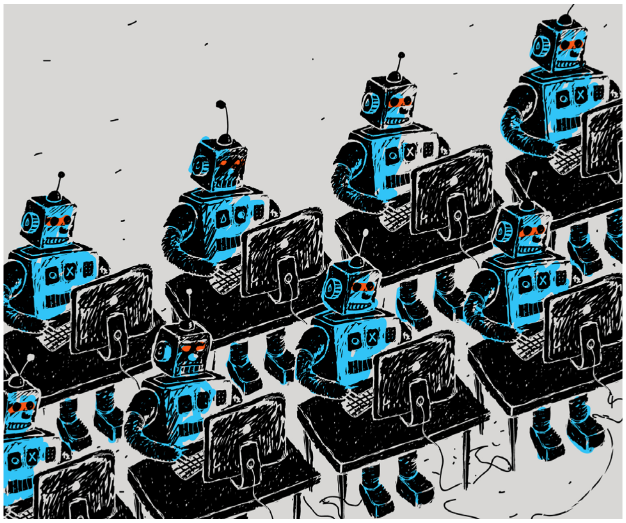
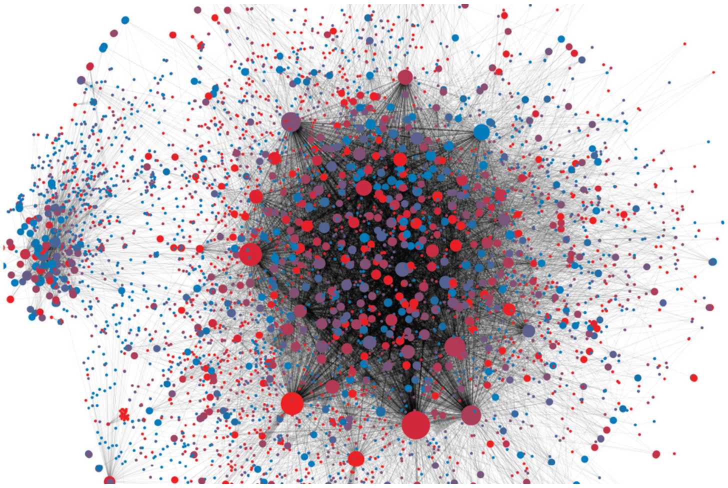
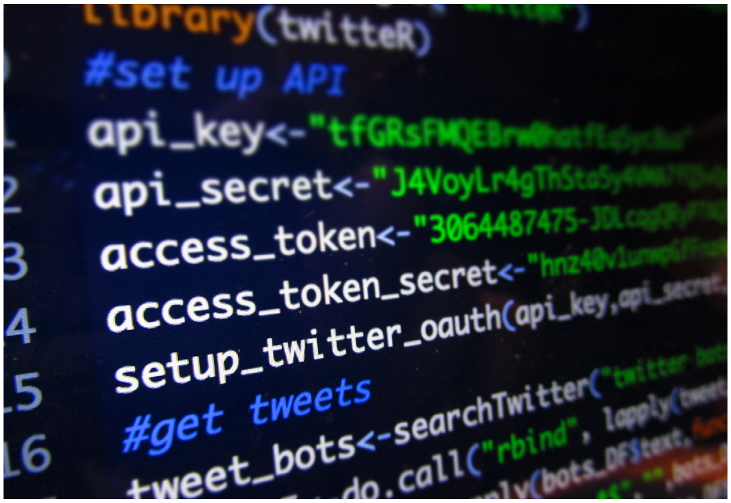
Bad Bots

The Weaponization of Social Media

Matthew | Bondy







```
library(twitteR)
#set up API
api_key<-"tfGRsFMQEBrw
api_secret<-"J4VoyLr4gThSta
access_token<-"3064487475-JDL
access_token_secret<-"hnz40v1
setup_twitter_oauth(api_key,api_secret,
#get tweets
tweet_bots<-searchTwitter("twitter bot
do.call("rbind", lapply(tweet
bots_DF$text,
```

Brief No. 9.2

P | I | P | S *The Project on International Peace and Security*
Institute for the Theory and Practice of International Relations
The College of William and Mary

Please direct inquiries to:
The Project on International Peace and Security (PIPS)
Institute for the Theory and Practice of International Relations
The College of William and Mary
427 Scotland Street
Williamsburg, Virginia 23185
tele. 757.221.1441
fax. 757.221.4650
pips@wm.edu

Electronic copies of this report are available at www.wm.edu/pips

The Project on International Peace and Security

Launched in 2008, the Project on International Peace and Security (PIPS) is an undergraduate think tank based at the College of William and Mary. PIPS represents an innovative approach to undergraduate education that highlights the value of applied liberal arts training to producing the next generation of foreign policy analysts, leaders, and engaged citizens.

PIPS is premised on two core beliefs: (1) rigorous policy-relevant research is a core component of a student's education; and (2) when guided by faculty and members of the foreign policy community, undergraduates can make meaningful contributions to policy debates; their creativity and energy are untapped resources. To this end, PIPS each year selects six research fellows and six research interns. Research fellows identify emerging international security challenges and develop original policy papers. Research interns support the work of the fellows and learn the craft of conducting policy research and writing briefs.

For more on PIPS, visit www.wm.edu/pips.

Amy Oakes
Dennis A. Smith
Co-directors

Bad Bots
The Weaponization of Social Media

APRIL 2017

Matthew Bondy

P|I|P|S *The Project on International Peace and Security*
Institute for the Theory and Practice of International Relations
The College of William and Mary

Bad Bots
The Weaponization of Social Media

In the next several years, hostile states or non-state actors will accelerate their use of social media bots to undermine democracy, recruit terrorists, disrupt markets, and stymie open-source intelligence collection. This report conducts an alternative futures analysis in order to help policymakers identify options to mitigate the threats of social media bots. In the worst-case and most-likely scenario, a technological stalemate between bots and bot-detection leads to a false sense of confidence in social media information, which allows for breakthroughs in bot technology to create disruptions until bot-detection technology advances.

Introduction

Software robots, or "bots" for short, generate roughly half of all Internet traffic.[1] Social media bots (SMBs), which are computer programs that control the activity of a social media account, were responsible for one out of five Tweets on the 2016 Presidential election and one-sixth of all Twitter traffic on the Brexit referendum.[2] Some of these bots may have been controlled by the Kremlin to undermine Western democracies.[3] Non-state actors including the Islamic State in Iraq and Syria, criminal networks, corporations, politicians, and private citizens also use SMBs to achieve political goals.

SMBs may be used against the United States for a wide array of purposes: interfering in elections, recruiting terrorists, meddling in markets, or thwarting open-source intelligence efforts. In the most likely and worst-case scenario, bot and bot-detection technologies will reach parity. The ability to detect bots will lead to a false sense of security in private industry and the government, exposing their analysis and decision-making to disruption from breakthroughs in bot technology. Meanwhile, the public will be at the mercy of social media companies, which may not take adequate action, leaving citizens in danger of misinformation and manipulation.

