



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

Samantha Bradshaw · University of Oxford

Philip N. Howard · University of Oxford



Executive Summary

Computational propaganda – the use of algorithms, automation, and big data to shape public life – is becoming a pervasive and ubiquitous part of everyday life.

Over the past three years, we have monitored the global organization of social media manipulation by governments and political parties. Our 2019 report analyses the trends of computational propaganda and the evolving tools, capacities, strategies, and resources.

- 1.** Evidence of organized social media manipulation campaigns which have taken place in 70 countries, up from 48 countries in 2018 and 28 countries in 2017. In each country, there is at least one political party or government agency using social media to shape public attitudes domestically (Figure 1).
- 2.** Social media has become co-opted by many authoritarian regimes. In 26 countries, computational propaganda is being used as a tool of information control in three distinct ways: to suppress fundamental human rights, discredit political opponents, and drown out dissenting opinions (Figure 2).
- 3.** A handful of sophisticated state actors use computational propaganda for foreign influence operations. Facebook and Twitter attributed foreign influence operations to seven countries (China, India, Iran, Pakistan, Russia, Saudi Arabia, and Venezuela) who have used these platforms to influence global audiences (Figure 3).
- 4.** China has become a major player in the global disinformation order. Until the 2019 protests in Hong Kong, most evidence of Chinese computational propaganda occurred on domestic platforms such as Weibo, WeChat, and QQ. But China's new-found interest in aggressively using Facebook, Twitter, and YouTube should raise concerns for democracies.
- 5.** Despite there being more social networking platforms than ever, Facebook remains the platform of choice for social media manipulation. In 56 countries, we found evidence of formally organized computational propaganda campaigns on Facebook. (Figure 4).

Contents

1	Introduction
7	Report Methodology
9	Organisational Form
11	Strategies, Tools, and Techniques
17	Organisational Budgets, Behaviours, and Capacity
21	Conclusion
22	References
23	Acknowledgements
23	Authors Biographies
ILLUSTRATIONS	
3	Figure 1 - The Global Disinformation Order
5	Figure 2 - Computational Propaganda as a Tool of Information Control
5	Figure 3 - Foreign Influence Operations on Social Media
6	Figure 4 - Prominent Platforms for Social Media Manipulation
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

Around the world, government actors are using social media to manufacture consensus, automate suppression, and undermine trust in the liberal international order.

Although propaganda has always been a part of political discourse, the deep and wide-ranging scope of these campaigns raise critical public interest concerns.

Cyber troops' are defined as government or political party actors tasked with manipulating public opinion online (Bradshaw and Howard 2017a). We comparatively examine the formal organization of cyber troops around the world, and how these actors use computational propaganda for political purposes. This involves building an inventory of the evolving strategies, tools, and techniques of computational propaganda, including 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 an army of 'trolls' to bully or harass political dissidents or journalists online. We also track the capacity and resources invested into developing these techniques to build a picture of cyber troop capabilities around the world.

The use of computational propaganda to shape public attitudes via social media has become mainstream, extending far beyond the actions of a few bad actors. In an information environment characterized by high volumes of information and limited levels of user attention and trust, the tools and techniques of computational propaganda are becoming a common – and arguably essential – part of digital campaigning and public diplomacy. In addition to building a globally comparative picture of cyber troop activity, we also hope to drive public and scholarly debate about how we define and understand the changing nature of politics online, and how technologies can and should be used to enhance democracy and the expression of human rights online.

In this year's report, we examine cyber troop activity in 70 countries: Angola, Argentina, Armenia, Australia, Austria, Azerbaijan, Bahrain, Bosnia & Herzegovina, Brazil, Cambodia, China, Colombia, Croatia, Cuba, Czech Republic, Ecuador, Egypt, Eritrea, Ethiopia, Georgia, Germany, Greece, Honduras, Guatemala, Hungary, India, Indonesia, Iran, Israel, Italy, Kazakhstan, Kenya, Kyrgyzstan, Macedonia, Malaysia, Malta, Mexico, Moldova, Myanmar, Netherlands, Nigeria, North Korea, Pakistan, Philippines, Poland, Qatar, Russia, Rwanda, Saudi Arabia, Serbia, South Africa, South Korea, Spain, Sri Lanka,

Sweden, Syria, Taiwan, Tajikistan, Thailand, Tunisia, Turkey, Ukraine, United Arab Emirates, United Kingdom, United States, Uzbekistan, Venezuela, Vietnam, and Zimbabwe.

Growing Evidence of Computational Propaganda Around the World

We found evidence of organised social media manipulation campaigns in 70 countries, up from 48 countries in 2018 and 28 countries in 2017. Some of this growth comes from new entrants who are experimenting with the tools and techniques of computational propaganda during elections or as a new tool of information control. However, journalists, academics, and activists are also better equipped with digital tools and a more precise vocabulary to identify, report, and uncover instances of formally organized social media manipulation. Over the past three years we have been able to refine our language and search terms for identifying instances of computational propaganda, and we found that many countries have displayed elements of formally organized social media manipulation for the past decade. As a result, we suggest that computational propaganda has become a ubiquitous and pervasive part of the digital information ecosystem.

