Working paper no. 2017.12

Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation

Samantha Bradshaw, ***University of Oxford***
Philip N. Howard, ***University of Oxford***

Contents

Executive summary

Cyber troops are government, military or political party teams committed to manipulating public opinion over social media. In this working paper, we report on specific organizations created, often with public money, to help define and manage what is in the best interest of the public. We compare such organizations across 28 countries, and inventory them according to the kinds of messages, valences and communication strategies used. We catalogue their organizational forms and evaluate their capacities in terms of budgets and staffing. This working paper summarizes the findings of the first comprehensive inventory of the major organizations behind social media manipulation.

We find that cyber troops are a pervasive and global phenomenon. Many different countries employ significant numbers of people and resources to manage and manipulate public opinion online, sometimes targeting domestic audiences and sometimes targeting foreign publics.

- The earliest reports of organized social media manipulation emerged in 2010, and by 2017 there are details on such organizations in 28 countries.
- Looking across the 28 countries, every authoritarian regime has social media campaigns targeting their own populations, while only a few of them target foreign publics. In contrast, almost every democracy in this sample has organized social media campaigns that target foreign publics, while political-party-supported campaigns target domestic voters.
- Authoritarian regimes are not the only or even the best at organized social media manipulation. The earliest reports of government involvement in nudging public opinion involve democracies, and new innovations in political communication technologies often come from political parties and arise during high-profile elections.
- Over time, the primary mode for organizing cyber troops has gone from involving military units that experiment with manipulating public opinion over social media networks to strategic communication firms that take contracts from governments for social media campaigns.

Social media and democracy

Social media has become a valuable platform for public life. It is the primary medium over which young people, around the world, develop their political identities and consume news. However, social media platforms—like Facebook and Twitter—have also become tools for social control. Many governments now spend significant resources and employ large numbers of people to generate content, direct opinion and engage with both foreign and domestic audiences. This working paper lays the groundwork for understanding the global trends in the organized and coordinated use of social media for manipulating public opinion.

In this paper we define cyber troops as government, military or political-party teams committed to manipulating public opinion over social media. Given that little is known about the differences in capacity, tools and techniques of these practices in different countries, we conducted a cross-national and comparative study of global cyber troops. Examining social media operations in 25 countries, we have undertaken an inventory of budget expenditures, staffing, organizational behavior and communication strategies to analyses the size, scale and extent to which different kinds of political regimes deploy cyber troops to influence and manipulate the public online.

In January 2015, the British Army announced that its 77th Brigade would "focus on non-lethal psychological operations using social networks like Facebook and Twitter to fight enemies by gaining control of the narrative in the information age" (Solon, 2015). The primary task of this unit is to shape public behavior through the use of "dynamic narratives" to combat the political propaganda disseminated by terrorist organizations. The United Kingdom is not alone in allocating troops and funding for influencing online political discourse. Instead, this is part of a larger phenomenon whereby governments are turning to Internet platforms to exert influence over information flows and communication channels to shape public opinion. We compare and summarize this phenomenon in the following 28 countries: Argentina, Azerbaijan, Australia, Bahrain, Brazil, China, the Czech Republic, Ecuador, Germany, India, Iran, Israel, Mexico, North Korea, the Philippines, Poland, Russia, Saudi Arabia, Serbia, South Korea, Syria, Taiwan, Turkey, Ukraine, the United Kingdom, the United States, Venezuela and Vietnam.

In terms of scope, there are several things we do not investigate. First, although cyber troops will often apply traditional offensive cyber tactics, such as hacking or surveillance, to target users for trolling or harassment campaigns, this is not a working paper about hackers or other cybersecurity professionals who work in a governmental capacity. An important distinction between cyber troops and other state-based actors operating in cyberspace is their role in actively shaping public opinion. Second, there are many countries that have no domestic organizations for social media manipulation, but participate in multilateral mutual defense pacts with programs for doing so. For example, NATO has an accredited international military

organization called the NATO Strategic Communication Center of Excellence with a list of sponsoring nations, not all of which are in the inventory we present here. Informal civil society organizations that use social media in a coordinated way are not included in this analytical frame, nor are private firms and industrial associations with organized campaigns to manipulate public opinion.

Methodology

We conducted the research for this working paper in three stages. First, we conducted a systematic content analysis of news media articles. Second, we supplemented the content analysis with other sources from think tanks, government agencies, civil society groups, universities and other sources of credible research. Finally, we consulted with country experts to check facts, find additional sources in multiple languages and assist in evaluating the quality of sources. This methodology allowed us to purposefully select the cases for comparison, draw widely from existing research and engage with country and region experts for points of clarification.

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 (Strange et al., 2013; Joyce et al., 2013; Edwards, 2013; Woolley, 2016). 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 analysis after Joyce et al. (2013), Edwards et al. (2013) and Woolley (2016), who conducted a qualitative content analysis using purposive sampling to build a coded spreadsheet of specific variables that appear in news articles. Our coded spreadsheet includes fields such as the size of the government teams, their organizational structure and place within government, strategies and tools, skills and training, and capacity and resources. We purposively selected the following keywords and used them in combination for our search: astroturf*; bot; Facebook; fake; fake account; government; information warfare; intelligent agent; military; persona management; pro-government; propaganda; psychological operations; psyops; social media; sock puppet*; troll*; Twitter.

Media bias is a significant concern when conducting a content analysis that uses purposive sampling (Earl, 2004; Joyce et al., 2013). To mitigate any biases in the preliminary content analysis, we used LexisNexis and the top three search engine providers—Google, Yahoo! and Bing—which provided hits to a variety of professional and amateur news sources. A total of 104 news stories were identified. We then ranked the articles based on their credibility using a similar ranking system to the one employed by Joyce et al. (2013) and Woolley (2016). The articles were scored on a three-point scale, with three being the most credible and one being the least

credible. Articles ranked at three came from major, professionally branded news organizations, including: *ABC News, BBC News, Reuters, The Economist, The Guardian, The Independent, The Mirror, The New York Times, The Telegraph, The Wall Street Journal, The Washington Post and Wired Magazine*. Articles ranked at two came from smaller professional news organizations, or commentary-oriented websites or expert blogs. These included websites such as: *Al-Monitor, Buzzfeed, Freedom House, Human Rights Watch, Medium, The New Republic, The New Statesman, The Observer, Quartz, The Register, The Atlantic, The Daily Dot, The Hill, The Intercept*, and *The Verge.* Articles ranked at one came from content farms, social media posts or personal or hyper-partisan blogs. These articles were removed from the sample.

A total of 83 news articles made up the final sample, and from these we were able to extract several different kinds of variables. More importantly, we defined three domains of comparative analysis that allowed us to set individual country programs into a global context: (1) strategies, tools and techniques of social media manipulation; (2) organizational form; and (3) organizational budget, behavior and capacity.

Assembling the existing corpus of public news reporting on the use of cyber troops around the world allowed us to establish cases of organized social media manipulation in 23 countries. We then moved to the corpus of more specialized working papers that have come out of think tanks, government agencies, civil society groups, universities and other sources of credible research. These reports yielded additional details on the known country comparison set, and provided additional evidence on cyber troop organization in two additional countries.

One limitation to our methodology was that we only accessed news media articles and think tank reports in the English language. In order to address this limitation, we made additional queries with cybersecurity experts or people familiar with the political system in particular countries where needed. This final stage of consultation involved double-checking news reports, rather than adding new information off the record. We did not include any additional observations by country experts that could not be verified in publication elsewhere.

We undertook additional research on additional countries where there is known trolling and automated political communication activity. If we found evidence of suspicious activity, but were unable to trace clear signs of organization behind the political communication campaign, the cases were dropped from the analysis. In other words, in this analysis we focus exclusively on organized social media campaigns that have the clear support of political parties and governments. Readers interested in those other countries where there is evidence of largely unorganized attempts at social media manipulation should consult some of our project's country-specific reports, for example on Canada (McKelvey and Dubois 2017).

Finally, there are almost certainly cyber troop operations that have not been publicly documented, and it is likely that the case list will grow over time. But for the moment it is safe to conclude that there are significant social media manipulation programs in the 28 countries we analyze here. There are similarities on the relative strategies and organizational behavior of these cyber troops.