The Emergence of Social Media Bots

As much as 15 percent of Twitter accounts are bots, according to a recent study.[4] The difference between SMBs and real users from a strategic standpoint is that SMBs are more efficient. A single amateur computer coder can create an army of bots that flood social media networks with a volume of messages that would have required a large group of full-time Internet posters, or "trolls." Networks of SMBs working together are called "botnets."[5]

What Can Bots Do?

Social media bots can be deployed for a variety of benign or malicious purposes, but broadly speaking, they tend to specialize in one of three tasks:

- *Increase follower counts.* The simplest bot accounts follow other users in order to inflate their popularity.[6] These bots are commercially available, although purchasing followers is a breach of most social networks' terms of service. Many public figures have large bases of bot followers on social media, but often are unaware of who controls these bots.[7]

- *Spread information and misinformation.* Botnets are capable of spreading information and creating a false consensus.[8] Clayton Davis describes a "majority illusion" effect whereby bots can magnify the popularity of a position. This appearance of popularity influences the attitudes of real users and therefore can manipulate public opinion.[9]

- *Interact with other users.* Some bots can react intelligently and influence human behavior. In one experiment, SMBs shamed users into reducing their use of racial slurs online, particularly if the bot accounts appeared to be white males.[10] A separate study demonstrated that bots were able to identify social media users who were dissatisfied with government corruption and recruit them to take action.[11]

Social media bots have the potential to benefit the public, but they can also be used for manipulative political purposes.[12] If SMBs can inflate the popularity of celebrities, they can lend credibility to dictators; if they can spread truth, they can also spread falsehood; if they can sell products, they might be able to sell ideology.

The Strategic Logic of Bots

Social media bots are not merely the latest medium through which misinformation passes. Rather, by automating information warfare, SMBs will have strategic implications, namely:

- *Stronger first-mover advantages.* From a psychological standpoint, it is easier to spread misinformation than it is to correct it.[13] Social media bots amplify this first-mover advantage because they can put out information rapidly, reducing the window of opportunity to introduce any sort of warning or counter-messaging.

- *Quantity is a form of quality.* Social media bots generally do not trick people into accepting a message based on the perceived credibility of the source or the persuasiveness of the argument itself. Rather, they operate based on scale, spreading information that is more outrageous than more traditional forms of propaganda, but seemingly credible because of the majority illusion effect.

The strategic impact of bots is already evident and will only become more pronounced as the technology continues to develop.

The Future of Bot Technology

Over the next five to ten years, bots will undergo increasing sophistication and proliferation as a result of technological changes.

- *Sophistication*. Most bots created around 2015 rely on heuristic algorithms, but rapid advances in the development of genetic algorithms will allow for more sophisticated bots.[14] On Twitter, bots have developed the ability to autonomously search the Internet for profile images, post messages at particular times of day, engage in conversation, and "clone" real users' behavior.[15]

- *Proliferation*. One thousand basic Twitter follower bots are already available for as little as $9.[16] Bots can be written in a variety of programming languages and are only becoming cheaper.[17]

More plentiful, more sophisticated bots pose a series of potential threats to the national security interests of the United States. Some incidents over the past several years may be the harbinger of what is to come.

Threats to U.S. Interests

Social media bots pose an emerging threat to the United States and its allies in several domains. The following discussion identifies ways that bots have already been used or could potentially be used against the United States at home and abroad.

Democracy

Social media plays an important role in our national political conversations, as it does in many countries around the world. But social media is not an inherently democratizing force. Bots could be used against democratic nations to:

- *Influence election outcomes.* A political operative who is currently serving a prison sentence in Colombia told American press that he used bots in conjunction with hacking to interfere in several Latin American elections.[18] Some observers have alleged that the Russian government created bots to amplify anti-Clinton propaganda during the 2016 presidential election. However, it is difficult to determine the number of such bots, let alone link them to the Kremlin.[19] German Chancellor Angela Merkel nonetheless requested a briefing on bots from a data scientist in late 2016 amid concern that the Russians might attempt to use SMBs to influence elections in Europe.[20] French government officials also remain concerned about the threat of SMBs in their elections.[21]

- *Undermine public confidence in elections or government.* Even when SMBs are unable to change voters' opinions, they can still launch mass social media campaigns to poison public discourse with negativity or muddy the waters of a political issue in such a way that people become disillusioned.[22] Such a strategy would be consistent with the Kremlin's efforts to undermine faith in American democracy during the 2016 election.[23]

- *Manipulate legislators' decision-making.* In a survey of Washington lobbyists, the majority of those polled said they believe social media will play a more substantial role in legislators' decision-making over the next five years.[24] If this trend holds, then there may be a greater potential for hostile actors to indirectly influence legislation to the extent that social media sentiment is determined by bots. Lobbyists could conceivably manufacture social media trends in an effort to trick legislators.[25]

Governments could also use bots to stifle anti-government movements within their own borders. Dan Swinslow argues many authoritarian regimes are engaged in "well-resourced program[s] of…polluting online democratic discourse through hate speech and disinformation," a process he calls "distributed denial-of-democracy."[26] If bots are able to provide comparable quality social media posts at a greater scale, regimes that currently use paid trolls may shift to bots in order to extend the reach of their counter-democratic activities.

- *Drowning out dissidents.* Bots sometimes engage in hashtag spamming in order to bury anti-government messages in a mess of irrelevant information or to fool social media algorithms into removing the hashtag from the trending list, for instance, in Syria and Russia.[27] So-called "Peñabots," which support Mexican President Peña Nieto, have engaged in these tactics and also issued death threats to dissidents.[28]

- *Rewriting the narrative.* Social media bots are also used to create fake trends, launch smear campaigns, and disseminate political propaganda. These strategies have been seen in Mexico, Russia, and elsewhere.[29]

So far we have seen that different kinds of regimes tend to employ bots differently. Leaders in established democracies primarily use bots for "follower padding," authoritarian governments tend to use bots for demobilizing the opposition and spreading propaganda, and mixed regimes employ all of the above.[30]

Economy

Social media bots can manipulate stock prices through two methods. First, criminals can program bots to persuade human investors into making particular trades.[31] Second, SMBs can spoof high-frequency trading systems if the algorithms factor social media feeds into stock price calculations.[32] To date we have seen bots used to:

- *Damage the overall market.* When the Free Syrian Army hacked the Associated Press Twitter account and used bots to spread a rumor that there had been an explosion at the White House, the U.S. stock market lost $200 billion in value in two minutes.[33]

- *Commit "pump and dump" crime.* In a pump-and-dump scheme, collaborators who control most shares in a shell company trade shares back and forth to gradually raise the price. The plotters then start to sell the shares to real investors.[34] A network of Twitter bots played a role in advertising shares of Cynk Technology Corp., as shares rose from a few cents to $21.95. The fake company reached a market capitalization of over $6 billion by the time federal regulators halted trading. The stock price subsequently collapsed.[35]

