Commanding the Trend: Social Media as Information Warfare

Lt Col Jarred Prier, USAF

Abstract

This article demonstrates how social media is a tool for modern information-age warfare. It builds on analysis of three distinct topics: social networking, propaganda, and news and information sharing. Two case studies are used to show how state and nonstate actors use social media to employ time-tested propaganda techniques to yield far-reaching results. The spread of the propaganda message is accomplished by tapping into an existing narrative, then amplifying that message with a network of automatic "bot" accounts to force the social media platform algorithm to recognize that message as a trending topic. The first case study analyzes Islamic State (IS) as a nonstate actor, while the second case observes Russia as a state actor, with each providing evidence of successful influence operations using social media. Coercion and persuasion will continue to be decisive factors in information warfare as more countries attempt to build influence operations on social media.

✳ ✳ ✳ ✳ ✳

For years, analysts in the defense and intelligence communities have warned lawmakers and the American public of the risks of a cyber Pearl Harbor. The fear of a widespread cyber-based attack loomed over the country following intrusions against Yahoo! email accounts in 2012, Sony Studios in 2014, and even the United States government Office of Personnel Management (OPM) in 2015. The average American likely did not understand exactly how, or for what purposes, US adversaries

---

Lt Col Jarred Prier, USAF, currently serves as director of operations for the 20th Bomb Squadron. He completed a USAF fellowship at the Walsh School of Foreign Service at Georgetown University and earned a master's degree from the School of Advanced Air and Space Studies at Air University, Maxwell Air Force Base, Alabama. Prier also holds a master of science degree in international relations from Troy University, Alabama. This article evolved from his thesis.

were operating within the cyber domain, but the implications of future attacks were not difficult to imagine. Enemies of the United States could target vulnerable power grids, stock markets, train switches, academic institutions, banks, and communications systems in the opening salvos of this new type of warfare.[1]

In contrast to more traditional forms of cyberattack, cyber operations today target people within a society, influencing their beliefs as well as behaviors, and diminishing trust in the government. US adversaries now seek to control and exploit the trend mechanism on social media to harm US interests, discredit public and private institutions, and sow domestic strife. "Commanding the trend" represents a relatively novel and increasingly dangerous means of persuasion within social media. Thus, instead of attacking the military or economic infrastructure, state and nonstate actors outside the United States can access regular streams of online information via social media to influence networked groups within the United States. This article analyzes how two US adversaries hijacked social media using four factors associated with command of the trend. First it provides a basis for commanding the trend in social media by analyzing social media as a tool for obtaining and spreading information. It then looks more specifically at how US adversaries use social media to command the trend and target US citizens with malicious propaganda. Next, the two most prominent, recent case studies provide evidence of how nonstate and state actors use social media to counter the United States. The first case study covers IS from 2014 to 2016 by examining the group's use of social media for recruiting, spreading propaganda, and proliferating terror threats. The second case describes the pattern of Russian hacking, espionage, disinformation, and manipulation of social media with a particular focus on the United States presidential election of 2016. Evidence for this second case study comes from nearly two years of research on Twitter accounts believed to be part of a Russian information warfare network. The article concludes with implications and predictions of how social media will continue to develop, what can be expected in the future, and how the United States can respond to the growing threat of adversaries commanding the trend.

Commanding the Trend in Social Media

The adaptation of social media as a tool of modern warfare should not be surprising. Internet technology evolved to meet the needs of

information-age warfare around 2006 with the dawn of Web 2.0, which allowed internet users to create content instead of just consuming online material. Instead, the individual could decide what was important and only read what was important, on demand. Not only could users select what news they want to see, but they could also use the medium to create news based on their opinions.[2] The social nature of humans ultimately led to virtual networking. As such, traditional forms of media were bound to give way to a more tailorable form of communication. US adversaries were quick to find ways to exploit the openness of the internet, eventually developing techniques to employ social media networks as a tool to spread propaganda. Social media creates a point of injection for propaganda and has become the nexus of information operations and cyber warfare. To understand this we must examine the important concept of the social media trend and look briefly into the fundamentals of propaganda. Also important is the spread of news on social media, specifically, the spread of "fake news" and how propaganda penetrates mainstream media outlets.