I. Strategies, tools and techniques for social media manipulation

Cyber troops use a variety of strategies, tools and techniques for social media manipulation. Generally speaking, teams have an overarching communications strategy that involves creating official government applications, websites or platforms for disseminating content; using accounts—either real, fake or automated—to interact with users on social media; or creating substantive content such as images, videos or blog posts. Teams also differ in the valence of their messages and interactions with users online. Valence is a term that is used to define the attractiveness (goodness) or averseness (badness) of a message, event or thing. Some teams use pro-government, positive or nationalistic language when engaging with the public online. Other teams will harass, troll or threaten users who express dissenting positions. The following section outlines in more detail the strategies, tools and techniques used for social media manipulation, and Table 1 summarizes the points of comparison across the country cases.

Commenting on social media posts

Cyber troops in almost every country in our sample actively engage with users by commenting on posts that are shared on social media platforms. The valence of these engagements differs across our sample. Some cyber troops focus on positive messages that reinforce or support the government's position or political ideology. Israel, for example, has a strict policy of engaging in positive interactions with individuals who hold positions that are critical the government (Stern-Hoffman, 2013). Negative interactions involve verbal abuse, harassment and so-called "trolling" against social media users who express criticism of the government. In many countries, cyber troops engage in these negative interactions with political dissidents. In connection with the government, Azerbaijan's IRELI Youth have been known to post abusive comments on social media (Geybulla, 2016). And in Mexico, journalists are frequently targeted and harassed over social media by government-sponsored cyber troops (O'Carrol, 2017).

However, the valence of comments is not always clearly positive or negative. Instead, some cyber troops will post neutral comments, designed to distract or divert attention from the issue being discussed. Saudi Arabia, for example, engages in "hashtag poisoning", where cyber troops spam trending hashtags to disrupt criticism or other unwanted conversations through a flood of unrelated tweets (Freedom House, 2013). Other countries, such as the Czech Republic, post comments that are neither positive nor negative, but rather fact-check information (Faiola, 2017). For the most part, the valence of commenting strategies does not occur in isolation: cyber troops will often use a mix of positive, negative and neutral posts when engaging with users on social media. This is best articulated by a member of the so-called "50 Cent Party", so-called because of a rumor that government-sponsored Internet commentators were paid 50 cents every time they posted messages online. The informant noted that a common strategy is to post emotive comments online in order to generate directed citizen rage towards the

commentator; thereby diverting criticism away from the government or political issue originally being discussed (Weiwei, 2012).

Individual targeting

Individual targeting is a cyber troop strategy that involves selecting an individual or group to influence on social media. In Poland, for example, opinion leaders, including prominent bloggers, journalists and activists, are carefully selected and targeted with messages in order to convince them that their followers hold certain beliefs and values (Gorwa 2017). Other, more popular forms of individual targeting involve harassment. Harassment generally involves verbal abuse, hate speech, discrimination and/or trolling against the values, beliefs or identity of a user or a group of users online. Individual targeting is different from negative valence posts on social media, as the harassment usually spans a long duration. Sometimes, the harassment takes place during important political events, such as elections. For example, in South Korea, employees from the National Intelligence Service launched a series of smear campaigns against South Korean opposition parties in the lead up to the 2012 presidential election (The Korean Herald, 2013). More often, individual targeting is a persistent aspect of the Internet ecosystem that is used to silence political dissent online. It is also one of the most dangerous forms of cyber troop activity, as individuals often receive real-life threats and suffer reputational damage. In Russia, cyber troops have been known to target journalists and political dissidents.

Following an investigation into a rising number of abusive pro-Russian posts on the Internet, Finnish Journalist Jessica Aro received a series of "abusive emails, was vilified as a drug dealer on social media, and mocked as a delusional bimbo in a music video posted to YouTube" (Higgins, 2016). In Azerbaijan, individuals are frequently targeted on Twitter and other social media platforms if they criticize the government (Geybulla, 2016). The trolling activities of Azerbaijan's IRELI Youth have even been shown to dissuade regular Internet users from supporting political protest and engaging in political discussions online (Pearce & Kendzior, 2012). Some cyber troop teams have a highly coordinated system for identifying and targeting individuals. In Turkey, ringleaders will post a screenshot of an oppositional account so that others can launch a smear campaign against that individual (Sozeri, 2015). In Ecuador, individual targeting is coordinated through the government using the web-based platform Somos + (Morla, 2015a). And in Russia, leaders of the Kremlin-aligned Nashi Youth Movement have sent around a list of human rights activists, declaring them "the most vile of enemies" (Elder, 2012).

Government-sponsored accounts, web pages or applications

Some countries run their own government-sponsored accounts, websites and applications designed to spread political propaganda. These accounts and the content that comes out of them are clearly marked as government operated. In the United Kingdom, for example, the 77th

Brigade maintains a small presence on Facebook and Twitter under its own name (Corfield, 2017). Other countries are much more active in an official capacity. Israel has more than 350 official government social media accounts, covering the full range of online platforms, from Twitter to Instagram, and operating in three languages: Hebrew, Arabic and English (Benedictus, 2016).

But it is not just social media platforms where cyber troops are active. In addition, there are a wide range of online platforms and applications that governments make use of to spread political propaganda or silence political dissent, including blogs, mobile applications and official government web pages. Sometimes these online resources help volunteers or other citizens retweet, share and like government-sponsored content. Ukraine's i-Army, also known as "the army of truth", operates a website where citizens and volunteers can access and share "truthful" information on social media (Benedictus, 2016). In other cases, government-sponsored online resources can be used to galvanize pro-government supporters. In Ecuador, the government launched a website called Somos + to investigate and respond to social media users who criticize the government. The website sends updates to subscribers when a social media user criticizes the government, allowing pro-government supporters to collectively target political dissidents (Morla, 2015a).

Fake accounts and computational propaganda

In addition to official government accounts, many cyber troop teams run fake accounts to mask their identity and interests. This phenomenon has sometimes been referred to as "astroturfing", whereby the identity of a sponsor or organization is made to appear as grassroots activism (Howard, 2003). In many cases, these fake accounts are "bots"—or bits of code designed to interact with and mimic human users. According to media reports, bots have been deployed by government actors in Argentina (Rueda, 2012), Azerbaijan (Geybulla, 2016), Iran (BBC News, 2016), Mexico (O'Carrol, 2017), the Philippines (Williams S, 2017), Russia (Duncan, 2016), Saudi Arabia (Freedom House, 2013), South Korea (Sang-Hun, 2013), Syria (York, 2011), Turkey (Shearlaw, 2016) and Venezuela (VOA News, 2015). These bots are often used to flood social media networks with spam and fake news. They can also amplify marginal voices and ideas by inflating the number of likes, shares and retweets they receive, creating an artificial sense of popularity, momentum or relevance. Not all governments make use of this form of automation.

In Serbia, for example, a handful of dedicated employees run fake accounts to bring attention to the government's agenda (Rujevic, 2017). Similarly, in Vietnam, pro-government bloggers are responsible for spreading the party line (Pham, 2013). Some commentators have suggested that the use of human-run accounts could be due to a lack of technical sophistication (Rujevic, 2017). But as bots become increasingly political, social media platforms have become stricter in their

take-down policies. As a result, many people have gone back to operating the accounts themselves, rather than automating them. For example, in Mexico, when many of the government-sponsored spam-bots that were used to target journalists and spread disinformation on social media were blocked, human agents went back to operating the accounts themselves (O'Carrol, 2017). Increasingly, cyber troops are using a blend of automation and human interaction. These so-called "cyborgs" are deployed to help avoid detection and make interactions feel more genuine. Finally, it is important to note that not all cyber troops use "fake accounts". North Korea is an interesting case, where stolen South Korean accounts—as opposed to fake identities—are used to spread political propaganda (Benedictus, 2016).

