



Samantha Bradshaw · University of Oxford
Hannah Bailey · University of Oxford
Philip N. Howard · University of Oxford

[illegible]

Executive Summary

The manipulation of public opinion over social media remains a critical threat to democracy. Over the past four years, we have monitored the global organization of social media manipulation by governments and political parties, and the various private companies and other organizations they work with to spread disinformation.

Our 2020 report highlights the recent trends of computational propaganda across 81 countries and the evolving tools, capacities, strategies, and resources used to manipulate public opinion around the globe. We identify three key trends in this year's inventory of disinformation activity:

1. Cyber troop activity continues to increase around the world. This year, we found evidence of 81 countries using social media to spread computational propaganda and disinformation about politics. This has increased from last years' report, in which we identified 70 countries with cyber troop activity.
2. Over the last year, social media firms have taken important steps to combat the misuse of their platforms by cyber troops. Public announcements by Facebook and Twitter between January 2019 and November 2020 reveal that more than 317,000 accounts and pages have been removed by the platforms. Nonetheless, almost US \$10 million has still been spent on political advertisements by cyber troops operating around the world.
3. Private firms increasingly provide manipulation campaigns. In our 2020 report, we found firms operating in forty-eight countries, deploying computational propaganda on behalf of a political actor. Since 2018 there have been more than 65 firms offering computational propaganda as a service. In total, we have found almost US \$60 million was spent on hiring these firms since 2009.



70
81 countries

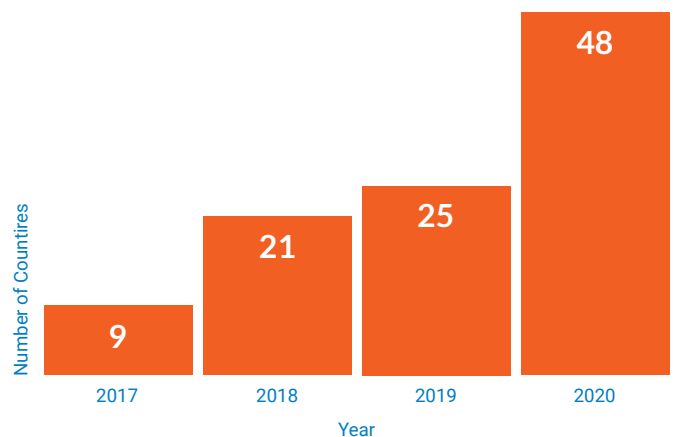
use social media to spread computational propaganda and disinformation



almost
US \$10M

spent on political adverts by cyber troops operating world wide

countries with evidence of private firms managing manipulation campaigns



Note: Growth of private firms operating in countries around the world overtime. Based on data presented in the annual cyber troops inventory between 2017-2020.

Contents

1	Introduction
6	Report Methodology
8	Organizational Form
11	Strategies, Tools, and Techniques
17	Organizational Behavior, Budgets, and Capacity
21	Conclusion
22	References
23	Acknowledgements
23	Authors' Biographies

ILLUSTRATIONS

3	Figure 1 - The Global Disinformation Order
5	Figure 2 - Facebook and Twitter Accounts Taken Down
10	Table 1 - Organizational Form and Prevalence of Social Media Manipulation
12	Table 2 - Fake Account Types
14	Table 3 - Messaging and Valence
16	Table 4 - Communication Strategies
18	Table 5 - Cyber Troop Capacity

Introduction

Social media platforms continue to play a critical role in the sharing of news, campaigning and elections, and political communication for over a billion people around the world.

While these technologies have created a number of opportunities, they have also introduced new challenges as foreign influence operations, disinformation, and state-sponsored trolling and harassment have undermined human rights, degraded the quality of political news in circulation, and undermined the legitimacy of democratically elected governments. From Chinese, Russian and Iranian-backed disinformation campaigns about the coronavirus (Barnes & Sanger, 2020; Molter & DiResta, 2020), to police forces in Belarus targeting high-profile activists with disinformation and smear campaigns (Freedom House, 2019) or private firms using computational propaganda to support local elections (Angel, 2019), many kinds of political actors are finding ways to exploit social networking technologies to spread propaganda online.

Since 2016 we have monitored the activity of "cyber troops", which we define as government or political party actors tasked with manipulating public opinion online (Bradshaw & Howard, 2017). Over the past four years, we have examined the formal organization of cyber troops around the world, and how these actors use computational propaganda for political purposes. This has involved building an inventory of the evolving strategies, tools, and techniques of computational propaganda, such as the use of "political bots" to amplify hate speech or other forms of manipulated content, the illegal harvesting of data or micro-targeting, or deploying armies of "trolls" to suppress political activism or freedom of the press. We have also tracked the capacity and resources invested into developing these techniques to build a picture of cyber troop capabilities around the world.

In this year's report, we identify cyber troop activity in 81 countries: Angola, Argentina, Armenia, Australia, Austria, Azerbaijan, Bahrain, Belarus, Bolivia, Bosnia & Herzegovina, Brazil, Cambodia, China, Colombia, Costa Rica, Croatia, Cuba, Czech Republic, Ecuador, Egypt, El Salvador, Eritrea, Ethiopia, Georgia, Germany, Ghana, Greece, Guatemala, Honduras, Hungary, India, Indonesia, Iran, Iraq, Israel, Italy, Kazakhstan, Kenya, Kyrgyzstan, Kuwait, Lebanon, Libya, Macedonia, Malaysia, Malta, Mexico, Moldova, Myanmar, Netherlands, Nigeria, North Korea, Oman, Pakistan, Philippines, Poland, Qatar, Russia, Rwanda, Saudi Arabia, Serbia, South Africa, South Korea, Spain, Sri Lanka,

Sudan, Sweden, Syria, Taiwan, Tajikistan, Thailand, Tunisia, Turkey, Ukraine, United Arab Emirates, United Kingdom, United States, Uzbekistan, Venezuela, Vietnam, Yemen, and Zimbabwe (see Figure 1). This year, we identified three key trends in cyber troop activity.

Cyber Troop Activity Continues to Rise Globally

Increasingly, states and other political actors are using social media to disrupt elections, democracy, and human rights. This year, we have found evidence of 81 countries with cyber troop activity, an increase from our previous report where we analyzed information operations in 70 countries. The strategies, tools, and techniques of social media manipulation continue to be a pervasive part of public life across all regime types. While we have identified many instances of social media manipulation used domestically during elections, they continue to be used as a tool of geopolitical influence. In 2020, for example, authoritarian countries like Russia, China and Iran capitalized on coronavirus disinformation to amplify anti-democratic narratives designed to undermine trust in health officials and government administrators.

Platform Companies Combat Cyber Troop Activity Through Account Takedowns

Platform companies try to limit the misuse of their platforms by taking down accounts that appear to be managed by cyber troops. Public announcements by Facebook and Twitter reveal that between January 2019 and November 2020 more than 10,893 Facebook accounts, 12,588 Facebook pages, 603 Facebook groups, 1,556 Instagram accounts, and 294,096 Twitter accounts were taken down by the platforms (see Figure 2). In this timeframe, Facebook also reported that almost US \$10 million was spent on political advertisements by cyber troops operating around the world.

