schectman, J. 2019. Special Report: Inside the UAE's secret hacking team of U.S. mercenaries. *Reuters*. https://www.reuters.com/article/us-usa-spying-raven-specialreport-idUSKCN1PO190.

Collier, K. 2018. How Persian Gulf Rivals Turned US Media into their Battleground. *BuzzFeed News*. https://www.buzzfeednews.com/article/kevincollier/qatar-uae-iran-trump-leaks-emails-broidy

DeYoung, K. and Nakashima, E. 2017. UAE orchestrated hacking of Qatari government sites, sparking regional upheaval, according to U.S. intelligence officials. *Washington Post*. https://www.washingtonpost.com/world/national-security/uae-hacked-qatari-government-sites-sparking-regional-upheaval-according-to-us-intelligence-officials/2017/07/16/00c46e54-698f-11e7-8eb5-cbccc2e7bfbf_story.html

European Parliament. 2017. Countering Terrorist Narratives. *European Parliament*. https://www.europarl.europa.eu/RegData/etudes/STUD/2017/596829/IPOL_STU(2017)596829_EN.pdf

Facebook. 2019. Removing Coordinated Inauthentic Behavior in UAE, Egypt and Saudi Arabia. *Facebook*. https://about.fb.com/news/2019/08/cib-uae-egypt-saudi-arabia/.

Freedom House. 2018. United Arab Emirates. *Freedom House*. https://freedomhouse.org/country/united-arab-emirates/freedom-world/2018.

Freedom House. 2019. Freedom of the Net UAE. *Freedom House*. https://freedomhouse.org/country/united-arab-emirates/freedom-net/2019#footnote2_wzy8oxq.

Jones, M. O. 2019. Propaganda, Fake News, and Fake Trends: The Weaponization of Twitter Bots in the Gulf Crisis. *International Journal of Communications*, 13, pp. 1389-1415.

Krieg, A. 2018. Never mind Russia, the UAE has united with AIPAC to capture Washington. *Middle East Eye*.

Marczak, B., & Scott-Railton, J. 2016. Keep Calm and (Don't) Enable Macros. *The Citizen Lab*. https://citizenlab.ca/2016/05/stealth-falcon/.

Marquis-Boire, M., Dalek, J., McKune, S., Carrieri, M., Crete-Nishihata, M., Deibert, R. Khan, O. S., Noman, H., Scott-Railton, J., & Wiseman, G. 2013. Planet Blue Coat. The Citizen Lab. https://citizenlab.ca/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/.

Rawnsley, A. 2020. Right-Wing Media Outlets Duped by a Middle East Propaganda Campaign. *The Daily Beast*. https://www.thedailybeast.com/right-wing-media-outlets-duped-by-a-middle-east-propaganda-campaign.

Ritzen, Y. 2019. The fake Twitter accounts influencing the Gulf crises. *Al Jazeera*. https://www.aljazeera.com/news/2019/07/fake-twitter-accounts-influencing-gulf-crisis-190717052607770.html .

Sardarizageh, S. 2019. Facebook removes 'fake' UAE, Egypt accounts for paid disinformation operation. *BBC monitor*. https://monitoring.bbc.co.uk/product/c2015157.

Shires, J. 2020. The cyber operation against Qatar News Agency. In Zweiri, M. (ed.), *The Gulf Crisis: Origins, Implications, Repercussions*. Springer Nature (forthcoming).

Siegelman, W. 2018. From the Seychelles to the White House to Cambridge Analytica, Erik Prince and the UAE are key parts of the Trump story. *Medium*. https://medium.com/@wsiegelman/from-the-seychelles-to-the-white-house-to-cambridge-analytica-erik-prince-and-the-uae-are-key-6d860808da91.

Stanford Internet Observatory. 2020. Analysis of April 2020 Twitter takedowns linked to Saudi Arabia, the UAE, Egypt, Honduras, Serbia, and Indonesia. *Stanford Internet Observatory*. https://cyber.fsi.stanford.edu/io/news/april-2020-twitter-takedown.

Twitter safety. 2019. Disclosing new data to our archive of information operations. *Twitter Blog*. https://blog.twitter.com/en_us/topics/company/2019/info-ops-disclosure-data-september-2019.html

Vice News. 2015. The US and United Arab Emirates Built an Anti-Jihad Propaganda Centre. *Vice*. https://www.vice.com/en_us/article/mbne38/the-us-and-united-arab-emirates-built-an-anti-jihad-propaganda-center

Wood, J. 2018. Here's how a diplomatic crisis among Gulf nations led to a fake news campaign in the U.S. *Pittsburgh Post-Gazette*. https://www.post-gazette.com/news/world/2018/08/02/Here-s-how-a-diplomatic-crisis-among-Gulf-nations-led-to-a-fake-news-campaign-in-the-US/stories/201807020364.

United States

Introduction

The United States has experienced large amounts of computational propaganda, both shared by its government and non-state actors. The adoption of techniques to influence political opinion online has become general electoral and political practice. This is perhaps partially due to the US's electoral framework, in that in the US there are frequent and localized elections, and as such more frequent and localized imperatives to manipulate media. While misleading information is from foreign actors is still targeting the US, such as recent pandemic disinformation being spread in the US by both China and Russia (see the case studies for these countries for further information), domestic misinformation has become much larger and a much more serious issue (Pen America, 2019).

The nature and sources of computational propaganda in the US vary widely: form interactive advertisements to live-streamed video, memes, and personalized messaging. According to Woolley and Guibeault (2017), the tacit goal of using these tools is to affect voter turnout, but also to "achieve other, less conventional goals. Namely: to sow confusion, to give a false impression of online support, to attack and defame the opposition, and to spread illegitimate news reports."

Organizational Form

One of the first systematic and organized efforts of computational propaganda can be traced to 2011, when DARPA set up its Social Media in Strategic Communication (SMISC) program with the double aim of detecting *and* conducting propaganda campaigns on social media. It financed a variety of studies regarding the potential use and manipulation of social media (Quinn & Ball, 2014). Research has also been undertaken by other organizations under the remit of the Department of Defense, such as the US Air Force Research Laboratory. Most of these operations target foreign audiences, with the US Smith-Mundt Act prohibiting "public diplomacy" with domestic audiences. However, the Smith-Mundt Modernization Act of 2012 overturned this provision. It is unclear whether domestic audiences have begun to be targeted as well. *The Washington Post* explicitly tied the overturning of the act to the involvement of the Pentagon in a counter-propaganda initiative against the US-based "extremist" Somalimidnimo.com website (Rawnsley, 2011).

Other efforts directed at foreign audiences include active campaigns of influence that are in line with the US tradition of public diplomacy through print media and broadcasting, as well as counter-propaganda activities. As first reported by *USA Today* in 2008 (Brook, 2012), the US Special Operations Command directs a collection of websites with a civilian appearance, also known as the Trans Regional Web Initiative (including Southeast Europe Times, SES Turkey, Magharebia, Mawtani al-Shorfa and Central Asia Online). Through these websites, the organization conducts psychological operations to combat violent extremist groups. The organization has subcontracted to Navanti Group to help conduct "information operations to engage local populations and counter nefarious influences" in Africa and Europe (Ibid).

In another case of state funded computational propaganda, in 2019 it was revealed that the Iran Disinformation Project, an organization created to counter foreign propaganda and disinformation, had been trolling US journalists, human rights activists, and academics it deemed to be "insufficiently hostile to the government in Tehran" (Borger, 2019). The organization, which was funded by the state department's global engagement center up until complaints began to rise, engaged in the denunciation of various advocates and journalist as being “mouthpieces” and supporters of the Iranian government through their Twitter account. The global engagement center was originally created to counter Russian and ISIS disinformation and propaganda. However, according to Brett Bruen, former director of the center, in recent years the center has turned towards “syphoning money off to attack the Iran [nuclear] deal and Iran” and that “the center in being treated by the Trump administration like it is a reserve for dipping in to for pet political projects” (Ibid).

The recent Democratic Party primaries have led to a surge in computational propaganda. For example, in February 2020 Twitter reported that it had suspended 70 accounts associated with the campaign of Michael Bloomberg for violating rules “against platform manipulation and spam” (Hussain and Bercovici, 2020). The accounts were reportedly operated by humans and disseminated identical messages in support of the Bloomberg campaign. The campaign employed hundreds of operators with salaries of thousands of dollars (Horowitz and Wells, 2020).

Some candidates in the Democratic party have also relied on astro-turfing to promote their campaigns. For example, during the presidential debate in 2016 the Clinton campaign signed up and trained a number of “grass-roots tweeters” who were asked to post specific messages and graphics at coordinated and strategic times. A similar strategy was adopted by the Bernie Sanders campaign, which coordinated with social media “volunteers” in closed Slack rooms (Dewey 2016). In the 2016 presidential campaign, the Clinton campaign also benefited from the support of the Brock network. This network includes organizations such as the watchdog website Media Matters for America, two pro-Clinton “super PACs”, the opposition research outfit American Bridge, the pro-Clinton fact-checking Correct the Record, and the Shareblue organization, which with a budget of USD $2 million was focused on exposing alleged news coverage against Hillary Clinton and extensively engaging in astro-turfing throughout the campaign (Horowitz, 2016).

For the Republicans, Donald Trump and Ted Cruz both hired Cambridge Analytica in 2016 to conduct various online psychographic strategies. It has also been reported that the Trump campaign have engaged in intense astro-turfing by means of viral videos and memes. More recently, Channel 4 News exclusively obtained leaked data from the Trump presidential campaign that revealed how over 3.5 million Black Americans were categorised by the campaign as ‘Deterrence’ voters, voters that they wanted to stay home on election day (Channel 4 News). The data leaked contained details on almost 200 million Americans that were separated into eight categories so that they can be targeted with tailored ads on Facebook and other platforms (Ibid). Furthermore, Nimble America, a non-profit funded by Silicon Valley millionaire Palmer Luckey, orchestrated an anti-Clinton campaign, and the Koch brothers have coached up a “grass-roots” army of their own, offering online certificate courses in things like “social media best practices” via their conservative advocacy group Americans for Prosperity (Dewey, 2016).

The threat of manipulative online activity is also posed by political actors not officially affiliated with election campaigns but working on their behalf. In December 2019, *The New York Times* published a piece revealing a group of Democrat-supporting tech experts who ran a “Russian-style” disinformation campaign (or “experiment”, as they called it) ahead of the 2017 Alabama senate race between Republican Roy Moore and Democrat Doug Jones (who eventually won). The group, apparently backed financially and technologically by prominent figures in the tech industry, used various tactics to discredit Moore and emphasize rifts between Republican voters to sway voters. Allegedly, among those involved in this activity were Jonathan Morgan, head of a cybersecurity firm that worked with the Senate Intelligence committee on disinformation in the 2016 elections, and American Engagement Technologies (AET), an anti-disinformation company funded by Reid Hoffman, the co-founder of LinkedIn. After the Times' publication, Facebook removed five accounts associated with this activity for coordinated inauthentic behavior, one of which belonged to Morgan (PEN America 2019, 42).

In April 2020, Facebook published a report stating it had removed accounts, pages and groups involved in two separate operations of coordinated inauthentic behavior in the US, both focused on domestic audiences. The first network had 5 pages, 20 Facebook accounts, and 6 groups removed by Facebook administrators, and was associated with the far-right QAnon conspiracy theory, a conspiracy alleging a "deep state" plot to overthrow Donald Trump (Facebook, 2020a). Recently, during the COVID-19 pandemic, QAnon has turned its focus towards pandemic conspiracy theories. Some of these arguments include: "Coronavirus is a cover-up for … child sex trafficking – a major issue in this world and nobody wants to report about it". This type of content has been spread through Twitter and Facebook groups that focus on parenting, health, fitness, lifestyle, etc. (Spring & Wendling, 2020). QAnon is particularly popular among some circles of the Trump Administration, which itself has legitimized the theory in various ways. For example, Trump's Director of National Intelligence, John Ratcliff, follows accounts that promote the theory on Twitter, and the president himself has retweeted content from QAnon-supporting users (Robertson 2020), including a recent tweet by a QAnon twitter account that claimed that the real number of deaths in the US from coronavirus was much less than what was being reported (Spring and Wendling, 2020).

The second network removed by Facebook was linked to the anti-immigration and white nationalist organization VDARE, and The Unz Review, a self-described "alternative media" website that actively promotes international Jewish domination conspiracy theories and other race-centric plots. Much of the content promoted by this network focused on topics such as far-right ideologies, President Trump, anti-immigration, hate speech about Asian Americans, and COVID-19-related conspiracies. Facebook removed 19 pages, 15 Facebook accounts, and one group related to this network (Facebook, 2020a).

Protests responding to the killing of George Floyd, an unarmed African-American man, by Minneapolis police, have also been a target for organized disinformation campaigns by far-right non-state actors, and have received sustained amplification by President Trump and his administration. The vast majority of this activity tried to discredit the nationwide protest movement by associating it with the Antifa movement. The goal of this campaign appears to have been to blur the lines between the hundreds of thousands of peaceful protestors and sporadic incidents of street violence. The first influential mention of the protests in relation to antifa came from a popular QAnon Twitter account on the second night of the protests. The tweet purported that the protests were backed by George Soros, a Jewish financier who is often the target of anti-Semitic conspiracy theories, and that the "deep state" was trying to start a race war (DFRLab, 2020). Another disinformation campaign that was falsely linked to the Black Lives Matter campaign was the spread of propaganda and social media posts calling for violence against white people. This disinformation also intended to characterize the BLM movement as violent and extremist (ADL, 2020).

On July 8th, 2020, Facebook announced that it had removed another 54 Facebook accounts, 50 pages, and 4 Instagram accounts that were involved in coordinated inauthentic behavior in the US. Many of these were associated with the Proud Boys, a far-right hate group banned by Facebook in 2018, and Roger Stone, a conservative political consultant and Trump campaign advisor who was convicted on seven felonies in connection to the Russian government's efforts to intervene in the 2016 US presidential elections (Facebook, 2020b). On July 10th, Trump granted executive clemency to Roger Stone, days before he was to report to prison (Baker et al., 2020). Graphika's analysis reported that the bulk of accounts associated with the network were highly active during the time of the 2016 US presidential election. However, some accounts were still active in 2020 and primarily focused on Stone's court case. 18 of the accounts taken down were located in Florida and had a strong Florida focus. The network posted about general Florida issues, including local politics and environmental issues, some of which directly connected to industries Stone has lobbied for in the past, such as sugar (Graphika, 2020).