These stock market manipulations have so far proven to be ephemeral, but one can imagine lower-profile but sustained attacks that evade detection and have long-run economic consequences.[36]

Terrorism

Social media is already widely used by terrorist groups like ISIS to enhance their operations and spread their influence. SMBs offer an attractive tool to bolster these pre-existing efforts. According to Samuel Wooley, "Bots are used as tools of magnification. They make the message of groups…seem much more popular than they actually are."[37] Therefore, bots could increase the effectiveness of:

- *Intimidation.* ISIS tweeted a picture of their fighters holding the group's flag with the message "We're coming, Baghdad." The message was widely disseminated by accounts associated with the Dawn of Glad Tidings app, which can publish ISIS propaganda by taking control of users' accounts.[38] The image, intended to "strike fear into the hearts of their enemies," temporarily became a top result on Twitter and any searches for "Baghdad" returned ISIS's message.[39]

- *Recruitment.* ISIS has already taken an interest in using SMBs to spread propaganda through organized hashtag campaigns and the tactic known as "twitter bombing." The goal of these operations is to flood Twitter with pro-ISIS content by creating a fake trend or hijacking a current hashtag.[40] ISIS is also attempting to make bots more human-like.[41] While there is no evidence to suggest they possess the capability to create such AI systems yet, it will be a threat in the future if ISIS is able to spread propaganda using accounts that can interact with humans and produce original content free from detection.[42]

Additionally, propaganda spread by SMBs has the potential to inspire acts of terrorism even if that violence was not the intended purpose of the botnet, as the "pizzagate" attack during the 2016 presidential election campaign season demonstrated.[43]

Intelligence Collection

Social media bots are also likely to have a distorting effect on the field of sentiment analysis, a forecasting method that is increasingly used in open-source intelligence. The technique uses machine-learning algorithms and natural language processing to extract the underlying attitudes within Internet posts and determine towards what end those sentiments are directed. Academic research has demonstrated the ability of sentiment analysis to accurately forecast the outbreak of diseases and political unrest weeks in advance.[44] The Intelligence Advanced Research Projects Activity, a former Deputy Director of the CIA, and other prominent players in the national security community have publicly touted social media sentiment analysis.[45] But if data analysts do not have a reliable method of separating bots from real users, possible results might include:

- *Erroneous conclusions.* Datasets derived from social media sources would be corrupted if there were systematic differences between bot and user sentiment and there were a significant number of bots. This bias in turn could lead to false social-media intelligence conclusions.

- *Adversary-planted conclusions*. A hostile actor with an understanding of sentiment analysis could embed bots within a social media network in order to trick the United States into drawing a particular intelligence conclusion.

- *Loss of sentiment analysis as a stream of information.* If it were apparent to the intelligence community that bots had made sentiment analysis inaccurate, a potentially valuable source of intelligence would be lost.

The intelligence risks of SMBs, as well as the threats they pose in the domains of democracy, the economy, and terrorism, will depend on technology and society's relationship with social media.

Alternative Futures Analysis: The World in 2025

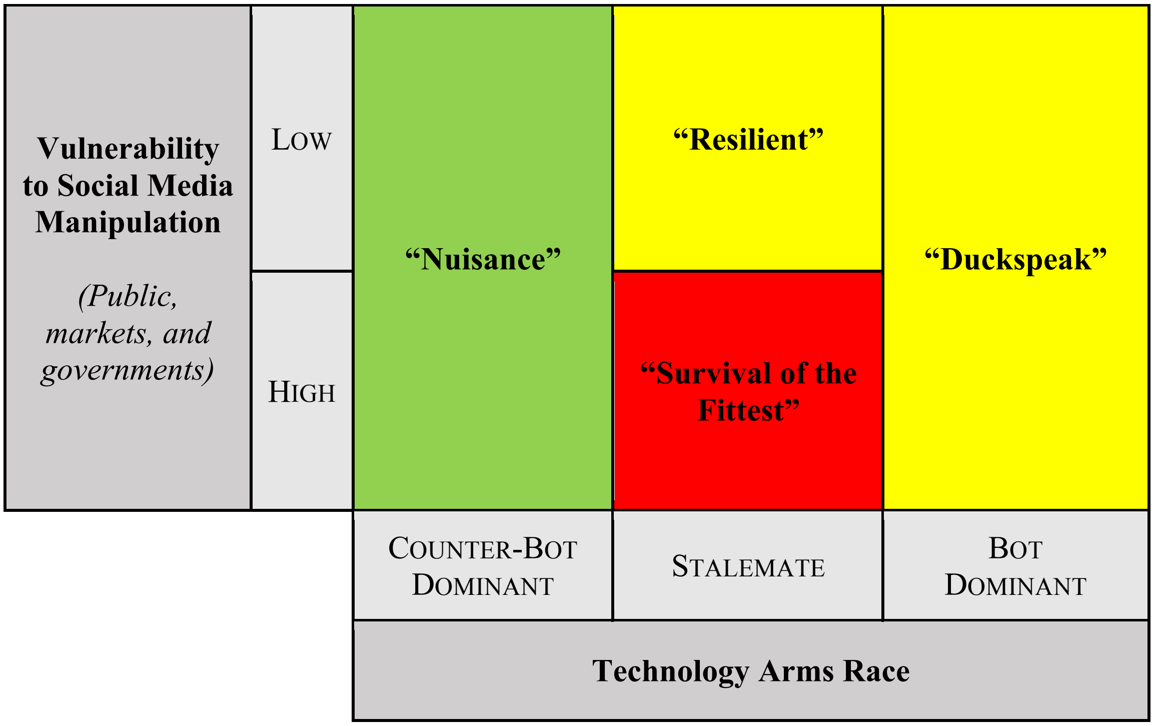
Rapid advances in the field of artificial intelligence and the wide array of actors involved in information warfare make it difficult to predict the future of SMBs with a high degree of certainty. Two "known unknowns," however, are likely to play a key role in the future of SMBs.

- *Primary factor: Bot versus counter-bot "arms race."* Emilio Ferrara et al. write that an arms race is likely to emerge between bot technology and bot-detection technology, which "will only be over when the effectiveness of early detection will sufficiently increase the cost of deception."[46] At present it is difficult to assess which side of the technology arms race will win. If social media companies start labeling bot posts or escalate efforts to eliminate harmful SMBs, that would be a sign that bot-detection technology is highly reliable.

- *Secondary factor: Vulnerability to social media manipulation.* This factor is the degree to which the public, private industry, and governments rely on social media for information. Metrics to assess this factor might include the percentage of people who claim they rely on social media for news, the weight of social media data in high-frequency trading algorithms, and the importance the intelligence community assigns to sentiment analysis.