Private Firms Increasingly Run Manipulation Campaigns

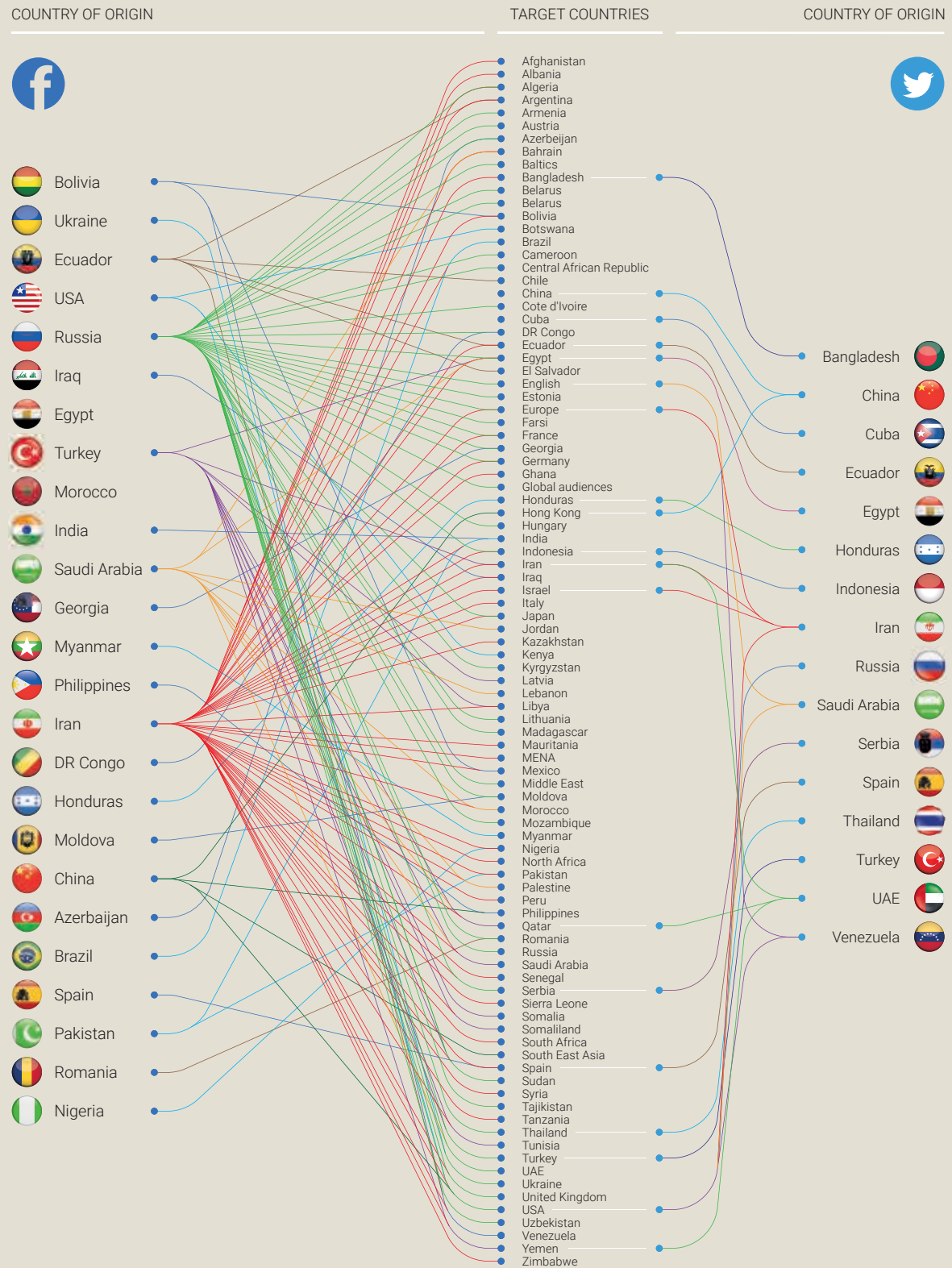
The number of cyber troop campaigns run by government or political party actors involving contracts with a private strategic communication firm has been steadily growing. In 2020, we found private firms operating in forty-eight countries deploying computational propaganda on behalf of a political actor. These companies often create sock puppet accounts, identify audiences for micro-targeting, or use bot or other amplification strategies to prompt the trending of certain political messages. Although tracking down contractual evidence of private contracting firms can be difficult, we found that almost US \$60 million was spent on hiring firms for computational propaganda since 2009.

FIGURE 1 - THE GLOBAL DISINFORMATION ORDER
COUNTRIES WITH CONFIRMED REPORTS OF CYBER TROOP ACTIVITY



Source: Authors (2021). **Note:** See page 2 for a full list of countries in this report.

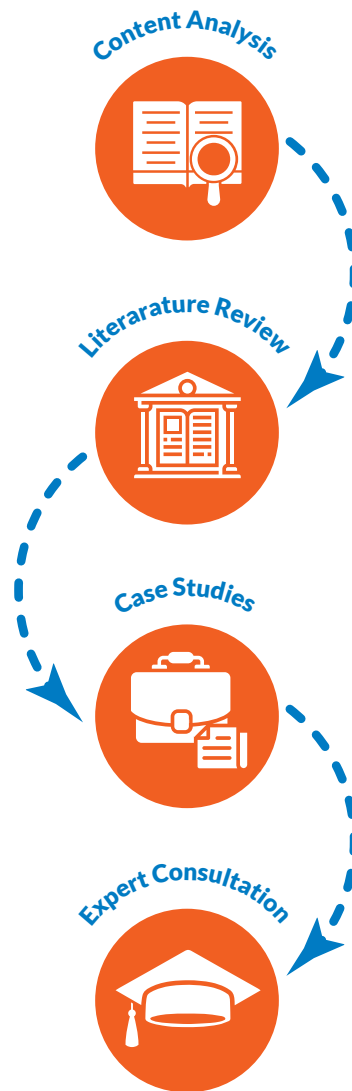
FIGURE 2 - FACEBOOK AND TWITTER ACCOUNT TAKEDOWNS
COUNTRIES DEPLOYING COMPUTATIONAL PROPAGANDA - HIGHEST FACEBOOK SPEND FROM TOP



Source: Authors' evaluations based on data collected. **Note:** Facebook column is organized by highest spend. Data based on Facebook and Twitter takedowns where state actors were attributed by the platforms. This does not include takedown data where non-state actors were attributed.

Report Methodology

Over the past four years, our four-stage methodology has allowed us to successfully capture and analyze a wide range of public documents that shed light on globally organized manipulation campaigns.



Given the nature of disinformation operations, there are almost certainly cyber troop activities that have not been publicly documented. However, for those that have been publicly identified, we have seen these cases grow in number over time (Bradshaw & Howard, 2017, 2018, 2019). While this report in no way is intended to provide a complete picture of how state actors are operating in this space, we can begin to build a bigger picture by piecing together public information. The methodology for this report consists of four stages:

- (1) a systematic content analysis of news articles reporting on cyber troop activity;
- (2) a secondary literature review of public archives and scientific reports;
- (3) drafting country case studies; and
- (4) expert consultations.

Content Analysis

Content analysis is an established research method in communication and media studies (Herring, 2009). It has been used to help understand how the Internet and social media interact with political action, regime transformation, and digital control (Bradshaw and Howard, 2018a, 2017b; Edwards, Howard & Joyce, 2013; Joyce, Antonio & Howard, 2013; Strange et al., 2013). This qualitative content analysis was conducted to understand the range of state actors who actively use social media to manipulate public opinion, as well as their capacity, strategies, and resources. We modelled our content analysis after last year's report, using purposive sampling to build a coded spreadsheet of specific variables that appear in news articles. The

following keywords were selected and used in combination for our search: bot; disinformation; fake account; fake news; information warfare; military; misinformation; propaganda; psychological operations; psyops; social media; sock puppet; troll.