An additional aspect of online misinformation in the United States is the content shared from President Trump's personal Twitter account. Misleading political content is often distributed online by Trump himself. In the past year Trump has been accused of promoting a number of false conspiracy theories through tweets he wrote on his own or retweets from known conspiracist accounts such as those related to the conspiracy theory QAnon (Freedom of the Net, 2019). Supporters of Trump have also been accused of organizing and participating in coordinated behavior online. For example, the pro-Trump youth group Turning Point Action, an affiliate of the prominent conservative youth organization Turning Point USA, has been accused of enlisting teens in a secretive campaign likened to a "troll farm" (Stanley-Becker, 2020a).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in the United States

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
	Social Media in Strategic Communication, DARPA, US Air Force Research Laboratory, US Special Operations Command , Global Engagement Centre	Democratic party, Michael Bloomberg, Bernie Sanders, Republican party, Donald Trump, Ted Cruz, Doug Jones	Navanti Group, Cambridge Analytica, Nimble America, American Engagement Technologies, Devumi, Cambridge Analytica	Brock network, Media Matters for America, American Bridge, Correct the Record, Shareblue, Americans for Prosperity, Proud Boys, VDare, Turning Point Action, Iran Disinformation Project	David Brock, Palmer Luckey, Koch brothers, Jonathan Morgan, Reid Hoffman, Roger Stone

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Driving division: The group of Democrat-supporting tech experts operating in relation to the 2017 Alabama Senate elections used a diverse set of strategies to achieve their goals. One strategy included the creation of a fake Facebook page for conservative Alabamians, endorsing a Republican write-in candidate in order to divide Republican voters and sway votes away from Moore (PEN American, 2019). Another strategy was an elaborate 'false flag' scheme whereby thousands of Russian-looking accounts began following Moore on Twitter, causing the illusion of a Moore-Russian amplification botnet. As a result of a report by *The New York Times*, this activity obtained national media attention (Shane and Blinder, 2018). *The New York Times* later reported on a similar Democrat-operated project aimed at defeating Moore in 2017. This project revolved around a Facebook page by the name of Dry Alabama, which seemed to be run by Baptist Moore supporters pushing for the ban of alcohol in Alabama. By doing so, the page operators aimed at intensifying the rift between religious conservatives and business conservatives in the state (PEN America, 2019).

Astro turfing: Astro-turfing appears to have become commonplace in US politics. For instance, the firm Devumi stands accused of stealing real people's identities for at least 55,000 bots out of a network of about two million it possesses. The company's clients covered the political spectrum, from liberal cable pundits to a reporter at the right-wing site Breitbart, political commentator Hilary Rosen, and US ironworker-turned politician Randy Bryce (Confessore et al., 2018). Such tactics are also used for specific political issues. For example, North Texans for Natural Gas, a seemingly "grass-roots" group, was discovered to have been funded by four Texas energy companies when it attracted the attention of several media outlets for launching a pro-fracking meme factory (Dewey, 2016). In another example, the Environmental Protection Agency, coordinated a campaign to promote the Clean Water Act rule, but failed to disclose the origin of the Thunderclap messages, by de facto engaging in astroturfing (Lipton & Shear, 2015).

Disinformation: Another tactic used in the US has been the spread of disinformation to steer public debate and delegitimize public protests. Research conducted by Buzzfeed on the spread of misinformation delegitimizing the George Floyd protests, found that nearly 30% of the examined content contained "a nonexistent attack" – a suspected murder, explosion, or act of animal cruelty in order to paint the protests as an extremely violent movement (Lytvynenko & Silverman, 2020). Similar attempts at delegitimizing the protestors came from the president himself. Between June 3rd and 7th, Trump's re-election campaign sent millions of emails to supporters describing protesters as "dangerous MOBS" and "THUGS" which were "DESTROYING our cities and rioting", without context of the wider protest's movement (DFRLab, 2020).

According to research by DFRLab, the days following the start of the protest movement saw a surge in publication and interaction with "antifa"-related content online, most of it alarming in nature. For example, seven of the ten most popular antifa-related posts on Instagram between May 25th (the day of the incident) and June 7th, directly associated antifa with domestic terrorism. On May 31st, president Trump stated that his administration will declare Antifa as a terrorist organization, which further increased speculation surrounding the protests both online and on traditional conservative media (DFRLab, 2020). This surge in information manipulation, amplified by Trump and his administration, has led to an increasing national panic, especially in smaller and more rural communities. DFRLabs reported that "Local U.S. newspapers have examined and debunked rumors that antifa has dispatched 'a planeload of their people' to Payette County, Idaho or that buses of violent infiltrators are descending on places like Klamath Falls, Oregon or Casper, Wyoming." DFRLabs claimed that this panic has contributed to multiple incidents of violence and social unrest in the country (Ibid).

There have also been a number of cases in which President Trump himself took part in distributing misleading and fraudulent messages through his Twitter account. For example, in 2019 Trump retweeted a video of congresswoman Ilhan Omar dancing, and which falsely claimed that Omar was partying on the anniversary of 9/11. The video was not filmed on 9/11 (Rupar, 2019). On another occasion Twitter restricted President Trump's campaign from tweeting after its account shared a video containing false claims about the coronavirus. The video showed an interview of Trump with Fox News in which he said that Children are "almost immune" to the virus. According to Twitter, this was a violation of Twitter Rules on Covid-19 misinformation (Iyengar, 2020). In another example, Twitter restricted one of Trump's tweets on the basis of a "glorification of violence". In the tweet Trump quoted Walter E. Headley, the police chief of Miami, Florida in 1967, by tweeting "when the looting starts the shooting starts" in response to Black Lives Matter protests (The Cube, 2020). Trump has also shared a tweet featuring a doctored video of rival presidential candidate Joe Biden. The video, shared by the Twitter user "The United Spot," showed Biden during a campaign event in Florida and replaced the song "Despacito" that was being played with the anti-police anthem by N.W.A. Twitter flagged the post as manipulated media and linked to the real video of Biden from an event celebrating Hispanic Heritage Month (Quinn, 2020).

One of the most prominent narratives recently disseminated by conservatives, Republicans, and Donald Trump himself, has focused on postal voting. One of Trump's tweets on this issue urged people voting by mail in North Carolina to show up to polling sites to makes sure that their vote was being counted, and if it wasn't to go vote again in person. Trump's tweet was later covered with a warning form Twitter explaining that they consider the tweet election misinformation that violates their Civic Integrity Policy (Breland, 2020). Trump's tweets are the latest in a campaign that is trying to discourage voters from using the U.S Postal Service to deliver their ballots in the upcoming election, arguing that there is widespread voter fraud involved. This is despite there being no evidence of substantial voter-fraud linked to postal voting. It is suggested that this is a strategy that is intended to cause chaos and confusion (Stanley-Becker, 2020b).

Smear campaigns: An additional strategy being used in the US is the promotion of smear campaigns to tarnish specific individuals. For example, a reporter and an editor at *USA Today* were targeted in an online propaganda campaign because of their investigations of Leonie Industries, the Pentagon contractor in charge of info ops in Afghanistan. According to *The Washington Post*, a minority owner of the firm admitted to having set up the smear campaign, which included the creation of fake websites under the journalists' names, the editing of their Wikipedia pages, the posting of fake information on forums with the intent of tarnishing the journalists' reputation, and fake Twitter accounts under their names (Cook, 2012).

In the case of the accounts associated with the Roger Stone network that were taken down by Facebook, Graphika found that many of the profile pictures used by these accounts were taken from other online sources, such as celebrities, random news articles, and Getty Images. Their activity varied, but one notable case of harassment associated with the network occurred on February 4th, 2017, after a judge from the Western District of Washington imposed a temporary restraining order on Trump's "Muslim ban". On February 12th, the network's largest page, "Stone Cold Truth", posted a meme denouncing the judge's decision and included his official work address and phone numbers, inviting followers to "call or email". Days later, two other accounts in this network posted the same meme (Graphika, 2020).

Anti-extremist campaigns: The Center for Strategic Counterterrorism Communications (CSCC) was set up in 2011 to coordinate anti-jihadist and violent extremist campaigns. It managed more than 350 Twitter accounts for the State Department, the Pentagon, the Department of Homeland Security and the accounts of foreign US allies in a sock-puppet network. On YouTube, Facebook and Twitter, US diplomats have started to actively trolling Isis, arguing with pro-Isis accounts and producing videos portraying Isis-conquered territory as a hellscape (Ackerman, 2014). US military Central Command coordinated an astroturfing campaign called "Operation Earnest Voice", officially targeting al-Qaeda, the Taliban, and other jihadist groups in the Middle East. It began as a psychological warfare operation in Iraq to combat the online influence of those opposed to the coalition's presence in the country (Fielding & Cobain, 2011).

The SMISC program set up by the Department of Defense in 2011 financed a variety of studies: some more theoretical in scope (topic trend analysis and sentiment detection, modelling emergent communities and network dynamics), and others more directly linked to online propaganda (automated and crowd-sourced content generation, persuasion campaign structures recognition and effects measurements, as well as counter-messaging tactics). Similar research, such as that undertaken by the US Air Force Research Laboratory, investigated how human behaviour could be manipulated through social networks, or the development of software for the use of "sock puppets" to manipulate social media and influence online conversations (Gallagher, 2014).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in the United States

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Fake, Human	Promotion of political campaigns and specific political issues, Delegitimizing Black Lives Matter protests, promoting messages connecting the Black Lives Matter protests to the Antifa movement, smear campaigns, anti- extremism campaigns abroad, driving division between republican voters, sowing confusion around voting by mail	Astro-turfing, spreading disinformation, troll farms, targeting ads , amplification	Facebook, Twitter, YouTube, Instagram

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

It is evident that federally-sponsored computational propaganda projects have very high budgets. As such, the SMISC program set up by the Department of Defense in 2011 received USD $50 million in funding (Waltzman, 2015). In 2014, the government spent USD $760 million to hire private advertising firms, according to USASpending.gov, from marketing research to opinion polling to message-crafting assistance, etc (Hamilton & Kosar, 2015). According to a 2008 USA Today report, the Trans Regional Web Initiative has operations in

22 countries. It's funding in 2009 peaked at USD $580 million a year (Brook 2012), but this was progressively reduced an was on the verge of extinction in 2014 (Locker, 2014). Operation Earnest Voice, coordinated by the US Military Central Command, is reported to have received more than $200 million in funding since its inception. The software it developed, contracted for USD $2.76 million to Ntrepid, allows for posting from different accounts, covered by a VPN to randomize location and avoid detection (Fielding & Cobain 2011).

The accounts taken down by Twitter and associated with the Bloomberg campaign have been budgeted with thousands of dollars. Hundreds of "deputy field organizers" received USD $2,500 per month each to promote Bloomberg's candidacy within their social circles and recruit friends (among other conventional duties) and echo the campaign messaging on social media. Many of these accounts were created after December 2019, with Bloomberg's campaign officially beginning in late November (Hussain and Bercovici, 2020).

Facebook reported that the network associated with VDARE and The Unz Review had spent around USD $114,000 on ads, and had over 207,000 accounts following it. It also found that the network associated with the QAnon conspiracy theory had about 133,000 accounts following one or more of their pages, and 30,000 accounts that were group members (Facebook, 2020a).

According to Facebook's ad library, the network associated with Roger Stone that was taken down in early July spent "over $4,500 on 82 sponsored ads between May 2018 and the end of October 2018" (Graphika, 2020). Facebook disclosed that less than USD $308,000 was spent on ads on Facebook and Instagram (Facebook 2020b). Some of the pages associated with the network appeared to have acquired followers from Pakistan and Egypt to increase the perception of their popularity. Most of the pages had a relatively low following, which averaged at around 5,000, but there were a few exceptions: the page named "Roger Stone – Stone Cold Truth" had over 140,000 followers (Graphika, 2020). Overall, about 260,000 accounts followed at least one of these pages, and 62,000 people followed at least one of these Instagram accounts (Facebook, 2020b).

Table 3: Cyber Troop Capacity in the United States

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
	SMISC funding: USD $50 million , USD $760 million spent on advertisement, USD $580 million paid to SOCOM and the Trans Regional Web in 2009 but it has since deflated. Bloomberg campaign online workers paid 2500 a month, Roger Stone network spent over USD 300,000 on advertising.			

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

References

ADL. 2020. Disinformation: Propaganda advocating for violence against white people using hashtags associated with Black Lives Matter and antifa. *Anti-Defamation League.* https://www.adl.org/disinformation-propaganda-advocating-for-violence-against-white-people-using-hashtags-associated.

Ackerman, S. 2014. Isis's online propaganda outpacing US counter-efforts, ex-officials warn. The Guardian. https://www.theguardian.com/world/2014/sep/22/us-battle-counter-isis-propaganda-online-officials-warn.

Baker, P., Haberman, M., & LaFraniere, S. 2020. Trump Commutes Sentence of Roger Stone in Case He Long Denounced. *The New York Times*. https://www.nytimes.com/2020/07/10/us/politics/trump-roger-stone-clemency.html

Blanchard, N. and Brown, R. 2020. Police: No, antifa not sending 'a plane load of their people' to Idaho to incite riots. *Idaho Statesman*. https://www.idahostatesman.com/news/local/article243180241.html#storylink=cpy

Borger, J. 2019. US cuts funds for 'anti-propaganda' Iran group that trolled activists. *The Guardian.* https://www.theguardian.com/us-news/2019/may/31/us-cuts-funds-for-anti-propaganda-group-that-trolled-activists.

Breland, A. 2020. Twitter Just Slapped Trump with Another Violation for Spreading Election Disinformation. *Mother Jones*. https://www.motherjones.com/2020-elections/2020/09/twitter-trump-violation-election-disinformation-voter-fraud/.

Brook, T. V. 2012. Special Operations Command Leads Propaganda Fight. *USA Today*. https://www.usatoday.com/story/news/world/2012/12/06/socom-leads-propaganda-fight/1746013/.

Channel 4 News. 2020. Revealed: Trump campaign strategy to deter millions of Black Americans from voting in 2016. *Channel 4 News.* https://www.channel4.com/news/revealed-trump-campaign-strategy-to-deter-millions-of-black-americans-from-voting-in-2016.

Confessore, N., Dance, G. J.X., Harris, R., & Hansen, M. 2018. The Follower Factory. *The New York Times.* https://www.nytimes.com/interactive/2018/01/27/technology/social-media-bots.html?searchResultPosition=1.

Cook, J. 2012. Propaganda Contractor Admits to Running Smear Campaign Against USA Today Reporters (UPDATE). *Gawker*. https://gawker.com/5913166/propaganda-contractor-admits-to-running-smear-campaign-against-usa-today-reporters.

Dewey, C. 2016. The three types of political astroturfing you'll see in 2016. *The Washington Post.* https://www.washingtonpost.com/news/the-intersect/wp/2016/09/26/the-three-types-of-political-astroturfing-youll-see-in-2016/.

DFRLab. 2020. The disinformation campaign to define US protesters as terrorists. *Medium.* https://medium.com/dfrlab/the-disinformation-campaign-to-define-u-s-protesters-as-terrorists-3ea8db0a4881

Facebook. 2020a. April 2020 Coordinated Inauthentic Behavior Report. *Facebook.* https://about.fb.com/wp-content/uploads/2020/05/April-2020-CIB-Report.pdf

Facebook. 2020b. Removing Coordinated Inauthentic Behavior. *Facebook.* https://about.fb.com/news/2020/07/removing-political-coordinated-inauthentic-behavior/.

Fielding, N. & Cobain, I. 2011. Revealed: US spy operation that manipulates social media. *The Guardian.* https://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks.

Freedom of the Net. 2019. United States Freedom on the Net. *Freedom House.* https://freedomhouse.org/country/united-states/freedom-net/2019.

Gallagher, S. 2014. Air Force research: How to use social media to control people like drones. *Ars Technica*. https://arstechnica.com/information-technology/2014/07/air-force-research-how-to-use-social-media-to-control-people-like-drones/.