The Co-Option of Social Media in Authoritarian Regimes

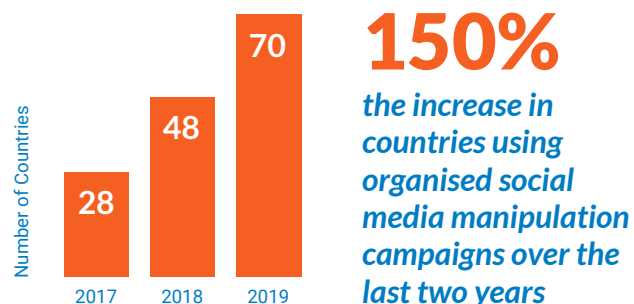
In many authoritarian regimes, computational propaganda has become a tool of information control that is strategically used in combination with surveillance, censorship, and threats of violence. We have catalogued the kinds of campaigns authoritarian countries have used against journalists, political dissidents, and the broader society, and found three distinct ways in which computational propaganda is used:

- (1) to suppress fundamental human rights;
- (2) to discredit political opposition; and
- (3) to drown out political dissent.

The co-option of social media technologies provides authoritarian regimes with a powerful tool to shape public discussions and spread propaganda online, while simultaneously surveilling, censoring, and restricting digital public spaces.

A Limited Number of Foreign Influence Operations by Highly Sophisticated Actors

Foreign influence operations are an important area of concern but attributing computational propaganda to foreign state actors remains a challenge. Facebook and Twitter – who



have begun publishing limited information about influence operations on their platforms – have taken action against cyber troops engaged in foreign influence operations in seven countries: China, India, Iran, Pakistan, Russia, Saudi Arabia, and Venezuela. Although this measure does not capture the extent to which foreign influence operations are taking place, we can confidently begin to build a picture of this highly secretive phenomenon.

China Flexes its Misinformation Muscle

Until recently, we found that China rarely used social media to manipulate public opinion in other countries. The audience for computational propaganda has mainly focused on domestic platforms, such as Weibo, WeChat, and QQ. However, in 2019 the Chinese government began to employ global social media platforms to paint Hong Kong's democracy advocates as violent radicals with no popular appeal (Lee Myers and Mozur 2019). Beyond domestically bound platforms, the growing sophistication and use of global social networking technologies demonstrates how China is also turning to these technologies as a tool of geopolitical power and influence.

Facebook is Still Number One

Despite there being more platforms than ever, Facebook remains the dominant platform for cyber troop activity. Part of the reason for this could be explained by its market size – as one of the world's largest social networking platforms – as well as the specific affordances of the platform, such as close family and friend communication, a source of political news and information, or the ability to form groups and pages. Since 2018, we have collected evidence of more cyber troop activity on image- and video-sharing platforms such as Instagram and YouTube. We have also collected evidence of cyber troops running campaigns on WhatsApp. We think these platforms will grow in importance over the next few years as more people use these social networking technologies for political communication.

FIGURE 1 - THE GLOBAL DISINFORMATION ORDER
COUNTRIES TAKING PART IN SOCIAL MEDIA MANIPULATION



FIGURE 2 - COMPUTATIONAL PROPAGANDA AS A TOOL OF INFORMATION CONTROL
AUTHORITARIAN COUNTRIES DEPLOYING COMPUTATIONAL PROPAGANDA



FIGURE 3 - FOREIGN INFLUENCE OPERATIONS ON SOCIAL MEDIA
COUNTRIES ATTRIBUTED BY FACEBOOK AND TWITTER FOR ENGAGING IN FOREIGN INFLUENCE OPERATIONS



Source: Authors' evaluations based on data collected. **Note:** Facebook has also taken down accounts engaged in 'coordinated inauthentic behaviour' that are not explicitly linked to a government or political party. These takedowns include accounts originating from: Egypt, Macedonia, Kosovo, Thailand, and the United Arab Emirates. Additionally, some cyber troop activity identified by Facebook and Twitter is domestically focused, such as in the case of Bangladesh and Honduras, and is therefore not included in this figure on foreign operations.

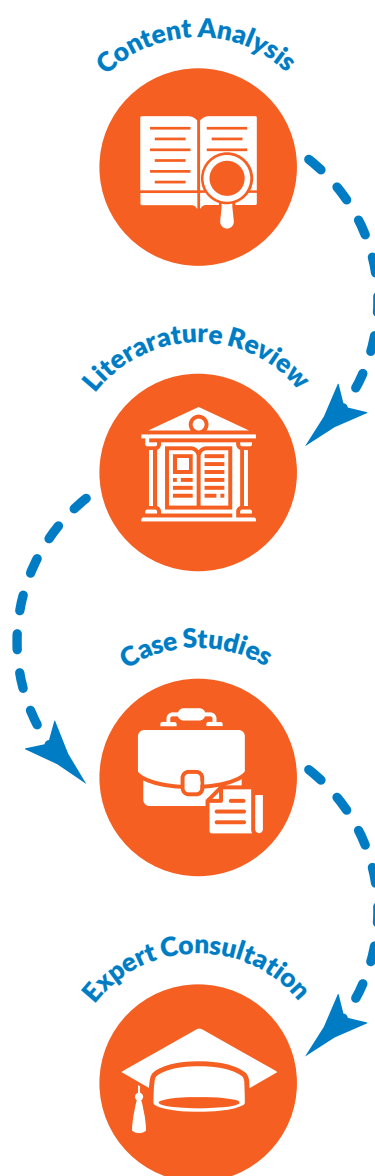
FIGURE 4 - PROMINENT PLATFORMS FOR SOCIAL MEDIA MANIPULATION
SOCIAL MEDIA PLATFORMS USED FOR CYBER TROOP ACTIVITY



Report Methodology

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.