Trending Social Media

Social media sites like Twitter and Facebook employ an algorithm to analyze words, phrases, or hashtags to create a list of topics sorted in order of popularity. This "trend list" is a quick way to review the most discussed topics at a given time. According to a 2011 study on social media, a trending topic "will capture the attention of a large audience for a short time" and thus "contributes to agenda setting mechanisms."[3] Using existing online networks in conjunction with automatic "bot" accounts, foreign agents can insert propaganda into a social media platform, create a trend, and rapidly disseminate a message faster and cheaper than through any other medium. Social media facilitates the spread of a narrative outside a particular social cluster of true believers by commanding the trend. It hinges on four factors: (1) a message that fits an existing, even if obscure, narrative; (2) a group of true believers predisposed to the message; (3) a relatively small team of agents or cyber warriors; and (4) a network of automated "bot" accounts.

The existing narrative and the true believers who subscribe to it are endogenous, so any propaganda must fit that narrative to penetrate the network of true believers. Usually, the cyber team is responsible for crafting the specific message for dissemination. The cyber team then generates

videos, memes, or fake news, often in collusion with the true believers. To achieve the effective spread of propaganda, the true believers, the cyber team, and the bot network combine efforts to take command of the trend. Thus, an adversary in the information age can influence the population using a variety of propaganda techniques, primarily through social media combined with online news sources and traditional forms of media.

A trending topic transcends networks and becomes the mechanism for the spread of information across social clusters. Here the focus is primarily on Twitter, a "microblogging" site where each post is limited to 140 characters.[4] Facebook also has a trends list, but it is less visible than the Twitter trends list, and the two applications serve different purposes. Facebook maintains a function of bringing friends and families together. On Facebook, your connections are typically more intimate connections than you would expect on Twitter, which focuses less on bringing people together and more on bringing ideas together. As a microblog, Twitter's core notion is to share your thoughts and feelings about the world around you with a group of people who share similar interests. The individuals who follow each other may not be friends but could be a team of like-minded academics, journalists, sports fans, or politicos. When a person tweets, that tweet can be viewed by anyone who follows that person, or anyone who searches for that topic using Twitter's search tool. Additionally, anyone can "retweet" someone else's tweet, which broadcasts the original to a new audience. Twitter makes real-time idea and event sharing possible on a global scale.[5] Another method for quick referencing on Twitter is using a "hashtag." The tweet would then be visible to anyone who clicked on the link along with all of the other tweets using the same hashtag.

A trend can spread a message to a wide group outside of a person's typical social network. Moreover, malicious actors can use trends to spread a message using multiple forms of media on multiple platforms, with the ultimate goal of garnering coverage in the mainstream media. Command of the trend is a powerful method of spreading information whereby, according to an article in the *Guardian*, "you can take an existing trending topic, such as fake news, and then weaponise it. You can turn it against the very media that uncovered it."[6]

Because Twitter is an idea-sharing platform, it is very popular for rapidly spreading information, especially among journalists and academics;

however, malicious users have also taken to Twitter for the same benefits in recent years. At one time, groups like al-Qaeda preferred creating websites, but now, "Twitter has emerged as the internet application most preferred by terrorists, even more popular than self-designed websites or Facebook."[7] Twitter makes it easy to spread a message to both supporters and foes outside of a particular network. Groups trying to disseminate a message as widely as possible can rely on the trend function to reach across multiple networks.

Three methods help control what is trending on social media: trend distribution, trend hijacking, and trend creation. The first method is relatively easy and requires the least amount of resources. Trend distribution is simply applying a message to every trending topic. For example, someone could tweet a picture of the president with a message in the form of a meme—a stylistic device that applies culturally relevant humor to a photo or video—along with the unrelated hashtag #SuperBowl. Anyone who clicks on that trend list expecting to see something about football will see that meme of the president. Trend hijacking requires more resources in the form of either more followers spreading the message or a network of "bots" (autonomous programs that can interact with computer systems or users) designed to spread the message automatically. Of the three methods to gain command of the trend, trend creation requires the most effort. It necessitates either money to promote a trend or knowledge of the social media environment around the topic, and most likely, a network of several automatic bot accounts.

Bot accounts are non-human accounts that automatically tweet and retweet based on a set of programmed rules. In 2014, Twitter estimated that only 5 percent of accounts were bots; that number has grown along with the total users and now tops 15 percent.[8] Some of the accounts are "news bots," which just retweet the trending topics. Some of the accounts are for advertising purposes, which try to dominate conversations to generate revenue through clicks on links. Some bots are trolls, which, like a human version of an online troll, tweet to disrupt the civil conversation.