Gleicher, Nathaniel. 2020. Removing Coordinated Inauthentic Behavior. *Facebook.* https://about.fb.com/news/2020/07/removing-political-coordinated-inauthentic-behavior/

Graphika Team. 2020. Facebook's Roger Stone Takedown. Graphika. https://public-assets.graphika.com/reports/graphika_report_roger_stone_takedown.pdf

Hamilton, J. M., & Kosar, Kevin. 2015. How the American government is trying to control what you think. *The Washington Post*. https://www.washingtonpost.com/posteverything/wp/2015/09/24/the-new-propaganda-how-the-american-government-is-trying-to-control-what-you-think/.

Horowitz, J. 2016. Shareblue galvanizes Twitter army to voice outrage on Clinton's behalf. *Seattle Times.* https://www.seattletimes.com/nation-world/shareblue-galvanizes-twitter-army-to-voice-outrage-on-clintons-behalf/.

Horowitz, J., & Wells, G. 2020. Bloomberg Bankrolls a Social Media Army to Push Message. *The Wall Street Journal*. https://www.wsj.com/articles/bloomberg-bankrolls-a-social-media-army-to-push-message-11582127768

Hussain, S. & Bercovici, J. 2020. Twitter is suspending 70 pro-Bloomberg accounts, citing 'platform manipulation'. *Los Angeles Times.* https://www.latimes.com/business/technology/story/2020-02-21/twitter-suspends-bloomberg-accounts

Iyengar, R. 2020. Facebook takes down Trump about COVID-19. The Mercury News. https://www.mercurynews.com/2020/08/05/facebook-takes-down-trump-post-about-children-covid-19/.

Learned, N. 2020. No, Those School Buses Did Not Bring Protesters to Casper. *K2 Radio.* https://k2radio.com/no-those-school-buses-did-not-bring-protesters-to-casper/?trackback=twitter_mobile

Lipton, E., & Shear, M. D. 2015. E.P.A. Broke Law With Social Media Push for Water Rule, Auditor Finds. The New York Times. https://www.nytimes.com/2015/12/15/us/politics/epa-broke-the-law-by-using-social-media-to-push-water-rule-auditor-finds.html.

Locker, R. 2014. Military Propaganda on the Verge of Extinction. USA Today. https://www.usatoday.com/story/nation/2014/01/02/trans-regional-web-initiative-defense-bill/4291467/,

Lytvynenko, J., & Silverman, C. 2020. We're Keeping a Running List of Hoaxes and Misleading Posts About the Nationwide Police Brutality Protests. *Buzzfeed News*. https://www.buzzfeednews.com/article/janelytvynenko/hoax-misleading-claims-george-floyd-protests

PEN America. 2019. Truth on the Ballot Report. *Pen America*.https://pen.org/wp-content/uploads/2019/03/Truth-on-the-Ballot-report.pdf

Quinn, B., & Ball, J. 2014. US military studied how to influence Twitter users in Darpa-funded research. *The Guardian*. https://www.theguardian.com/world/2014/jul/08/darpa-social-networks-research-twitter-influence-studies.

Quinn, M. 2020. Trump tweets doctored video of Biden, prompting flag by Twitter. *CBS News.* https://www.cbsnews.com/news/trump-tweet-doctored-biden-video/.

Rawnsley, A. 2011. Pentagon Wants a Social Media Propaganda Machine. *Wired.* https://www.wired.com/2011/07/darpa-wants-social-media-sensor-for-propaganda-ops/.

Robertson, A. 2020. Facebook removes QAnon 'fringe conspiracy' groups ahead of 2020 election. T*he Verge.*https://www.theverge.com/2020/5/5/21248268/facebook-qanon-group-removal-conspiracy-theory-2020-election

Rupar, A. 2019. Trump retweets lie that Ilhan Omar “partied” on 9/11 anniversary. *Vox.* https://www.vox.com/2019/9/18/20872316/trump-ilhan-omar-9-11-partied-retweet-terrence-williams.

Shane, S., & Blinder, A. 2018. Secret Experiment in Alabama Senate Race Imitated Russian Tactics. The New York Times. https://www.nytimes.com/2018/12/19/us/alabama-senate-roy-jones-russia.html.

Spring, M., & Wendling, M. 2020. How Covid-19 myths are merging with the QAnon conspiracy theory. *BBC Trending*. https://www.bbc.com/news/blogs-trending-53997203.

Stanley-Becker, I. 2020a. Pro-Trump youth group enlists teens in secretive campaign likened to a ‘troll farm,’ prompting rebuke by Facebook and Twitter. *The Washington Post.* https://www.washingtonpost.com/politics/turning-point-teens-disinformation-trump/2020/09/15/c84091ae-f20a-11ea-b796-2dd09962649c_story.html.

Stanley-Becker, I. 2020b. Google greenlights ads with ‘blatant disinformation’ about voting by mail. *The Washington Post*. https://www.washingtonpost.com/technology/2020/08/28/google-ads-mail-voting/.

The cube. 2020. Twitter explains why not all Trump’s misleading tweets are flagged. *Euro News.* https://www.euronews.com/2020/06/24/twitter-explains-why-not-all-trump-s-misleading-tweets-are-flagged-thecube,

Waltzman, R. 2015. The Story Behind the DARPA Social Media in Strategic Communication (SMISC) Program. *Information Professionals Association.* https://information-professionals.org/the-darpa-social-media-in-strategic-communication-smisc-program/.

Woolley, S. C., & Guibeault, D. R. 2017. Computational Propaganda in the United States of America: Manufacturing Consensus Online. *Computational Propaganda Research Project*.

Zadrozny, B. & Collins, B. 2020. In Klamath Falls, Oregon, victory declared over antifa, which never showed up. *NBC News*. https://www.nbcnews.com/tech/social-media/klamath-falls-oregon-victory-declared-over-antifa-which-never-showed-n1226681

UZBEKISTAN

Introduction

In Uzbekistan there is evidence of cyber troop activity that is focused on trolling attacks and defending government policies. The cyber troop activity that does exist takes place in a context of a tightly controlled Internet (Freedom House, 2019). Uzbekistan has experienced a degree of liberalisation following the death of autocratic president Islam Karimov in 2016 and the subsequent presidency of Shavkat Mirziyoyev. However, official state media and the press offices of state organisations have a low level of credibility amongst the population. As a result citizens increasingly trust information that comes from abroad and this has created an environment in which the spreading of disinformation in Uzbekistan derives from foreign-based agents such as Russia.

Disinformation relating to the global COVID-19 pandemic has spread on social media platforms that are popular in Uzbekistan. According to an Interior Ministry announcement on 17th March, 2020, a special working group identified 33 accounts (on undisclosed platforms) that were disseminating harmful information and contributing to public panic (Yeniseyev, 2020). President Mirziyoyev stated in an address to the nation on 18th March 2020 that "we must not allow unreliable, unsubstantiated information to circulate in the media or on social networks" (Yeniseyev, 2020). According to a resident of Tashkent interviewed by Yeniseyev (2020), an example of coronavirus-related disinformation was the propagation on radical Islamist Facebook and Telegram channels that the word 'coronavirus' contains the word 'Koran' as the virus is punishing infidels. In response to disinformation, a Telegram channel called 'Koronavirus Info' was created by the Ministry of Health, Press and Information Agency, the National Foundation for Support and Development of National Mass Media and the Youth Union, amassing 1.4 million members – making it the largest Telegram channel in the country.

An Overview of Cyber Troop Activity in Uzbekistan

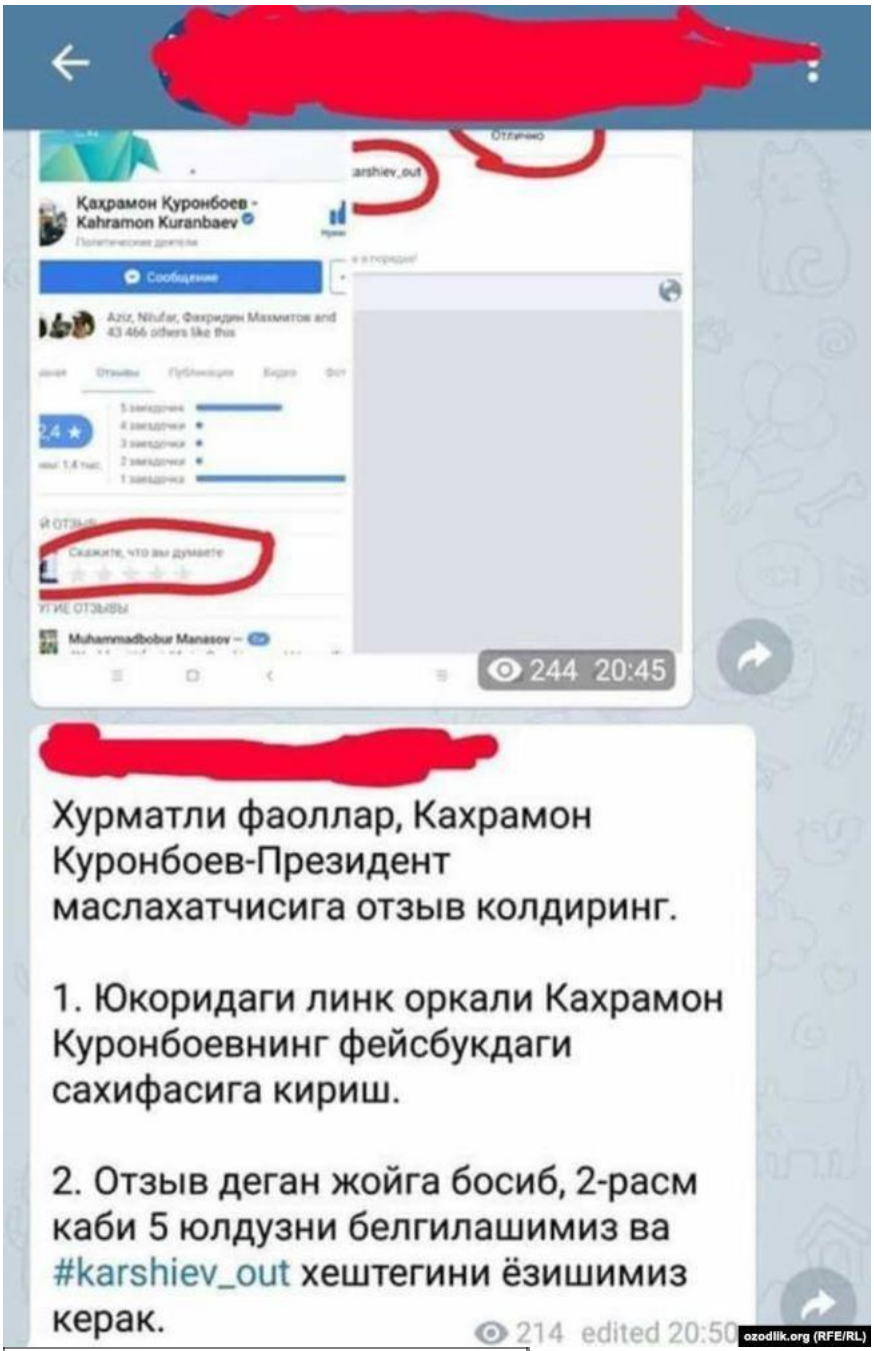
Organizational Form

Researchers from the Institute for War and Peace Reporting (IWPR) suggest trolling is closely linked to the National Security Service (now the State Security Service), which came to the fore after the 2005 Andijan violence, in which government forces violently repressed protestors (Rysaliev et al., 2012). Rysaliev et al. allege that whenever the Andijan killings are mentioned online, a barrage of comments appears blaming the bloodshed on Islamic terrorists. Likewise, in 2011, anonymous pro-government comments on social media appeared in defence of the daughter of former president, Islam Karimov (ACCA, 2020). Similar language and arguments from separate posters suggest that these attacks are either centrally organised or originate from the same person. For example, a reporter from Tashkent cited by the ACCA (2020) said that the National Security Service sometimes hired journalists in the state media to pose as anonymous commentators.

According to the ACCA (2020), the Youth Union of Uzbekistan took control of trolls and bots in 2018. Freedom House note that this government-affiliated youth organization smears government critics and spreads misinformation, such as the false claim that VPNs are illegal in Uzbekistan (Freedom House, 2019). An investigation by Radio Liberty's Uzbek service, Ozodlik, uncovered that there was an active group of members of Uzbekistan's Youth Union that were involved in trolling by using fake Facebook accounts (Бекиева, 2018). The youth involved say they were ordered by the union's management to each create 4-5 fake accounts to attack individuals who expressed negative sentiments towards the organisation. Fake accounts were coordinated through a "special group [that] had been set up on Telegram" called 'The Loyal Young Reporters' which had 85 members. Members were instructed to share links to Facebook posts on this Telegram channel, so that the other fake accounts could like, share, and comment on the post. An example of this coordination is evidenced by Ozodlik in figure 1. The image shows a post on the Loyal Young Reporters Telegram group, encouraging support for the head of Uzbekistan's Youth Union, Qahramon Quronboyev. The text beneath the image reads:

> Dear activists, write a post on the account of Qahramon Quronboyev, a presidential aide. 1) Open Qahramon Quronboyev's Facebook account via the link above. 2) Click Comment, rate five stars as shown on the second picture and put hashtag #karshiev_out. (Бекиева, 2018)

The Telegram group was eventually closed, but the group's coordinator stated that "now every team will work with its press secretary" (Бекиева, 2018).



[redacted]

Хурматли фаоллар, Кахрамон Куронбоев-Президент маслахатчисига отзыв колдиринг.

1. Юкоридаги линк оркали Кахрамон Куронбоевнинг фейсбукдаги сахифасига кириш.

2. Отзыв деган жойга босиб, 2-расм каби 5 юлдузни белгилашимиз ва #karshiev_out хештегини ёзишимиз керак.

214 edited 20:50

Figure 1: Trolling coordination on Telegram (Бекиева, 2018)

The Analytical Center for Central Asia (ACCA) found that an online attack on blogger Cyril Altman was undertaken by students at the University of Journalism and Mass Communications. In response to a satirical post by the blogger, “dozens of students began to post angry posts” and “accused the blogger of laughing at the state” (ACCA, 2020).

In April 2020, the Ministry of Internal Affairs published a draft governmental resolution to create a group of ‘patriotic bloggers’, comprised of students from the Tashkent University of Information Technologies, members of the Youth Union, and volunteers (gazeta.uz, 2020). Activists mocked the proposal, suggesting that it resembled a troll factory. The head of the Youth Union, Alisher Sadullayev, claimed that the organisation had nothing to do with the proposals. There were no further developments, and the proposal has possibly been abandoned.