At the extremes of the arms race spectrum, the degree of reliance on social media would not be pertinent to the outcome. If bot-detection technology were dominant, there would be few bots capable of distorting social media, and therefore the degree of reliance on social media would not affect outcomes. Likewise, if bot technology outpaces bot-detection technology, consumers of social media information would likely adapt to the new environment in order to reduce their vulnerability. The degree of reliance on social media only becomes relevant in the event of a technological stalemate. This analysis results in four possible scenarios (see Figure 1).

Figure 1: Alternative Futures



Vulnerability to Social Media Manipulation *(Public, markets, and governments)*				
	LOW	**"Nuisance"**	**"Resilient"**	**"Duckspeak"**
	HIGH		**"Survival of the Fittest"**	
		COUNTER-BOT DOMINANT	STALEMATE	BOT DOMINANT
		Technology Arms Race		

Threat Levels: 🟩 Low 🟨 Moderate 🟥 High

"Nuisance" Scenario

In a world where there is abundant technology to identify and label SMBs, bots become taboo. Low-quality bots that can be created *en masse* more quickly than social media companies can delete them are occasionally used as a form of annoyance.

- *Public.* Social media companies take action to curb SMBs, which prevents the public from being politically manipulated. Rather than buying bots for themselves, political candidates clandestinely purchase bots for their opposition in order to accuse them of attempting to manipulate the public. Terrorist botnets are quickly shut down.

- *Industry.* Investors easily determine which accounts are bots and filter these out of their analysis when making financial decisions.

- *Government.* Social media-based intelligence collection is easily able to distinguish between bot posts and real posts, allowing for analysis to proceed unhindered.

"Resilient" Scenario

If the bot technology arms race reaches a stalemate, breakthroughs in bot technology could create disruptions, but there would still be potential fail-safes if individuals, markets, and governments were not reliant on social media for information.

- *Public.* In this scenario, people do not rely on social media for news. The public remains skeptical of propaganda, fake news, and other suspicious content posted online. Hostile actors therefore have fewer opportunities and fewer incentives to use SMBs for political purposes, especially in countries where a lower percentage of people rely on social media for their news. Terrorists are able to create SMB accounts more rapidly than authorities can detect and delete them. Terrorist networks appear more legitimate online than they actually are, but only in countries where the popularity of traditional social media lingers.

- *Industry.* High-frequency trading algorithms do not often use social media for information, but high-end bots are occasionally able to trick human investors into making particular trading decisions. This manipulation allows for a modest amount of bot-based financial crime. Financial industries that engage in high-frequency trading would likely be able to afford sophisticated bot-detection systems, further mitigating the risk of stock price manipulation. Human investors would likely be suspicious of bot activity on social media.

- *Government.* The intelligence community occasionally has difficulty using sentiment analysis due to the inability to distinguish bots from real users. The defense community allocates some money to making sentiment analysis useful, but these efforts do not come to fruition. Policymakers are aware of the risks in social media data and regard conclusions from social media intelligence with a healthy degree of skepticism.

"Survival of the Fittest" Scenario (Most Likely and Worst-Case)[47]

A false sense of confidence in social media information leaves room for sophisticated actors to engage in devastating deception. Bots are virtually indistinguishable from real users to the average citizen. Governments and corporations invest modestly in technologies that can filter out bot traffic. Only actors with relatively significant resources are capable of using these bots to any great effect, and only people with the most advanced bot-detection technologies can avoid SMB influence. Cheap, spamming SMBs fall out of fashion since low-end bots are quickly rooted out by the bot-detection systems that do exist. But the most high-end SMBs are still able to occasionally bypass detection, and when they do, they inflict severe damage.

- *Public.* Social media users are unable to distinguish high-technology bots from real users. Authoritarian regimes use high-end bots to shape conversation within their own countries, redirecting anger away from the regime. Russia and China continue to retain "troll armies," but also use bots to augment their impact. Terrorist organizations develop greater cyber capabilities and pour significant resources into bots for online recruiting to expand their reach. Terrorists even launch their own chatbots to communicate basic information to potential recruits.

- *Industry.* High-frequency trading makes a comeback due to the big data revolution and advances in artificial intelligence. Individual investors face a collective action problem in dealing with SMBs, because bot-detection technology is prohibitively expensive compared to the perceived risk. Criminal networks use highly advanced artificial intelligence and SMBs for financial crime, occasionally using breakthrough technologies in billion-dollar heists.

- *Government.* The defense and intelligence communities make investments in proprietary counter-bot technologies, which are initially successful in preserving the integrity of sentiment analysis. Rapid advances in artificial intelligence make sentiment analysis a highly useful tool, which leads to overconfidence in predictive analytics. Hostile actors develop new SMBs that can circumvent detection systems. Intelligence agencies attribute analytic failures at first to the imperfect nature of predictive analytics, so it takes a while before anyone realizes that a pattern has emerged and stealthy SMBs are the underlying problem.

"Duckspeak" Scenario

People, markets, and government agencies would likely choose not to rely on social media information if it was known that bots had overrun social media platforms. In this scenario, negative SMB-generated rhetoric overruns social media, turning platforms into meaningless duck-like "quacking" as in *1984.*This deterioration causes people to shift away from platforms like Facebook and Twitter, at least for news content. Mainstream journalism begins to make a comeback. Even though SMBs continue to exist, society and governments adapt to the new environment in a way that makes them less vulnerable.

- *Public.* High-tech sophisticated bots are extremely effective at manipulating public opinion on social media for the relatively modest portion of people who still rely on it as a source of news. Most people discount social media news, because they are aware that bots have permeated the social media sphere, much like many Eastern Europeans discounted news they believed to be Russian propaganda.[48] Terrorist networks obtain access to sophisticated artificial intelligence techniques that allow them to more effectively target individual social media users for recruitment. With just a few more years of development, chatbots will be capable of passing as real people, engaging in sensitive operations, such as recruitment.

- *Industry.* Wall Street and other financial centers are aware that bots have made social media data unusable in trading decisions, and so they discount it entirely. The loss of this data has virtually no downside to the overall economy.

- *Government.* Much like investors, government agencies also determine that SMBs have corrupted social media data to the extent that it is unusable for sentiment analysis, and so social-media-based predictive analytics fall by the wayside. A potentially useful stream of intelligence has been lost, but that is preferable to drawing false conclusions.

Possible X-Factors

The scenarios outlined above paint a fairly comprehensive picture of what may happen in the future, but it is worth noting some additional factors that may play a decisive role in the future of SMBs. These changes are plausible and consequential, but not critical to the alternative futures analysis.

- *A new revolution in social media.* Ten years ago nobody could have anticipated the social media world of today, and it is difficult to predict the future. Platforms like Snapchat that offer high levels of privacy and have strong youth followings may grow relatively more important.[49]

- *Intentional de-legitimization of social media.* What if actors used SMBs not for subtle manipulation, but brazenly infiltrated social media with bots to delegitimize those platforms as a whole? A "Cyber Pearl Harbor" or "Cyber 9/11" event could also push people off of social media, and the Internet in general.

Regardless of what the future may hold, policymakers will need to be prepared to deal with the threat of SMBs.