For the past three years, our three-stage methodology has allowed us to successfully capture a wide range of public documents that shed light on the organized manipulation campaigns globally. There are almost certainly cyber troop operations that have not been publicly documented, and we have already seen these cases grow over time. 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 country-specific profiles and a full list of news items and secondary literature sources can be found on the 2019 report homepage.

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, and Joyce 2013; Joyce, Antonio, and 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; Cambridge Analytica; disinformation; Facebook; fake account; information warfare; Instagram; military; misinformation; propaganda; psychological operations; psyops; social media; sock puppet; troll; Twitter; WhatsApp; YouTube.

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, English, French, German, Greek, Hungarian, Italian,

Persian, Polish, Portuguese, 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 Bosnia, Croatia, Georgia, Kazakhstan, Kyrgyzstan, Malaysia, North Macedonia, Taiwan, Tajikistan, Turkmenistan, Uzbekistan. We relied on English-language-only reporting for: Armenia, Azerbaijan, Cambodia, China, Czech Republic, Eritrea, Ethiopia, Hungary, Israel, Moldova, Myanmar, Netherlands, North Korea, Pakistan, Philippines, Serbia, South Korea, Sri Lanka, Thailand, Turkey, and Vietnam.

After conducting a content analysis, a team of research assistants completed a **secondary literature review** to provide an in-depth profile of cyber troop activity in a specific country context. These case studies drew from the data collected in the content analysis, as well as an in-depth secondary literature review, 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 an online Zotero database. We hope this public library will help inform future research.

After completing a qualitative content analysis and secondary literature review, research assistants synthesized the findings into short **country case studies**. The 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. In addition to the content analysis and secondary literature review, we completed a case study for 84% of the countries, which can be online in a data supplement alongside the report.

Finally, 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. In the cases of Poland, Sri Lanka, Taiwan, Tunisia, and Ukraine, we consulted experts on the data collected from the content analysis and literature review.

¹ <https://monitoring.bbc.co.uk/>

Organisational 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 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. In 44 countries, we found evidence of a government agency using computational propaganda to shape public attitudes. This category of actors includes communication or digital ministries or military-led campaigns. In countries considered ‘not free’ according to Freedom House, we found evidence of a government ministry or ruling party using computational propaganda to shape attitudes domestically. In a small number of democracies, we found evidence of government or military-led initiatives. For this report, we counted the activities of the Joint Threat Research Intelligence Group (JTRIG) in the United Kingdom, who set up Facebook groups and created YouTube videos containing persuasive communications designed to “discredit, promote distrust, dissuade, deter, delay [and] disrupt” (Greenwald 2015). We also counted activities in the United States, such as the United States Agency for International Development (USAID) programme that created a fake social network in Cuba (Greenwald 2014). As computational propaganda becomes an increasingly ubiquitous tool for politics, national security, and intelligence operations, we hope these examples drive further

conversations around what are appropriate, democratic and acceptable uses of these tools by state actors.

In addition to government or military-led initiatives, we also looked at political parties. In 45 out of the 70 countries we analysed, we found evidence of political parties or politicians running for office who have used the tools and techniques of computational propaganda during elections. Here, we counted instances of politicians amassing fake followers, such as Mitt Romney in the United States (Carroll 2012), Tony Abbott in Australia (Rolfe 2013), or Geert Wilders in the Netherlands (Blood 2017). We also counted instances of parties using advertising to target voters with manipulated media, such as in India (Gleicher 2019), or instances of illegal micro-targeting such as the use of the firm Cambridge Analytica in the UK Brexit referendum by Vote Leave (Cadwalladr 2017). Finally, we further counted instances of political parties purposively spreading or amplifying disinformation on social networks, such as the WhatsApp campaigns in Brazil (Rio 2018), India (Dwoskin and Gowen 2018), and Nigeria (Hitchen et al. 2019).

One important feature of the organization of manipulation campaigns is that cyber troops often work in conjunction with private industry, civil society organizations, Internet subcultures, youth groups, hacker collectives, fringe movements, social media influencers, and volunteers who ideologically support their 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, rather than campaigns that might be implicitly sanctioned because of factors such as overlapping ideologies or goals. In 25 out of the 70 countries we found evidence of state actors working with private companies or strategic communication firms who offer computational propaganda as a service. In 30 out of the 70 countries, we found evidence of formal coordination between governments and citizens or civil society organizations. In some cases, like in Azerbaijan, Israel, Russia, Tajikistan, Uzbekistan, student or youth groups are hired by government agencies to use computational propaganda.