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Uzbekistan

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
2005/2011	National Security Service, Youth Union				University of Journalism and Mass Communication; Paid Journalists

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Trolling

The IWPR claims that Uzbek trolls are "gradually evolving more sophisticated ways of waging online war". For example, instead of using foul language to derail discussions, accounts now try to undermine the reputation of journalists or their news organisations (Rysaliev et al., 2012). Reporting by the website Centre-1 notes that "activists of the youth organisation started a smear campaign against Kun.uz journalist Aziz Qarshiyev, who criticised Qahramon Quronboyev", by spreading the hashtag #karvhiev_out on social media (Centre-1, 2018). Members of the Loyal Young Reporters group interviewed by Ozodlik said that they had carried out trolling attacks on social media users who had made negative comments about the Youth Union. Negative comments were also shared on the Loyal Young Reporters Telegram group so that other group members could carry out a "united trolling attack on that commenter" (Бекиева, 2018).

Government ministers are also the target of online attacks. Sherzod Shermatov, Public Education Minister, was attacked on social media in 2019 when appeals to dismiss him appeared on Facebook and Telegram from both real and fake accounts. Jamshid Kuchkarov, current Economy and Poverty Reduction Minister, was also a target during his tenure as Minister of Finance. The campaign started after he announced the liberalization of the energy sector and tariff increases. The cases could be perceived as orchestrated media attacks amid power contests between different political groupings.

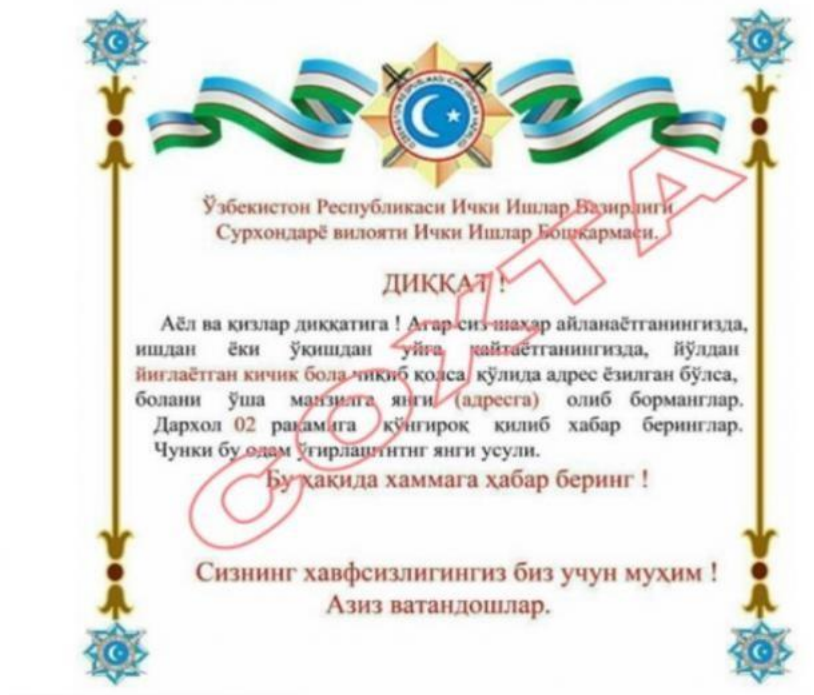
Fake accounts

There is evidence of fake social media accounts on Twitter, Facebook, and Telegram.

Gazeta reported the creation of a fake Twitter account for presidential candidate Hotamion Ketmonov that posted offensive tweets that ultimately damaged the politician's reputation (gazeta.uz, 2018). In 2019, the State Customs Committee (SCC) requested that Facebook close fake accounts that were created in the United Kingdom. The Committee stated that fake accounts set up in the name of SCC Chairman Behzod Musayev were accompanied by phone numbers traceable to London. According to the SCC, accounts were used to discredit the image and reputation of the chairman (podrobno.uz, 2019a). The website Kun.uz reported that several fake Kun.uz channels had appeared on Telegram -- illegally using the website's name and logo to distribute information (kun.uz, 2018a). Further, fake accounts are used on Telegram to artificially inflate the number of a channel's subscribers. Kun.uz reported that in the latest clean up of bot accounts by Telegram, channels in Uzbekistan lost 13 million fake followers (kun.uz, 2020).

Disinformation

Figure 2: Falsified Uzbek Interior Ministry message (upl.uz, 2019)



Ўзбекистон Республикаси Ички Ишлар Вазирлиги
Сурхондарё вилояти Ички Ишлар Бошқармаси.

ДИҚҚАТ !

Аёл ва қизлар диққатига ! Агар сиз шаҳар айланаётганингизда, ишдан ёки ўқишдан уйга қайтаётганингизда, йўлдан йиғлаётган кичик бола чиқиб қолса, қўлида адрес ёзилган бўлса, болани ўша манзилга янги (адресга) олиб борманглар. Дархол 02 рақамига қўнғироқ қилиб хабар беринглар. Чунки бу одам ўғирлашнинг янги усули.

Бу ҳақида хаммага ҳабар беринг !

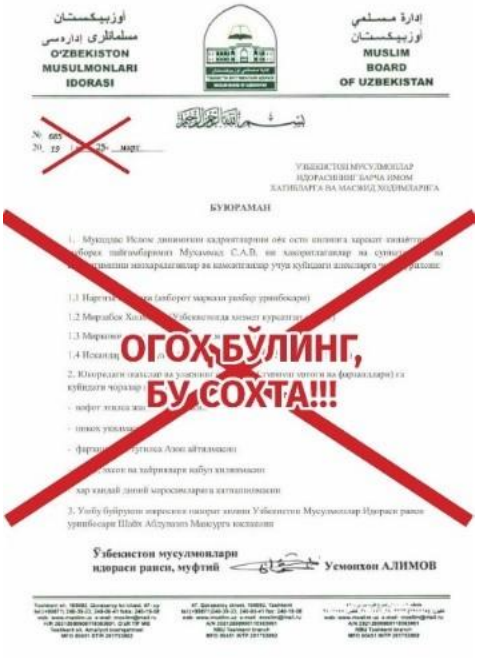
Сизнинг хавфсизлигингиз биз учун муҳим !
Азиз ватандошлар.

СОХТА

The Uzbek Agency for Information and Mass Communications (AIMC) issued a statement calling on foreign and local media outlets “to abide by the journalistic ‘code of honour’ and not to allow the spread of groundless rumours and speculation” (gazeta.uz, 2019). Government ministries have frequently been compelled to deny the validity of impersonations of official announcements spreading false information on social media platforms. For instance, the Interior Ministry was forced to reject as misinformation a report supposedly by the ministry’s southern Surkhandaryo regional that help should not be offered to lost children with an address in their hands, as it was a trap for luring, abducting and trafficking women (upl.uz, 2019). The falsified Interior Ministry report can be seen in figure 2. The Interior Ministry also denied a falsely attributed message circulating on social media that warned of representatives from an electrical company, Escom, entering homes and abducting children (kun.uz, 2018b).

Polarisation

The Uzbekistan Muslim Board website issued a statement on 25th March 2019 denouncing a fake letter using official Muslim Board of Uzbekistan headed paper that was circulating on social media (figure 3). The false report’s contents aimed to incite religious tensions. The statement said that the “circulation of such groundless and false reports are aimed at denouncing the positive changes made in the religious sphere in Uzbekistan and sowing the seeds of nothing more than discord between Muslims” (muslim.uz, 2019).



ОГОХ БЎЛИНГ,
БУ СОХТА!!!

O'ZBEKISTON MUSULMONLARI IDORASI

MUSLIM BOARD OF UZBEKISTAN

№ 685
20 19 й. 25- март

ЎЗБЕКИСТОН МУСУЛМОНЛАР ИДОРАСИНИНГ БАРЧА ИМОМ ХАТИБЛАРГА ВА МАСЖИД ХОДИМЛАРИГА

БУЮРАМАН

1. [illegible]

1.1 [illegible]

1.2 [illegible]

1.3 [illegible]

1.4 [illegible]

2. [illegible]

3. [illegible]

Ўзбекистон мусулмонлари идораси раиси, муфтий Усмонхон АЛИМОВ

Figure 3: Disinformation to incite religious tensions (muslim.uz, 2019)

Harassment

Journalists and bloggers reported in August 2020 of attempts to hack into their Telegram accounts. Although the origins and motivations of the attempted hacks are unclear, Komil Allamzhonov, Charmain of the Board of Trustees of the Public Fund for Support and Development of National Mass Media, said that it was an attempt to silence the media and bloggers (gazeta.uz, 2020).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Uzbekistan

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Human, Fake	Pro-Government messages, Attacks on Opposition, Polarization, Trolling	Disinformation, Coordinated trolling attacks, amplification of content	Facebook, Telegram, Twitter

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

The Uzbekistan Youth Union is reported to receive 200bn Uzbekistani Soms per year (US$19.7 million). Tashkent-based analyst Anvar Nazir asked "I am wondering if the organization spends any part of this money on such rottenness as trolling?" (Бекиева, 2018). Although the Youth Union appears to be well-funded, the extent of funding for trolling purposes is unknown.

It is reported that instructions were distributed to the 'Loyal Young Reporters' of the Youth Union at a training seminar during a media camp on 28-30 May 2018 in Tashkent, attended by 150 young people. Training was given on how to create multiple accounts, on uploading profile pictures, and how to "make your profile as realistic as possible so that users could not figure out that your account is fake" (Бекиева, 2018).

Table 3: Cyber Troop Capacity in Uzbekistan

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
85		Permanent	Centralised	Low

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Uzbekistan has been the target of foreign influence campaigns based in Russia. DFRLab reported that in January 2019, Facebook removed 300 pages for coordinated inauthentic behaviour that targeted former-Soviet countries (@DFRLab, 2019). These pages attempted to amplify content from Rossiya Segodnya, the Kremlin's media agency. Facebook pages that have specifically targeted Uzbekistan have included a page claimed to be run by "fans of Shavkat Miromonovich [Mirziyoyez], as the spiritual and national leader", and "Uzbekistan, I've brought you news" which posted Sputnik Uzbekistan articles and memes. DFRLab explain that Sputnik Uzbekistan was attempting to drive traffic to its website whilst masking the source by using Google's URL shortener. Central News Asia has reported that around 18,000 Uzbekistanis follow Russian pages (Yeniseyev, 2018).

References

ACCA. (2020, January 30). In Uzbekistan, future journalists are forced to trolling. *ACCA*. https://acca.media/en/in-uzbekistan-future-journalists-are-forced-to-trolling/

Centre-1. (2018, June 12). Глава Союза молодежи РУз соврал о кортеже с новобрачными? *Центр-1 / Centre1.com - Новости*. https://centre1.com/uzbekistan/glava-soyuza-molodezhi-ruz-sovral-o-kortezhe-s-novobrachnymi/

@DFRLab. (2019, January 17). *Facebook's Sputnik Takedown—In Depth—DFRLab—Medium*. https://medium.com/dfrlab/facebooks-sputnik-takedown-in-depth-f417bed5b2f8

Freedom House. (2019). *Freedom on the Net | Uzbekistan*. Freedom House. https://freedomhouse.org/country/uzbekistan/freedom-net/2019

gazeta.uz. (2018, February 2). *Чем опасны фейковые аккаунты и как с ними бороться*. Газета.uz. https://www.gazeta.uz/ru/2018/02/02/fake/

gazeta.uz. (2019, March 20). *Комил Алламжонов назвал работу «Озодлик» не соответствующей этике*. Газета.uz. https://www.gazeta.uz/ru/2019/05/20/ozodlik/

gazeta.uz. (2020, April 13). МВД предложило создать группу «патриотичных блогеров». *Газета.uz*. https://www.gazeta.uz/ru/2020/04/13/troll-factory/

gazeta.uz. (2020, August 8). «Попытками „заткнуть рот" СМИ и блогерам ничего нельзя добиться»—Комил Алламжонов. *Газета.uz*. https://www.gazeta.uz/ru/2020/08/08/media/

kun.uz. (2018a, January 14). *«Kun.uz» телеграмдаги сохта каналлардан огоҳлантиради*. Kun.uz. https://kun.uz/news/2018/01/14/kunuz-telegramdagi-sohta-kanallardan-ogolantiradi

kun.uz. (2018b, November 23). *МВД Узбекистана разыскивает распространителей фейковой информации*. Kun.uz. https://kun.uz/ru/news/2018/11/23/mvd-uzbekistana-razyskivaet-rasprostranitelej-fejkovoj-informacii

kun.uz. (2020, February 26). *Telegram keeps deleting false accounts: Channels in Uzbekistan lost 13 million fake subscribers*. Kun.Uz. https://kun.uz/en/news/2020/02/26/telegram-keeps-deleting-false-accounts-channels-in-uzbekistan-lost-13-million-fake-subscribers muslim.uz. (2019, March 25). *Ижтимоий тармоқлардаги сохта хабарларга ишонманг!* http://muslim.uz/index.php/yangiliklar-2016/uzbekistan/item/13578-izhtimoij-tarmo-lardagi-sokhta-khabarlarga-ishonmang

podrobno.uz. (2019, March 17). *Фейковые аккаунты главы ГНК Узбекистана были созданы из Великобритании*. Podrobno.uz. https://podrobno.uz:443/cat/obchestvo/feykovye-akkaunty-glavy-gnk-uzb/

Rysaliev, A., Tokbaeva, D., & Olimova, L. (2012, February 12). *Central Asia's 'Troll Wars'*. Institute for War and Peace Reporting. https://iwpr.net/global-voices/central-asias-troll-wars

Tashkent Times. (2020, January 23). *Public Fund for Support and Development of National Mass Media set up*. https://tashkenttimes.uz/national/4897-public-fund-for-support-and-development-of-national-mass-media-set-up

upl.uz. (2019, March 19). *МВД ищет распространителей фейковой информации*. Новости Узбекистана. https://upl.uz/incidents/10601-news.html

Yeniseyev, M. (2018, April 16). Revelations erode Uzbekistanis' trust in Russia-backed media outlets. *Caravanserai*. https://central.asia-news.com/en_GB/articles/cnmi_ca/features/2018/04/16/feature-01

Yeniseyev, M. (2020, March 25). Uzbekistan urges public to be wary of coronavirus falsehoods. *Caravanserai*. https://central.asia-news.com/en_GB/articles/cnmi_ca/features/2020/03/25/feature-01

Бекиева, М. (2018, September 17). Расследование «Озодлика»: Первые шаги группы троллей Союза молодежи Узбекистана. *Радио Озодлик*. https://rus.ozodlik.org/a/29491841.html

Venezuela

Introduction

Venezuela is one of the least free countries in the world (Freedom House, 2019) and has been suffering from a profound economic crisis and an authoritarian regime, that has increasingly undermined political competition (Corrales & Penfold, 2015). Since the 2018 elections, Venezuela has remained locked in a political stalemate between Nicolas Maduro, incumbent president since the death of Hugo Chávez in 2013, and Juan Guaidó, President of the National Assembly. Guaidó claimed that the elections were rigged and in January 2019, invoking Article 233 of the Constitution, appointed himself the new president of Venezuela. He is recognized as interim president by the Organization of American States, the European Parliament and almost sixty countries. Venezuela has since been deeply embroiled in a presidential crisis.

Plunged into a major recession, communication has been weaponized by both the government and the opposition in a struggle to maintain—or break—control over an increasingly dissatisfied population. The country scores only 30 in the Freedom on the Net ranking (Freedom House, 2019), which is a sign of the permanent threats and ongoing verbal or physical abuse of journalists, academics, media outlets and communication infrastructure.