Content creation

Some cyber troop teams create substantive content to spread political messages. This content creation amounts to more than just a comment on a blog or social media feed, but instead includes the creation of content such as blog posts, YouTube videos, fake news stories, pictures or memes that help promote the government's political agenda. In the United Kingdom, cyber troops have been known to create and upload YouTube videos that "contain persuasive messages" under online aliases (Benedictus, 2016). Some of these "psychological operations", or psyops, have been framed as "anti-radicalization" campaigns designed to deter British Muslims from going to Syria (Williams, 2015). In Russia, some cyber troops create appealing online personas and run blogs on websites such as LiveJournal. According to Chen's (2015) story, one Russian cyber trooper ran a fortune-telling blog that provided insight into "relationships, weight loss, Feng Shui—and, occasionally, geopolitics", with the goal of "weaving propaganda seamlessly into what appeared to be the non-political musings of an everyday person".

Table 1: Strategies, tools and techniques for social media manipulation

Country	Messaging and valence		Communication strategy		
	Social media comments	Individual targeting	Fake accounts	Government websites, accounts or applications	Content creation
Argentina	+/-	Evidence found	Automated	..	..
Australia	+/-	..	Automated	..	..
Azerbaijan	+/-/n	Evidence found	Automated	..	..
Bahrain	-	Evidence Found	Automated, Human	..	..
Brazil	+/n	Evidence found	Automated, Human, Cyborg	..	Evidence found
China	+/-/n	..	Human	..	Evidence found
Czech Republic	n	..	..	..	..
Ecuador	+/-	Evidence found	Automated, Human	Evidence found	..
Germany	+/-	Evidence found	Automated	Evidence found	Evidence found
India	+/-	..	..	..	Evidence found
Iran	+/n	..	Automated	..	Evidence found
Israel	+	..	..	Evidence found	Evidence found
Mexico	+/-	Evidence found	Automated, Human, Cyborg	..	Evidence found
North Korea	+/-	..	Human	..	..
Poland	-	Evidence Found	Human	..	..
Philippines	+/-	Evidence found	Automated	..	..
Russia	+/-/n	Evidence found	Automated, Human	..	Evidence found
Saudi Arabia	+/n	..	Automated	..	..
Serbia	+/-	..	Human	..	..
South Korea	+/-	Evidence found	Automated, Human	..	..
Syria	+	Evidence found	Automated	..	..
Taiwan	+/-/n	Evidence found	Cyborg, Human	Evidence found	Evidence found
Turkey	+/-	Evidence found	Automated, Human	Evidence found	
United Kingdom		Evidence found	Human	Evidence found	Evidence found
Ukraine	+/-	..	Human	Evidence found	
United States	+/-/n	..	Automated, Human, Cyborg	..	Evidence found
Venezuela	+	..	Automated, Human	Evidence found	..
Vietnam	+	..	Human	..	Evidence found

Source: Authors' evaluations based on data collected 2010–2017.

Note: This table reports on automated and trolling political activity, even if not clearly associated with a sponsoring organization. For social media comments: + = pro-government or nationalistic comments, - = harassment, trolling or negative interactions with users, n = distracting or changing the topic of discussion, or fact-checking information. No information noted with "..".

II. Organizational forms

Cyber troops are often made up of an assortment of different actors. In some cases, governments have their own in-house teams that are employed as public servants. In other cases, talent is outsourced to private contractors or volunteers. See Table 2 for a summary of the findings reported in this section.

Government

Government-based cyber troops are public servants tasked with influencing public opinion. These individuals are directly employed by the state as civil servants, and often form a small part of a larger government administration. Within the government, cyber troops can work within a government ministry, such as in Vietnam, in Hanoi Propaganda and Education Department (Pham, 2013), or in Venezuela, in the Communication Ministry (VOA News, 2016). In the United Kingdom, cyber troops can be found across a variety of government ministries and functions, including the military (77th Brigade) and electronic communications (GCHQ) (Greenwald, 2014c; MacAskill, 2015). And in China, the public administration behind cyber troop activities is incredibly vast. There are many local offices that coordinate with their regional and national counterparts to create and disseminate a common narrative of events across the country (Weiwei, 2012). Other cyber troops are employed under the executive branch of government. For example, in Argentina and Ecuador, cyber troop activities have been linked to the office of the President (Rueda, 2012; Morla, 2015a, 2015b).

Politicians and parties

Political parties or candidates often use social media as part of a broader campaign strategy. Here we are interested in political parties or candidates that use social media to manipulate public opinion during a campaign, either by purposefully spreading fake news or disinformation, or by trolling or targeting any support for the opposition party. This is different to traditional digital campaign strategies, which have generally focused on spreading information about the party or candidate's platform, or sent advertisements out to voters.

Social media is used by political parties to manipulate the public is to use fake accounts to artificially inflate the number of followers, likes, shares or retweets a candidate receives, creating a false sense of popularity. This was a technique that the Australian Coalition party used during its campaign in 2013 (Peel, 2013). Sometimes, when political parties or candidates use social media manipulation as part of their campaign strategy, these tactics are continued when they assume power. For example, in the Philippines, many of the so-called "keyboard trolls" hired to spread propaganda for presidential candidate Duterte during the election continue to spread and amplify messages in support of his policies now he's in power (Williams, 2017).

Private contractors

In some cases, cyber troops are private contractors hired by the government. Private contractors are usually temporary, and are assigned to help with a particular mission or cause. For example, the United States government hired a public relations firm to develop a persona management tool to develop and manage fake profiles on social media (Monbiot, 2011). Of course, the boundary between a private contractor and the state is not always very clear. In Russia, the Internet Research Agency, a private company, is known to coordinate some of the Kremlin's social media campaigns (Chen, 2015; Benedictus, 2016).

Volunteers

Some cyber troops are volunteer groups that actively work to spread political messages on social media. They are not just people who believe in the message and share their ideals on social media. Instead, volunteers are individuals who actively collaborate with government partners to spread political ideology or pro-government messages. In many cases, volunteer groups are made up solely of youth advocacy organizations, such as IRELI in Azerbaijan (Geybulla, 2016) or Nashi in Russia (Elder, 2012). In Israel, the government actively works with student volunteers from Jewish organizations or other pro-Israel groups around the world (Stern-Hoffman, 2013). These cyber troops are considered "volunteers" because they are not on a formal payroll, as a public servant or private contractor would be. In many cases, however, volunteers receive other rewards for their time. For example, in Israel, the top-performing students are awarded scholarships for their work (Stern-Hoffman, 2013), and in Azerbaijan, volunteer work with IRELI is considered a stepping-stone to more senior roles in public administration (Geybulla, 2016).

Paid citizens

Some cyber troops are citizens who are actively recruited by the government and are paid or remunerated in some way for their work. They are not official government employees working in public service, nor are they employees of a company contracted to work on a social media strategy. They are also not volunteers, because they are paid for their time and efforts in supporting a cyber troop campaign. Normally, these paid citizens are recruited because they hold a prominent position in society or online. In India, for example, citizens are actively recruited by cyber troop teams in order to help propagate political ideologies and messages (Kohlil, 2013). Since these citizens are not officially affiliated with the government or a political party, their "independent voice" can be used to help disseminate messages from a seemingly neutral perspective.