For malicious actors seeking to influence a population through trends on social media, the best way to establish trends is to build a network of bot accounts programmed to tweet at various intervals, respond to certain words, or retweet when directed by a master account. Figure 1 illustrates the basics of a bot network. The top of the chain is a small

core group. That team is composed of human-controlled accounts with a large number of followers. The accounts are typically adversary cyber warriors or true believers with a large following. Under the core group is the bot network. Bots tend to follow each other and the core group. Below the bot network is a group consisting of the true believers without a large following. These human-controlled accounts are a part of the network, but they appear to be outsiders because of the weaker links between the accounts. The bottom group lacks a large following, but they do follow the core group, sometimes follow bot accounts, and seldom follow each other.

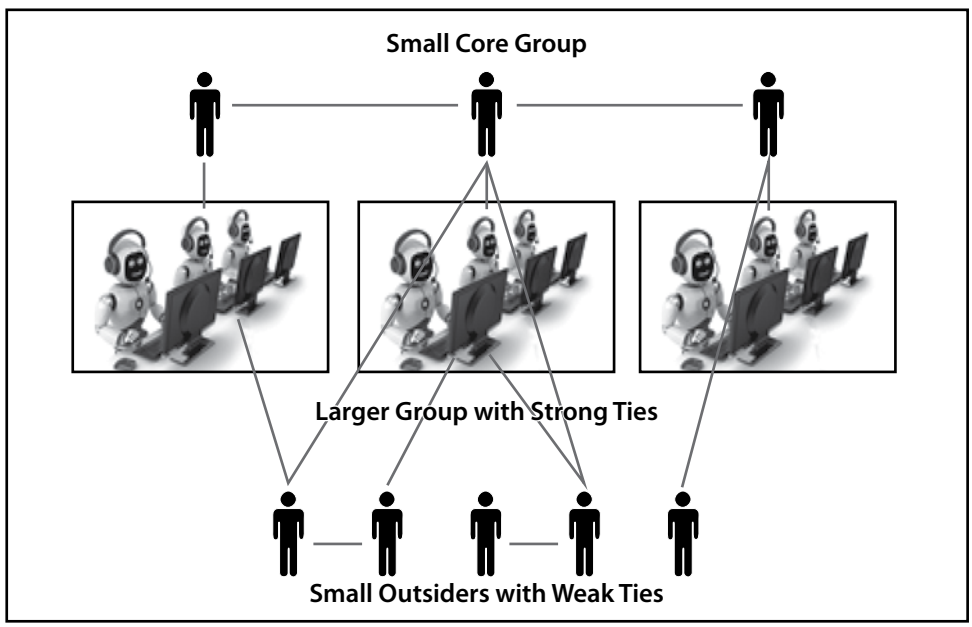

Figure 1. Illustration of a bot network

Enough bots working together can quickly start a trend or take over a trend, but bot accounts themselves can only bridge the structural hole between networks, not completely change a narrative. To change a narrative, to conduct an effective influence operation, requires a group to combine a well-coordinated bot campaign with essential elements of propaganda.

Propaganda Primer

Messaging designed to influence behavior has been around for centuries but became easier as methods of mass communication enabled wider dissemination of propaganda. Observing the rise of mass media and its presence in daily life, French philosopher Jacques Ellul noted the simplicity of propaganda in 1965. According to Ellul, "Propaganda ceases where simple dialogue begins."[9] That said, it is worth noting Eric Hoffer's comments that "propaganda on its own cannot force its way into unwilling minds, neither can it inculcate something wholly new."[10] For propaganda to function, it needs a previously existing narrative to build upon, as well as a network of true believers who already buy into the underlying theme. Social media helps the propagandist spread the message through an established network. A person is inclined to believe information on social media because the people he chooses to follow share things that fit his existing beliefs. That person, in turn, is likely to share the information with others in his network, to others who are like-minded, and those predisposed to the message. With enough shares, a particular social network accepts the propaganda storyline as fact. But up to this point, the effects are relatively localized. The most effective propaganda campaigns are not confined just to those predisposed to the message. Essentially, propaganda permeates everyday experiences, and the individual targeted with a massive media blitz will never fully understand that the ideas he has are not entirely his own. A modern example of this phenomenon was observable during the Arab Spring as propaganda spread on Facebook "helped middle-class Egyptians understand that they were not alone in their frustration."[11] In short, propaganda is simpler to grasp if everyone around a person seems to share the same emotions on a particular subject. Even a general discussion among the crowd can provide the illusion that propaganda is information.[12] In other words, propaganda creates heuristics, which is a way the mind simplifies problem solving by relying on quickly accessible data. The availability heuristic weighs the amount and frequency of information received, as well as recentness of the information, as more informative than the source or accuracy of the information.[13] Essentially, the mind creates a shortcut based on the most—or most recent—information available, simply because it can be remembered easily. Often, the availability heuristic manifests itself in information received through media coverage. The availability heuristic is important to understanding individual opinion formation and how propaganda can exploit the shortcuts our minds make to form opinions. The lines in figure 2 show formation

of opinions temporally, with bold arrows influencing a final opinion more than light arrows. The circled containers indicate a penetration point for propaganda exploitation. As previously described, mass media enables rapid spread of propaganda, which feeds the availability heuristic. The internet makes it possible to flood the average person's daily intake of information, which aids the spread of propaganda.