The tightening of internet censorship is often related to the escalation of political tension (Azpúrua et al., 2019). For instance, CANTV, the state-owned telecommunication provider that represents around 70% of the (deteriorated) service in the country (Rendon & Kohan, 2019), blocked Wikipedia in response to the first set of edits on Juan Guaidó's page that described him as President of Venezuela. CANTV also blocked YouTube, Twitter, and Instagram when a group of members of the Bolivarian National Guard disseminated anti-government videos and a call to join them in their uprising against Maduro (Azpúrua et al., 2019). According to Azpúrua et al. (2019), these blockings were non-deterministic and used "a combination of SNI filtering and HTTP blocking". Similarly, on February 2019 the opposition portal VoluntariosxVenezuela.com [Volunteers for Venezuela] was a target of phishing and it redirected users to a defaced website (Azpúrua & Guerra, 2019). The government has also shut down circumvention tools, such as TOR, and blocked access to the Google Play store, among others (Rendon & Kohan, 2019).

As a result of the media context and quality of the internet service, social media has a central role to access political information (Quintero & Coscojuela, 2019). However, coordinated operations to manipulate the debates on social media are long-established in Venezuela. It was the first country in Latin America to use such techniques (Quintero & Coscojuela, 2019). Since 2010 the government has pushed its agenda on the digital media and disinformation is a substantial concern, especially in a context with limited access to diverse sources of information and censorship. As a result, as of early 2020, six fact-checking units have been operating in Venezuela: Cotejo, Efecto Cocuyo, Observatorio Venezolano de Fake News, Cazadores de Fake News, Observatorio Venezolano de Desinformación, and Espaja.com.

An Overview of Cyber Troop Activity in Venezuela

Organizational Form

Online propaganda had already been identified in 2010, during the Hugo Chávez regime (2002-2013), when the then-president announced his usage of Twitter (MrBarbacoa, 2011). The Chávez government produced wide-scale propaganda, including disseminating YouTube campaigns and summoning people to follow him on Twitter during presidential speeches. In

2011 and 2012 there was already evidence of the hijacking of social media accounts belonging to political opponents (Puyosa, 2019).

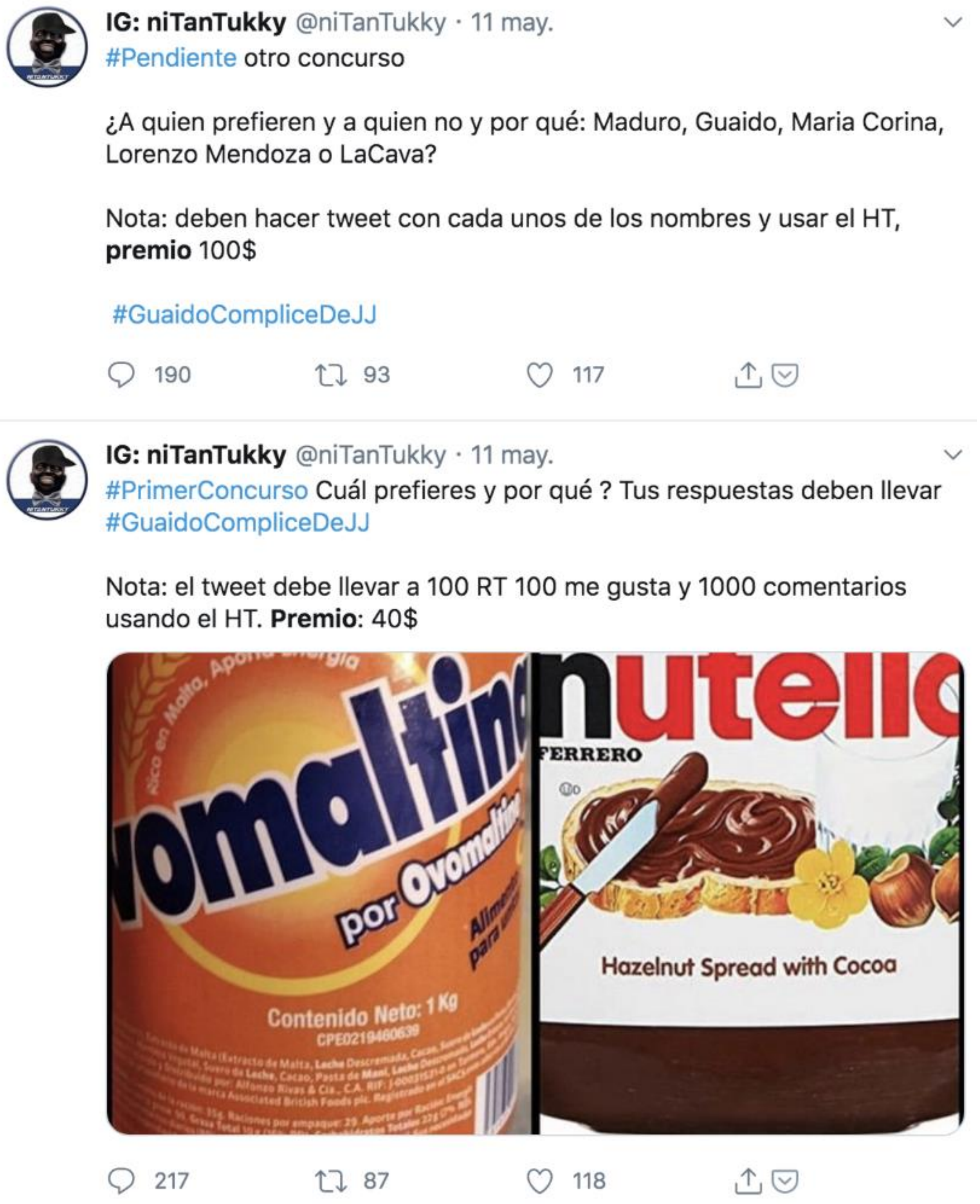
In 2018, a major leak of governmental documents showed how the department of interior was creating a cyber-militia, with structured teams and incentive systems for propaganda dissemination (Riley, Michael et al., 2018). This included instructions to build social media accounts, guidelines on the creation of strategy groups, incentives and even the creation of specialized tasks such as content creation, distraction, or attack. According to Iria Puyosa (Quintero & Coscojuela, 2019), while the use of bots "was initially coordinated by the Vice Presidency", it was then the Ministry of Communication and Information that sent strategies and content to volunteers. Moreover, these cyber troops are both linked to volunteers within public administration agencies and troll factories who provide these services for the government (Puyosa, 2019).

It is not uncommon for political figures to use their public communication capacities to promote attacks against their opponents using propaganda. For example, in 2016, former vice-president Diosdado Cabello used his TV channels and Twitter accounts to promote a hashtag attacking opposition politician Luis Florido (Nyst & Monaco, 2018). Others use social media to amplify hashtags in their favor. Deputy Luis Parra, who claims to be the legitimate President of the National Assembly in opposition to Juan Guaidó, boosted bots' activities in February 2020 to position a hashtag as trending topic, supporting the government's agenda (Coscojuela & Quintero, 2020). However, by April his account was suspended—with no further explanation by Twitter—and he had to open a new one.

Online propaganda activities have also been detected by the Strategic Integral Defense Regions and the Comprehensive Defense Operational Zone, operating within the structures of the National Bolivarian Armed Forces (Puyosa, 2019).

However, the United Socialist Party of Venezuela (PSUV) is not alone in its use of online manipulation. During Spain's 2019 general election, the largest network of bots found was formed by 2,882 bot accounts originating in Venezuela. They disseminated Islamophobic and pro-Vox (the extreme right-wing political party) messages. The network had previously been used to attack the Venezuelan regime but was reactivated in 2017. Although there is not enough evidence, it has been suggested that the network was managed by the Youtuber Alberto Franceschi, a member of the most radical opposition movement in Venezuela (Peinado, 2019). Lastly, it is worth noting that among the accounts that have been found to be part of an anti-Guaidó network on Twitter (DFRLab, 2020a), @niTanTukky was identified. This account has been promoting raffles of money to reward people who disseminated specific content or hashtags (IG: niTanTuky, 2020a and 2020b).

Figure 1. Twitter content by @niTanTukky to announce raffles to reward active users



IG: niTanTukky @niTanTukky · 11 may.
#Pendiente otro concurso

¿A quien prefieren y a quien no y por qué: Maduro, Guaido, Maria Corina, Lorenzo Mendoza o LaCava?

Nota: deben hacer tweet con cada unos de los nombres y usar el HT, **premio** 100$

#GuaidoCompliceDeJJ

190 93 117

IG: niTanTukky @niTanTukky · 11 may.
#PrimerConcurso Cuál prefieres y por qué ? Tus respuestas deben llevar #GuaidoCompliceDeJJ

Nota: el tweet debe llevar a 100 RT 100 me gusta y 1000 comentarios usando el HT. **Premio**: 40$

217 87 118

Source: IG: niTanTukky (2020a, 2020b)

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Venezuela

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
2010	Ministry of Communication and Information	Evidence found (e.g. Diosdado Cabello in 2016	Evidence found		Evidence found

	Strategic Integral Defense Regions and the Comprehensive Defense Operational Zone (both operational structures of the National Bolivarian Armed Forces)	and Luis Parra in 2020) and political parties			

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Cyber troop activity is present on most mainstream social media platforms, including YouTube, Facebook, Instagram, Telegram, Google+ (now extinct), WhatsApp, and especially Twitter. An automated Twitter account linked to the government incentivized the daily retweeting of governmental hashtags. There has also been plenty of evidence of state-sponsored trolling, where people were hired to attack social media accounts of journalists and opposition supporters (DFRLab, 2019a).

Iria Puyosa (2019) identified four strategies of the government's cyber troops. Firstly, the interactivity with the daily trending topics by official accounts and bots. Secondly, the creation of misleading, fake, and emotional content by cyborgs and bots. Thirdly, what Puyosa calls "the hijacking of opposition hashtags" by automated techniques, which are aimed to distort messages. And finally, infiltration within opposition networks in order to promote divisions.

Information warfare intensified during the 2018 campaigns. Pro-Maduro cyber troops consisted of "public officials' accounts, government social service accounts, party activists, semi-automated accounts, and bots" (Freedom House, 2019). When Maduro's runner up in the presidential elections challenged the results, the opposition used social media to spread false information in an attempt to rally citizens to protest against the government, break the morale of government supporters and counteract the intense governmental propaganda machine.

These tensions led to an uprising on 30 April 2019, where Juan Guaidó claimed to have control over Venezuela's main airbase and support from military generals to take over the government (Smith & Torchia, 2019). During the uprising, false information circulated that Maduro had resigned, while protestors took to the streets. Since January 2019, rumours of Maduro resigning have been strategically spread during moments of tension (Garsd, Jasmine, 2019). At the height of the crisis, the United States sent over humanitarian aid trucks and John Bolton claimed that these rescues were being set on fire by the Maduro government. It was later revealed that the only truck that caught on fire was provoked by the protestors themselves, who were throwing Molotov cocktails at the police and accidentally set one of the trucks of fire (Casey, Nicholas et al., 2019).

Moreover, in January and June 2019, Twitter removed 764 (Twitter Safety, 2019) and 33 accounts (Roth, 2019), respectively. These accounts were located in Venezuela and were involved in a foreign campaign to generate polarization. Although the company initially suggested an association with the Russian Internet Research Agency (IRA), it later suspected that they were operated by a private Venezuelan agency (Roth, 2019). In January another 1,196 accounts that seemed to be state-backed and also located in Venezuela were removed because of their local campaign to influence online debate (Twitter Safety, 2019). Some of the accounts focused on content creation and others amplified that content through retweets, responses, or automatic mentions. Moreover, many of these accounts had identical content that was posted within a short time frame, which suggested the use of bots. It is worth mentioning that one of the biggest accounts was that of the Ministry of Communication and Information (Andrino, 2019).

In August 2019, responding to the announcement of new of sanctions against the oil industry by the United States, the Venezuelan government called the population to protest against Trump and the blockade. As a result, the pro-Maduro cyber troops posted attacks against Trump and the United States, as well as against the Venezuelan opposition—mainly the National Assembly and Juan Guaidó. According to Probox, the initial tweet with the hashtag #TrumpDesbloqueaAVenezuela [Trump, Unblock Venezuela] was posted by the official account of the Ministry of Foreign Relations, and 87% of tweets with that hashtag were promoted by bots (Quintero & Coscojuela, 2019). Although with fewer tweets, the opposition and the radical Chavism also coordinated their narratives around the event (Quintero & Coscojuela, 2019). They both used bots to amplify their messages.

Another event that manifested the increase of coordinated activities during moments of crisis occurred in late 2019, when Maduro called people to join the militia and #somostodosmilicia, #rumboalos3millones, and #miliciapubeloenarmas became trending topics on Twitter. More than 50% of the accounts involved were institutional accounts of the militias and presented automated behaviour (DFRLab, 2019b).

As has been previously mentioned, some opposition groups also promote coordinated activities. In early 2020, a small network of real right-wing accounts coordinated a campaign against Maduro and Guaidó, with the aim of presenting a pro-military intervention narrative and "portraying themselves as the competent opposition" (DFRLab, 2020c).

In January 2020 pro-Maduro cyber troops amplified anti-Guaidó hashtags (DFRLab, 2020a) and boosted a disinformation campaign that claimed that Guaidó received funding from the United States (DFRLab, 2020b). This disinformation was amplified via local blogs and Facebook groups, and state-backed media outlets from Russia (e. g. RT in Spanish), Iran, and Cuba also replicated the content and targeted users in other Latin American countries (DFRLab, 2020b).

Similar rumours of military intervention by the United States, backed by Guaidó, were spread across the country by anti-Maduro media outlets. The most popular content was published by Alexa News and the YouTube Channel Parecen Noticias Extra [Seems Like Extra News]. They were mainly disseminated through YouTube and Facebook groups, some of which impersonated popular media outlets (eg. CNN in Spanish) (DFRLab, 2020d). However, as has been suggested, a set of fan pages and Facebook groups amplifying content published by Alexsnews.com and Sharesocial.app, may have more financial than political motivations, as the websites are using advertising monetization (DFRLab, 2020e).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Venezuela

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Automation, human. Fake and real.	Pro-government, attacks on opposition, distracting messages, driving polarization, trolling	Disinformation, trolls, amplification techniques	Twitter, Facebook, YouTube, Instagram, Google+ (now extinct), WhatsApp

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

According to documents leaked in 2018, disinformation teams were organized following a military structure, where each person (or crew) could manage twenty-three accounts, and be part of a squad (ten people), a company (fifty people), a battalion (one hundred people), or a brigade (five hundred people). The brigade could operate as many as 11,500 accounts (Riley, Michael et al., 2018). The guide for cyber troops also suggested that armies must be divided by type of content: Pro-Government, Opponents, Neutrals, Distraction, and Fake News. Whilst Opponents squads focused on interference and infiltration, Fake News and Distraction focused on distraction techniques (Puyosa, 2019).