Table 2: Organizational forms

Country	Government	Politicians and Parties	Civil Society	Citizens	Private Contractor	Number of Forms
Argentina	Ministry of Communication President's Office	Republican Proposal Party	..	..	..	2
Australia	..	The Coalition	..	..	..	1
Azerbaijan	..	..	IRELI, the IT Academy	..	..	1
Bahrain	National Cyber Crime Unit	..	..	..	..	1
Brazil	..	Brazilian Social Democracy Party (PSDB), Worker's Party (PT)	..	Evidence Found	Agencia Pepper / no.bot	3
China	State Internet Information Office, Ministry of Industry and Information Technology, Ministry of Public Security, Communist Party	..	..	Evidence Found	..	2
Czech Republic	Centre Against Terrorism and Hybrid Threats	..	..	..	..	1
Germany	Cyber-Kommando der Bundeswehr	Alternative for Germany (AFD)	..	..	..	2
Ecuador	Ministry of Strategic Sectors President's Office	..	..	..	Ribeney, Percera and Ximah Digital	2
India	..	Bharatiya Janata Party (BJP)	..	Evidence Found	..	2
Iran	Revolutionary Guard, Supreme Council of Cyberspace	..	..	..	..	1
Israel	Israel Defence Force Prime Minister's Office	..	Israel Under Fire	..	..	2
Mexico	..	Institutional Revolutionary Party (PRI)	..	Evidence Found	Andreas Sepulveda	3
North Korea	United Front Department and Reconnaissance General Bureau	..	..	..	..	1
Poland	..	Evidence Found		..	Evidence Found	1
Philippines	..	The Partido Demokratiko Pilipino-Lakas ng Bayan	Evidence Found	Evidence Found	Nic Gabunada	4
Russia	GRU The Kremlin	..	Nashi	Evidence Found	Internet Research Agency	4
Saudi Arabia	Ministry of Defense – The Saudi ideological Warfare Center	..	Saudi Electronic Army, Salmani Army	Evidence Found	Qorvis	4
Serbia	Prime Minister's Office	Serbian Progressive Party	..	..	..	2
South Korea	National Intelligence Service	..	..	..	..	1
Syria	Syrian Electronic Army	..	..	..	EGHNA	2
Taiwan	..	Democratic Progressive Party (DPP), Nationalist Party (KMT)	..	..	..	1
Turkey	..	Justice and Development Party (AKP)	..	Evidence Found	..	2
United Kingdom	77th Brigade, GCHQ	..	..	..	..	1
Ukraine	Information Policy Ministry	..	Evidence Found	..	..	2
United States	DARPA, US Cyber Command, US Agency for International Development, Air Force, Pentagon	Democratic Party Republican Party	Evidence Found	Evidence Found	Centcom, HB Gary	5
Venezuela	Communication Ministry	..	Evidence Found	..	..	2
Vietnam	Hanoi Propaganda and Education Department	..	..	..	..	1

Source: Authors' evaluations based on data collected 2010–2017. Note: No information noted with "..".

III. Organizational budget, behavior and capacity

Cyber troop teams differ in their budgets, behaviors and capacity. Our study has found that team sizes range from a small team of less than 20 (e.g. in the Czech Republic) to a vast network of two million individuals working to promote the party line (e.g. in China). Table 3 presents comparative data on government capacity and estimated budgets. The budget column includes the best estimate of resources and how that money is allocated. The management column describes the organizational practices of the offices tasked with social media manipulation. These categories are described in further detail below.

Budget information

Cyber troops spend various amounts of funds on their operations. The amount of publicly available information on budgets and spending is relatively limited. Nevertheless, we are able to report on a few numbers. Most of the budgetary information highlighted in this section refers to contractual amounts for one operation, as opposed to an overall annual expenditure for staffing, technical equipment or other resources required. For example, Ecuador, which contracts out cyber troop activity to private firms, spends, on average, USD200,000 per contract (Morla, 2015). EGHNA, which contracts out work for the Syrian government, notes that the usual project cost is about USD4,000 (EGHNA, 2017). In a few cases, such as in Russia, there have been suggestions that military expenditures for social media manipulation operations have been increasing over the years (Sindelar, 2014).

Organizational behavior

We have identified several organizational practices of cyber troop teams: (1) a clear hierarchy and reporting structure; (2) content review by superiors; and (3) strong coordination across agencies or team; (4) weak coordination across agencies or teams; (5) liminal teams. In some cases, teams are highly structured with clearly assigned duties and a reporting hierarchy, much like the management of a company or typical government bureaucracy. Tasks are often delegated on a daily basis. In Russia and China, for example, cyber troops are often given a list of opinions or topics that are supposed to be discussed on a daily basis. These topics usually relate to a particular political issue that is taking place (Cook, 2011; Chen, 2015). As part of the reporting structure, managers or superiors will often review the work of the team.

In Serbia, for example, cyber troops and their work are closely monitored and reviewed by managers and leaders (Rujevic, 2017). Sometimes there is more than one agency or team working on propaganda campaigns, such as in China, where propaganda offices exist at the local levels of government. Here, each of these offices focuses on local issues, but also coordinates broader messages across the country depending on the domestic political issues being discussed at the time (Weiwei, 2012; Lam, 2013). In other cases, teams are less organized, structured, supervised, and coordinated. For example, the Saudi Electronic Army and the Salmani Army

have several members conducting campaigns on social media. These teams are often less coordinated and less formal than other cyber troop teams, but nonetheless have effects on the social media environment (Hussein 2017).

Capacity building

Cyber troops will often engage in capacity-building activities. These include: (1) training staff to improve skills and abilities associated with producing and disseminating propaganda; (2) providing rewards or incentives for high-performing individuals; and (3) investing in research and development projects. When it comes to training staff, governments will offer classes, tutorials or even summer camps to help prepare cyber troops for engaging with users on social media. In Russia, English teachers are hired to teach proper grammar for when they communicate with Western audiences (Seddon, 2014). Other training measures focus on "politology", which aims to outline the Russian perspective on current events (Chen, 2015). In Azerbaijan, young people are provided with blogging and social media training to help make their microblogging websites more effective at reaching desired audiences. Reward systems are sometimes developed to encourage cyber troops to disseminate more messages. For example, in Israel, the government provides students with scholarships for their work on pro-Israel social media campaigns (Stern-Hoffman, 2013). It is important to note that training and reward programs often occur together. In North Korea, for example, young computer experts are trained by the government, and top performers are selected to join the military university (Firn, 2013). Finally, some cyber troops in some democracies are investing in research and development in areas such as "network effects" and how messages can spread and amplify across social media. For example, in the United States, in 2010, DARPA funded a USD8.9 million study to see how social media could be used to influence people's behavior by tracking how they responded to content online (Quinn and Ball, 2014).

Table 3: Organizational budget, behavior and capacity

Country	Year of earliest report	Budget information (USD)	Organizational behavior	Staff capacity	Capacity building
Argentina	2012	..	..	35–40	..
Australia	2013	..	..		..
Azerbaijan	2011	..	Clear hierarchy and reporting structure, coordination across agencies	50,000	Training is provided
Bahrain	2013	..		..	..
Brazil	2010	3m	Clear hierarchy and reporting structure, coordination across agencies, integrated with campaign and party organization	..	Extended use, beyond election day
China	2011	..	Clear hierarchy and reporting structure, coordination across agencies	2,000,000	Training is provided, reward system
Czech Republic	2017	..	Coordination across agencies	20	..
Ecuador	2014	Multiple contracts to private companies, estimated at 200,000	..	..	..
Germany	2016	..	..	<300	..
India	2013	..	..	..	..
Iran	2012	..	..	20,000	..
Israel	2013	..	..	400	Reward system
Mexico	2017	600,000	Informal, liminal teams	..	limited
North Korea	2013	..	..	200	Training is provided, reward system
Poland	2015	..	Some coordination across teams	..	Training is provided
Philippines	2016	200,000	Liminal membership, but some coordination across teams	400-500	..
Russia	2012	10m	Clear hierarchy and reporting structure, content is reviewed by superiors, coordination across agencies	400	Training is provided
Saudi Arabia	2013	..	Liminal membership, less coordinated across teams.	..	..
Serbia	2017	..	Clear hierarchy and reporting structure, coordination across agencies	..	..
South Korea	2013	..	..	<20	..
Syria	2011	4,000 per contract with EGHNA	Liminal membership	..	..
Taiwan	2010		..	..	..
Turkey	2013	Multiple programs, one valued at 209,000	Highly coordinated teams	6,000	Training is provided
United Kingdom	2014	..	..	1,500	..
Ukraine	2015	..	..	20,000	..
United States	2011	Multiple programs, valued at 2.7m, 42m and 8.9m	..	..	Invests in Research and Development
Venezuela	2015	..	..	..	..
Vietnam	2013	..	..	1,000	..