There are two major limitations to conducting our qualitative content analyses: media bias and language. To help mitigate bias, we used LexisNexis and the top three search engine providers — Google, Yahoo!, and Bing — which provided hits to a variety of professional, local, and amateur news sources. To ensure that only high-quality news sources were being used to build our dataset, each article was given a credibility score using a three-point scale. Articles ranked at one came from major, professionally branded news organizations. Articles ranked at two came from smaller professional news organizations, local news organizations, or expert commentary and professional blogs. Articles ranked at three came from content farms, or personal or hyper-partisan blogs. These articles were removed from the sample.

Language was a second limitation to conducting our qualitative content analysis. For this year's global inventory, we were able to draw upon news articles and secondary resources written in Arabic, Dutch, English, French, German, Hebrew, Russian, and Spanish. We also worked with BBC monitoring¹ who provided an additional portal for collecting and aggregating high-quality news and information on cyber troop activity, as well as translation services for news articles for: Ghana, Eritrea, Iraq, Kuwait, Libya, Oman, Rwanda, and Yemen. We relied on English language reporting for: Armenia, Azerbaijan, Bosnia & Herzegovina, Brazil, Cambodia, China, Croatia, Czech Republic, Ethiopia, Georgia, Greece, Hungary, India, Indonesia, Kazakhstan, Kyrgyzstan, Macedonia, Malaysia, Moldova, North Korea, Pakistan, Philippines, Poland, Russia, Serbia, South Korea, Sri Lanka, Sweden, Syria, Taiwan, Tajikistan, Ukraine, Uzbekistan, Vietnam and Zimbabwe.

Secondary Literature Review

After conducting a content analysis, a team of research assistants completed secondary literature reviews to provide in-depth profiles of cyber troop activity in specific country contexts. These case studies drew from the data collected in the content analysis, as well as in-depth secondary literature reviews, where case study authors searched for other high-quality open source information about cyber troop activity. This involved looking for government reports, think tank papers, academic and scholarly studies, and research conducted by civil society organizations. A complete archive of the news

sources and secondary literature used in this report can be found in our public Zotero database, where country-specific sources are tagged by country name.

Country Case Studies

After completing this qualitative content analysis and secondary literature review, research assistants synthesized the findings into short country case studies. These case studies provide more information about instances of computational propaganda we identified in the content analysis, as well as detailed information about the specific country context and media environment in which social media manipulations are taking place. The case studies also provide greater details about the kinds of actors involved, examples of cyber troop activity, as well as a detailed bibliography of news articles and secondary sources about social media manipulation in that country.

Expert Consultations

The last step of our research methodology — consultations with experts — allowed us to peer review the case studies, as well as get feedback on the quality of English and local-language news reporting and secondary literature we found and discuss additional resources and citations in alternative languages with native speakers. Experts were asked to review the case studies drafted by research assistants, and (1) fact-check the information and data for accuracy; (2) provide additional citations to open source material; and (3) provide general feedback on the reliability of the data. Researchers would implement feedback from their expert consultations to finalize the draft of the case study, which was used as evidence to build this report. The final case studies can be found in a data supplemental published alongside this report.

¹ <https://monitoring.bbc.co.uk/>

Organizational Form

Cyber troop activity takes on many organizational forms and diverse actors are leveraging social media to shape public opinion, set political agendas, and propagate ideas.

While many countries have seen an increase in computational propaganda activities on social media, attribution back to a particular actor remains difficult. In this report, we focus specifically on cyber troops – or government or political party use of social media to manipulate public opinion (see Table 1).

Government Agencies

Government agencies are increasingly using computational propaganda to direct public opinion. In sixty-two countries, we found evidence of a government agency using computational propaganda to shape public attitudes. This category of actors includes communication or digital ministries, military campaigns, or police force activity. This year, we also included counts for state-funded media under our government agency banner, as some states used their state-funded media organizations as a tool to spread computational propaganda both domestically and abroad. Between 2019-2020, recent examples of government-led activity include the Philippine Police who used Facebook to influence narratives about military activities against terrorism (Gleicher, 2020b), or ongoing cyber conflicts between the Government of National Accord and the Libyan National Army who have used social media to shape narratives about the ongoing civil war (Kassab & Carvin, 2019). An example of state-funded media includes the Belarussian media infrastructure, where the government controls more than six hundred news outlets, many of which show evidence of propaganda and manipulation (Bykovskyy, 2020; Freedom House, 2019).

Political Parties

In addition to government or military-led initiatives, we also looked at political parties using computational propaganda during elections. In sixty-one countries, we found evidence of political parties or politicians running for office who have used the tools and techniques of computational propaganda as part of their political campaigns. Indeed, social media has become a critical component of digital campaigning, and some political actors have used the reach and ubiquity of these platforms to spread disinformation, suppress political

participation, and undermine oppositional parties. Over the last year we found examples of political parties and politicians using computational propaganda in countries such as Tunisia, where Facebook pages without direct links to candidates amplified disinformation and polarizing content in the lead-up to the vote (Jouini, 2019; Elswah & Howard 2020). Another example includes the use by Michael Bloomberg, a candidate in the US Democratic Party's Presidential Primary. Here, Bloomberg used fake Twitter accounts for his campaign, hiring hundreds of operators to artificially amplify support (Axelrod, 2020).

Private Firms

One growing trend is the increasing number of private companies involved in computational propaganda. Evidence from platform take-downs of coordinated inauthentic behavior, as well as ongoing journalistic investigations, have helped identify a growing number of political communication firms involved in spreading disinformation for profit. In forty-eight countries, we found evidence of state actors working with private companies or strategic communication firms who offer computational propaganda as a service. These contracts can be highly lucrative: since 2009, we found almost US \$60 million spent on contracts with private firms. It is important to remember that these amounts are only from confirmed reports: we suspect the actual amount is much higher. Between 2019-2020, examples of private firms include the Israeli-based Archimedes Group, who ran several campaigns across Africa, Latin America and South East Asia (Timberg & Room, 2019), or the Spanish company Eliminalia, who used computational propaganda to support local elections in Colombia, as well as campaigns in Ecuador and the Dominican Republic (Angel, 2019).

Citizen Influencers and Civil Society

One important feature of the organization of manipulation campaigns is that cyber troops often work in conjunction with civil society organizations, Internet subcultures, youth groups, hacker collectives, fringe movements, social media influencers, and volunteers who ideologically support a cause. The distinction between these groups can often be difficult to draw, especially since activities can be implicitly and explicitly sanctioned by the state. In this report, we look for evidence of formal coordination or activities that are officially sanctioned by the state or by a political party, rather than campaigns that might be implicitly sanctioned because of factors such

as overlapping ideologies or goals. We found twenty-three countries who worked in conjunction with civil society groups and fifty-one countries that worked with influencers to spread computational propaganda. An example from 2019-2020 would include Indonesia's "buzzer groups" who would volunteer to work with political campaigns during the 2019 elections (Potkin & Da Costa, 2019).