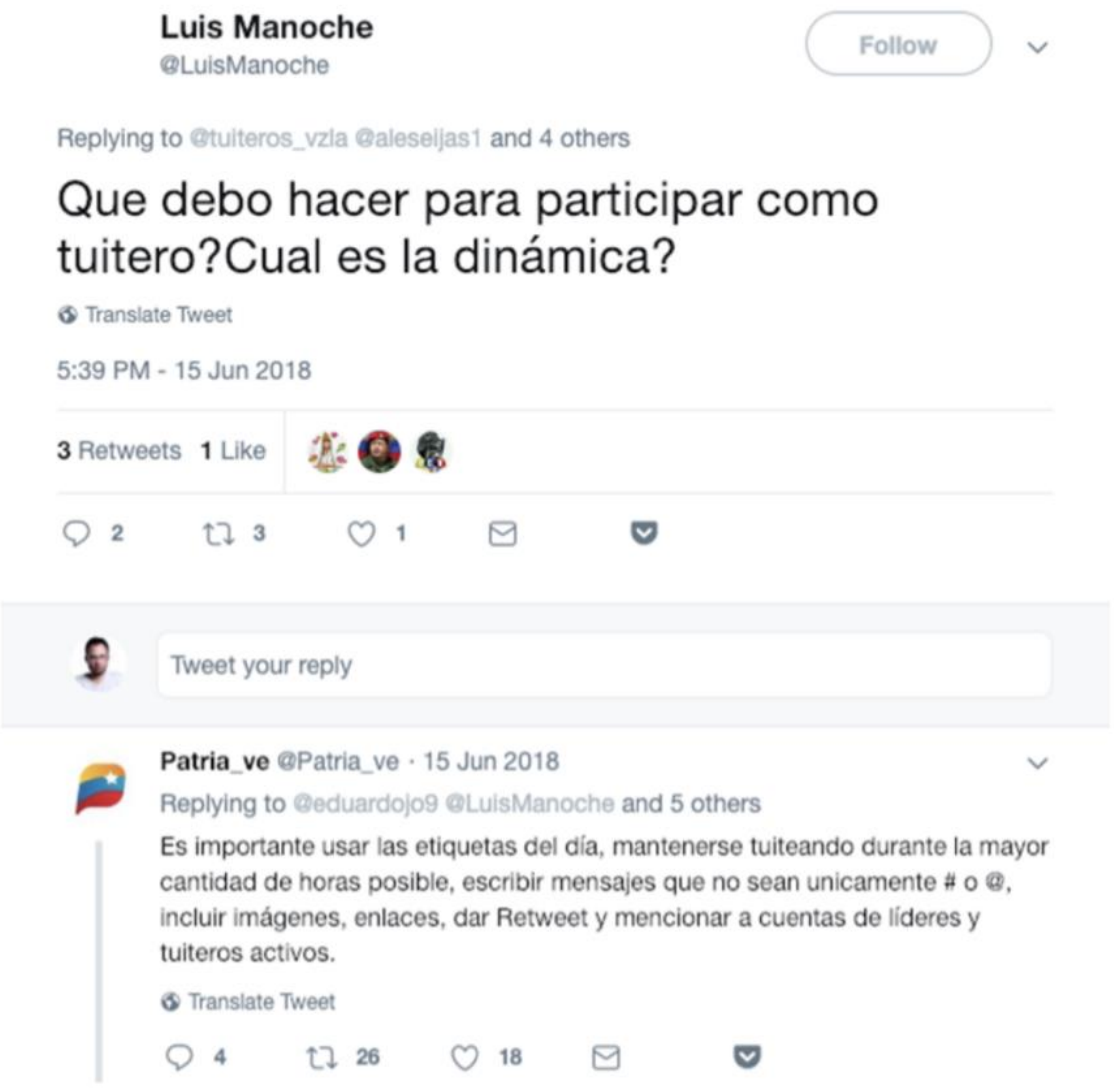
People participating in these operations signed up "for Twitter and Instagram accounts at government-sanctioned kiosks" and were rewarded with coupons for food and goods, which are particularly valuable in the current state of scarcity (Riley, Michael et al., 2018), or other governmental benefits (Quintero & Coscojuela, 2019).

During the 2018 elections, the official account of the Ministry of Communication and Information and Telegram channels, to which government officials had to subscribe, informed the trending topics to position the following day. Over 63,000 accounts were active and around 500,000 automated accounts or bots were used for the dissemination of campaign propaganda (Puyosa, 2018).

Tuiteros Patriotas or @Tuiteros_Vzla on Twitter, is a community that was created during the campaign in order to coordinate volunteers' social media activity. During that period, it reached more than 38,000 followers, but it subsequently continued its central role as amplifier of the social media operations of the State. The account coordinated volunteers and posted indications on hashtags, alerts of trending topics, and recognition of top users, and communication was done through a Telegram channel. There is evidence of linkages with state propaganda: its initial website domain was owned by the United Socialist Party of Venezuela (Penarredonda & Karan, Kanishk, 2019).

Additionally, during the 2018 campaign, volunteers of Tuiteros Patriotas who used the daily hashtag were entered into a daily raffle, which consisted of around U$S2-3—a month's minimum wage (Puyosa, 2018). Afterwards, @Tuiteros_Vzla detected the most active users who tweeted with the hashtag of the day and sent money via their digital wallets as rewards for online activities. Their registered Twitter accounts were associated with VeMonedero, which is a digital wallet "where the government deposits aid money to an account tied to Venezuelan people’s Carnet de la Patria (Motherland Card), an ID card that identifies social aid recipients” (Penarredonda & Karan, Kanishk, 2019).

Figure 2. Twitter content by Tuiteros Patriotas to explain the terms of participation in the daily raffle



Luis Manoche
@LuisManoche

Replying to @tuiteros_vzla @aleseljas1 and 4 others

Que debo hacer para participar como tuitero?Cual es la dinámica?

5:39 PM - 15 Jun 2018

3 Retweets 1 Like

Patria_ve @Patria_ve · 15 Jun 2018
Replying to @eduardojo9 @LuisManoche and 5 others

Es importante usar las etiquetas del día, mantenerse tuiteando durante la mayor cantidad de horas posible, escribir mensajes que no sean unicamente # o @, incluir imágenes, enlaces, dar Retweet y mencionar a cuentas de líderes y tuiteros activos.

A response from @Patria_Ve to a user asking how to be part of the raffle. Translation from Spanish: @LuisManoche: What should I do to take part as a tweeter in the raffle? @PatriaVe: It is important to use the hashtags of the day, keep tweeting for as many hours as possible, write messages that are not only # [hashtags] or @ [mentions], include images, links, and to retweet and mention accounts from leaders and active tweeters. (Source: @LuisManoche/archive)

Source: Penarredonda & Karan, Kanishk, 2019

Whilst the account was suspended on January 2019 and its activity has declined, the community is still coordinating volunteers’ actions with the hashtag #TuiterosActivos.

Table 3: Cyber Troop Capacity in Venezuela

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
Brigades of up to 500 people		Permanent and temporary	Top-down indications by the Ministry of Communication and Information. Communities (e.g. Tuiteros Patriotas) coordinate communication with volunteers and reward the most active ones.	High

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

References

Andrino, B. (2019, February 16). Venezuela: Así opera la propaganda venezolana en Twitter. *El País*. https://elpais.com/tecnologia/2019/02/07/actualidad/1549571078_716504.html

Azpúrua, A., Chirinos, M., Filastò, A., & Xynou, M. (2019, January 29). *From the blocking of Wikipedia to Social Media: Venezuela's Political Crisis*. https://vesinfiltro.com/noticias/report-jan-2019/

Azpúrua, A., & Guerra, C. (2019, February 15). *Phishing by Venezuelan government puts activists and internet users at risk.* https://vesinfiltro.com/noticias/Phishing_by_Venezuelan_government_targets_activists/

Casey, Nicholas, Koettl, Christoph, & Acosta, Deborah. (2019, March 10). *Footage Contradicts U.S. Claim That Nicolás Maduro Burned Aid Convoy—The New York Times*. https://www.nytimes.com/2019/03/10/world/americas/venezuela-aid-fire-video.html

Corrales, J., & Penfold, M. (2015). *Dragon in the Tropics: The Legacy of Hugo Chávez* (2.ª ed.). Brookings Institution Press; JSTOR. https://www.jstor.org/stable/10.7864/j.ctt7zsw23

Coscojuela, S., & Quintero, L. (2020, April 26). Luis Parra, el diputado que el chavismo ayuda hasta en redes sociales. *TalCual*. https://talcualdigital.com/luis-parra-el-diputado-que-el-chavismo-ayuda-hasta-en-redes-sociales/

DFRLab. (2019a, March 21). *Venezuelan Pro-Regime Accounts Publish Personal Data of Phishing Victims*. Medium. https://medium.com/dfrlab/venezuelan-pro-regime-accounts-publish-personal-data-of-phishing-victims-1b41ffc256bd

DFRLab. (2019b, May 1). Civilian Militias in Venezuela Coordinate on Twitter. *Medium*. https://medium.com/dfrlab/civilian-militias-in-venezuela-coordinate-on-twitter-aadcd86d6186

DFRLab. (2020a, January 14). Network of pro-Maduro Twitter accounts pushed anti-Guaidó hashtags. *Medium*. https://medium.com/dfrlab/network-of-pro-maduro-twitter-accounts-pushed-anti-guaid%C3%B3-hashtags-530f034f3628

DFRLab. (2020b, January 28). Misleading claim against Venezuela's Guaidó spread abroad. *Medium*. https://medium.com/dfrlab/misleading-claim-against-venezuelas-guaid%C3%B3-spread-abroad-a5eb538af050

DFRLab. (2020c, February 19). Anti-Guaidó and anti-Maduro hashtags trend on Twitter. *Medium*. https://medium.com/dfrlab/anti-guaid%C3%B3-and-anti-maduro-hashtags-trend-on-twitter-40403cee3694

DFRLab. (2020d, March 6). Rumors of a U.S. military intervention in Venezuela grow. *Medium*. https://medium.com/dfrlab/rumors-of-a-u-s-military-intervention-in-venezuela-grow-daf243c410eb

DFRLab. (2020e, March 27). Venezuelan fringe websites impersonate media outlets on Facebook. *Medium*. https://medium.com/dfrlab/venezuelan-fringe-websites-impersonate-media-outlets-on-facebook-a8ec4fe097c8

Freedom House. (2019). *Freedom of the Net | Venezuela*. Freedom House. https://freedomhouse.org/country/venezuela/freedom-net/2019

Garsd, Jasmine. (2019, January 26). *Amid Chaos, Venezuelans Struggle To Find The Truth, Online*. NPR.Org. https://www.npr.org/2019/01/26/688868687/amid-chaos-venezuelans-struggle-to-find-the-truth-online

IG: niTanTukky [niTanTukky]. (2020, May 11). ##Pendiente otro concurso. ¿A quien prefieren y a quien no y por qué: Maduro, Guaido, Maria Corina, Lorenzo Mendoza o LaCava? Nota: deben hacer tweet con cada unos de los nombres y usar el HT, premio 100$ #GuaidoCompliceDeJJ [Tweet]. Retrieved from https://twitter.com/niTanTukky/status/1259976881270591494

IG: niTanTukky [niTanTukky]. (2020, May 11). #PrimerConcurso Cuál prefieres y por qué? Tus respuestas deben llevar #GuaidoCompliceDeJJ Nota: el tweet debe llevar a 100 RT 100 me gusta y 1000 comentarios usando el HT. Premio: 40$ [Tweet]. Retrieved from https://twitter.com/niTanTukky/status/1259966234793304065

MrBarbacoa. (2011). *Chavez Candanga llega a twitter*. Recuperado 2 de julio de 2019, de https://www.youtube.com/watch?v=xsIzvwMfjYk

Nyst, C., & Monaco, N. (2018). *IFTF: Government Sponsored Trolling*. Institute for the Future. http://www.iftf.org/statesponsoredtrolling/

Peinado, F. (2019, April 26). Elecciones generales 2019: Una red de cuentas falsas de Twitter promueve a Vox en campaña | España | EL PAÍS. *El País*. https://elpais.com/politica/2019/04/25/actualidad/1556203502_359349.html

Penarredonda, J. L., & Karan, Kanishk. (2019, February 4). *#InfluenceForSale: Venezuela's Twitter Propaganda Mill*. Medium. https://medium.com/dfrlab/influenceforsale-venezuelas-twitter-propaganda-mill-cd20ee4b33d8

Puyosa, I. (2018). *Chavism information war strategies on Twitter* (Observatory of Disinformation and Propaganda in Latin America). Counterpart International. https://www.counterpart.org/wp-content/uploads/2018/09/INFORMATION-WAR-STRATEGIES-Final-Report.pdf

Puyosa, I. (2019). *Venezuela's 21st Century Authoritarianism in the Digital Sphere* (Policy Brief No. 62). Toda Peace Institute. https://toda.org/assets/files/resources/policy-briefs/t-pb-62_iria-puyosa_venezuelas-21st-century-authoritarianism.pdf

Quintero, L., & Coscojuela, S. (2019, December 4). *Bombardeo virtual sobre las redes para desinformar en Venezuela*. openDemocracy. https://www.opendemocracy.net/es/democraciaabierta-es/tropa-virtual-de-maduro-bombardea-las-redes-para-desinformar-en-venezuela/

Rendon, M., & Kohan, A. (2019, December 4). *The Internet: Venezuela's Lifeline*. Center for Strategic & International Studies. https://www.csis.org/analysis/internet-venezuelas-lifeline

Riley, Michael, Etter, Lauren, & Pradhan, Bibhudatta. (2018, July 19). *A Global Guide to State-Sponsored Trolling*. https://www.bloomberg.com/features/2018-government-sponsored-cyber-militia-cookbook/

Roth, Y. (2019, June 13). Information operations on Twitter: Principles, process, and disclosure. *Twitter*. https://blog.twitter.com/en_us/topics/company/2019/information-ops-on-twitter.html

Smith, S., & Torchia, C. (2019, May 1). *Clashes rock Venezuela as Guaido, Maduro vie for power.* AP NEWS. https://apnews.com/0153cace08c84c8fbf34f9c6a7bdd4dd

Twitter Safety. (2019, January 31). *Empowering further research of potential information operations*. https://blog.twitter.com/en_us/topics/company/2019/further_research_information_operations.html

Vietnam

Introduction

In late 2017, around 54% of the population of Vietnam had active Facebook accounts (52 million) (Luong, 2018). According to the *New York Times* YouTube and Facebook account for two thirds of the domestic digital media market (Luong, 2017). The Vietnamese government allows social media and uses it as a platform to disseminate its own media as well as monitor critical content. However, throughout the years, it has tightened its control of the internet.
The government issued various laws and decrees that addressed its different concerns. As a result of the rising influence of personal bloggers and citizen media, in 2013 the government introduced Decree 72 that banned the discussion of current affairs on the Internet, arguing that instead social media and blogs should only be used to share personal information (BBC News, 2017).

As people were increasingly accessing news (and organizing) through social media, the government proceeded with actions to counter the influence of these platforms and to favour state-owned media. In early 2017, the information ministry issued a circular to websites, social media sites and apps that have over a million users in Vietnam to work with the authorities to block or remove “toxic” content online (Luong, 2018). Google partially complied with a request to remove 2,300 videos on YouTube by removing under 1,500. Facebook set up a separate channel to communicate directly with the Communication and Information Ministry to prioritise governmental issues with fake news that circulates as content or as ads (Luong, 2017).