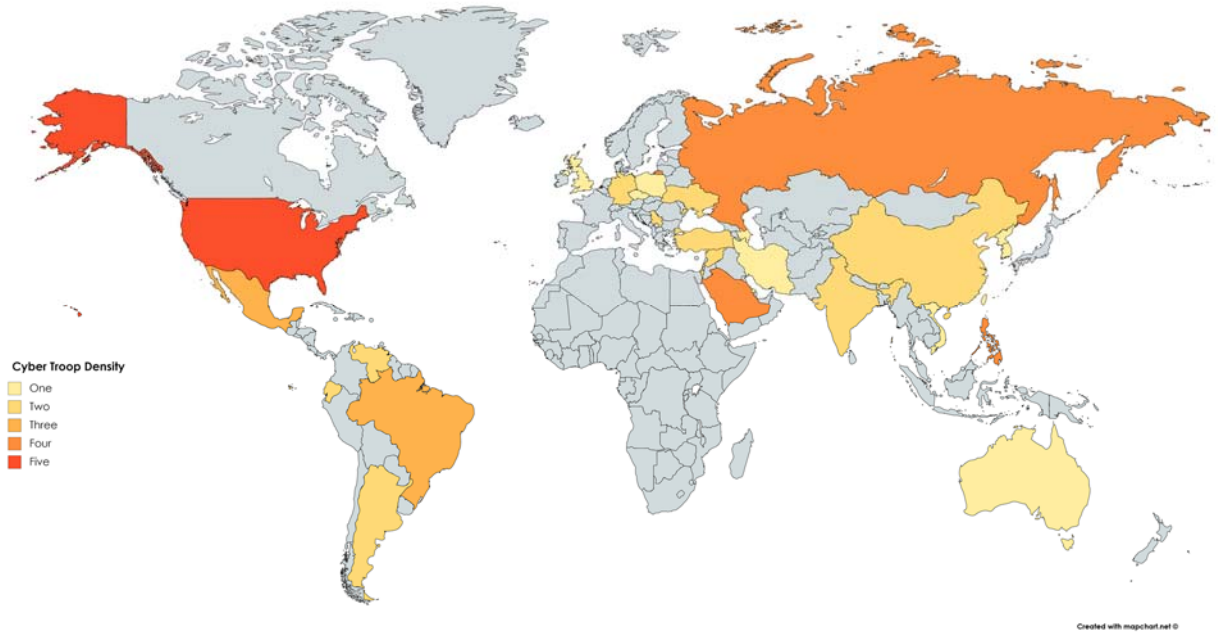
Source: Authors' evaluations based on data collected 2010–2017. Note: All currency values in USD from year of report. No information noted with "..".

Conclusion

There is no doubt that individual social media users can spread hate speech, troll other users, or set up automated political communication campaigns. Unfortunately, this is also an organized phenomenon, with major governments and political parties dedicating significant resources towards the use of social media for public opinion manipulation.

Figure 1 is a country heat map of cyber troop capacity, defined by the number of different organizational types involved. In many countries, political actors have no reported ability to field social media campaigns. In some countries, one or two known political actors occasionally use social media for political messaging, and in a few other countries there are multiple government agencies, political parties, or civil society groups organizing trolling and fake news campaigns.

Figure 1: Organizational density of cyber troops, 2017



In this figure, countries with many kinds of organizations (governments, political parties, civil society groups, organized citizens, or independent contractors) are in darker shades of red. Data is taken from the far right column of Table 2, and this figure reveals which countries have multiple kinds of actors, all using organized social media campaigns, to battle for public opinion.

Organized social media manipulation occurs in many countries around the world. In authoritarian regimes it tends to be the government that funds and coordinates propaganda campaigns on social media. In democracies, it tends to be the political parties that are the primary organizers of social media manipulation.

In many countries, cyber troops have multiple affiliations, funders, or clients. So while the primary organizers of social media manipulation may be government agencies or political parties, it is also important to distinguish those countries where many kinds of actors make use of cyber troops. No doubt the organization of cyber troops will continue to evolve. It will likely remain, however, a global phenomenon.

References

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

Baldor, L. C. (2016, February 26). US military launches campaign of cyberattacks against Islamic State. *US News & World Report*. Retrieved from https://www.usnews.com/news/politics/articles/2016-02-26/apnewsbreak-dod-launches-aggressive-cyberwar-against-is

Ball, A. (2014, July 25). No Tweets for You: Correa's Opponents Censored. *PanAm Post*. Retrieved from https://panampost.com/anneke-ball/2014/07/25/no-tweets-for-you-correas-opponents-censored/

Ball, J. (2014, July 14). GCHQ has tools to manipulate online information, leaked documents show. *The Guardian*. Retrieved from https://www.theguardian.com/uk-news/2014/jul/14/gchq-tools-manipulate-online-information-leak

BBC Trending. (2016a, March 16). Who's at the controls of Iran's bot army? *BBC News*. Retrieved from http://www.bbc.co.uk/news/blogs-trending-35778645

BBC Trending. (2016b, December 7). Trolls and triumph: a digital battle in the Philippines. *BBC News*. Retrieved from http://www.bbc.co.uk/news/blogs-trending-38173842

Bender, V. J., & Oppong, M. (2017, July 2). Frauke Petry und die Bots. *Franffurter Allgemeine*. Retrieved from http://www.faz.net/aktuell/politik/digitaler-wahlkampf-frauke-petry-und-die-bots-14863763.html

Benedictus, L. (2016, November 6). Invasion of the troll armies: from Russian Trump supporters to Turkish state stooges. *The Guardian*. Retrieved from https://www.theguardian.com/media/2016/nov/06/troll-armies-social-media-trump-russian

Bloom, A. J. (2012, February 23). DARPA And Their Robot Army Are Coming For Your "Memes." *The American Conservative*. Retrieved from http://www.theamericanconservative.com/2012/02/23/darpa-and-their-robot-army-are-coming-for-your-memes/

Brooking, E. T., & Singer, P. W. (2016, November). War Goes Viral. *The Atlantic*. Retrieved from https://www.theatlantic.com/magazine/archive/2016/11/war-goes-viral/501125/

Bugorkova, O. (2015, March 19). Ukraine conflict: Inside Russia's "Kremlin troll army." *BBC News*. Retrieved from http://www.bbc.co.uk/news/world-europe-31962644

Butler, D., Gillum, J., & Arce, A. (2014, April 4). White House defends "Cuban Twitter" to stir unrest. *Yahoo News*. Retrieved from http://news.yahoo.com/white-house-defends-cuban-twitter-stir-unrest-222510641.html

Carroll, R. (2012, August 9). Fake Twitter accounts may be driving up Mitt Romney's follower number. *The Guardian*. Retrieved from https://www.theguardian.com/world/2012/aug/09/fake-twitter-accounts-mitt-romney

Chen, A. (2015, June 2). The Agency. *The New York Times*. Retrieved from https://www.nytimes.com/2015/06/07/magazine/the-agency.html

Cook, S. (2011, October 11). China's growing army of paid internet commentators. *Freedom House*. Retrieved from https://freedomhouse.org/blog/china%E2%80%99s-growing-army-paid-internet-commentators#.VRMVvTSsUrM

Corfield, G. (2017, January 3). Army social media psyops bods struggling to attract fresh blood. *The Register*. Retrieved from https://www.theregister.co.uk/2017/01/03/77_brigade_struggling_recruit_40_pc_below_establishment/

Czech News Agency. (2017, May 22). Disinformation webs to be active before Czech elections, expert says. *Prague Monitor*. Retrieved from http://praguemonitor.com/2017/05/22/disinformation-webs-be-active-czech-elections-expert-says

Daily Sabah. (2015, May 11). AK Party founded New Turkey Digital Office for the general elections on June 7. *Daily Sabah*. Retrieved from http://www.dailysabah.com/elections/2015/05/11/ak-party-founded-new-turkey-digital-office-for-the-general-elections-on-june-7

Defense News. (2016, April 1). Germany outlines plan to create Bundeswehr cyber command. Retrieved from https://defensenews-alert.blogspot.co.il/2016/04/germany-outlines-plan-to-create.html

Duncan, J. (2016, October 16). Russia launches "troll factory" to flood internet with lies about UK. *Mail Online*. Retrieved from http://www.dailymail.co.uk/~/article-3840816/index.html

Earl, J., Martin, A., McCarthy, J. D., & Soule, S. A. (2004). The Use of Newspaper Data in the Study of Collective Action. *Annual Review of Sociology*, *30*(1), 65–80.