One of the primary principles of propaganda is that the message must resonate with the target. Therefore, when presented with information that is within your belief structure, your bias is confirmed and you accept the propaganda. If it is outside of your network, you may initially reject the story, but the volume of information may create an availability heuristic in your mind. Over time, the propaganda becomes normalized—and even believable. It is confirmed when a fake news story is reported by the mainstream media, which has become reliant on social media for spreading and receiving news.

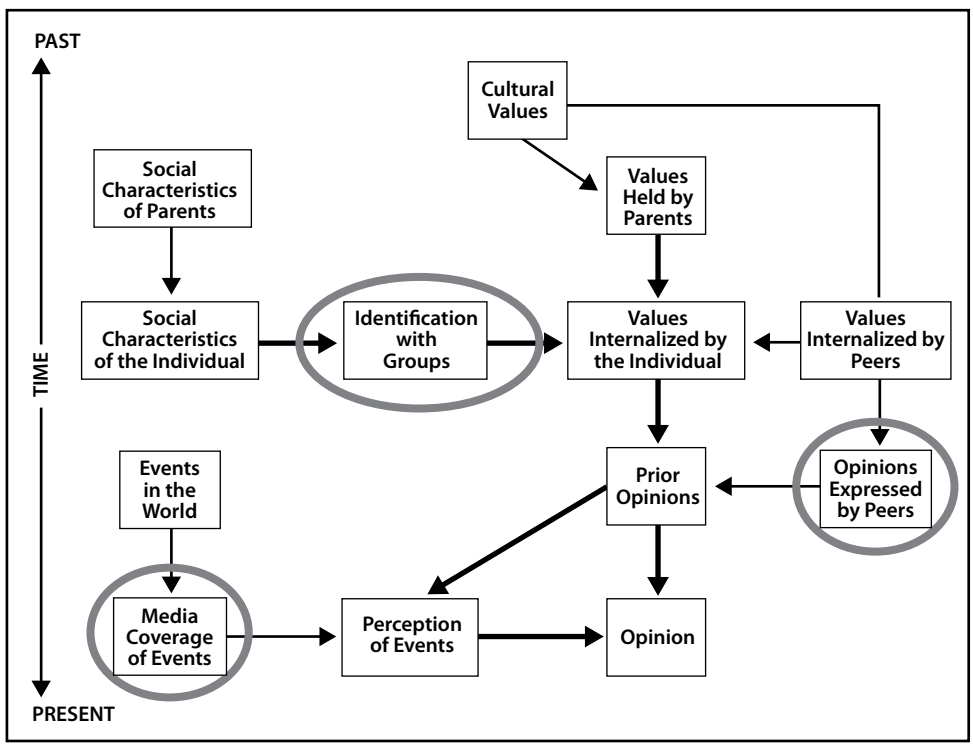

Figure 2. Model of individual opinion formation. (Reproduced by permission from Alan D. Monroe, *Public Opinion in America* [New York: Dodd, Mead, and Co., 1975], 147.)

Figure 3 maps the process of how propaganda can penetrate a network that is not predisposed to the message. This outside network is a group that is ideologically opposed to the group of true believers. The outside network is likely aware of the existing narrative but does not necessarily subscribe to the underlying beliefs that support the narrative.