Countering Social Media Bots

> *"Don't expect to counter the firehose of falsehood with the squirt gun of truth."*
>
> – RAND Corporation, 2016[50]

Compared to financiers and intelligence agencies, private citizens will have very little incentive to screen social media information for accuracy. In light of this reality, the following section emphasizes SMB policy with respect to the public. A good defense against SMBs will serve as an important starting point for policy, but Washington will also need to consider offensive strategies to deter SMB-based attacks, while also upholding American democratic values.

Current Approach

The U.S. government and social media companies have the capacity to counter the SMB threat, however they have not yet demonstrated their full potential to tackle the problem.

- *U.S. government.* Defense, intelligence, and diplomatic officials will need to work together to craft a counter-SMB strategy, but the current counter-propaganda efforts led by the State Department face significant challenges. The National Defense Authorization Act for the fiscal year 2017 broadened the mission of the State Department's Global Engagement Center (GEC) to include coordination among government agencies to identify and respond to foreign propaganda.[51] In theory, the GEC could play a central role in counter-SMB strategy. However, the State Department does not possess the legal authority to conduct research on social media to the same degree as the intelligence community.[52] In addition, neither the GEC nor the joint State/U.S. European Command (EUCOM) Russian Information Group have adequate resources to fulfill their missions, according to the current chief of EUCOM.[53] In light of these obstacles and possible future cuts to the State Department budget, a civilian or military element within the intelligence community could serve as an alternative hub for counter-SMB policy.[54] Regardless of which agency is ultimately responsible, conservative interpretations of laws that prohibit the government from influencing domestic public opinion remain an obstacle to countering foreign propaganda.[55]

- *Social media companies.* Social media companies have taken some action to counter SMBs and fake news, but have also been hesitant to act as arbiters of the truth. Mark Zuckerberg, for instance, has indicated that Facebook will "focus less on banning misinformation, and more on surfacing additional perspectives…."[56] Even if social media companies were fully committed to wiping out botnets, it is clear that they do not yet have the ability to detect them immediately. In January 2017, for example, researchers detected a 350,000-strong botnet on Twitter had existed for months.[57]

Even if Silicon Valley executives are unable or unwilling to eliminate bots on their own, Washington has several options at its disposal for mitigating the threat from SMBs.

Policy Instrument 1: Investing in Bot-Detection Technology

The United States has an interest in ensuring that the national security community, the financial sector, and social media companies have adequate bot-detection capabilities. Academics have developed three categories of methods to detect SMBs at acceptable false-positive and false-negative rates: graph-based analysis, crowdsourcing, and machine learning.[58] Government-academic partnerships, such as DARPA's competition among university teams in 2015 to detect bots, may be useful toward that end.[59] Good bot-detection technology would facilitate other potentially useful policy changes, such as:

- *Incentivizing bad bot elimination.* Governments may need to push social media companies to delete political SMBs if corporate policies do not protect national security.

- *Flagging bots*. Social media companies will be challenged to find ways to warn users about misinformation, while avoiding the perception that they are biased gatekeepers of information. Psychology research shows that one of the most effective ways to counter misinformation is by marking it as such from the outset.[60] Challenges arise, however, when the misinformation matches a user's worldview because counter-messaging efforts may be perceived as threatening.[61] For this reason, an explicit written warning that an account is an SMB or is providing fake news may backfire. Social media platforms might find more success with a visual cue that a source is potentially unreliable, based on an objective metric.[62]

Additionally, social media platforms might be able to reduce bot influence by amending their trending algorithms to reward time spent on an article rather than the number of clicks or shares.[63] Social media companies cannot realistically be expected to bear all of the burden, however, in tackling the SMB threat.

Policy Instrument 2: Hardening Our Society

Even in the best-case scenario, some SMB botnets will likely evade early detection systems, and the next layer of defense is the consumer of social media information. Policymakers will need to help the public buck the trend towards consuming less reliable sources of information.

- *Formal education.* One option is to teach children at an early age about concepts such as social media bots and fake news. In California, for instance, legislators have introduced bills that create new media literacy curricula.[64]

- *Public education campaigns.* Policymakers may consider using funds to promote public awareness of bots and social media literacy, similar to Media Smarts' campaign in Canada.[65] NGOs could play a role in this effort.

- *Satirical debunking.* A program devoted to satirizing foreign propaganda or other misinformation could be an effective approach. For example, a television show in Ukraine strictly broadcasts and ridicules news that is unverifiable.[66]

Training individuals to recognize SMBs is more efficient than trying to counter falsehoods, because of the sheer volume of information that automated social media accounts can produce and the first-mover advantage.

Policy Instrument 3: Maintaining Multi-Domain Deterrence

If Washington is serious about deterring SMB-based attacks, it will need to make clear that the United States maintains the capability and right to respond in other domains—including covert, cyber, diplomatic, or even military action. Multi-domain deterrence is necessary because, as a democracy, the United States would not enjoy escalation dominance in an SMB-based competition with a non-democratic adversary, such as China or Russia. A tit-for-tat strategy of SMB-based electoral interference, for instance, would run counter to American democratic values. Using SMBs to manipulate public opinion abroad could do serious harm to the U.S. image if details of such a program ever came to light. Fighting fire with fire is dangerous.

Conclusion

If left unchecked, SMBs are likely to complicate a wide array of U.S. foreign policy and national security objectives. Even modest problems in several domains or several regions of the world could quickly become a major issue for Washington. It is difficult to say for certain what is likely to happen over the next five to ten years, but policymakers and warfighters would be wise to consider these issues sooner rather than later. A delayed response could do irreparable damage to our democracy and our national security.

Appendix A. Summary of Threats

Threat	Vulnerable Actor	Possible Hostile Actors / Threat Source
Democracy	Public	Foreign intelligence agencies, politicians acting against their own populations, or non-state actors
Terrorism	Public	Terrorist organizations
Economy	Private industry	Criminal networks or terrorist organizations
Intelligence	Government	Foreign intelligence agencies or accidental threat

[1] Igal Zeifman, "2015 Bot Traffic Report: Humans Take Back the Web, Bad Bots Not Giving Any Ground," Imperva Incapsula, December 9, 2015, accessed January 23, 2017, https://www.incapsula.com/blog/bot-traffic-report-2015.html.

[2] Caitlin Dewey, "How Online Bots Conned Brexit Voters," *The Intersect* (blog), The Washington Post, June 27, 2016, accessed November 12, 2016, https://www.washingtonpost.com/news/the-intersect/wp/2016/06/27/how-online-bots-conned-brexit-voters/?tid=a_inl. For a definition of social media bots, see Emilio Ferrara, Onur Varol, Clayton Davis, Filippo Menczer, and Alessandro Flammini, "The Rise of Social Bots," *Communications of the ACM* 59, no. 7 (July 2016): 96-104, doi: 10.1145/2818717.