EGHNA. (2012). EGHNA Marketplace. Retrieved June 26, 2017, from https://www.drupal.org/eghna

Elder, M. (2012, February 7). Emails give insight into Kremlin youth group's priorities, means and concerns. *The Guardian*. Retrieved from

https://www.theguardian.com/world/2012/feb/07/nashi-emails-insight-kremlin-groups-priorities

Elliot, C. (2014, May 4). The readers' editor on… pro-Russia trolling below the line on Ukraine stories. *The Guardian*. Retrieved from https://www.theguardian.com/commentisfree/2014/may/04/pro-russia-trolls-ukraine-guardian-online

Faiola, A. (2017, January 22). As Cold War turns to Information War, a new fake news police combats disinformation. *Washington Post*. Retrieved from https://www.washingtonpost.com/world/europe/as-cold-war-turns-to-information-war-a-new-fake-news-police/2017/01/18/9bf49ff6-d80e-11e6-a0e6-d502d6751bc8_story.html

Fassihi, F. (2012, March 16). Iran's Censors Tighten Grip. *Wall Street Journal*. Retrieved from https://www.wsj.com/articles/SB10001424052702303717304577279381130395906

Fiedler, V. M. (2016, December 16). AfD stellt App für verunsicherte Bürger vor. *Der Tagesspiegel*. Retrieved from http://www.tagesspiegel.de/politik/nrw-wahlkampf-afd-stellt-app-fuer-verunsicherte-buerger-vor/14991488.html

Fielding, N., & Cobain, I. (2011, March 17). Revealed: US spy operation that manipulates social media. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks

Finley, K. (2015, August). Pro-Government Twitter Bots Try to Hush Mexican Activists. Retrieved July 14, 2017, from https://www.wired.com/2015/08/pro-government-twitter-bots-try-hush-mexican-activists/

Firn, M. (2013, August 13). North Korea builds online troll army of 3,000. *The Telegraph*. Retrieved from http://www.telegraph.co.uk/news/worldnews/asia/northkorea/10239283/North-Korea-builds-online-troll-army-of-3000.html

Freedom House. (2013). Saudi Arabia. Retrieved April 10, 2017, from https://freedomhouse.org/report/freedom-net/2013/saudi-arabia

Gallagher, P. (2015, March 27). The Orwellian "troll factories" spouting pro-Kremlin propaganda. *The Independent*. Retrieved from http://www.independent.co.uk/news/world/europe/revealed-putins-army-of-pro-kremlin-bloggers-10138893.html

Gavilan, J. (2016, June 4). Duterte's P10M social media campaign: Organic, volunteer-driven. *Rappler*. Retrieved from http://www.rappler.com/newsbreak/rich-media/134979-rodrigo-duterte-social-media-campaign-nic-gabunada

Geybulla, A. (2016, November 21). In the crosshairs of Azerbaijan's patriotic trolls. *Open Democracy*. Retrieved from https://www.opendemocracy.net/od-russia/arzu-geybulla/azerbaijan-patriotic-trolls

Glowacki, W. (2015, September 28). Prawo i Sprawiedliwość króluje w polskim internecie. Pomaga w tym zdyscyplinowana armia trolli. *Gazeta Krakowska*. Retrieved from http://www.gazetakrakowska.pl/artykul/8866523,prawo-i-sprawiedliwosc-kroluje-w-polskim-internecie-pomaga-w-tym-zdyscyplinowana-armia-trolli,3,id,t,sa.html

Gorwa, R. (2017). Computational Propaganda in Poland: False Amplifiers and the Digital Public Sphere. *Computational Propaganda Project Working Paper Series*. Retrieved from http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Comprop-Poland.pdf

Greenwald, G. (2014a, February 24). How Covert Agents Infiltrate the Internet to Manipulate, Deceive, and Destroy Reputations. *The Intercept*. Retrieved from https://theintercept.com/2014/02/24/jtrig-manipulation/

Greenwald, G. (2014b, April 4). The "Cuban Twitter" Scam Is a Drop in the Internet Propaganda Bucket. *The Intercept*. Retrieved from https://theintercept.com/2014/04/04/cuban-twitter-scam-social-media-tool-disseminating-government-propaganda/

Greenwald, G. (2014c, July 14). Hacking Online Polls and Other Ways British Spies Seek to Control the Internet. *The Intercept*. Retrieved from https://theintercept.com/2014/07/14/manipulating-online-polls-ways-british-spies-seek-control-internet/

Greenwald, G. (2015, June 22). Controversial GCHQ Unit Engaged in Domestic Law Enforcement, Online Propaganda, Psychology Research. *The Intercept*. Retrieved from https://theintercept.com/2015/06/22/controversial-gchq-unit-domestic-law-enforcement-propaganda/

Hazazi, Hussein. 2017. "150 سعودية يتسلحن في «السلماني الجيش» لصد الهجمات الإلكترونية المعادية." *Okaz*. June 14.

Herring, S. C. (2009). Web Content Analysis: Expanding the Paradigm. In J. Hunsinger, L. Klastrup, & M. Allen (Eds.), *International Handbook of Internet Research* (pp. 233–249). Springer Netherlands. Retrieved from http://link.springer.com/chapter/10.1007/978-1-4020-9789-8_14

Higgins, A. (2016, May 30). Effort to Expose Russia's "Troll Army" Draws Vicious Retaliation. *The New York Times*. Retrieved from https://www.nytimes.com/2016/05/31/world/europe/russia-finland-nato-trolls.html

Ho, Catherine. 2016. "Saudi Government Has Vast Network of PR, Lobby Firms in U.S." *Washington Post*, April 20.

https://www.washingtonpost.com/news/powerpost/wp/2016/04/20/saudi-government-has-vast-network-of-pr-lobby-firms-in-u-s/.

Howard, P. N. (2003). Digitizing the Social Contract: Producing American Political Culture in the Age of New Media. *The Communication Review*, *6*(3), 213–245. https://doi.org/10.1080/10714420390226270

Hunter, I. (2015, June 6). Turkish ruling party's social media campaigners deny being a troll. *The Independent*. Retrieved from http://www.independent.co.uk/news/world/europe/turkish-president-s-social-media-campaigners-deny-being-a-troll-army-10301599.html

Hürriyet Daily News. (2015, June 15). Erdoğan attends "Ak troll" wedding, chats with well-known suspect. *Hürriyet Daily News*. Retrieved from http://www.hurriyetdailynews.com/erdogan-attends-ak-troll-wedding-chats-with-well-known-suspect.aspx?PageID=238&NID=84013&NewsCatID=338

Jacobs, A. (2014, July 21). It's Another Perfect Day in Tibet! *The New York Times*. Retrieved from https://www.nytimes.com/2014/07/22/world/asia/trending-attractive-people-sharing-upbeat-news-about-tibet-.html

Jones, M. (2017, June 7). Hacking, bots and information wars in the Qatar spat. *Washington Post*. Retrieved from https://www.washingtonpost.com/news/monkey-cage/wp/2017/06/07/hacking-bots-and-information-wars-in-the-qatar-spat/

Jones, M. O. (2016, June 22). Around 51% of Tweets on #Bahrain Hashtag Created by Automated Sectarian Bots. Retrieved July 14, 2017, from https://marcowenjones.wordpress.com/2016/06/22/around-51-of-tweets-on-bahrain-hashtag-by-automated-sectarian-bots/

Joyce, M., Antonio, R., & Howard, P. N. (2013). Global Digital Activism Data Set. ICPSR. Retrieved from http://www.icpsr.umich.edu/icpsrweb/ICPSR/studies/34625/version/2

Kaiman, J. (2014, July 22). Free Tibet exposes fake Twitter accounts by China propagandists. *The Guardian*. Retrieved from https://www.theguardian.com/world/2014/jul/22/free-tibet-fake-twitter-accounts-china-propagandists

Kililkaya, E. (2015, September 4). Are Turkey's AKP Twitter trolls heading for unemployment? *Al-Monitor*. Retrieved from http://www.al-monitor.com/pulse/originals/2015/09/turkey-elections-akp-mulls-dumping-social-media-trolls.html

Kizilkaya, E. (2013, November 15). AKP's social media wars. *Al-Monitor*. Retrieved from http://www.al-monitor.com/pulse/originals/2013/11/akp-social-media-twitter-facebook.html