US \$60M

spent by state actors on contracts with private firms for computational propaganda services

TABLE 1 - ORGANIZATIONAL FORM AND PREVALENCE OF SOCIAL MEDIA MANIPULATION

Country	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organisations	Citizens and Influencers
Angola					
Argentina					
Armenia					
Australia					
Austria					
Azerbaijan					
Bahrain					
Belarus					
Bolivia					
Bosnia & Herzegovina					
Brazil					
Cambodia					
China					
Colombia					
Costa Rica					
Croatia					
Cuba					
Czech Republic					
Ecuador					
Egypt					
El Salvador					
Eritrea					
Ethiopia					
Georgia					
Germany					
Ghana					
Greece					
Guatemala					
Honduras					
Hungary					
India					
Indonesia					
Iran					
Iraq					
Israel					
Italy					
Kazakhstan					
Kenya					
Kyrgyzstan					
Kuwait					
Lebanon					
Libya					
Macedonia					
Malaysia					
Malta					
Mexico					
Moldova					
Myanmar					
Netherlands					
Nigeria					
North Korea					
Oman					
Pakistan					
Philippines					
Poland					
Qatar					
Russia					
Rwanda					
Saudi Arabia					
Serbia					
South Africa					
South Korea					
Spain					
Sri Lanka					
Sudan					
Sweden					
Syria					
Taiwan					
Tajikistan					
Thailand					
Tunisia					
Turkey					
Ukraine					
United Arab Emirates					
United Kingdom					
United States					
Uzbekistan					
Venezuela					
Vietnam					
Yemen					
Zimbabwe					

Source: Authors' evaluations based on data collected. **Note:** This table reports on the types of political actors using social media influence operations, and where examples of those organizations found. For Government Agencies, Political Parties, Private Contractors, Civil Society Organizations and Citizens and Influencers. ■ = Organizations found □ = No evidence found.

Strategies, Tools, and Techniques

Cyber troops make use of a variety of strategies, tools, and techniques to spread computational propaganda. Although propaganda is not new, the affordability of social networking technologies changes the scale, scope, and precision of how disinformation is transmitted.

 **57**
countries used automated accounts

 **79**
countries used human-curated accounts

 **14**
countries used hacked, stolen or impersonation accounts

These digital tools are constantly changing and adapting alongside innovations in technology. We have identified common tools and tactics used by cyber troops to comparatively assess the threat landscape.

Account Types

Cyber troops use both real and fake accounts to spread computational propaganda. These accounts can also be "human curated" or make use of automation. **Automated accounts** (sometimes referred to as political bots) are often used to amplify certain narratives while drowning out others. We found evidence of automated accounts being used in fifty-seven countries. An example of a highly automated cyber troop campaign includes bots set up by various public institutions in Honduras, including the National Television Station. These accounts were all traced to a single IP address range in Honduras, and pushed content designed to undermine the public conversation (Cryst & Garcia Camargo, 2020).

Increasingly more common is the use of **human-curated accounts**, which might use low levels of automation but also engage in conversations by posting comments or tweets, or by private messaging individuals via social media platforms. Human-operated accounts have been found in seventy-nine countries. It is important to note that human-curated accounts can be both real and fake. For example, in the United States teenagers were enlisted by a pro-Trump youth group, Turning Point Action, to spread pro-Trump narratives, as well as disinformation about topics such as mail-in ballots or the impact of the coronavirus (Stanley-Becker, 2020).

Another type of real-human account includes **hacked, stolen, or impersonation accounts** (including groups, pages, or channels), which are then co-opted to spread computational propaganda. However, these types of accounts make up a small portion of account types involved in computational propaganda. We have found only fourteen instances of hacked, stolen, or impersonated accounts. One example includes a fake Instagram profile that was created to impersonate Ali Karimli, the leader of the Popular Front Party in Azerbaijan (Azerbaijan Internet Watch, 2019).

TABLE 2 - FAKE ACCOUNT TYPES

Country	Bots	Human	Hacked or Stolen
 Angola			
 Argentina			
 Armenia			
 Australia			
 Austria			
 Azerbaijan			
 Bahrain			
 Belarus			
 Bolivia			
 Bosnia & Herzegovina			
 Brazil			
 Cambodia			
 China			
 Colombia			
 Costa Rica			
 Croatia			
 Cuba			
 Czech Republic			
 Ecuador			
 Egypt			
 El Salvador			
 Eritrea			
 Ethiopia			
 Georgia			
 Germany			
 Ghana			
 Greece			
 Guatemala			
 Honduras			
 Hungary			
 India			
 Indonesia			
 Iran			
 Iraq			
 Israel			
 Italy			
 Kazakhstan			
 Kenya			
 Kyrgyzstan			
 Kuwait			
 Lebanon			
 Libya			
 Macedonia			
 Malaysia			
 Malta			
 Mexico			
 Moldova			
 Myanmar			
 Netherlands			
 Nigeria			
 North Korea			
 Oman			
 Pakistan			
 Philippines			
 Poland			
 Qatar			
 Russia			
 Rwanda			
 Saudi Arabia			
 Serbia			
 South Africa			
 South Korea			
 Spain			
 Sri Lanka			
 Sudan			
 Sweden			
 Syria			
 Taiwan			
 Tajikistan			
 Thailand			
 Tunisia			
 Turkey			
 Ukraine			
 United Arab Emirates			
 United Kingdom			
 United States			
 Uzbekistan			
 Venezuela			
 Vietnam			
 Yemen			
 Zimbabwe			

Source: Authors' evaluations based on data collected. **Note:** This table reports on the types of fake accounts identified between 2010-2020. Bots refer to highly-automated accounts. For fake social media account types:  = Automated Accounts,  = Human Accounts,  = Hacked, Stolen or Impersonation Accounts,  = No evidence found.

Messaging and Valence

Cyber troops use a variety of messaging and valence strategies when communicating with users online. Valence describes the attractiveness (goodness) or averseness (badness) of a message, event, or thing. For our 2020 report, we have classified the valence and messaging strategies used by cyber troops into four categories.

The first is **pro-government or pro-party propaganda**, which involves using computational propaganda to artificially amplify supportive messages about the state or political party. An example of pro-government narratives from 2019-2020 includes the use of automated bot accounts in Lebanon which were used to artificially amplify hashtags supportive of Hezbollah's secretary general (Atallah, 2019).

The second type of messaging and valence strategy involves **attacking the opposition or mounting smear campaigns**. One example includes China-backed cyber troops who continue to use social media platforms to launch smear campaigns against Hong Kong Protestors (Shao, 2019).

The third type of messaging and valence strategy includes **suppressing participation through trolling or harassment**. Cyber troops are increasingly adopting the vocabulary of harassment to silence political dissent and freedom of the press. One example from 2019-2020 includes the Guatemalan "net centers" which use fake accounts that label individuals as "terrorists or foreign invaders" and target journalists with vocabulary associated with war, such as "enemies of the country" (IACHR, 2020).

Fourth, we are increasingly seeing populist political parties use social media narratives that **drive division and polarize citizens**. A recent example includes troll farms in Nigeria, with suspected connections to the Internet Research Agency in Russia. These troll farms are spreading disinformation and conspiracies around social issues in order to polarize online discourse, within Nigeria and as part of Russia's foreign influence operations targeting the United States and the United Kingdom (Hern & Harding, 2020).