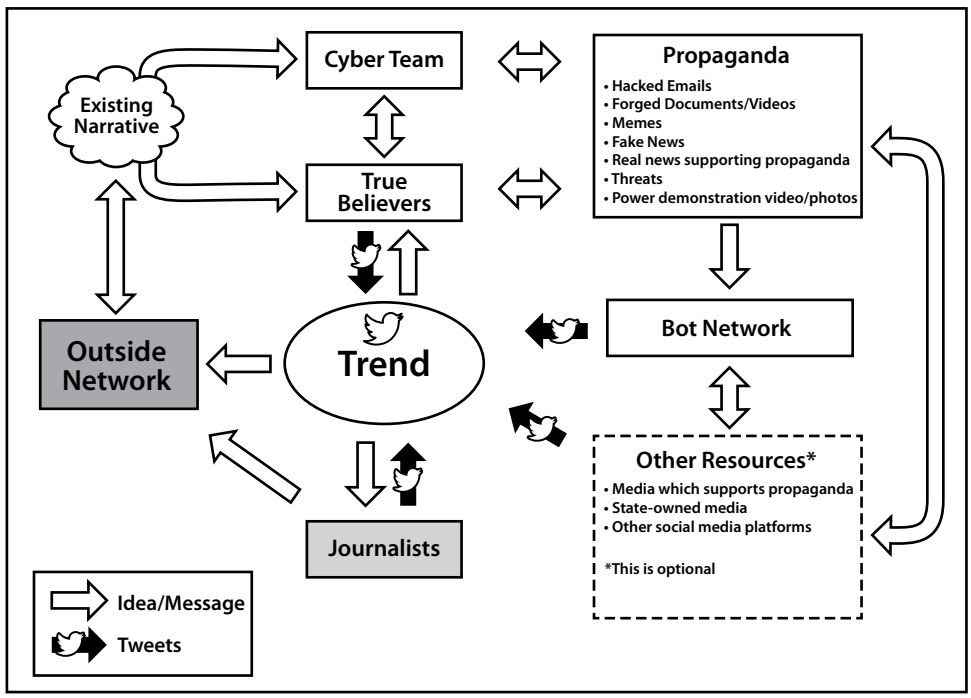

Figure 3. Process map of how propaganda spreads via the trend

Command of the trend enables the contemporary propaganda model, to create a "firehose of information" that permits the insertion of false narratives over time and at all times.[14] Trending items produce the illusion of reality, in some cases even being reported by journalists. Because untruths can spread so quickly now, the internet has created "both deliberate and unwitting propaganda" since the early 1990s through the proliferation of rumors passed as legitimate news.[15] The normalization of these types of rumors over time, combined with the rapidity and volume of new false narratives over social media, opened the door for "fake news."

The availability heuristic and the firehose of disinformation can slowly alter opinions as propaganda crosses networks by way of the trend, but

the amount of influence will likely be minimal unless it comes from a source that a nonbeliever finds trustworthy. An individual may see the propaganda and believe the message is popular because it is trending but still not buy into the message itself. Instead, the individual will likely turn to a trusted source of news to test the validity of the propaganda. Therefore, we must now analyze modern journalism to determine how command of the trend can transform propaganda from fake news to real news.

Social Networks and Social Media

Currently, 72 percent of Americans get digital news primarily from a mobile device, and people now prefer online news sources to print sources by a two-to-one ratio.[16] The news consumer now selects from an abundance of options besides a local newspaper, based on how the consumer perceives the credibility of the resource. As social media usage has become more widespread, users have become ensconced within specific, self-selected groups, which means that news and views are shared nearly exclusively with like-minded users. In network terminology, this group phenomenon is called homophily. More colloquially, it reflects the concept that "birds of a feather flock together." Homophily within social media creates an aura of expertise and trustworthiness where those factors would not normally exist. Along the lines of social networking and propaganda, people are more willing to believe things that fit into their worldview. Once source credibility is established, there is a tendency to accept that source as an expert on other issues as well, even if the issue is unrelated to the area of originally perceived expertise.[17] Ultimately, this "echo chamber" can promote the scenario in which your friend is "just as much a source of insightful analysis on the nuances of U.S. foreign policy towards Iran as regional scholars, arms control experts, or journalists covering the State Department."[18]

If social media facilitates self-reinforcing networks of like-minded users, how can a propaganda message traverse networks where there are no overlapping nodes? This link between networks is only based on that single topic and can be easily severed. Thus, to employ social media effectively as a tool of propaganda, an adversary cannot rely on individual weak links between networks. Instead, an adversary must exploit a feature within the social media platform that enables cross-network data sharing on a massive scale: the trending topics list. Trends are visible to everyone. Regardless of who follows whom on a given social media plat-

form, all users see the topics algorithmically generated by the platform as being the most popular topics at that particular moment. Given this universal and unavoidable visibility, "popular topics contribute to the collective awareness of what is trending and at times can also affect the public agenda of the community."[19] In this manner, a trending topic can bridge the gap between clusters of social networks. A malicious actor can quickly spread propaganda by injecting a narrative onto the trend list.