Kohlil, K. (2013, October 11). Congress vs BJP: The curious case of trolls and politics. *The Times of India*. Retrieved from http://timesofindia.indiatimes.com/india/Congress-vs-BJP-The-curious-case-of-trolls-and-politics/articleshow/23970818.cms

Lam, O. (2013, October 17). China Beefs Up '50 Cent' Army of Paid Internet Propagandists. *Global Voices Advocacy*. Retrieved from https://advox.globalvoices.org/2013/10/17/china-beefs-up-50-cent-army-of-paid-internet-propagandists/

MacAskill, E. (2015, January 31). British army creates team of Facebook warriors. *The Guardian*. Retrieved from https://www.theguardian.com/uk-news/2015/jan/31/british-army-facebook-warriors-77th-brigade

Marczak, B. (2013, July 31). Bahrain Govt using fake Twitter accounts to track online critics. Retrieved July 14, 2017, from https://bahrainwatch.org/blog/2013/07/31/bahrain-govt-using-fake-twitter-accounts-to-track-online-critics/

McKelvey, F., & Dubois, E. (2017). Computational Propaganda in Canada: The Use of Political Bots. *The Computational Propaganda Project Working Paper Series*. Retrieved from http://comprop.oii.ox.ac.uk/2017/06/19/computational-propaganda-in-canada-the-use-of-political-bots/

Monbiot, G. (2011, February 23). The need to protect the internet from "astroturfing" grows ever more urgent. *The Guardian*. Retrieved from https://www.theguardian.com/environment/georgemonbiot/2011/feb/23/need-to-protect-internet-from-astroturfing

Morla, R. (2015a, January 26). Ecuador's Correa Recruits Legion of Social-Media Trolls. Retrieved from https://panampost.com/rebeca-morla/2015/01/26/ecuadors-correa-recruits-legion-of-social-media-trolls/

Morla, R. (2015b, March 25). Correa's Social-Media Troll Center Exposed in Quito. *PanAm Post*. Retrieved from https://panampost.com/rebeca-morla/2015/03/25/correas-social-media-troll-center-exposed-in-quito/

Mukherji, A. (2015, February 10). Has Arvind Kejriwal murdered BJP's Twitter trolls? *Times of India Blog*. Retrieved from http://blogs.timesofindia.indiatimes.com/point-and-shoot/has-arvind-kejriwal-murdered-bjps-twitter-trolls/

News AZ. (2011, June 8). Ireli youth union focusing on IT. *News AZ*. Retrieved from http://news.az/articles/society/38037

O'Carroll, T. (2017, January 24). Mexico's misinformation wars. *Medium*. Retrieved from https://medium.com/amnesty-insights/mexico-s-misinformation-wars-cb748ecb32e9#.n8pi52hot

Orcutt, M. (2012, June 21). Twitter Mischief Plagues Mexico's Election. *MIT Technology Review*. Retrieved from https://www.technologyreview.com/s/428286/twitter-mischief-plagues-mexicos-election/

Parfitt, T. (2015, June 24). My life as a pro-Putin propagandist in Russia's secret "troll factory." *The Telegraph*. Retrieved from http://www.telegraph.co.uk/news/worldnews/europe/russia/11656043/My-life-as-a-pro-Putin-propagandist-in-Russias-secret-troll-factory.html

Pearce, K. E., & Kendzior, S. (2012). Networked Authoritarianism and Social Media in Azerbaijan. *Journal of Communication*, *62*(2), 283–298. https://doi.org/10.1111/j.1460-2466.2012.01633.x

Peel, T. (2013, August 26). The Coalition's Twitter fraud and deception. *Independent Australia*. Retrieved from https://independentaustralia.net/politics/politics-display/the-coalitions-twitter-fraud-and-deception

Pham, N. (2013, January 12). Vietnam admits deploying bloggers to support government. *BBC News*. Retrieved from http://www.bbc.co.uk/news/world-asia-20982985

Phillips, T. (2016, May 20). Chinese officials "create 488m bogus social media posts a year." *The Guardian*. Retrieved from https://www.theguardian.com/world/2016/may/20/chinese-officials-create-488m-social-media-posts-a-year-study-finds

Quinn, B., & Ball, J. (2014, July 8). US military studied how to influence Twitter users in Darpa-funded research. *The Guardian*. Retrieved from https://www.theguardian.com/world/2014/jul/08/darpa-social-networks-research-twitter-influence-studies

Rawnsley, A. (2011, July 15). Pentagon Wants a Social Media Propaganda Machine. *WIRED*. Retrieved from https://www.wired.com/2011/07/darpa-wants-social-media-sensor-for-propaganda-ops/

Rebello, A. (2016). Guerra pelo voto. *UOL Eleicoes*. Retrieved from https://www.uol/eleicoes/especiais/a-campanha-por-tras-das-timelines.htm#um-caso-de-policia

Ressa, M. A. (2016, October 3). Propaganda war: Weaponizing the internet. *Rappler*. Retrieved from http://www.rappler.com/nation/148007-propaganda-war-weaponizing-internet

Reyes, R. R., & Mallari, M. R. (2016, November 27). Money and credulity drive Duterte's "keyboard army." *BusinessMirror*. Retrieved from http://www.businessmirror.com.ph/money-and-credulity-drive-dutertes-keyboard-army/

Rockefeller, H. (2011, February 17). UPDATED: The HB Gary Email That Should Concern Us All. Retrieved July 14, 2017, from https://www.dailykos.com/story/2011/2/16/945768/-

Rosenkranz, B. (2017, May 31). Was Margot Käßmann wirklich über die AfD gesagt hat. *Übermedien*. Retrieved from http://uebermedien.de/16231/was-margot-kaessmann-wirklich-ueber-die-afd-gesagt-hat/

Rueda, M. (2012, December 27). 2012's Biggest Social Media Blunders in LatAm Politics. *ABC News*. Retrieved from http://abcnews.go.com/ABC_Univision/ABC_Univision/2012s-biggest-social-media-blunders-latin-american-politics/story?id=18063022

Rujevic, N. (2017, January 5). Serbian government trolls in the battle for the internet. *Deutsche Welle*. Retrieved from http://www.dw.com/en/serbian-government-trolls-in-the-battle-for-the-internet/a-37026533

Sang-hun, C. (2013a, June 14). South Korean Intelligence Agents Accused of Tarring Opposition Online Before Election. *The New York Times*. Retrieved from http://www.nytimes.com/2013/06/15/world/asia/south-korean-agents-accused-of-tarring-opposition-before-election.html

Sang-hun, C. (2013b, November 21). Prosecutors Detail Attempt to Sway South Korean Election. *The New York Times*. Retrieved from http://www.nytimes.com/2013/11/22/world/asia/prosecutors-detail-bid-to-sway-south-korean-election.html

Schimmeck, V. T. (2017, March 31). Das neue Cyber-Kommando der Bundeswehr - Militärs mit Computermaus und Laptop. *Deutschlandfunk*. Retrieved from http://www.deutschlandfunk.de/das-neue-cyber-kommando-der-bundeswehr-militaers-mit.724.de.html?dram:article_id=382767

Seddon, M. (2014, June 2). Documents Show How Russia's Troll Army Hit America. *BuzzFeed*. Retrieved from http://www.buzzfeed.com/maxseddon/documents-show-how-russias-troll-army-hit-america

Shearlaw, M. (2015, April 2). From Britain to Beijing: how governments manipulate the internet. *The Guardian*. Retrieved from https://www.theguardian.com/world/2015/apr/02/russia-troll-factory-kremlin-cyber-army-comparisons

Shearlaw, M. (2016, November 1). Turkish journalists face abuse and threats online as trolls step up attacks. *The Guardian*. Retrieved from https://www.theguardian.com/world/2016/nov/01/turkish-journalists-face-abuse-threats-online-trolls-attacks

Sindelar, D. (2014, August 12). The Kremlin's Troll Army. *The Atlantic*. Retrieved from https://www.theatlantic.com/international/archive/2014/08/the-kremlins-troll-army/375932/

Slovyansk, B. P. (2014, April 27). Putin's 300 whip up Ukrainian turmoil. *The Times*. Retrieved from https://www.thetimes.co.uk/article/putins-300-whip-up-ukrainian-turmoil-53h79xl77jx