[3] Robert Gorwa, "On the Internet, Nobody Knows That You're A Russian Bot," *Net Politics* (blog), Council on Foreign Relations, March 20, 2017, accessed March 26, 2017, http://blogs.cfr.org/cyber/2017/03/20/internet-nobody-knows-youre-russian-bot/; Craig Timberg, "Russian Propaganda Effort Helped Spread 'Fake News' During Election, Experts Say," *The Washington Post,* November 24, 2016, accessed January 23, 2017, https://www.washingtonpost.com/business/economy/russian-propaganda-effort-helped-spread-fake-news-during-election-experts-say/2016/11/24/793903b6-8a40-4ca9-b712-716af66098fe_story.html?utm_term=.f743bf304b30.

[4] Onur Varol, Emilio Ferrara, Clayton A. Davis, Filippo Menczer, and Alessandro Flammini, "Online Human-Bot Interactions: Detection, Estimation, and Characterization," paper to be presented at the 2017 International AAAI Conference on Wed and Social Media (ICWSM-17), first posted March 9, 2017, accessed March 26, 2017, https://arxiv.org/pdf/1703.03107.pdf.

[5] The term "botnet" is often used to describe networks of internet-connected devices that are used for a particular purpose, having been compromised by a virus, for instance, in a distributed denial of service (DDOS) attack. Norah Abokhodair, Daisy Yoo, and David W. McDonald, "Dissecting a Social Botnet: Growth, Content and Influence in Twitter," *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Programming* (2015): 840.

[6] Fake follower bots are still oftentimes eggs. Ben Schreckinger, "Inside Trump's 'cyborg' Twitter army," *Politico*, September 30, 2016, accessed January 8, 2017, http://www.politico.com/story/2016/09/donald-trump-twitter-army-228923.

[7] For more on how some U.S. Congressional candidates most likely purchase bots to increase follower counts, see Ben Schreckinger, "Inside Trump's 'cyborg' Twitter army." In addition to the United States, bots have also been used for "follower padding" in Australia, Italy, Mexico, South Korea, Turkey, the United Kingdom. Samuel C. Woolley, "Automating Power: Social Bot Interference in Global Politics," *First Monday* 21, no. 4 (April 2016), accessed March 2, 2017, doi: doi:10.5210/fm.v21i4.6161.

[8] David Cook, Benjamin Waugh, Maldini Abdipanah, Omid Hashemi, and Shaquille Abdul Rahman, "Twitter Deception and Influence: Issues of Identity, Slacktivism, and Puppetry," *Journal of Information Warfare* 13, 1 (2014), https://www.jinfowar.com/twitter-deception-influence-issues-identity-slacktivism-puppetry/. Cook argues that new media, political parties, and the public engage in "slacktivism," meaning that they regularly mistake auto-generated online content for genuine political discussion.

[9] Dewey, "One in Four Debate Tweets Comes From a Bot." The phenomenon of using bots to create the appearance of consensus around an issue is commonly referred to as "astroturfing." Abokhair et al., "Dissecting a Social Botnet," 849.

[10] Kevin Munger, "Tweetment Effects on the Tweeted: Experimentally Reducing Racist Harassment," *Political Behavior* (2016), accessed January 8, 2017, doi:10.1007/s11109-016-9373-5.

[11] Saiph Savage, Andres Monroy-Hernandez, and Tobias Hollerer, "Botivist: Calling Volunteers to Action Using Online Bots," *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing* (2016): 813-822, accessed January 23, 2017, doi: 10.1145/2818048.2819985.

[12] Philip N. Howard, *Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up* (New Haven: Yale University Press, 2015), 202-204.

[13] Stephan Lewandowsky, Ullrich K. H. Eckner, Colleen M. Seifert, Norbert Schwarz, and John Cook. "Misinformation and Its Correction: Continued Influence and Successful Debiasing," *Psychological Science in the Public Interest* 13, no. 2 (2012): 106-131, accessed March 9, 2017, doi: 10.1177/1529100612451018.

[14] Sean Gourley, "Get Ready for the Robot Propaganda Machine," WIRED, February 5, 2015, accessed January 9, 2017, http://www.wired.co.uk/article/robot-propaganda.

[15] Emilio Ferrara et al., "The Rise of Social Bots," 99-100.

[16] "Top Twitter Followers Providers," Buy Twitter Followers Reviews, accessed November 15, 2016, http://buytwitterfollowersreview.org/top-10/.

[17] Rob Dubbin, "The Rise of Twitter Bots," *The New Yorker*, November 14, 2013, accessed November 15, 2016, http://www.newyorker.com/tech/elements/the-rise-of-twitter-bots.

[18] Jordan Robertson, Michael Riley, and Andrew Willis, "How to Hack an Election," *Bloomberg Businessweek*, March 31, 2016, accessed January 17, 2017, https://www.bloomberg.com/features/2016-how-to-hack-an-election/. The political operative, Sepúlveda, reportedly used high-tech Twitter bots to steer online conversation in support of now-President of Mexico Enrique Peña Nieto and employed 30,000 less-sophisticated Twitter bots to generate trends that damaged opposition candidates. He also developed software to manage Twitter bots and used fake computer-generated calls and fake Facebook profiles in Mexican gubernatorial races. For more on how bots have been used in Argentina, Ecuador, and Mexico, see Manuel Rueda, "2012's biggest social media blunders in LatAm politics," *ABC News*, December 26, 2012, http://abcnews.go.com/ABC_Univision/ABC_Univision/2012s-biggest-social-media-blunders-latin-american-politics/story?id=18063022.

[19] Robert Gorwa, "On the Internet, Nobody Knows That You're A Russian Bot."

[20] Caroline Copley, "Merkel Fears Social Bots May Manipulate German Election," *Reuters,* November 24, 2016, accessed January 13, 2017, http://www.reuters.com/article/us-germany-merkel-socialbots-idUSKBN13J1V0; James Carstensen, "Germany's Merkel, Eyeing Election and a Fourth Term, Expresses Concerns About Social Media Bots," *CNS News,* November 30, 2016, accessed January 13, 2017, http://www.cnsnews.com/news/article/james-carstensen/germanys-merkel-eyeing-election-and-fourth-term-expresses-concerns; James Glenday, "Australia Needs to be Better Prepared for an Onslaught of 'Social Bots,' Researchers Warn," *Australian Broadcasting Corporation*, December 6, 2016, accessed January 13, 2017, http://www.abc.net.au/news/2016-12-07/are-social-bots-a-threat-to-australian-democracy/8096120. Additional examples of bots being used to manipulate election outcomes include the Massachusetts Senate special election in 2010 and South Korean intelligence officers posting 1.2 million messages to Twitter in an effort to manipulate their own 2013 national elections. For Massachusetts, see Jacob Ratkiewicz, Michael Conover, Mark Meiss, Bruno Goncalves, Snehal Patil, Alessandro Flammini, and Filippo Menczer, "Truthy: Mapping the spread of astroturf in microblog streams," *WWW '11: Proceedings of the 20th International Conference Companion on World Wide Web*, (2011): 249–252, doi: http://doi.org/10.1145/1963192.1963301. For South Korea, see Choe Sang-Hun, "Prosecutors detail attempt to sway South Korean election," *The New York Times,* November 21, 2013, accessed March 26, 2017, http://www.nytimes.com/2013/11/22/world/asia/prosecutors-detail-bid-to-sway-south-korean-election.html.