The combination of networking on social media, propaganda, and reliance on unverifiable online news sources introduces the possibility of completely falsified news stories entering the mainstream of public consciousness. This phenomenon, commonly called fake news, has generated significant criticism from both sides of the American political spectrum, with some labeling any contrary viewpoints fake. In reality, fake news consists of more than just bad headlines, buried ledes, or poorly sourced stories.[20] Fake news is a particular form of propaganda composed of a false story disguised as news. On social media, this becomes particularly dangerous because of the viral spread of sensationalized fake news stories.

A prime example of fake news and social media came from the most shared news stories on Facebook during the 2016 US presidential election. The source of the fake news was a supposedly patriotic American news blog called "End the Fed," a website run by Romanian businessperson Ovidiu Drobota. One story stating that the pope endorsed Donald Trump for president received over one million shares on Facebook alone, not to mention shares on Twitter.[21] Other fake news stories from that site and others received more shares in late 2016 than did traditional mainstream news sources (see figure 4).[22]

It is important to recognize that more people were exposed to those fake news stories than what is reflected in the "shares" data. In some cases, people would just see the story in a Facebook or Twitter feed; in many cases, people actively sought out news from those sources, which are fiction at best and foreign propaganda at worst. Over time, those fake news sources become trusted sources for some people. As people learn to trust those sources, legitimate news outlets become less trustworthy. A 2016 poll by Gallup showed American trust in mass media is at an all-time low.[23]

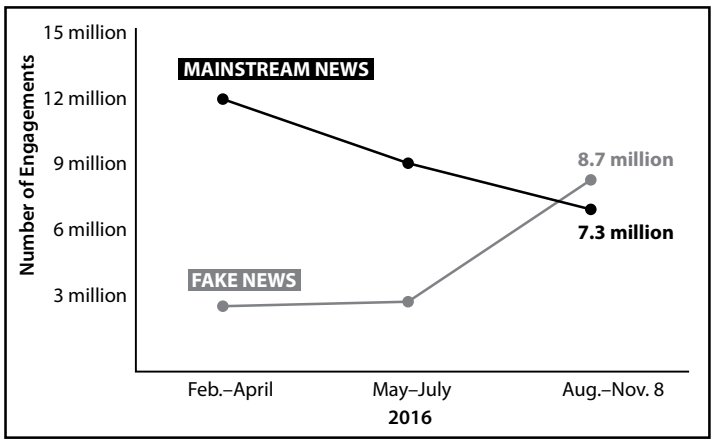

Figure 4. Total Facebook engagements for top 20 election stories

When news is tailorable to one's taste and new stories are popping up around the world every second, mainstream journalists have to change their methods to compete with other sources of news. Therefore, if social media is becoming a source for spreading news and information, journalists will try to keep up by using social media to spread their stories and to acquire information first. According to an Indiana University School of Journalism study, the most common use of social media for journalists is to check for breaking news.[24] As a result, mainstream journalists tend to use tweets as a legitimate source, especially when there is a lack of more valid or confirmed sources.[25] Overreliance on social media for breaking news can become problematic in the midst of an ongoing information operation. If an adversary takes control of a trend on Twitter, the trend is likely to be noticed by mainstream media journalists who may provide legitimacy to a false story—essentially turning fake news into real news. This is the initial setup for how social media became extremely influential via an adversary's propaganda. IS and Russia successfully manipulated social media, particularly Twitter. Although they had different objectives, the tools and techniques were similar. Both foreign actors used command of the trend to spread propaganda that influenced the emotions, opinions, and behavior of US citizens in a manner antithetical to US interests. In essence, IS and Russia hijacked social media through propaganda narratives, true believers, cyber warriors, and a bot network.

Hijacking Social Media—the Case of IS

IS could be considered either a large terrorist organization or a very fragile state with a weak army. However, the perception of IS varies. To believers, IS is a religious caliphate, but much of the rest of the world assumes it is a terrorist group that represents a perversion of faith. IS managed to master the art of manipulation because a single message simultaneously targeted potential allies and foes alike. Its use of social media is a case study in effective propaganda techniques that bolstered recruiting, increased brand recognition, and spread terror with minimal effort. It quickly became the first organization to use social media effectively to achieve its goals.