90%

of study countries have misinformation campaigns that involve pro-government and pro-party propaganda



94%

of study countries have misinformation campaigns that attack the opposition and mount smear campaigns



73%

of study countries have misinformation campaigns that suppress participation through trolling or harassment



48%

of study countries have misinformation campaigns that drive division and polarize citizens

TABLE 3 - MESSAGING AND VALENCE

Country	Pro-Government	Attack Opposition	Distracting	Suppressing	Polarization
Angola	👍	👊	🗣️	🔇	🗣️
Argentina	👍	👊	🗣️	🔇	🗣️
Armenia	👍	👊	🗣️	🔇	🗣️
Australia	👍	👊	🗣️	🔇	🗣️
Austria	👍	👊	🗣️	🔇	🗣️
Azerbaijan	👍	👊	🗣️	🔇	🗣️
Bahrain	👍	👊	🗣️	🔇	🗣️
Belarus	👍	👊	🗣️	🔇	🗣️
Bolivia	👍	👊	🗣️	🔇	🗣️
Bosnia & Herzegovina	👍	👊	🗣️	🔇	🗣️
Brazil	👍	👊	🗣️	🔇	🗣️
Cambodia	👍	👊	🗣️	🔇	🗣️
China	👍	👊	🗣️	🔇	🗣️
Colombia	👍	👊	🗣️	🔇	🗣️
Costa Rica	👍	👊	🗣️	🔇	🗣️
Croatia	👍	👊	🗣️	🔇	🗣️
Cuba	👍	👊	🗣️	🔇	🗣️
Czech Republic	👍	👊	🗣️	🔇	🗣️
Ecuador	👍	👊	🗣️	🔇	🗣️
Egypt	👍	👊	🗣️	🔇	🗣️
El Salvador	👍	👊	🗣️	🔇	🗣️
Eritrea	👍	👊	🗣️	🔇	🗣️
Ethiopia	👍	👊	🗣️	🔇	🗣️
Georgia	👍	👊	🗣️	🔇	🗣️
Germany	👍	👊	🗣️	🔇	🗣️
Ghana	👍	👊	🗣️	🔇	🗣️
Greece	👍	👊	🗣️	🔇	🗣️
Guatemala	👍	👊	🗣️	🔇	🗣️
Honduras	👍	👊	🗣️	🔇	🗣️
Hungary	👍	👊	🗣️	🔇	🗣️
India	👍	👊	🗣️	🔇	🗣️
Indonesia	👍	👊	🗣️	🔇	🗣️
Iran	👍	👊	🗣️	🔇	🗣️
Iraq	👍	👊	🗣️	🔇	🗣️
Israel	👍	👊	🗣️	🔇	🗣️
Italy	👍	👊	🗣️	🔇	🗣️
Kazakhstan	👍	👊	🗣️	🔇	🗣️
Kenya	👍	👊	🗣️	🔇	🗣️
Kyrgyzstan	👍	👊	🗣️	🔇	🗣️
Kuwait	👍	👊	🗣️	🔇	🗣️
Lebanon	👍	👊	🗣️	🔇	🗣️
Libya	👍	👊	🗣️	🔇	🗣️
Macedonia	👍	👊	🗣️	🔇	🗣️
Malaysia	👍	👊	🗣️	🔇	🗣️
Malta	👍	👊	🗣️	🔇	🗣️
Mexico	👍	👊	🗣️	🔇	🗣️
Moldova	👍	👊	🗣️	🔇	🗣️
Myanmar	👍	👊	🗣️	🔇	🗣️
Netherlands	👍	👊	🗣️	🔇	🗣️
Nigeria	👍	👊	🗣️	🔇	🗣️
North Korea	👍	👊	🗣️	🔇	🗣️
Oman	👍	👊	🗣️	🔇	🗣️
Pakistan	👍	👊	🗣️	🔇	🗣️
Philippines	👍	👊	🗣️	🔇	🗣️
Poland	👍	👊	🗣️	🔇	🗣️
Qatar	👍	👊	🗣️	🔇	🗣️
Russia	👍	👊	🗣️	🔇	🗣️
Rwanda	👍	👊	🗣️	🔇	🗣️
Saudi Arabia	👍	👊	🗣️	🔇	🗣️
Serbia	👍	👊	🗣️	🔇	🗣️
South Africa	👍	👊	🗣️	🔇	🗣️
South Korea	👍	👊	🗣️	🔇	🗣️
Spain	👍	👊	🗣️	🔇	🗣️
Sri Lanka	👍	👊	🗣️	🔇	🗣️
Sudan	👍	👊	🗣️	🔇	🗣️
Sweden	👍	👊	🗣️	🔇	🗣️
Syria	👍	👊	🗣️	🔇	🗣️
Taiwan	👍	👊	🗣️	🔇	🗣️
Tajikistan	👍	👊	🗣️	🔇	🗣️
Thailand	👍	👊	🗣️	🔇	🗣️
Tunisia	👍	👊	🗣️	🔇	🗣️
Turkey	👍	👊	🗣️	🔇	🗣️
Ukraine	👍	👊	🗣️	🔇	🗣️
United Arab Emirates	👍	👊	🗣️	🔇	🗣️
United Kingdom	👍	👊	🗣️	🔇	🗣️
United States	👍	👊	🗣️	🔇	🗣️
Uzbekistan	👍	👊	🗣️	🔇	🗣️
Venezuela	👍	👊	🗣️	🔇	🗣️
Vietnam	👍	👊	🗣️	🔇	🗣️
Yemen	👍	👊	🗣️	🔇	🗣️
Zimbabwe	👍	👊	🗣️	🔇	🗣️

Source: Authors' evaluations based on data collected. **Note:** This table reports on the types of messaging and valence strategies of cyber troop activity between 2010-2019. For social media comments: 👍 = Pro-Government, 👊 = Attack Opposition, 🗣️ = Distracting, 🔇 = Suppressing, 🗣️ = Polarization. 🗣️ = No evidence found.

Strategies and Tactics

Cyber troops use a variety of communication strategies. We have categorized these activities into four categories. The first type of communication strategy is **the creation of disinformation or manipulated media**. This includes creative so-called “fake news” websites, doctored memes, images or videos, or other forms of deceptive content online. This is the most prominent type of communication strategy, with cyber troops in seventy-six countries using disinformation and other forms of manipulated media as part of their campaigns. While there have been growing concerns about the use of “deep fake” technology to spread disinformation, our 2019-2020 report found few examples of this technology being used for political deception. Rather than using deep fake technologies, doctored images and videos are still the most important form of manipulated media. For example, in the lead-up to the 2019 election in Argentina a manipulated video of the Minister of Security Patricia Bullrich was edited to make her appear intoxicated (Gardel, 2019). When we do find examples of deep fake technology, it is currently more commonly used in fake account generation, where generative adversarial networks are used to create fake profile pictures (Alba, 2019; Stanford Internet Observatory, 2020).

The second type of communication strategy involves using **data-driven strategies** to profile and target specific segments of the population with political advertisements. We count instances of data-driven strategies that use advertisements to spread disinformation or other false narratives. For example, during the 2019 General Election in the UK, First Draft News identified that 90% of the Conservative Party's Facebook advertisements in the early days of December 2019 promoted claims labelled as misleading by Full Fact (Reid & Dotto, 2019). This is an example of an instance that would fall under the scope of our report. In thirty countries, we identified instances of data-driven strategies. In many cases, instances of data-driven strategies were being facilitated by private firms who would use social media platforms' advertising infrastructure to target advertisements towards both domestic and foreign audiences. For example, the Canadian-based firm Estraterra, which worked for political consultants in Ecuador, spent approximately US \$1.38 million on Facebook ads targeting audiences in Ecuador, as well as other countries across Latin America (Gleicher, 2020a).

The third type of strategy adopted by cyber troops is the use of **trolling, doxing or online harassment**. In fifty-nine countries, we found evidence of trolls being used to attack political opponents, activists, or journalists on social media. Although trolls are often thought of as being constituted by networks of young adults and students, these teams can be comprised of

a wide range of individuals. One recent and unique example of trolling includes the cyber troop activity in Tajikistan. Here, the Ministry of Education and Science assigns trolling activities to teachers and university professors who will initiate coordinated campaigns to discredit opponents (Justice for Journalists, 2020).