Smith, M. (2017, January 5). Russia used cyber propaganda to influence opinion in Europe, US Senate told. *The Mirror*. Retrieved from http://www.mirror.co.uk/news/uk-news/russia-used-cyber-propaganda-influence-9569457

Solon, O. (2015, January 31). Twitter, the @BritishArmy needs YOU! *The Mirror*. Retrieved from http://www.mirror.co.uk/news/technology-science/technology/cyber-warfare-army-seeks-twitter-5076931

Sonnad, N. (2014, December 18). Hacked emails reveal China's elaborate and absurd internet propaganda machine. *Quartz*. Retrieved from https://qz.com/311832/hacked-emails-reveal-chinas-elaborate-and-absurd-internet-propaganda-machine/

Sozeri, E. K. (2015, October 22). Mapping Turkey's Twitter trolls. *The Daily Dot*. Retrieved from https://www.dailydot.com/layer8/turkey-twitter-trolls/

Sozeri, E. K. (2016, September 30). RedHack Leaks Reveal the Rise of Turkey's Pro-Government Twitter Trolls. *The Daily Dot*. Retrieved from https://www.dailydot.com/layer8/redhack-turkey-albayrak-censorship/

Stern-Hoffman, G. (2013, August 14). Government to use citizens as army in social media war. *The Jerusalem Post*. Retrieved from http://www.jpost.com/Diplomacy-and-Politics/Government-to-use-citizens-as-army-in-social-media-war-322972

Strange, A., Parks, B. C., Tierney, M. J., Dreher, A., & Ramachandran, V. (2013). *China's Development Finance to Africa: A Media-Based Approach to Data Collection* (Working Paper No. 323). Retrieved from https://www.cgdev.org/publication/chinas-development-finance-africa-media-based-approach-data-collection

Telesur. (2016, July 17). Argentina: Macri Hires "Army of Trolls" to Blast Online Critics. Retrieved from http://www.telesurtv.net/english/news/Argentina-Macri-Hires-Army-of-Trolls-to-Blast-Online-Critics-20160717-0010.html

The Chosunilbo. (2013, August 13). North Korea's Vast Cyber Warfare Army. *The Chosunilbo*. Retrieved from http://english.chosun.com/site/data/html_dir/2013/08/13/2013081300891.html

The Daily Mail. (2016, May 20). Chinese government-backed social media users flood Web. *Mail Online*. Retrieved from http://www.dailymail.co.uk/wires/ap/article-3600250/Chinese-government-backed-social-media-users-flood-Web.html

The Economist. (2015, March 12). Battle of the memes. *The Economist*. Retrieved from http://www.economist.com/news/europe/21646280-russia-has-shown-its-mastery-propaganda-war-ukraine-struggling-catch-up-battle-web

The Guardian. (2015, February 2). Ecuador's president wages social media counterattack aimed at "defamers." *The Guardian*. Retrieved from https://www.theguardian.com/world/2015/feb/02/ecuador-president-social-media-counterattack

The Korean Herald. (2013, December 19). 11 cyber warfare agents face indictment. *The Korean Herald*. Retrieved from http://www.koreaherald.com/view.php?ud=20131219000660

The Telegraph. (2011, July 21). Pentagon looks to social media as new battlefield. *The Telegraph*. Retrieved from http://www.telegraph.co.uk/technology/social-media/8651284/Pentagon-looks-to-social-media-as-new-battlefield.html

Toor, A. (2014, July 22). China reportedly uses fake Twitter accounts to spread Tibet propaganda. *The Verge*. Retrieved from http://www.theverge.com/2014/7/22/5925703/china-reportedly-uses-fake-twitter-accounts-to-spread-tibet-propaganda

Vivanco, J. M. (2014, December 15). Censorship in Ecuador has made it to the Internet. *Human Rights Watch*. Retrieved from https://www.hrw.org/news/2014/12/15/censorship-ecuador-has-made-it-internet

VOA News. (2015, August 4). Venezuela Ruling Party Games Twitter for Political Gain. *VOA*. Retrieved from http://www.voanews.com/a/venezuela-ruling-party-games-twitter-for-political-gain/2902007.html

Wator, J. (2017, June 23). Trolle w polskim internecie. Najczęściej fałszywki wypuszcza prawica. *Wyborcza*. Retrieved from http://wyborcza.pl/7,156282,22001141,trolle-w-polskim-internecie-najczesciej-falszywki-wypuszcza.html?disableRedirects=true

Weiwei, A. (2012, October 17). China's Paid Trolls: Meet the 50-Cent Party. *New Statesman*. Retrieved from http://www.newstatesman.com/politics/politics/2012/10/china%E2%80%99s-paid-trolls-meet-50-cent-party

Whitaker, B. (2016, July 28). How Twitter robots spam critics of Saudi Arabia. *Al Bab*. Retrieved from http://al-bab.com/blog/2016/07/how-twitter-robots-spam-critics-saudi-arabia

Williams, C. (2015, August 4). Military marketers target Isil with anti-radicalisation campaign. *The Telegraph*. Retrieved from http://www.telegraph.co.uk/finance/newsbysector/mediatechnologyandtelecoms/digital-media/11782880/Military-marketers-target-Isil-with-anti-radicalisation-campaign.html

Williams, K. B. (2016, February 26). US launches aggressive cyberwar campaign against ISIS. *The Hill*. Retrieved from http://thehill.com/policy/cybersecurity/270889-us-launches-aggressive-cyberwar-campaign-against-isis

Williams, S. (2017, January 4). Rodrigo Duterte's Army of Online Trolls. *New Republic*. Retrieved from https://newrepublic.com/article/138952/rodrigo-dutertes-army-online-trolls

Woolley, S. C. (2015, August 4). #HackingTeam Leaks: Ecuador is Spending Millions on Malware, Pro-Government Trolls. *Global Voices Advocacy*. Retrieved from https://advox.globalvoices.org/2015/08/04/hackingteam-leaks-ecuador-is-spending-millions-on-malware-pro-government-trolls/

Woolley, S. C. (2016). Automating power: Social bot interference in global politics. *First Monday*, *21*(4). Retrieved from http://firstmonday.org/ojs/index.php/fm/article/view/6161

Yinanc, B. (2017, April 27). "AK trolls" were detrimental to the "Yes" camp. *Hürriyet Daily News*. Retrieved from http://www.hurriyetdailynews.com/ak-trolls-were-detrimental-to-the-yes-camp.aspx?pageID=449&nID=112472&NewsCatID=412

York, J. C. (2011, April 21). Syria's Twitter spambots. *The Guardian*. Retrieved from https://www.theguardian.com/commentisfree/2011/apr/21/syria-twitter-spambots-pro-revolution

Series acknowledgements

The authors gratefully acknowledge the support of the European Research Council, 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 has been provided by the Ford Foundation. Project activities were approved by the University of Oxford's Research Ethics Committee (CUREC OII C1A15-044). 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 or the University.

For their assistance and advice on this research, we are grateful to Gillian Bolsover, Rob Gorwa, Marc Owen Jones, Lisa-Maria Neudert, Fadi Salem, Akin Unver, and Samuel Woolley.

Author biographies

Samantha Bradshaw is a DPhil. candidate at the Oxford Internet Institute and works on the Computational Propaganda project as a research assistant. Prior to joining the COMPROP team, she worked at the Centre for International Governance Innovation in Waterloo, Canada, where she was a key member of a small team facilitating the Global Commission on Internet Governance. She holds an MA in global governance from the Balsillie School of International Affairs, and a joint honors BA in political science and legal studies from the University of Waterloo. Samantha tweets from @sbradshaww.

Philip N. Howard is a statutory Professor of Internet Studies at the Oxford Internet Institute and a professorial fellow at Balliol College at the University of Oxford. He has published eight books and over 120 academic articles and public essays on information technology, international affairs and public life. Howard's books include *The Managed Citizen* (Cambridge, 2006), the *Digital Origins of Dictatorship and Democracy* (Oxford, 2010) and most recently *Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up* (Yale, 2015). He blogs at www.philhoward.org and tweets from @pnhoward.