Alleging concerns on cybersecurity and the spread of fake news, the government passed a cybersecurity law in June 2018, which has been criticized to seek out formal control over social media, requiring foreign technology firms like Google, Facebook, Viber, Uber, and Skype to set up offices and data servers in Vietnam (Luong, 2018; Tuoi Tre News Staff, 2017). Nguyen Hong Van of the Vietnam Institute of Information Security argued that domestic data ownership would safeguard the country’s cybersecurity. The law was inspired to “prevent news sites and blogs with bad and dangerous content”, according to President Tran Dai Quang, which “undermined the prestige of the leaders of the party and the state” (Luong, 2017). If the firms do not comply, they will not be allowed to offer their services in Vietnam. The law received criticism for going beyond cybersecurity and taking aim at controlling content. A few hours before the bill was passed, websites that were against the cybersecurity law were targeted with DDoS attacks (Qurium Media Foundation, 2018). It has also enabled the arrest of activists for their social media posts criticizing the government, such as environmentalist Le Dinh Luong (Funk, 2019) and journalist Truong Duy Nhat (CIVICUS, 2020).

Most recently, in February 2020, the Prime Minister signed a Decree to fine (USD 430-860) anyone using social media to spread disinformation about the COVID-19 or “share information that promotes outdated customs and superstition; describes details of horror, scary accidents and criminal actions; causes confusion among people; or incites violence, crimes, and social issues” (CIVICUS, 2020).

An Overview of Cyber Troop Activity in Vietnam.

Organizational Form

In 2013, the Vietnamese government admitted it employed around one thousand, who engage in online discussions, on social media and forums, and post comments that support the

Communist Party's policies (Pham, 2013). They are referred to as "public opinion shapers". The BBC reported that the head of the Hanoi Propaganda and Education Department, Ho Quang Loi, stated that "Internet polemists" were used to combat "online hostile forces" (Pham, 2013).

In December 2017, Colonel General Nguyen Trong Nghia, deputy chairman of the General Political Department of the People's Army, announced the existence of an army of cyber-soldiers. This unit operates under the name of Force 47 and is run by the Ministry of Public Security. Its goal is to combat false news, "wrongful views" and anti-government content online (BBC News, 2017; Luong, 2018). The government also often requests Google, YouTube, and Facebook to remove or restrict content, especially in reaction to incidents, such as recent clashes at Dong Tam over land (Amnesty International, 2020).

There is also evidence of the deployment of hacker groups to target foreign actors. For instance, APT32/OceanLotus, which was "linked to the Vietnamese government or working on its behalf" hacked websites of ministries and government agencies of other Southeast Asian countries, as well as the Association of Southeast Asian Nations (ASEAN); it also targeted "foreign multinationals and dissidents in Vietnam" («Vietnam's Neighbors, ASEAN, Targeted by Hackers», 2017).

Other private contractors and citizens have also been involved in the interference with foreign issues. In December 2019 Facebook removed a network of pro-Trump pages, groups, and accounts on Facebook and Instagram that mostly targeted the United States, but also aimed content at Vietnamese people outside of Vietnam (Gleicher, 2019). Facebook groups were followed—and sometimes managed—by fake accounts that originated in Vietnam and the United States. Pages like "America Needs President Trump," "TRUMP MAGA 2020," and "Make America Great Again" had admins located in Vietnam (Graphika & DFRLab, 2019). Their activities mainly focused on the conservative The BL media company and its company Epoch Media Group. The latter is a pro-Trump US media organization that was banned from publicizing on Facebook due to its violations of the platform's political ad policies, and that employs people in Vietnam (Gleicher, 2019). Also, according to CNET (Nieva, 2020) a pro-Trump YouTube disinformation network has ties with individuals in Vietnam. Examples include the Breaking News channel, which is managed by a person based in Vietnam who has experience in marketing through social media, and the News 24H channel that focusses US politics from a right-wing perspective has three old videos with a woman speaking Vietnamese and talking about "the time of day or what fruit she was eating" (Nieva, 2020). Although the details of the Vietnamese involved have not been confirmed, CNET identified that one of the individuals managing a channel within the network was hired on Fiverr.

Finally, in February 2020, Facebook removed an additional network of accounts and pages that "originated in Myanmar and Vietnam and targeted audiences in Myanmar" (Gleicher, 2020). Facebook linked the activities to MyTel in Myanmar, Viettel in Vietnam, and Gapit Communications (a PR firm in Vietnam) (Gleicher, 2020). MyTel is "indirectly owned by the Myanmar and Vietnamese militaries" (DFRLab, 2020).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Vietnam.

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
2013	Task Force 47 (Ministry of Public Security)		Viettel and Gapit Communications		Evidence found

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

According to the head of the Hanoi Propaganda and Education Department in 2013, Ho Quang Loi, the "public opinion shapers" aim to contribute to the government's digital strategy to stop the spread of negative rumours and restrict the capacity to organise mass gatherings (Pham, 2013).

Force 47 has been known to target and harass Vietnamese activists and civil society organizations (BBC News, 2017; Luong, 2018). They use mass reporting techniques to ban critical content creators from Facebook (Deprez & Haffner, 2020). For instance, in April 2020 Facebook restricted access to the profile of a number of activists, and YouTube disabled the channel of Radio Free Asia for seven days. As stated by CIVICUS, "these restrictions were likely prompted by the Vietnamese authorities' deployment of cyber troop capabilities to flood Facebook with reports complaining of individual users' social media activity" (CIVICUS, 2020). The Liberal Publishing House, whose publications have frequently been censored by the government and whose workers have been targets of attacks and harassment, was also affected by the mass-report against its Facebook page (Human Rights Watch, 2019).

The task force also actively defends the government, through multiple Facebook pages, when incidents occur (The Phuong, 2018). Not only does the task force engage in social media interactions, spreading a pro-government narrative, but the government also patrols online discussions and take action in response to posted criticism. During the dispute in Dong Tam village, a number of bloggers were isolated because they streamed onsite reports, and activists were arrested for posts they made online (CIVICUS, 2020). The Department of Cyber Security and High-tech Crime Prevention has also accused a social media commentator of spreading fake news and unverified information (CIVICUS, 2020).

To date Facebook has not acted on real trolls' accounts directly linked to the government, it has instead acted on fake accounts or bots. As regards the two networks of groups, pages, and accounts identified and removed by Facebook in 2019 and 2020, they followed inauthentic behaviour. The network linked to The BL and Epoch Media Group were characterized by posts with automated behaviour, and posted conservative content about US politics and family values, among other issues. Also, Vietnamese-language pages posted translated and neutral content on US politics but linked to pro-Trump content (Graphika & DFRLab, 2019). In analysis by Graphika and DFRLab, the campaign was also observed on Twitter and YouTube (Graphika & DFRLab, 2019). On the other hand, the network linked to the telco companies in Myanmar and Vietnam was promoted by fake accounts that presented themselves either as telecom consumer news hubs or customers and posted content and comments against competitors of the two telecom providers (Gleicher, 2020).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Vietnam.

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Bot and Human	Support, Attack opposition, Suppressing	Disinformation, Mass reporting, Trolls, Amplifying content	YouTube, Facebook, Instagram

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

The "public opinion shapers" the Vietnamese government admitted employing in 2013, were made up of around one thousand staff (Pham, 2013). The Hanoi Propaganda and Education Department managed four hundred accounts and twenty microblogs (Pham, 2013).

Task Force 47 has an informal and flexible structure and, as announced by Colonel General Nguyen Trong Nghia in December 2017, is made of 10,000 "core fighters", who are military officials and personnel (BBC News, 2017; Luong, 2018; The Phuong, 2018). Members are trained to act "independently and actively in the Internet", countering what are referred to as "wrongful opinions" by the Vietnam Communist Party (The Phuong, 2018).

Finally, as stated by Facebook, the campaigns promoted by the network of accounts linked to Mytel, Viettel, and Gapit Communications spent $1,155,000 on Facebook ads, which were paid in US dollars and Vietnamese dong (Gleicher, 2020).

Table 3: Cyber Troop Capacity in Vietnam

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
10,000		Permanent and temporary	Somewhat centralised	High

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

References

Amnesty International. (2020, January 16). *Viet Nam: Arrests and social media crackdown follow deadly clashes over land*. https://www.amnesty.org/en/latest/news/2020/01/viet-nam-arrests-social-media-crackdown-deadly-clashes-land/

BBC News. (2017, December 27). Vietnam army hires censors to fight «internet chaos». *BBC News*. http://www.bbc.com/news/technology-42494113

CIVICUS. (2020, April 7). *Online debate on Dong Tam incident followed by pandemic silenced by Vietnam authorities*. CIVICUS. https://monitor.civicus.org/updates/2020/04/07/online-debate-dong-tam-incident-followed-pandemic-silenced-vietnam-authorities/

Deprez, M., & Haffner, A. (2020, March 13). *RSF: Vietnam, Philippine state among worst for spreading fake news*. Southeast Asia Globe. https://southeastasiaglobe.com/reporters-without-borders-vietnam-philippines/

DFRLab. (2020, February 12). Facebook shut down commercial disinformation network based in Myanmar and Vietnam. *Medium*. https://medium.com/dfrlab/facebook-shutdown-commercial-disinformation-network-based-in-myanmar-and-vietnam-d8c07c518c04

Funk, A. (2019, December 2). *Internet Freedom in Asia Hits Unprecedented Low*. Freedom House. https://freedomhouse.org/article/internet-freedom-asia-hits-unprecedented-low

Gleicher, N. (2019, December 20). Removing Coordinated Inauthentic Behavior From Georgia, Vietnam and the US - About Facebook. *About Facebook*. https://about.fb.com/news/2019/12/removing-coordinated-inauthentic-behavior-from-georgia-vietnam-and-the-us/

Gleicher, N. (2020, February 12). Removing Coordinated Inauthentic Behavior From Russia, Iran, Vietnam and Myanmar. *About Facebook*. https://about.fb.com/news/2020/02/removing-coordinated-inauthentic-behavior/

Graphika, & DFRLab. (2019). *#OperationFFS: Fake Face Swarm*. https://public-assets.graphika.com/reports/graphika_report_operation_ffs_fake_face_storm.pdf

Human Rights Watch. (2019, November 27). *Vietnam: Stop Intimidation and Harassment of Independent Publishing House*. Human Rights Watch. https://www.hrw.org/news/2019/11/27/vietnam-stop-intimidation-and-harassment-independent-publishing-house

Luong, D. (2017, November 30). Vietnam Wants to Control Social Media? Too Late. *The New York Times*. https://www.nytimes.com/2017/11/30/opinion/vietnam-social-media-china.html

Luong, D. (2018, February 19). Vietnam's Internet Is In Trouble. *The Washington Post*. https://www.washingtonpost.com/news/theworldpost/wp/2018/02/19/vietnam-internet/?utm_term=.b3fe9947aa9b

Nieva, R. (2020, March 20). *Inside a pro-Trump YouTube disinformation network that spans Vietnam to Bosnia*. CNET. https://www.cnet.com/features/inside-a-pro-trump-youtube-disinformation-network-that-spans-vietnam-to-bosnia/

Pham, N. (2013, January 12). Vietnam admits deploying bloggers to support government. *BBC News*. http://www.bbc.co.uk/news/world-asia-20982985

Qurium Media Foundation. (2018, July 10). *DDOS against luatkhoa.org and thevietnamese.org – Qurium Media Foundation*. https://www.qurium.org/alerts/vietnam/ddos-against-luatkhoa-org-and-thevietnamese-org/

The Phuong, N. (2018, January 10). *The Truth About Vietnam's New Military Cyber Unit*. The Diplomat. https://thediplomat.com/2018/01/the-truth-about-vietnams-new-military-cyber-unit/

Tuoi Tre News Staff. (2017, November 3). Draft law requires Facebook, Google to open data centers in Vietnam. *Tuoi Tre News*. https://tuoitrenews.vn/news/business/20171103/draft-law-requires-facebook-google-to-open-data-centers-in-vietnam/42438.html

Vietnam's neighbors, ASEAN, targeted by hackers: Report. (2017, November 7). *Reuters*. https://www.reuters.com/article/us-cyber-attack-vietnam-idUSKBN1D70VU

YEMEN

Introduction

Yemen is currently in the midst of an ongoing conflict, which has led to a humanitarian crisis among its citizens, and the halting of normal political activity (Freedom House, 2020). In 2011, President Ali Abdullah Saleh was removed during the Arab Spring uprisings, and the position was taken by his deputy Abdrabbuh Mansour Hadi (Freedom House, 2020). The Houthi rebel movement, however, opposed the transition. The Houthi movement was founded in the 1990s, and is rooted Yemen's Zaidi Shia Muslim minority. Between 2014 and 2015, the Houthi movement gradually took over the capital Sanaa and overthrew the new president, Abd Rabbu Mansour Hadi (BBC News, 2020). The actions of the Houthi movement were supported by Iran. At this point foreign powers, led by Saudi Arabia, have intervened to support the government forces.

The conflict has continued into 2020. Saudi Arabia attempted to instigate a unilateral ceasefire due to COVID-19, but it was rejected by the Houthis, who demanded that air and sea blockades be lifted in Sanaa and Hudaydah (BBC News, 2020). A report by the United Nations Development Programme (United Nations Development Programme, 2019) estimates that 233,000 Yemenis have been killed, and two decades of human development have been lost as a result of the conflict. All recent computational propaganda efforts therefore take place within this turbulent domestic environment.

An Overview of Cyber Troop Activity in Yemen

Organizational Form

Throughout the duration of the war, social media has gained more popularity and became an important source of news for Yemeni citizens, as the reach of traditional media has been more restricted than ever before (IJNET, 2019). Reports state that traditional media outlets have faced restrictions, closure and harassment by militias (DW, 2016). Journalists are either associated with the government, or controlled by the Houthis (Daraj, 2017).

As the consumption of news from online social media has expanded, so has the scale of computational propaganda within Yemen. However, given the multiplicity of actors and the level of hostilities mixed with the persecution of free media reporting, it is difficult to uncover the veracity of competing claims of computational propaganda.

In May 2020, a Houthi-controlled court convicted 10 journalists for “broadcasting controversial rumours and fake news aimed at weakening the possibility of defending the country and the moral of the citizens” (Farsides, 2020). The court accused the journalists of spreading disinformation in an effort to support the Saudi offensive (Farsides, 2020).

Saudi Arabia is also among the nation-states conducting computational propaganda that target Yemeni users. A Twitter investigation found a network of Saudi monarchy accounts to be praising Saudi leadership, and criticising Qatar and Turkish intervention in Yemen (Social Media Today, 2020).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Yemen

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
	Evidence found	Houthi groups			

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Amplification is a key strategy used by political groups in Yemen. A report by English channel Telesur revealed that bot Twitter accounts have been mass posting on the hashtag #Yemen, drowning out other news (Al Mawqea Post, 2017). Yemeni activists are artificially amplifying the Twitter hashtag "#Yemeni_Electronic_ Army" to criticise military intervention by the United Arab Emirates in Yemen (Al Estiklal, 2019). The activists state in their tweets that their objective is to create a network of human-operated accounts that artificially amplify one another (Al Estiklal, 2019).