TABLE 1 - ORGANIZATIONAL FORM AND PREVALENCE OF SOCIAL MEDIA MANIPULATION

Country	Government Agencies	Politicians and Parties	Private Contractors	Civil Society Organisations	Citizens and Influencers
 Angola					
 Argentina					
 Armenia					
 Australia					
 Austria					
 Azerbaijan					
 Bahrain					
 Bosnia & Herzegovina					
 Brazil					
 Cambodia					
 China					
 Colombia					
 Croatia					
 Cuba					
 Czech Republic					
 Ecuador					
 Egypt					
 Eritrea					
 Ethiopia					
 Georgia					
 Germany					
 Greece					
 Guatemala					
 Honduras					
 Hungary					
 India					
 Indonesia					
 Iran					
 Israel					
 Italy					
 Kazakhstan					
 Kenya					
 Kyrgyzstan					
 Macedonia					
 Malaysia					
 Malta					
 Mexico					
 Moldova					
 Myanmar					
 Netherlands					
 Nigeria					
 North Korea					
 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					
 Zimbabwe					

Source: Authors' evaluations based on data collected. **Note:** This table reports on the types of political actors using social media influence operations, and the number of examples of those organizations found. For government agencies, political parties, civil society groups, and private contractors, ■ = one organization found, ■ = two organizations found, ■ = three or more organizations found. Since it is difficult to assess the number of individual citizens using these tools, evidence of citizen use is indicated by ■.

Strategies, Tools, and Techniques

Although there is nothing necessarily new about propaganda, the affordances of social networking technologies – algorithms, automation, and big data – change the scale, scope, and precision of how information is transmitted in the digital age.



87%
of countries used
Human accounts



80%
of countries used
Bot accounts



11%
of countries used
Cyborg accounts



7%
of countries used
Hacked or Stolen
accounts

Account Types

Fake accounts are used by cyber troops to spread computational propaganda. Over the past three years we have tracked the prevalence of three types of fake accounts: bot, human, and cyborg. Bots are highly automated accounts designed to mimic human behaviour online. They are often used to amplify narratives or drown out political dissent. We found evidence of bot accounts being used in 50 of the 70 countries. However, even more common than bots are human-run accounts, which do not make use of automation. Instead they engage in conversations by posting comments or tweets, or by private messaging individuals via social media platforms. Human-operated accounts were found in 60 out of the 70 countries in this year's report. Cyborg accounts, which blend automation with human curation, are another account type we identified.

This year, we have added hacked or stolen accounts to our typology of fake accounts. Although these accounts are not 'fake' per se, high profile accounts are strategically used by cyber troops in order to spread pro-government propaganda or to censor freedom of speech by revoking access to the account by its rightful owner. A small number of state actors have begun using stolen or hacked accounts as part of their campaigns, highlighting the interconnectivity of computational propaganda with more traditional forms of cyber-attacks.

Finally, it is important to note that not all accounts used in cyber troop activities are fake. In some countries, like Vietnam or Tajikistan, state actors encourage cyber troops to use their real accounts to spread pro-government propaganda, troll political dissidents, or mass-report content. As social media companies become more aggressive in taking down accounts associated with cyber troop activity, the co-option of real accounts could become a more prominent strategy.

TABLE 2 - FAKE ACCOUNT TYPES

Country	Bots	Human	Cyborg	Hacked or Stolen
Angola				
Argentina				
Armenia				
Australia				
Austria				
Azerbaijan				
Bahrain				
Bosnia & Herzegovina				
Brazil				
Cambodia				
China				
Colombia				
Croatia				
Cuba				
Czech Republic				
Ecuador				
Egypt				
Eritrea				
Ethiopia				
Georgia				
Germany				
Greece				
Guatemala				
Honduras				
Hungary				
India				
Indonesia				
Iran				
Israel				
Italy				
Kazakhstan				
Kenya				
Kyrgyzstan				
Macedonia				
Malaysia				
Malta				
Mexico				
Moldova				
Myanmar				
Netherlands				
Nigeria				
North Korea				
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				
Zimbabwe				

Source: Authors' evaluations based on data collected. **Note:** This table reports on the types of fake accounts identified between 2010-2019. For fake social media account types: = automated accounts, = human accounts, = cyborg accounts, = Hacked or Stolen accounts, = no evidence found.

**71%**

spread pro-government or pro-party propaganda

**89%**

use computational propaganda to attack political opposition

**34%**

spread polarising messages designed to drive divisions within society

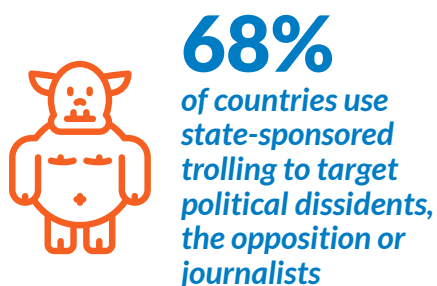
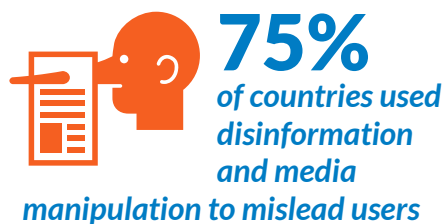
Messaging and Valence

Cyber troops use a variety of messaging and valence strategies when communicating with users online. Valence describes how attractive or unattractive a message, event, or thing is. For the 2019 report, we have expanded our typology of messaging and valence strategies that cyber troops use when engaging in conversations with users online:

- (1) spreading pro-government or pro-party propaganda;
- (2) attacking the opposition or mounting smear campaigns;
- (3) distracting or diverting conversations or criticism away from important issues;
- (4) driving division and polarization; and
- (5) suppressing participation through personal attacks or harassment.