[21] Nathalie Guibert and Martin Untersinger, "Cybersécurité : 'Le résultat de la présidentielle ne peut être faussé," *Le Monde,* January 25, 2017, accessed March 21, 2017, http://www.lemonde.fr/election-presidentielle-2017/article/2017/01/25/le-resultat-de-la-presidentielle-ne-peut-etre-fausse_5068760_4854003.html?xtmc =election_presidentielle_francaise&xtcr=216#meter_toaster. Researchers found evidence suggesting that bots are supporting Marine Le Pen. See Ben Nimmo and Nika Aleksejeva, "Le Pen's (Small) Online Army," *Medium,* posted by the Atlantic Council's Digital Forensic Research Lab, March 26, 2017, accessed March 26, 2017, https://medium.com/dfrlab/le-pens-small-online-army-c754058630f0#.dcho17c8b.

[22] Ben Schreckinger, "Inside Trump's 'cyborg' Twitter army."

[23] Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections,* Intelligence Community Assessment 2017-01D, January 6, 2017, accessed January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf. This intelligence community report assesses Russia's intentions but does not specifically mention bots.

[24] Catherine Ho, "K Street Says Social Media are Growing Faster than Lobbying as Way to Influence Washington, *PowerPost* (Newsletter), The Washington Post, November 3, 2016, accessed November 12, 2016, https://www.washingtonpost.com/news/powerpost/wp/2016/11/03/k-street-says-social-media-is-growing-faster-than-traditional-lobbying-as-way-to-influence-washington/?postshare=9841478374831316&tid=ss_fb.

[25] Philip N. Howard, *Pax Technica*, 208.

[26] Dan Swinslow, "The Distributed Denial of Democracy," *Democracy Works* (blog), National Democratic Institute, November 9, 2016, accessed January 17, 2017, https://www.demworks.org/distributed-denial-democracy.

[27] Erin Gallagher, "Mexican Botnet Dirty Wars," video, August 8, 2015, https://media.ccc.de/v/camp2015-6795-mexican_botnet_dirty_wars#video&t=283. Similar tactics have also been used in Syria to support President Bashar al-Assad and the Kremlin. See Abokhodair et al., 839-851. For Russia, see Brian Krebs, "Twitter Bots Drown Out Anti-Kremlin Tweets," *Krebs on Security*, December 8, 2011, http://krebsonsecurity.com/2011/12/twitter-bots-drown-out-anti-kremlin-tweets/.

[28] Mike Orcutt, "Twitter mischief plagues Mexico's election," *MIT Technology Review*, June 21, 2012, http://www.technologyreview.com/news/428286/twitter-mischief-plagues-mexicos-election/. Erin Gallagher, "Mexican Botnet Dirty Wars," video, August 8, 2015, https://media.ccc.de/v/camp2015-6795-mexican_botnet_dirty_wars#video&t=283; Erin Gallagher, "Mexican Botnet Dirty Wars," video, August 8, 2015, https://media.ccc.de/v/camp2015-6795-mexican_botnet_dirty_wars#video&t=283.

[29] For Mexico, see Erin Gallagher, "Mexican Botnet Dirty Wars," video, August 8, 2015, https://media.ccc.de/v/camp2015-6795-mexican_botnet_dirty_wars#video&t=283; Carlos Alonso Cruz, "Los bots que protegen a Enrique Peña Nieto en Twitter," *The Huffington Post,* May 28, 2015, accessed March 19, 2016, http://www.huffingtonpost.com/carlos-alonso-cruz/bots-enrique-pena-nieto_b_7438724.html. For Russia, see Lawrence Alexander, "Social Network Analysis Reveals Full Scale of Kremlin's Twitter Bot Campaign," *Global Voices*, April 2, 2015, accessed March 2, 2017, https://globalvoices.org/2015/04/02/analyzing-kremlin-twitter-bots/; Lawrence Alexander, "The Curious Chronology of Russian Twitter Bots," *Global Voices*, April 27, 2015, accessed March 2, 2017, https://globalvoices.org/2015/04/27/the-curious-chronology-of-russian-twitter-bots/.

[30] Woolley, "Automating Power"

[31] Zeke Faux and Dune Lawrence, "Searching for Cynk: The $6 Billion Penny-Stock Debacle, From Belize to Las Vegas," *Bloomberg*, July 24, 2014, accessed December 1, 2016, http://www.bloomberg.com/news/articles/2014-07-24/cynk-the-6-billion-penny-stock-debacle-stretches-from-belize-to-las-vegas. This strategy is usually accomplished by posting positive comments on a trader's social media account to gain trust over time and then providing a stock recommendation.

[32] Emilio Ferrara et al., "The Rise of Social Bots," 99.

[33] Ibid.

[34] Ibid.

[35] Ibid.

[36] In each case, the market restored itself to equilibrium once news outlets dispelled the bot-fueled rumors. However, SMB-based market meddling should still raise alarm bells because enormous sums of money are redistributed during these volatile processes. Of particular concern, those who planned the bot campaign can take advantageous market positions in advance of the scheme, deriving their gains at the expense of other investors. In addition, one can imagine hostile actors using SMBs to perpetrate a large series of lower-profile schemes against companies, some of which go undetected but altogether inflict have long-term consequences rather than just a temporary anomaly.

[37] Leanna Garfield, "ISIS Has Created Thousands of Political Bots – and Hactivists Want You to Destroy Them," *Business Insider*, December 14, 2015, accessed November 13, 2016, http://www.businessinsider.com/anonymous-battles-isis-political-bots-2015-12.

[38] J.M. Berger, "How ISIS Games Twitter," *The Atlantic*, June 16, 2014, https://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/.

[39] Alexander Trowbridge, Jihadists on the move in Iraq with weapons, hastags," *CBS News*, June 16, 2014, http://www.cbsnews.com/news/isis-jihadists-on-move-in-iraq-using-weapons-and-twitter-hashtags/.

[40] Leanna Garfield, "ISIS Has Created Thousands of Political Bots – and Hactivists Want You to Destroy Them," *Business Insider*, December 14, 2015, accessed November 13, 2016, http://www.businessinsider.com/anonymous-battles-isis-political-bots-2015-12.

[41] Ibid.

[42] Robert J. Bunker, "The Use of Social Media Bots and Automate (AI Based) Text Generator: Key Technologies in Winning the Propaganda War Against Islamic State/Daesh?" *Trends Research and Advisory*, August 10, 2015, http://trendsinstitution.org/the-use-of-social-media-bots-and-automated-ai-based-text-generators-key-technologies-in-winning-the-propaganda-war-against-islamic-statedaesh/.