In addition to direct trolling attacks, sometimes cyber troops censor speech and expression through **the mass-reporting of content or accounts**. Posts by activists, political dissidents or journalists can be reported by a coordinated network of cyber troop accounts in order to game the automated systems social media companies use to flag, demote, or take down inappropriate content. In seven countries we found evidence of the mass-reporting of content and accounts. One example of this phenomenon is the human networks of cyber troops in Pakistan, who both artificially boost political campaigns, but also mass report tweets that oppose their agenda as spam, causing the Twitter algorithm to block that issue's access to the trending panel (Poplaj & Jahangir, 2019). Recently, however, Twitter has maintained a 0% compliance rate with government requests to take down content that would fall under cyber troop activities (Twitter Transparency Report, 2019). Twitter is not the only platform involved. Facebook and Google have also been a focus of cyber troops in Pakistan: on Facebook, Pakistan successfully restricted more than 5,700 posts between January and June 2019 (Facebook Transparency Report, 2019) and on Google more than 3,299 posts were requested to be removed between January and June 2019 (Google Transparency Report, 2019). Facebook, Twitter and Google have expressed their concern at these restrictive activities and have also recently threatened to remove their services from Pakistan in response to legislative attempts to censor digital content, but they have yet to act on this threat (Singh, 2020).

 **76**
countries used disinformation and
media manipulation to mislead users

 **59**
countries use state-sponsored trolling
to target political opponents,
activists or journalists

 **7**
countries use mass-reporting of
content & accounts

TABLE 4 - COMMUNICATION STRATEGIES

Country	Disinfo	Mass Reporting	Data-Driven Strategies	Trolling	Amplifying Content
Angola					
Argentina					
Armenia					
Australia					
Austria					
Azerbaijan					
Bahrain					
Belarus					
Bolivia					
Bosnia & Herzegovina					
Brazil					
Cambodia					
China					
Colombia					
Costa Rica					
Croatia					
Cuba					
Czech Republic					
Ecuador					
Egypt					
El Salvador					
Eritrea					
Ethiopia					
Georgia					
Germany					
Ghana					
Greece					
Guatemala					
Honduras					
Hungary					
India					
Indonesia					
Iran					
Iraq					
Israel					
Italy					
Kazakhstan					
Kenya					
Kyrgyzstan					
Kuwait					
Lebanon					
Libya					
Macedonia					
Malaysia					
Malta					
Mexico					
Moldova					
Myanmar					
Netherlands					
Nigeria					
North Korea					
Oman					
Pakistan					
Philippines					
Poland					
Qatar					
Russia					
Rwanda					
Saudi Arabia					
Serbia					
South Africa					
South Korea					
Spain					
Sri Lanka					
Sudan					
Sweden					
Syria					
Taiwan					
Tajikistan					
Thailand					
Tunisia					
Turkey					
Ukraine					
United Arab Emirates					
United Kingdom					
United States					
Uzbekistan					
Venezuela					
Vietnam					
Yemen					
Zimbabwe					

Source: Authors' evaluations based on data collected. **Note:** This table reports on the communication strategies used by cyber troops. For communication strategies: = Disinformation and Manipulated Media, = Mass Reporting of Content/Accounts, = Data-Driven Strategies, = Trolling, = Amplifying Content, = No evidence found.

Organizational Behavior, Budgets, and Capacity

Although there is limited public information about the size and operations of cyber troop teams, over the past four years we have assembled the most comprehensive evidence of how they are resourced and coordinated.

Team Size and Permanency

The size and permanency of teams vary from country to country. In some countries, teams emerge temporarily around elections or to shape public attitudes around other important political events. In others, cyber troops are integrated into the media and communication landscape with full-time staff working to control, censor, and shape conversations and information online. In Venezuela, for example, leaked documents in 2018 described how 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), company (fifty people) a battalion (one hundred people) or a brigade (five hundred people), which could operate as many as 11,500 accounts (Riley et al., 2018). As part of these teams, people would “sign up for Twitter and Instagram accounts at government sanctioned kiosks” and were rewarded with coupons for food and goods (Riley et al., 2018) as well as other governmental benefits (Quintero & Coscojuela, 2019).

Budget and Expenditures

Computational propaganda remains big business. We have documented several expenditures made by cyber troops — either through purchasing political advertisements or by signing contracts with strategic communications firms. Between January 2019 and November 2020, cyber troop actors have spent over US \$10 million on Facebook advertisements, and governments have signed more than US \$60 million worth of contracts with private firms.

Cyber Troop Capacity

By looking comparatively across the behaviours, expenditures, tools, and resources cyber troop employ, we can begin to build a larger comparative picture of the global organization of social media manipulation. National contexts are always important to consider. However, we suggest it is also worth generalizing about the experience of organized disinformation campaigns across regime types to develop a broad and comparative understanding of this phenomenon. We have begun to develop a simplistic measure to comparatively assess the capacity of cyber troop teams in relation to one another, taking into

consideration the number of government actors involved, the sophistication of tools, the number of campaigns, the size and permanency of teams, and budgets or expenditures made. We describe cyber troop capacity on a three-point scale:

- 1. High cyber troop capacity** involves large numbers of staff, and large budgetary expenditure on psychological operations or information warfare. There might also be significant funds spent on research and development, as well as evidence of a multitude of techniques being used. These teams do not only operate during elections but involve full-time staff dedicated to shaping the information space. High-capacity cyber troop teams focus on foreign and domestic operations. They might also dedicate funds to state-sponsored media for overt propaganda campaigns. High-capacity teams include: Australia, China, Egypt, India, Iran, Iraq, Israel, Myanmar, Pakistan, Philippines, Russia, Saudi Arabia, Ukraine, United Arab Emirates, United Kingdom, United States, Venezuela, and Vietnam.
- 2. Medium cyber troop capacity** involves teams that have a much more consistent form and strategy, involving full-time staff members who are employed year-round to control the information space. These medium-capacity teams often coordinate with multiple actor types, and

experiment with a wide variety of tools and strategies for social media manipulation. Some medium-capacity teams conduct influence operations abroad. Medium-capacity teams include: Armenia, Austria, Azerbaijan, Bahrain, Belarus, Bolivia, Brazil, Cambodia, Cuba, Czech Republic, Eritrea, Ethiopia, Georgia, Guatemala, Hungary, Indonesia, Kazakhstan, Kenya, Kuwait, Lebanon, Libya, Malaysia, Malta, Mexico, Nigeria, North Korea, Poland, Rwanda, South Korea, Sri Lanka, Syria, Taiwan, Tajikistan, Thailand, Turkey, and Yemen.

- 3. Low cyber troop capacity** involves small teams that may be active during elections or referenda but stop activity until the next election cycle. Low capacity teams tend to experiment with only a few strategies, such as using bots to amplify disinformation. These teams operate domestically, with no operations abroad. Low capacity teams include: Angola, Argentina, Bosnia & Herzegovina, Colombia, Costa Rica, Croatia, Ecuador, El Salvador, Germany, Ghana, Greece, Honduras, Italy, Kyrgyzstan, Moldova, Netherlands, Oman, Qatar, Republic of North Macedonia, Serbia, South Africa, Spain, Sudan, Sweden, Tunisia, Uzbekistan, and Zimbabwe.