Although IS may use terrorism as a tactic, the organization behaves differently than any other terrorist organization in the world.[26] The differences are apparent in every aspect, from operations to recruiting to governing. The last factor is the key discriminator. As a descendant of al-Qaeda in Iraq, the group struggled to find its way after the death of leader Abu Musab al-Zarqawi in 2006; under the leadership of Abu Bakr al-Baghdadi the group has established clear lines of authority, taxation and educational systems, trade markets, even policing and a judiciary (covering civil, criminal, and religious complaints).[27] Gaining and holding land is just a part of what IS believes is the destiny of the organization and its followers. Certainly, the desire is to create a caliphate,[28] but its ultimate purpose is more apocalyptic in nature: IS seeks to usher in the end of the world.[29] Its members believe that their actions will bring the forces of the world to attack their caliphate and result in the imminent defeat of the infidel army in the Syrian town of Dabiq, thus triggering the end of the world and the final purge of evil.[30] IS is a revolutionary force with doomsday cult beliefs.[31]

To advance the organization's objectives, IS used messages that served to spread its propaganda on social media to a broad audience that fit within a narrative of strength for the supporter and a narrative of terror for the adversary. In other words, IS cyber warriors combined propaganda with command of the trend to accomplish three things with one message. First, they demonstrated the weakness and incompetence of the international community to fight them online and on the battlefield. Second, they injected terror into the mainstream media. Finally and most importantly, they recruited new fighters to join them on the battlefield in Iraq and Syria—and online.

Islamic State Commanding the Trend

Through a combination of ingenious marketing and cyber mastery, IS bolstered its message around the world. First, the group refined IS branding. The organization projects a very specific image to the world that affects the viewer differently based on beliefs. To a follower, the images that are shared via social media demonstrate strength and power. To the nonfollower, the images are grotesque and horrifying. In other words, no matter what IS puts out in social media the result is a win for the organization because the same message successfully targets two different groups. The amplification of those messages by creating trends on Twitter is guaranteed to get further attention once the tweet falls into the mainstream media. Thus, IS is capable of using relatively small numbers of Twitter users (see table 1) to project an aura of strength.

The method for expanding the reach of a single IS tweet or hashtag involves a network of legitimate retweets combined with bots and unwitting Twitter users. While IS does maintain a strong network of true believers, the numbers are relatively small and spread thinly across the Middle East. Therefore, IS must game the system and rig Twitter for a message to go viral. One high-tech method for creating a bot network was a mobile app called "Dawn of Glad Tidings." The app, designed by IS cyber warriors, provides updates on IS activities and spiritual guidance to the user. When users download the app, they create an account that links to their Twitter account, which then gives the app generous permissions, allowing the app to tweet using that user's account.[32] The app then retweets on behalf of the user when a master account sends an IS-branded tweet.

Over time, the hashtag generates enough tweets to start localized trends. Once the trend surfaces, it is broadcast over trend-monitoring networks, like the Arabic Twitter account @ActiveHashtags.[33] That causes the hashtag to gather more attention across the region and then be retweeted by real followers and other bot accounts. The final step in the process is when the trend goes global.

Table 1. Snapshot of Islamic State Twitter activity

Twitter-related activity studied	Related statistics
Estimated number of overt IS Twitter accounts	46,000
Number of "bot" accounts	6,216
Average number of tweets per day per user	7.3
Average number of followers	1,004
Most common year accounts created	2014
Top languages	Arabic (73%), English (18%), French (6%)
Top locations	"Islamic State," Syria, Iraq, Saudi Arabia[a]

Source: J. M. Berger and Jonathon Morgan, "The ISIS Twitter Census," Brookings Institute, accessed 20 March 2015, https://www.brookings.edu/research/the-isis-twitter-census-defining-and-describing-the-population-of-isis-supporters-on-twitter/.
[a]Based on location-enabled users and self-defined account locations

Worldwide trends on Twitter have been a boon for IS. Creating and hijacking trends garnered attention for the group that would otherwise have gone unnoticed on social media. The peak of IS trend hijacking was during the World Cup in 2014—as one of the world's most popular sporting events, it was no surprise that the hashtag #WorldCup2014 trended globally on Twitter nonstop during the tournament. At one point though, nearly every tweet under this hashtag had something to do with IS instead of soccer. The network of IS supporters and bot accounts hijacked the trend. Because people were using the hashtag to discuss the matches and advertisers were using the trend for marketing, Twitter struggled to stop the trend and the subsequent IS propaganda effort.

In fact, IS cyber warriors and true believers foiled most of the early attempts by Twitter to stop IS from using their platform to spread propaganda. Twitter's initial reaction was to suspend accounts that violated the user terms of the agreement. The result was creative user names by IS supporters; for example, a user named @jihadISIS42 was created after @jihadISIS41 was suspended, which was set up after @jihadISIS40 was suspended.[34] Each new account demonstrated a deep dedication to the cause that, when combined with the seemingly significant presence on social media, presented the group as dominating social media.