TABLE 3 - MESSAGING AND VALENCE

Country	Support	Attack Opposition	Distracting	Driving Divisions	Suppressing
 Angola					
 Argentina					
 Armenia					
 Australia					
 Austria					
 Azerbaijan					
 Bahrain					
 Bosnia & Herzegovina					
 Brazil					
 Cambodia					
 China					
 Colombia					
 Croatia					
 Cuba					
 Czech Republic					
 Ecuador					
 Egypt					
 Eritrea					
 Ethiopia					
 Georgia					
 Germany					
 Greece					
 Guatemala					
 Honduras					
 Hungary					
 India					
 Indonesia					
 Iran					
 Israel					
 Italy					
 Kazakhstan					
 Kenya					
 Kyrgyzstan					
 Macedonia					
 Malaysia					
 Malta					
 Mexico					
 Moldova					
 Myanmar					
 Netherlands					
 Nigeria					
 North Korea					
 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					



Communication Strategies

Cyber troops use a variety of communication strategies. We have categorized these activities into four categories:

- (1) the creation of disinformation or manipulated media;
- (2) mass-reporting of content or accounts;
- (3) data-driven strategies;
- (4) trolling, doxing or harassment;
- (5) amplifying content and media online.

The creation of disinformation or manipulated media is the most common communication strategy. In 52 out of the 70 countries we examined, cyber troops actively created content such as memes, videos, fake news websites or manipulated media in order to mislead users. Sometimes, the content created by cyber troops is targeted at specific communities or segments of users. By using online and offline sources of data about users, and paying for advertisements on popular social media platforms, some cyber troops target specific communities with disinformation or manipulated media.

The use of trolling, doxing or harassment is a growing global challenge and threat to fundamental human rights. In 2018, we identified 27 countries that used state-sponsored trolls to attack political opponents or activists via social media. This year, 47 countries have used trolling as part of their digital arsenal. Cyber troops also censor speech and expression through the mass-reporting of content or accounts. Posts by activists, political dissidents or journalists often get reported by a coordinated network of cyber troop accounts in order to game the automated systems social media companies use to take down inappropriate content. Trolling and the takedown of accounts or posts can happen alongside real-world violence, which can have a deep and chilling effect on the expression of fundamental human rights.

TABLE 4 - COMMUNICATION STRATEGIES

Country	Disinfo	Mass Reporting	Data-Driven Strategies	Trolls	Amplifying Content
Angola					
Argentina					
Armenia					
Australia					
Austria					
Azerbaijan					
Bahrain					
Bosnia & Herzegovina					
Brazil					
Cambodia					
China					
Colombia					
Croatia					
Cuba					
Czech Republic					
Ecuador					
Egypt					
Eritrea					
Ethiopia					
Georgia					
Germany					
Greece					
Guatemala					
Honduras					
Hungary					
India					
Indonesia					
Iran					
Israel					
Italy					
Kazakhstan					
Kenya					
Kyrgyzstan					
Macedonia					
Malaysia					
Malta					
Mexico					
Moldova					
Myanmar					
Netherlands					
Nigeria					
North Korea					
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					
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.

Organisational Budgets, Behaviours, and Capacity

Although there is limited public information about the size and operations of cyber troop teams, we can begin to assemble a picture of how much money they budget, how they cooperate, and the kinds of organizational capacities and behaviours they assume.

Team Size and Permanency

The size and permanency of teams vary from country to country. In some countries, teams appear 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. Some teams are comprised of a handful of people who manage hundreds of fake accounts. In other countries – like China, Vietnam or Venezuela – large teams of people are hired by the state to actively shape public opinions and police speech through online channels

Budgets and Expenditures

Computational propaganda remains big business. We found large amounts of money being spent on ‘PR’ or strategic communication firms to work on campaigns in countries such as the Philippines (Mahtani and Cabato 2019), Guatemala (Currier and Mackey 2018), and Syria (York 2011). These contracts can range in size from smaller spends with boutique national or regional firms, to multi-million-dollar contracts with global companies like Cambridge Analytica (see, for example, Kazeem 2018). The rise of the troll industry is a growing area of public and academic interest, and an area to watch for future research and journalistic inquiry.

Skills and Knowledge Diffusion

There is also evidence of formal and informal knowledge diffusion happening across geographic lines. For example, during the investigations into cyber troop activity in Myanmar, evidence emerged that military officials were trained by Russian operatives on how to use social media (Mozur 2018). Similarly, cyber troops in Sri Lanka received formal training in India (Expert consultation 2019). Leaked emails also showed evidence of the Information Network Agency in Ethiopia sending staff members to receive formal training in China (Nunu 2018). While there are many gaps in how knowledge and skills in computational propaganda are diffusing globally, this is also an important area to watch for future research and journalistic inquiry. .