[43] Marc Fisher, John Woodrow Cox, and Peter Hermann, "Pizzagate: From rumor, to hashtag, to gunfire in D.C.," *The Washington Post*, December 6, 2016, accessed March 26, 2017, https://www.washingtonpost.com/local/pizzagate-from-rumor-to-hashtag-to-gunfire-in-dc/2016/12/06/4c7def50-bbd4-11e6-94ac-3d324840106c_story.html?utm_term=.3226bbd00efc.

[44] For a literature review on social media intelligence as it relates to online radicalization and unrest, see Swati Agarwal, "Applying Social Media Intelligence for Predicting and Identifying On-line Radicalization and Civil Unrest Oriented Events," Literature review, Ph.D. Comprehensive Examination, November 12, 2015, accessed January 16, 2017, https://arxiv.org/pdf/1511.06858.pdf.

[45] Office of the Director of National Intelligence, IARPA, "Open Source Indicators (OSI)," August 23, 2011, accessed January 17, 2017, https://www.iarpa.gov/index.php/research-programs/osi/baa; Patrick Tucker, "The Military Is Already Using Facebook to Track Your Mood," *Defense One*, July 2, 2014, accessed January 18, 2017,

http://www.defenseone.com/technology/2014/07/military-already-using-facebook-track-moods/87793/; Patrick Tucker, "Meet the Man Reinventing the CIA for the Big Data Era," *Defense One*, October 1, 2015, accessed January 17, 2017, http://www.defenseone.com/technology/2015/10/meet-man-reinventing-cia-big-data-era/122453/.

[46] Emilio Ferrara et al., "The Rise of Social Bots," 103-104

[47] This scenario is the most likely because, first, many of the techniques that are used to detect bots, for example, machine learning, are also used to create them. This symmetry prevents either side from advancing too far ahead of the other in the arms race. Second, social media information is currently an important information source and is only growing in importance. See Nic Newman, Richard Fletcher, David A.L. Levy, and Rasmus Kleis Nielsen, *Digital News Report 2016* (University of Oxford/Reuters Institute for the Study of Journalism, 2016), accessed March 26, 2017, http://reutersinstitute.politics.ox.ac.uk/sites/default/files/Digital-News-Report-2016.pdf.

[48] Angus King, interview by Steve Inskeep, *Morning Edition*, NPR, February 15, 2017, transcript, accessed March 26, 2017, http://www.npr.org/2017/02/15/515357044/u-s-must-probe-the-extent-to-what-russia-did-sen-king-says.

[49] Timothy Carter, "How Snapchat is Building the Future of Social Media," August 12, 2016, accessed March 15, 2017, http://marketingland.com/snapchat-building-future-social-media-heres-181479.

[50] Christopher Paul and Miriam Matthews, *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It* (Santa Monica: RAND Corporation, 2016), accessed January 8, 2017, http://www.rand.org/pubs/perspectives/PE198.html.

[51] National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114-328, (2016), https://www.congress.gov/bill/114th-congress/senate-bill/2943/text#toc-H533D0AE113D24D90A6BD9F8A0B9D679C.

[52] Department of State, Minutes and Transcript from the Quarterly Meeting on "Data Driven Public Diplomacy: Progress Towards Measuring the Impact of Public Diplomacy and International Broadcasting Activities," September 16, 2014, accessed March 26, 2017, https://2009-2017.state.gov/documents/organization/232892.pdf.

[53] Joe Gould, "EUCOM commander: US needs stronger response to Russian disinformation," *DefenseNews*, March 23, 2017, accessed March 26, 2017, http://www.defensenews.com/articles/eucom-commander-america-needs-stronger-response-to-russian-disinformation.

[54] Glen Thrush and Coral Davenport, "Donald Trump Budget Slashes Funds for the E.P.A. and State Department," *The New York Times,* March 15, 2017, accessed March 16, 2017, https://www.nytimes.com/2017/03/15/us/politics/budget-epa-state-department-cuts.html?_r=0. Patrick Tucker, "The U.S. Is Losing at Influence Warfare. Here's Why," *Defense One*, December 5, 2016, accessed March 16, 2017, http://www.defenseone.com/threats/2016/12/us-losing-influence-warfare-heres-why/133654/.

[55] Patrick Tucker, "The US Is Losing at Influence Warfare. Here's Why," *Defense One*, December 5, 2016, accessed March 26, 2017, http://www.defenseone.com/threats/2016/12/us-losing-influence-warfare-heres-why/133654/.

[56] Mark Zuckerberg, "Building Global Community," Facebook, February 16, 2017, https://www.facebook.com/notes/mark-zuckerberg/building-global-community/10154544292806634/.

[57] Juan Echeverria and Shi Zhou, "The 'Star Wars' botnet with >350k Twitter bots," *Computing Research Repository* (2017), arXiv: 1701.02405.

[58] Emilio Ferrara et al., "The Rise Social Bots," 100-103.

[59] V.S. Subrahmanian, Amos Azarla, Skylar Durst, Vadim Kagan, Aram Galstyan, Kristina Lerman, Linhong Zhu, Emilio Ferrara, Alessandro Flammini, and Filippo Menczer, "The DARPA Twitter Bot Challenge," *Computer* 49, no. 6 (2016): 38-46, doi: 10.1109/MC.2016.183.

[60] Stephan Lewandowsky et al., "Misinformation and Its Correction," 122-123.

[61] Ibid.

[62] Jamie Settle, "Chapter 9," *Friends and Enemies: How Social Media Has Polarized the American Public* (unpublished book manuscript, forthcoming).

[63] John Borthwick, "Media hacking," *Render*, March 7, 2015 https://render.betaworks.com/media-hacking-3b1e350d619c#.f2csbvk4d.

[64] An act to add Section 51206.5 to the Education Code, relating to pupil instruction, SB 135, 2017-2018 Regular Session of the California Legislature. (2017), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB135; An act to add Section 51226.8 to the Education Code, relating to pupil instruction, AB 155, 2017-2018 Regular Session of the California Legislature. (2017), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180AB155.

[65] "Media Smarts: Canada's Centre for Digital Media Literacy," accessed March 26, 2017, http://mediasmarts.ca/.

[66] Andrew E. Kramer, "To Battle Fake News, Ukrainian Show Features Nothing but Lies," *The New York Times*, February 26, 2017, accessed March 2, 2017, https://www.nytimes.com/2017/02/26/world/europe/ukraine-kiev-fake-news.html.

Robots at computers image
Photo Credit: joebakal, stock.adobe.com

Botnet detection image
Photo Credit: Copyright Indiana University. See Emilio Ferrara, Onur Varol, Clayton Davis, Filippo Menczer, and Alessandro Flammini, "The Rise of Social Bots," *Communications of the ACM* 59, no. 7 (July 2016): 96-104, doi: 10.1145/2818717.

Code image
Photo Credit: Chris Elsner