TABLE 5 - CYBER TROOP CAPACITY

HIGH CAPACITY					
Country	Recent Activity	Status	Coordinated Cybertroop Team	Resources Spent	Coordination
 China	✓	Permanent			Centralised
 Egypt	✓	Permanent			Decentralised
 India	✓	Permanent			Centralized
 Iran	✓	Permanent			Centralised
 Iraq	✓	Permanent			Somewhat Centralised
 Israel	✓	Permanent			Centralised
 Myanmar	✓	Permanent			Centralized
 Pakistan	✓	Permanent			Decentralised
 Philippines	✓	Permanent			Centralized
 Russia	✓	Permanent			Centralized
 Saudi Arabia	✓	Permanent			Centralised
 Ukraine	✓	Permanent			Centralized
 United Arab Emirates	✓	Permanent			Centralised
 United Kingdom	✓	Permanent			Decentralised
 United States	✓	Permanent			Decentralised
 Venezuela	✓	Permanent			Centralized
 Vietnam	✓	Permanent			Somewhat Centralised

TABLE 5 - CYBER TROOP CAPACITY continued

MEDIUM CAPACITY						
Country		Recent Activity	Status	Coordinated Cybertroop Team	Resources Spent	Coordination
	Armenia	✓	Temporary			Decentralised
	Australia	✓	Temporary			Decentralised
	Austria	✗	Temporary			Decentralised
	Azerbaijan	✓	Permanent			Somewhat Centralised
	Bahrain	✗	Temporary			Centralised
	Belarus	✓	Permanent			Somewhat Centralised
	Bolivia	✓	Temporary			Somewhat Centralised
	Brazil	✓	Permanent			Somewhat Centralised
	Cambodia	✓	Permanent			Somewhat Centralised
	Cuba	✓	Permanent			Centralized
	Czech Republic	✓	Temporary			Decentralised
	Eritrea	✓	Permanent			Centralized
	Ethiopia	✓	Permanent			Centralized
	Georgia	✓	Temporary			Centralised
	Guatamala	✓	Permanent			Centralized
	Hungary	✓	Temporary			Centralised
	Indonesia	✓	Temporary			Decentralised
	Kenya	✓	Temporary			Somewhat Centralised
	Kazakhstan	✓	Permanent			Centralised
	Kuwait	✓	Temporary			Decentralised
	Lebanon	✓	Temporary			Decentralised
	Libya	✓	Temporary			Somewhat Centralised
	Malaysia	✗	Permanent			Centralised
	Malta	✓	Permanent			Centralized
	Mexico	✓	Temporary			Decentralised
	Nigeria	✓	Temporary			Decentralised
	North Korea	✓	Permanent			Centralized
	Poland	✓	Temporary			Decentralised
	Rwanda	✓	Permanent			Centralized
	South Korea	✓	Permanent			Centralized
	Sri Lanka	✓	Permanent			Somewhat Centralised
	Syria	✓	Permanent			Somewhat Centralised
	Taiwan	✓	Temporary			Decentralised
	Tajikistan	✓	Permanent			Centralized
	Thailand	✓	Permanent			Centralized
	Turkey	✓	Temporary			Somewhat Centralised
	Yemen	✓	Permanent			Centralised

TABLE 5 - CYBER TROOP CAPACITY continued

Low Capacity						
Country		Recent Activity	Status	Coordinated Cybertroop Team	Resources Spent	Coordination
	Angola		Temporary			Decentralised
	Argentina		Temporary			Decentralised
	Bosnia & Herzegovina		Temporary			Decentralised
	Colombia		Temporary			Decentralised
	Costa Rica		Temporary			Decentralised
	Croatia		Temporary			Decentralised
	Ecuador		Temporary			Centralised
	El Salvador		Temporary			Decentralised
	Germany		Temporary			Decentralized
	Ghana		Temporary			Centralized
	Greece		Temporary			Decentralised
	Honduras		Temporary			Centralised
	Italy		Temporary			Somewhat Centralised
	Kyrgyzstan		Temporary			Somewhat Centralised
	Macedonia		Temporary			Decentralised
	Moldova		Temporary			Decentralized
	Netherlands		Temporary			Decentralised
	Oman		Temporary			Somewhat Centralised
	Qatar		Temporary			Centralised
	Serbia		Permanent			Centralized
	South Africa		Temporary			Centralized
	Spain		Temporary			Decentralised
	Sudan		Temporary			Centralized
	Sweden		Temporary			Decentralised
	Tunisia		Temporary			Somewhat centralised
	Uzbekistan		Permanent			Centralised
	Zimbabwe		Temporary			Centralised

Source: Authors' evaluations based on data collected. **Note:** These tables reports on the capacity of cyber troop actors. Recent activity is defined as publicly documented activity between 2019-2020. For cyber troop capacity:  = Evidence of recent activity over the past year,  = Evidence of coordinated cybertroop teams,  = Evidence of resources spent,    = No evidence found.

Conclusion

We find that industrialized disinformation has become more professionalized, and produced on a large scale by major governments, political parties, and public relations firms.

This report has highlighted the ways in which government agencies and political parties have used social media to spread political propaganda, pollute the digital information ecosystem, and suppress freedoms of speech and press. In our annual inventory for 2020, we also find a clear trajectory in

professionalized, industrialized misinformation production by mainstream communications and public relations firms. While social media can enhance the scale, scope, and precision of disinformation (Bradshaw & Howard, 2018), many of the issues at the heart of computational propaganda — polarization, distrust and the decline of democracy — have pre-dated social media and even the Internet itself. The co-option of social media technologies should cause concern for democracies around the world—but so should many of the long-standing challenges facing democratic societies.

Both the Covid-19 pandemic and the US election forced many social media firms to better flag misinformation, close fake accounts, and raise standards for both information quality and civility in public conversation. Not everyone agrees that these initiatives are sufficient. It is also not clear whether these more aggressive responses by social media firms will be applied to other issue areas or countries.

Computational propaganda has become a mainstay in public life. These techniques will also continue to evolve as new technologies — including Artificial Intelligence, Virtual Reality, or the Internet of Things — are poised to fundamentally reshape society and politics. But computational propaganda does not exist or spread independently. It is the result of poor technology design choices, lax public policy oversight, inaction by the leadership of social media platforms, investments by authoritarian governments, political parties, and mainstream communications firms. Computational propaganda is also a driver of further democratic ills, including political polarization and diminished public trust in democratic institutions.

Social media platforms can be an important part of democratic institutions, which can be strengthened by high-quality information. A strong democracy requires access to this information, where citizens are able to come together to debate, discuss, deliberate, empathize, make concessions and work towards consensus. There is plenty of evidence that social media platforms can be used for these things. But in this annual inventory, we find significant evidence that in more countries than ever, social media platforms serve up disinformation at the behest of major governments, political parties and public relations firms.