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 four-point scale:

(1) Minimal cyber troop teams are newly formed or teams that were previously active but whose present activities are uncertain. Newly formed teams have minimal resources and only apply a few tools of computational propaganda to a small number of platforms. Minimal cyber troop activity also includes states where we have seen only one or two politicians who experiment with computational propaganda tools. These teams operate domestically, with no operations abroad. Minimal teams include: Angola, Argentina, Armenia, Australia, Croatia, Ecuador, Greece, Netherlands, South Korea, Sweden, Taiwan and Tunisia.

(2) 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: Austria, Colombia, Czech Republic, Eritrea, Germany, Honduras, Hungary, Indonesia, Italy, Kenya, Macedonia, Moldova, Nigeria, North Korea, Poland, Rwanda, Serbia, South Africa, Spain, Zimbabwe.

(3) 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: Azerbaijan, Bahrain, Bosnia & Herzegovina, Brazil, Cambodia, Cuba, Ethiopia, Georgia, Guatemala, India, Kazakhstan, Kyrgyzstan, Malaysia, Malta, Mexico, Pakistan, Philippines, Qatar, Sri Lanka, Sudan, Tajikistan, Thailand, Turkey, Ukraine, United Kingdom, and Uzbekistan.

(4) 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. High-capacity teams include: China, Egypt, Iran, Israel, Myanmar, Russia, Saudi Arabia, Syria, United Arab Emirates, Venezuela, Vietnam, and the United States.

TABLE 5 - CYBER TROOP CAPACITY

HIGH CAPACITY			
Country	Status	Notes on Team Size, Training and Spending	
 China	Permanent	Team size estimates of 300,000-2,000,000 people working in local and regional offices	
 Egypt	Permanent	–	
 Iran	Permanent	6,000 USD spent on FB advertisements	
 Israel	Permanent	Team size estimates of 400 people. Evidence of Formal Training. Multiple contracts valued at 778K USD and 100M USD.	
 Myanmar	Permanent	Evidence of Formal Training in Russia	
 Russia	Permanent	–	
 Saudi Arabia	Permanent	Estimated costs of 150 Pounds for Twitter Hashtag Trends	
 Syria	Permanent	Multiple Contracts valued at 4,000 USD	
 United Arab Emirates	Permanent	Multiple Expenditures valued at over 10M USD	
 United States	Permanent & Temporary	–	
 Venezuela	Permanent	Team size estimates of multiple brigades of 500 people. Evidence of Formal Training	
 Vietnam	Permanent & Temporary	Team size estimates of 10,000 people	

TABLE 5 - CYBER TROOP CAPACITY continued

MEDIUM CAPACITY		
Country	Status	Notes on Team Size, Training and Spending
 Azerbaijan	Permanent	–
 Bahrain	Permanent	Multiple contracts with estimates valued at 32M USD
 Bosnia & Herzegovina	Temporary	–
 Brazil	Temporary	Multiple contracts valued at 10M R, 130K R, 24K R, 12M R
 Cambodia	Permanent & Temporary	–
 Cuba	Permanent	–
 Ethiopia	Permanent	Evidence of Training in China. Estimated salaries of 300 USD/mont
 Georgia	Temporary	–
 Guatemala	Permanent	Multiple contracts valued at 100,000 USD
 India	Temporary	Multiple teams ranging in size from 50-300 people. Multiple contracts and advertising expenditures valued at over 1.4M USD
 Kazakhstan	Temporary	–
 Kyrgyzstan	Permanent & Temporary	Team size estimates of 50 people. Multiple contracts valued at 2000 USD. Salaries are estimated to be 3-4 USD/day
 Malaysia	Permanent	Staff estimates between 50-2000 people. Evidence of formal training found
 Malta	Permanent	–
 Mexico	Temporary	–
 Pakistan	Permanent	–
 Philippines	Permanent	300-500
 Qatar	Temporary	–
 Sri Lanka	Permanent & Temporary	Evidence of Formal Training in India
 Sudan	Permanent	–
 Tajikistan	Permanent	Team size estimates of 400 people
 Thailand	Permanent	Evidence of Formal Training
 Turkey	Permanent	Team size estimates of 500 people
 Ukraine	Permanent	Team size estimates of 20,000 people
 United Kingdom	Temporary	3.5M GBP spent on Cambridge Analytica by Leave Campaigns
 Uzbekistan	Permanent	–