As previously noted, limiting access to online content is also a form of online information manipulation in Yemen, Houthi authorities have reportedly blocked access to particular news websites and social media platforms (Freedom House, 2020).

Lastly, bot-driven campaigns aim to distract and distort the online environment. A report claims that the Saudi regime was behind a bot-driven social media campaign called "don't be their reporter", which sought to convince citizens not to share photos of Yemeni missiles targeting the Saudi military (Yemen Press Agency, 2019). However, there are also reports that Iran has employed websites to support the Houthis in Yemen (Elswah et al., 2019).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Yemen

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Human and bot	Attacks on political groups, support for own political faction	Amplifying content, limiting access	Twitter

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

Due to the complex domestic environment in Yemen, it is difficult to reliably estimate the size and scale of its computational propaganda efforts. However, in April 2020 Twitter removed a network of accounts operating from Saudi Arabia, Egypt and the United Arab Emirates, engaged in criticizing Qatar and Turkish intervention in Yemen (Social Media Today, 2020). This network comprised 5,350 accounts and tweeted 3.5 million times (Social Media Today, 2020).

Table 3: Cyber Troop Capacity in Yemen

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure

At least 5,350 accounts		Permanent	High	Medium

Source: Authors’ evaluations based on data collected. Blank spaces indicate no evidence was found.

References

Al Estiklal. (2019, September 8). لمواجهة “ذباب” الإمارات.. ناشطون: هذه مهام #الجيش_الإلكتروني_اليمني. *Al Estiklal*. https://www.alestiklal.net/ar/view/2347/dep-news-1567942583

Al Mawqea Post. (2017, November 24). مختصون يكشفون عن حسابات وهمية في تويتر تزيف الاخبار عن اليمن ويتهمون السعودية وأمريكا. *Al Mawqea Post*. https://almawqeapost.net/news/25247

BBC News. (2020, June 19). Yemen crisis: Why is there a war? *BBC News*. https://www.bbc.co.uk/news/world-middle-east-29319423

Daraj. (2017, November 30). نحن و”الأخبار الملفقة” وإعلامنا الممول من أنظمة الحروب في اليمن والعراق وسورية. *Daraj*. https://daraj.com/1885/

DW. (2016, January 31). اليمن ـ انتشار وسائل التواصل الاجتماعي بسبب التضييق الاعلامي. *DW*.

Elswah, M., Howard, P. N., & Narayanan, V. (2019). Iranian digital Interference in the Arab World. *Data Memo. Project on Computational Propaganda, Oxford, United Kingdom*, 1850–1867.

Farsides, S. (2020, May 1). *Yemen: Houthi-controlled court convicts 10 journalists and sentences 4 to death on Spurious Charges*. https://observatoryihr.org/news/yemen-houthi-controlled-court-convicts-10-journalists-and-sentences-4-to-death-on-spurious-charges/

Freedom House. (2020). *Yemen*. Freedom House. https://freedomhouse.org/country/yemen

IJNET. (2019, July 17). كيف يواجه الصحفيون اليمنيون الشائعات والأخبار المزيفة على السوشيال ميديا؟. *IJNET*.

Social Media Today. (2020, April 4). New Fake Account Removals Highlight Twitter’s Bot Problem Once Again. *Social Media Today*. https://www.socialmediatoday.com/news/new-fake-account-removals-highlight-twitters-bot-problem-once-again/575488/

United Nations Development Programme. (2019, April 23). *Assessing the Impact of War on Development in Yemen—Yemen*. ReliefWeb. https://reliefweb.int/report/yemen/assessing-impact-war-development-yemen

Yemen Press Agency. (2019, May 22). الذباب الإلكتروني يشن حملة تعتيم على المواطنين في السعودية. *Yemen Press Agency*. http://www.ypagency.net/163811

Zimbabwe

Introduction

As with other African countries, mobile phones are the most common way through which Zimbabweans connect to the world. Still, millions of citizens remain disconnected due to poor networks and high prices (Freedom House, 2019b) and their main sources of information remain print media and radio, which are, for the most part, controlled by the government (Freedom House, 2019a). Much of online communication happens via social media platforms, mainly WhatsApp, Facebook and Twitter, and internet access is provided by five services, two of which are government-owned, and three privately owned (Freedom House, 2019b). In July 2018 Zimbabwe held its first election in which social media played a significant role. The spread of misinformation had already been increasing significantly, especially during the military intervention that led to the resignation of Robert Mugabe in late 2017 (Freedom House, 2019b; Mberi, 2019). In 2019 the country was hit by an economic crisis leading to outbreaks of violence and other forms of harassment and infringements on personal freedoms by the military and police as activists and citizens were organising protests and looking for ways to support themselves (Freedom House, 2019a). At present, both the online and offline media landscape of the country function as political battlefields characterised by distrust and fear (Banya, 2019).

An Overview of Cyber Troop Activity in Zimbabwe

Organizational Form

The ZANU-PF has been the ruling party in Zimbabwe since 1980, first under the leadership of Robert Mugabe, who was forced to resign in late 2017, and now led by Emmerson Mnangagwa (Freedom House, 2019a). Allegedly the ZANU-PF pays pro-government commentators to engage in influence operations on social media, mainly Twitter and Facebook (Zimeye, 2018), supported by state-owned news outlets controlled by ZANU-PF (Melber, 2004). Other reports claim that both the ZANU-PF and the main oppositional party Movement for Democratic Change (MDC), have "cyber-warriors", both humans and bots, who actively influence opinions online through various channels (Banya, 2019; Moyo, 2018).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in Zimbabwe

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
	State-owned media	X			x

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

The "cyber-warriors" of the ZANU-PF and the MDC mainly engage in "churning out propaganda through commentaries on 'real news stories', gossip and planting misleading information" (Banya, 2019). At the same time major politicians and governmental institutions have established their own channels of communication on social media platforms, predominantly on Twitter. There have been incidents of false information being spread by politicians themselves, such as senior oppositional leader Tendai Biti, who claimed that the Reserve Bank of Zimbabwe would introduce a new currency amidst the 2019 (and on-going) economic and currency crisis (Kaiyo, 2019).

In general, though, Zimbabwe's government does not impose censorship or produce its own online content, though they have attempted to do so in the past, and have arrested citizens over their online activity (CPJ, 2020; Nzekwe, 2020). They also control broader access to the internet and social media: in July 2016 WhatsApp was reportedly blocked during nation-wide anti-governmental protests; the independent advocacy organization Zimbabwe Election 2018 was blocked by the state-owned internet provider TelOne in July 2018 (Magadlela, 2018); in early 2019 the internet was blacked out and social media shut down for days when citizens took to the streets to protest against rising fuel prices during the current economic crisis (Freedom House, 2019a; BBC News, 2019). However, in times of crisis the government does shift its focus from controlling other people's narratives to creating their own: in early 2019 critical voices and independent media have called out state media for spreading what they call pro-government propaganda by reporting that the government is on its way to restoring Zimbabwe's economy with headlines such as "Fuel and wheat storage already fixed"[1]. Such narratives are also often spread through Twitter accounts by state officials, particularly during the recent COVID-19 pandemic (Harding, 2020).

The government initially denied having anything to do with the blackout, claiming it was network congestion (Mberi, 2019), but soon warrants emerged which showed that state-owned, and some privately owned, internet providers were ordered to stop their service by the National Security Minister (The Zimbabwe Independent, 2019). Hashtags such as #ShutdownZimbabwe started trending as citizens aired their frustration about the government's continued control over internet access. Interestingly, the warrants issued to blackout the internet were technically legal and were made possible through the Interception and Communication Act introduced in 2007, which enables the government to intercept telecommunication for the purpose of protecting national security. However, a group of lawyers called on the High Court of Zimbabwe to rule the shutdown unconstitutional, and in late January 2019 the High Court announced that the government had exceeded their mandate in shutting down the internet and access was restored within a few days (Dzirutwe, 2019). Still, it appears that this ruling did not deter the Zimbabwean administration and they are willing to shut-down the internet again, if they deem it necessary (newsday, 2019). Moreover, many observers fear that the High Court's explicit language stating that the minister who ordered the shut-down had no authority to do so leaves a loophole for future shut-downs which could be ordered directly by the president or other governmental bodies that are given the necessary authority (Freedom House, 2019b; *The Herald*, 2019).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in Zimbabwe

Account Types	Messaging and Valence	Content and Communication Strategies	Platforms
Human	Support of government Attack opposition	Disinformation Access control[1]	WhatsApp Twitter Facebook

[1] While this is not an official strategy, it is probably the most likely to be used by the government. Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Organizational Capacity and Resources

The cyber troop capacity of the country is generally low in the sense that there is no continuous and organized effort to maintain online influence campaigns. Rather, the government tends to rely on less sophisticated measures such as simply shutting down the internet or particular social media and controlling or discouraging any flow of information that did not originate from them or affiliated organizations. A series of laws grants the Zimbabwean administration the necessary authority. In 2016 Mugabe introduced the Computer Crime and Cyber Crime Bill which would penalize the dissemination of communications "with intent to coerce, intimidate, harass, threaten, bully or cause substantial emotional distress" with fines and up to ten years in prison. Critics have said that the bill would mainly restrict the freedom of expression online. In January 2019, the bills passed into legislation as part of the Cybercrime and Cyber Security bill after it was fast-tracked by Zimbabwe's Information Minister. Allegedly, this was done as a reaction to the ongoing protests against the economic situation in Zimbabwe. Critics, such as Charlton Hwende, chairperson of the Parliamentary Portfolio Committee on Information Communication Technology, say the bill "lays the foundations of a police state" as the bill can be used to legitimize the surveillance of government critics and citizens on social media" (Karombo, 2019). Additionally, in March 2018 the National Policy for Information and Communications Technology passed into legislation, aiming to centralize the control over the country's internet infrastructure. Officially, it is supposed to foster growth in the ICT sector and eradicate corruption by eliminating bureaucratic bottlenecks (Machivenyika, 2018). However, the policy appears to be intended to function as part of a greater effort to bring internet service providers under governmental control.

Table 3: Cyber Troop Capacity in Zimbabwe

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure
		Temporary	Centralised	Low

Note: Capacity in terms of access control to the internet and intimidation to drown out dissent is quite high Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

All in all, intimidation tactics seem to only be worsening: Freedom House (2019a) reported a total of twenty-two cases in which activists were charged with treason or subversion during their reporting period and also highlighted the increasing number of abductions and arrests of opposition figures, civil society activists, and trade union leaders. Thus, self-censorship remains high as the government controls most information narratives available to the public and is successfully drowning out most other voices (Freedom House, 2019b). Recent developments give little reason to hope that the Zimbabwean administration will change its course to one less draconian: according to recent local news reports there are plans in place to jail individuals who have spread information deemed false by the government in relation to the COVID-19 pandemic for up to twenty years (Matenga, 2020).

References

Banya, N. (2019, July 18). Zimbabwe: The Challenge of False News and Disinformation. *ZimFact*. https://zimfact.org/zimbabwe-the-challenge-of-false-news-and-disinformation/

BBC News. (2019, January 18). Zimbabwe blocks WhatsApp amid crackdown. *BBC News*. https://www.bbc.com/news/world-africa-46917259

CPJ. (2020, September 2). Journalist Hopewell Chin'ono released on bail, with restrictions, in Zimbabwe. *Committee to Protect Journalists*. https://cpj.org/2020/09/journalist-hopewell-chinono-released-on-bail-with-restrictions-in-zimbabwe/

Dzirutwe, M. (2019, January 21). Zimbabwe court says internet shutdown illegal as more civilians detained. *Reuters*. https://www.reuters.com/article/us-zimbabwe-politics-idUSKCN1PF11M

Freedom House. (2019a). *Freedom House | Zimbabwe*. https://freedomhouse.org/country/zimbabwe/freedom-world/2020

Freedom House. (2019b). *Freedom on the Net | Zimbabwe*. https://freedomhouse.org/country/zimbabwe/freedom-net/2019

Harding, A. (2020, June 17). Zimbabwe—Once more on the brink of collapse? *BBC News*. https://www.bbc.com/news/world-africa-53062503

Kaiyo, D. (2019, February 20). Zimbabwe: Disinformation, Misinformation the New Battlefront—AllAfrica.com. *All Africa*. https://allafrica.com/stories/201902200302.html

Karombo, S. (2019, January 31). Zimbabwe fast-tracks cybercrime legislation. *ITWeb Africa*. http://www.itwebafrica.com/security/887-zimbabwe/245414-zimbabwe-fast-tracks-cybercrime-legislation

Machivenyika, F. (2018, March 15). UPDATED: President launches national ICT policy. *The Herald*. https://www.herald.co.zw/just-in-president-launches-ict-policy-framework/

Magadlela, M. (2018, August 9). Zimbabwean election website blocked following 2018 general elections. *Koliwemajama.Co.Zw*. https://koliwemajama.co.zw/zimbabwean-election-website-blocked-following-2018-general-elections/

Matenga, M. (2020, March 29). 20 years in jail for spreading fake coronavirus news. *NewsDay Zimbabwe*. https://www.newsday.co.zw/2020/03/20-years-in-jail-for-spreading-fake-coronavirus-news/

Mberi, R. (2019, February 5). Zimbabwe: Fake news and its effects in a time of crisis. *Africa Portal*. https://www.africaportal.org/features/zimbabwe-fake-news-and-its-effects-time-crisis/

Melber, H. (2004). MEDIA, PUBLIC DISCOURSE AND POLITICAL CONTESTATION IN ZIMBABWE. *CURRENT AFRICAN ISSUES*, *27*, 7–39.

MNOs restore full Internet services. (2019, January 22). *The Herald*. https://www.herald.co.zw/mnos-restore-full-internet-services/

Moyo, D. (2018, July 24). A vicious online propaganda war that includes fake news is being waged in Zimbabwe. *The Conversation*. http://theconversation.com/a-vicious-online-propaganda-war-that-includes-fake-news-is-being-waged-in-zimbabwe-99402

Muckraker. (2019, February 22). Zimbabwe: Floods of Propaganda Won't Conceal Failure. *All Africa, Zimbabwe Independent (Harare)*. https://allafrica.com/stories/201902220272.html

newsday. (2019, January 30). Govt won't hesitate shutting down Internet again: Mutodi. *NewsDay Zimbabwe*. https://www.newsday.co.zw/2019/01/govt-wont-hesitate-shutting-down-internet-again-mutodi/

Nzekwe, H. (2020, August 31). Zimbabwe's Speedy Social Media Law Is Africa's Latest Internet Censorship Plot. *Weetracker*. https://weetracker.com/2020/08/31/zimbabwe-africa-social-media-laws/

The Zimbabwe Independent. (2019, January 18). Legality of Zim's internet shutdown. *The Zimbabwe Independent*. https://www.theindependent.co.zw/2019/01/18/legality-of-zims-internet-shutdown/

Zimeye. (2018, September 3). *Mnangagwa Unleashes Social Media Cyber “Attack Dogs” Against Opponents | ZimEye*. https://www.zimeye.net/2018/03/09/mnangagwa-unleashes-social-media-cyber-attack-dogs-against-opponents/