References

- Alba, D. (2019, 20 December). **Facebook Discovers Fakes that Show Evolution of Disinformation.** *New York Times*. <https://www.nytimes.com/2019/12/20/business/facebook-ai-generated-profiles.html>
- 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>
- Atallah, N. M. (2019, December 26). **How internet has become a battleground in the Lebanese revolution.** *Le Commerce*. <https://www.lecommercedulevant.com/article/29508-how-internet-has-become-a-battleground-in-the-lebanese-revolution>
- Axelrod, T. (2020). **Twitter Suspends 70 pro-Bloomberg ‘spam’ accounts.** <https://thehill.com/policy/technology/484168-twitter-suspends-70-pro-bloomberg-accounts-citing-platform-manipulation>
- 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/>
- Barnes, J. E. and D. E. Sanger. 2020. **“Russian Intelligence Agencies Push Disinformation on Pandemic.”** *The New York Times*, July 28. www.nytimes.com/2020/07/28/us/politics/russia-disinformation-coronavirus.html
- Bradshaw, Samantha and Philip N. Howard (2019) **The Global Disinformation Disorder: 2019 Inventory of Social Media Manipulation.** *Computational Propaganda Project Working Paper Series*. Working Paper 2019.3.
- (2018) **Challenging Truth and Trust: A Global Inventory of Social Media Manipulation.** *Computational Propaganda Project Working Paper Series*. Working Paper 2018.1
- (2017) **Troops, Trolls and Trouble Makers: A Global Inventory of Social Media Manipulation.** *Computational Propaganda Project Working Paper Series*, Working paper 2017.12.
- 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 mae. Otchet o prokremlenskikh 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-prokremlenskikh>
- Cryst, E., & García Camargo, I. (2020). **#VivaJOH o #FueraJOH. An analysis of Twitter’s takedown of Honduran accounts.** *Stanford Internet Observatory*. <https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/04022020-hondurastakedown.pdf>
- Edwards, Frank, Philip N. Howard, and Mary Joyce. 2013. **Digital Activism & Non-Violent Conflict.** <http://digital-activism.org/2013/11/report-on-digital-activism-and-non-violent-conflict/> (May 17, 2017)
- 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 Transparency. (2019). **Content Restrictions—PK.** <https://transparency.facebook.com/content-restrictions/country/PK>
- Freedom House. (2019). **Freedom on the Net 2019: Belarus.** Freedom House. <https://freedomhouse.org/country/belarus/freedom-net/2019>
- Gardel, 2019. <https://reversoar.com/los-falsos-mas-virales-de-la-campana-que-desmintio-reverso/>
- Gleicher, N. (2020a). **Removing Coordinated Inauthentic Behavior.** Facebook Newsroom. July <https://about.fb.com/news/2020/07/removing-political-coordinated-inauthentic-behavior/>
- Gleicher, N. (2020b). **Removing Coordinated Inauthentic Behavior.** Facebook Newsroom. September. <https://about.fb.com/news/2020/09/removing-coordinated-inauthentic-behavior-china-philippines/>
- Google Transparency Report. (2019). **Government requests to remove content — Google Transparency Report.** Google. <https://transparencyreport.google.com/government-removals/by-country/PK?hl=en>
- 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>
- Herring, Susan C. 2009. **“Web Content Analysis: Expanding the Paradigm.”** In *International Handbook of Internet Research*, eds. Jeremy Hunsinger, Lisbeth Klastrup, and Matthew Allen. Springer Netherlands, 233–49. http://link.springer.com/chapter/10.1007/978-1-4020-9789-8_14 (May 17, 2017).
- 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>
- 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/>
- Joyce, Mary, Rosas Antonio, and Philip N. Howard. 2013. **“Global Digital Activism Data Set.”** <http://www.icpsr.umich.edu/icpsrweb/ICPSR/studies/34625/version/2>.
- 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/>
- 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>
- 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/>

Molter, V. & DiResta, R. (2020). **Pandemics & propaganda: how Chinese state media creates and propagates CCP coronavirus narratives.** <https://cyber.fsi.stanford.edu/io/publication/pandemics-propaganda>

Popalzai, R., & Jahangir, S. (2019). **While Twitter trends may be artificial, hashtag merchants are real people.** Dawn. <https://www.dawn.com/news/1518967>

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-idUSKBN1QU0AS>

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/>

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/>

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/>

Shao, G. (2019). **Social media has become a battleground in Hong Kong Protests.** CNBC. <https://www.cnbc.com/2019/08/16/social-media-has-become-a-battleground-in-hong-kongs-protests.html>

Singh, M. (n.d.). **Google, Facebook and Twitter threaten to leave Pakistan over censorship law.** TechCrunch. Retrieved 13 December 2020, from <https://social.techcrunch.com/2020/11/20/google-facebook-and-twitter-threaten-to-leave-pakistan-over-censorship-law/>

Stanford Internet Observatory. (2020). **Reply-Guys Go Hunting: An Investigation into a U.S. Astroturfing operation on Facebook, Twitter, and Instagram.** <https://cyber.fsi.stanford.edu/io/publication/reply-guys-go-hunting-investigation-us-astroturfing-operation-facebook-twitter-and>

Strange, Austin et al. 2013. **China's Development Finance to Africa: A Media-Based Approach to Data Collection.** Working Paper. <https://www.cgdev.org/publication/chinas-development-finance-africa-media-based-approach-data-collection> (May 17, 2017)

Stanley-Becker, I. (2020). **Pro-Trump youth group enlists teens in secretive campaign likened to a "troll farm," prompting rebuke by Facebook and Twitter.** Washington Post. https://www.washingtonpost.com/politics/turning-point-teens-disinformation-trump/2020/09/15/c84091ae-f20a-11ea-b796-2dd09962649c_story.html

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/>

Twitter Transparency Report. (2019). **Pakistan.** Twitter. <https://transparency.twitter.com/en/countries/pk.html>

Acknowledgments

The authors gratefully acknowledge the support of the European Research Council for the research project, "Computational Propaganda: Investigating the Impact of Algorithms and Bots on Political Discourse in Europe," Proposal 648311, 2015–2020, Philip N. Howard, Principal Investigator. Additional support for this study has been provided by the Adessium Foundation, Civitates Initiative, Ford Foundation, Hewlett Foundation, Luminate, Newmark Philanthropies, and Open Society Foundation.

For their assistance and advice on this research, we are grateful to Ualan Campbell-Smith, Amelie Henle, Antonella Perini and Sivanne Shavel for collecting the preliminary data and drafting country profiles about social media manipulation for the countries outlined in this report. We would also like to thank Rutendo Chabikwa for her assistance with further research and data analysis for this report. We are also extremely grateful to Rosana Aleksoska, Daniel Arnaudo, Ana Brakus, Darko Brkan, Muslimbek Buriev, Rutendo Chabikwa, Niki Cheong, Thomas Colley, Regina Coyula, Tijana Cvjetićanin, Brian Dooley, Iyad el-Baghdadi, Roberto Gelado Marcos, Marlon Hernández-Anzora, Katarína Klingová, Peter Kreko, Cristian León, Allison McManus, Olivier Milland, Nargiza Muratalieva, Vidya Narayanan, Lisa-Marie Neudert, Ben Nimmo, Alina Ostling, Belén Puebla Martínez, Khadeja Ramali, Talal Raza, Tom Sear, James Shire, Tehilla Shwartz Altshuler, and Weaam Youssef, as well as the many anonymous experts we consulted for this project. Their country-specific expertise and networks were essential for ensuring the reliability and validity of our data. We thank them for their time and assistance in reviewing country profiles, and for providing us with additional sources, citations, and data-points to include in this report.

Authors' Biographies

Samantha Bradshaw completed her PhD at the Oxford Internet Institute, University of Oxford. Between 2016-2020, Samantha worked for the Computational Propaganda Project as a core member of the research team, where conducted research on foreign influence operations and the spread of disinformation by state-backed actors. Samantha's research has been featured in numerous media articles, including the Washington Post, the Financial Times, and CNN. Currently, Samantha is a postdoctoral fellow at the Internet Observatory & the Digital Civil Society Lab at Stanford University.

Hannah Bailey is a doctoral candidate in Social Data Science at the Oxford Internet Institute, and a researcher at the Computational Propaganda Project. Her research focuses on China's use of state-sponsored digital disinformation.

Philip N. Howard is Director of the Oxford Internet Institute, and a statutory Professor at Balliol College, Oxford. He writes about information politics and international affairs, and is the author of eight books, including *The Managed Citizen*, *The Digital Origins of Dictatorship and Democracy*, and *Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up*. He has won multiple "best book" awards, and his research and commentary writing has been featured in the New York Times, Washington Post, and many international media outlets. Foreign Policy magazine named him a "Global Thinker" for 2017 and the National Democratic Institute awarded him their "Democracy Prize" for pioneering the social science of fake news.



The Computational Propaganda Project

at the Oxford Internet Institute

University of Oxford

1 St Giles • Oxford OX1 3JS

Website: www.oii.ox.ac.uk



This work is licensed under a Creative Commons Attribution

- Non Commercial - Share Alike 4.0 International License