TABLE 5 - CYBER TROOP CAPACITY continued

LOW CAPACITY			
Country	Status	Notes on Team Size, Training and Spending	
 Austria	Temporary	–	
 Colombia	Temporary	–	
 Czech Republic	Temporary	–	
 Eritrea	Permanent	–	
 Germany	Temporary	–	
 Honduras	Temporary	–	
 Hungary	Temporary	–	
 Indonesia	Temporary	Multiple contracts valued between 1M-50M Rupias	
 Italy	Temporary	–	
 Kenya	Temporary	One contract with Cambridge Analytica valued at 6M USD	
 Macedonia	Temporary	–	
 Moldova	Temporary	20,000USD spent on Facebook and Instagram Ads	
 Nigeria	Temporary	One contract with Cambridge Analytica Valued at 2.8M USD	
 North Korea	Permanent	Team size estimates of 200 people	
 Poland	Temporary	–	
 Rwanda	Temporary	–	
 Serbia	Permanent	Salary Estimates valued at 370 EURO/month	
 South Africa	Temporary	Multiple contracts valued at 2M USD	
 Spain	Temporary	–	
 Zimbabwe	Temporary	–	

MINIMAL CAPACITY			
Country	Status	Notes on Team Size, Training and Spending	
 Angola	Temporary	–	
 Argentina	Temporary	30-40 Staff. Multiple Contracts valued at 14M Pesos, 11M Pesos in 2015. 200M Pesos in 2017	
 Armenia	Temporary	–	
 Australia	Temporary	–	
 Croatia	Temporary	–	
 Ecuador	No Longer Active	Multiple contracts valued at 200,000 USD	
 Greece	Temporary	–	
 Netherlands	Temporary	–	
 South Korea	No Longer Active	Previously active team of less than 20 people	
 Sweden	Temporary	–	
 Taiwan	No Longer Active	–	
 Tunisia	Temporary	–	

Source: Authors' evaluations based on data collected. **Note:** These tables reports on the capacity of cyber troop actors.

Conclusion

Social media, which was once heralded as a force for freedom and democracy, has come under increasing scrutiny for its role in amplifying disinformation, inciting violence, and lowering levels of trust in media and democratic institutions.

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 freedom of speech and freedom of the press. While the affordances of social media can serve to enhance the scale, scope, and precision of disinformation (Bradshaw and Howard 2018b), it is important to recognize that many of the issues at the heart of computational propaganda – polarization, distrust or the decline of democracy – have existed long before 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.

Computational propaganda has become a normal part of the digital public sphere. 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 since computational propaganda is a symptom of long-standing challenges to democracy, it is important that solutions take into consideration these systemic challenges. However, it must also consider the role social media platforms have played in shaping the current information environment. A strong democracy requires access to high-quality information and an ability for citizens to come together to debate, discuss, deliberate, empathize, and make concessions. Are social media platforms really creating a space for public deliberation and democracy? Or are they amplifying content that keeps citizens addicted, disinformed, and angry?

References

- Blood, David. 2017. **Is Social Media Empowering Dutch Populism?** *The Financial Times*. <https://www.ft.com/content/b1830ac2-07f4-11e7-97d1-5e720a26771b>.
- Bradshaw, Samantha, and Philip N. Howard. 2017a. **The Global Organization of Social Media Disinformation Campaigns**. *Journal of International Affairs* 71(1.5).
- Bradshaw, Samantha, and Philip N. Howard. 2017b. **Troops, Trolls, and Troublemakers: A Global Inventory of Organized Social Media Manipulation**. Oxford: Oxford Internet Institute. Working Paper.
- . 2018a. **Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation**. COMRPOP Working Paper Series 2018(1): 26.
- Bradshaw, Samantha, and Philip N. Howard. 2018b. **Why Does Junk News Spread So Quickly Across Social Media? Algorithms, Advertising and Exposure in Public Life**. Knight Foundation Working Paper. https://kf-site-production.s3.amazonaws.com/media_elements/files/000/000/142/original/Topos_KF_White-Paper_Howard_V1_ado.pdf.
- Cadwalladr, Carole. 2017. **The Great British Brexit Robbery: How Our Democracy Was Hijacked**. *The Guardian*. <http://www.theguardian.com/technology/2017/may/07/the-great-british-brexite-robbery-hijacked-democracy>.
- Carroll, Rory. 2012. **Fake Twitter Accounts May Be Driving up Mitt Romney's Follower Number**. *The Guardian*. <https://www.theguardian.com/world/2012/aug/09/fake-twitter-accounts-mitt-romney>.
- Currier, Cora, and Danielle Mackey. 2018. **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/> (August 5, 2019).
- Dwoskin, Elizabeth, and Annie Gowen. 2018. **On WhatsApp, Fake News Is Fast — and Can Be Fatal**. *Washington Post*. https://www.washingtonpost.com/business/economy/on-whatsapp-fake-news-is-fast-and-can-be-fatal/2018/07/23/a2dd7112-8ebf-11e8-bcd5-9d911c784c38_story.html (September 3, 2019).
- 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).
- Gleicher, Nathaniel. 2019. **Removing Coordinated Inauthentic Behavior and Spam From India and Pakistan**. <https://newsroom.fb.com/news/2019/04/cib-and-spam-from-india-pakistan/>.
- Greenwald, Glenn. 2014. **The 'Cuban Twitter' Scam Is a Drop in the Internet Propaganda Bucket**. *The Intercept*. <https://theintercept.com/2014/04/04/cuban-twitter-scam-social-media-tool-disseminating-government-propaganda/> (April 10, 2017).
- . 2015. **Controversial GCHQ Unit Engaged in Domestic Law Enforcement, Online Propaganda, Psychology Research**. *The Intercept*. <https://theintercept.com/2015/06/22/controversial-gchq-unit-domestic-law-enforcement-propaganda/> (April 10, 2017).
- 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).
- Hitchen, Jamie, Jonathan Fisher, Nic Cheeseman, and Idayat Hassan. 2019. **How WhatsApp Influenced Nigeria's Recent Election — and What It Taught Us about 'Fake News'**. *Washington Post*. <https://www.washingtonpost.com/news/monkey-cage/wp/2019/02/15/its-nigerias-first-whatsapp-election-heres-what-were-learning-about-how-fake-news-spreads/> (September 3, 2019).
- 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>.
- Kazeem, Yomi. 2018. **Cambridge Analytica Tried to Sway Nigeria's Last Elections with Buhari's Hacked Emails**. *Quartz*. <https://qz.com/1234916/cambridge-analytica-tried-to-sway-nigerias-last-elections-with-buharis-hacked-emails/>.
- Lee Myers, Steven, and Paul Mozur. 2019. **China Is Waging a Disinformation War Against Hong Kong Protesters**. *New York Times*. <https://www.nytimes.com/2019/08/13/world/asia/hong-kong-protests-china.html> (September 3, 2019).
- Mahtani, Shibani, and Regine Cabato. 2019. **Why Crafty Internet Trolls in the Philippines May Be Coming to a Website near You**. *Washington Post*. 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 (September 4, 2019).
- Mozur, Paul. 2018. **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> (July 24, 2019).
- Nunu. 2018. **Leaked Documents Show That Ethiopia's Ruling Elites Are Hiring Social Media Trolls (And Watching Porn)**. *Global Voices*. <https://globalvoices.org/2018/01/20/leaked-documents-show-that-ethiopias-ruling-elites-are-hiring-social-media-trolls-and-watching-porn/> (July 24, 2019).
- Rio, I. T. S. 2018. **Computational Power: Automated Use of WhatsApp in the Elections**. *ITS FEED*. <https://feed.itsrio.org/computational-power-automated-use-of-whatsapp-in-the-elections-59f62b857033> (March 2, 2019).
- Rolfe, John. 2013. **Fake Twitter Followers for Tony Abbott Being Investigated by Liberal Party**. *Perth Now*. <https://www.perthnow.com.au/politics/federal-politics/fake-twitter-followers-for-tony-abbott-being-investigated-by-liberal-party-ng-90b331e9e3ca2542ec9cbdf6d994f986>.
- 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).
- York, Jillian C. 2011. **Syria's Twitter Spambots**. *The Guardian*. <https://www.theguardian.com/commentisfree/2011/apr/21/syria-twitter-spambots-pro-revolution> (April 10, 2017).

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 Hewlette Foundation, Luminate and the Adessium Foundation. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the funders, the Oxford Internet Institute, or University of Oxford.

For their assistance and advice on this research, we are grateful to Ualan Campbell-Smith, Amelie Henle, Caio Machado, and Cailean Osborne for collecting the preliminary data and drafting country profiles about social media manipulation for the countries outlined in this report. We are also extremely grateful to Akin Unver, Alberto Lalama, Alexi Abrahams, Angelina Huyun, Arzu Geybulla, Ben Nimmo, Bence Kollanyi, Chris Roper, Darko Brkan, Didac Fabregas-Badosa, Gabby Lim, Ingrid Grodnig, Iva Nenedic, Lisa-Maria Neudert, Marc Owen Jones, Martin Becerra, Mimie Liotsiou, Monika Kaminska, Nahema Marchal, Nick Monaco, Niki Cheong, Olivier Milland, Philip Di Salvo, Ralph Schroeder, Rosemary Ajayi, Sabine Niederer, Sanjana Hattotuwa, Vidya Narayanan, Tamar Kintsurashvili, and Tom Sear, 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 is a leading expert on technology and democracy. Her dissertation research examines the producers and drivers of disinformation, and how technology—artificial intelligence, automation and big data analytics—enhance and constrain the spread of disinformation online. At the forefront of theoretical and methodological approaches for studying, analysing and explicating the complex relationship between social media and democracy, Samantha’s research has helped advance academic debate, public understanding and policy discussions around the impact of technology on political expression and privacy. Samantha is completing her PhD at the Oxford Internet Institute, University of Oxford and is a Researcher on the Computational Propaganda Project. Samantha tweets from @sbradshaww.

Philip N. Howard is a professor and writer. He teaches at the University of Oxford, directs the Oxford Internet Institute, and is a statutory Professor at Balliol College. He writes about information politics and international affairs, and he is the author of eight books, including *The Managed Citizen*, *Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up*, and most recently *Computational Propaganda*. 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 2018 and the National Democratic Institute awarded him their ‘Democracy Prize’ for pioneering the social science of fake news. His next book, *Lie Machines: How to Save Democracy from Troll Armies, Deceitful Robots, Junk News Operations and Political Operatives* is forthcoming from Yale University Press in early 2020. He blogs at www.philhoward.org and tweets from @pnhoward.