In the case of #WorldCup2014, IS took command of the trend by hijacking, using the opportunity to push recruiting messages, and making

terror threats against the tournament venues in Brazil. Additionally, the co-opted hashtag often directed users to other hashtags in what was ultimately a successful attempt to generate worldwide trends of other IS-related themes. One successful hashtag-creation effort was #StevensHeadinObamasHands, which included memes of President Barack Obama and IS-held American journalist Steven Sotloff. The implication was that the president of the United States did not care to or was powerless to stop the murder of an American citizen. Once again, IS appeared to be disproportionately powerful because of the command of the trend.

Due to the organization's aggressive communications strategy and branding, the IS social media presence consistently outperforms similar jihadist groups in the region that have the same number of, or more, followers.[35] Unlike al-Qaeda, which largely limited its online activity to websites, IS wanted to communicate with a broader audience—it wants to communicate directly to the whole world. In addition to spreading terror threats, the appearance of the group as a powerful state appealed to a group of true believers who turned to IS as new recruits to fight in Iraq and Syria. IS used social media from 2014 to 2016 to demonstrate power, sow fear in the international audience, and recruit the true believers. All the while, they used the true believers following on social media to boost their trends on social media. However, the group currently finds itself altering its modus operandi due to the recent loss of territories in Iraq and Syria, combined with a spate of successful terrorist-style attacks in Europe. The ongoing worry for counterterrorism experts is finally beginning to come to fruition: the recruit staying home to fight instead of joining IS overseas.

After years of maintaining a significant presence on social media, IS is using Twitter less now for official communication. The reasoning is likely twofold. First, the group has lost territory in Iraq and Syria and is adjusting its strategies. Second, Twitter has removed over 600,000 IS-related accounts consisting of bots, cyber warriors, and true believers.[36] Additionally, Twitter has adjusted the program to find terror-related videos, memes, and photos soon after an account from the IS network posts the propaganda. The reasons IS seemed so powerful is that, when viewed through the lens of terrorist groups, it advertised using weaponized social media campaigns. Its intense social media presence, ghastly videos, massive

recruiting, and victories against Iraqi security forces made IS seem disproportionately stronger than it was.

In summation, IS serves as a model for any nonstate group attempting to use social media for cyber coercion. Table 2 summarizes its use of the four requirements to gain command of the trend based on the analysis within this case study.

Table 2. Islamic State case study analysis

Requirement	Example
Propaganda narratives	1. IS is strong; everyone else is weak. 2. True believers should join the cause.
True believers	Muslims believing in the caliphate of al-Baghdadi
Cyber warriors	Propaganda makers, video editors, app programmers, recruiters, spiritual leaders using low- and high-tech tools to advertise IS on social media
Bot network	Unwitting victims of spiritual-guidance app "Dawn of Glad Tidings"

At the same time IS was weaponizing Twitter, Russia was using it to simultaneously cause confusion and garner support for its invasion of Crimea. Soon, Russia's command of the trend would be used to target the United States 2016 presidential election.

Russia: Masters of Manipulation

Russia is no stranger to information warfare. The original technique of Soviet actors was through *aktivnyye meropriyatiya* (active measures) and *dezinformatsiya* (disinformation). According to a 1987 State Department report on Soviet information warfare, "active measures are distinct both from espionage and counterintelligence and from traditional diplomatic and informational activities. The goal of active measures is to influence opinions and/or actions of individuals, governments, and/or publics."[37]

In other words, Soviet agents would try to weave propaganda into an existing narrative to smear countries or individual candidates. Active measures are designed, as retired KGB General Oleg Kalugin once explained, "to drive wedges in the Western community alliances of all sorts, particularly NATO, to sow discord among allies, to weaken the United States in the eyes of the people in Europe, Asia, Africa, Latin America, and thus to prepare ground in case the war really occurs." Editor, translator, and analyst of Russian Federation trends Michael Weiss says,

"The most common subcategory of active measures is *dezinformatsiya*, or disinformation: feverish, if believable lies cooked up by Moscow Centre and planted in friendly media outlets to make democratic nations look sinister."[38]

The techniques Russia uses today are similar to those they used during the Cold War, but dissemination is more widespread through social media. Recently, the Russian minister of defense acknowledged the existence of their cyber warriors in a speech to the Russian parliament, announcing that Russia formed a new branch of the military consisting of information warfare troops.[39] The Internet Research Agency, as it was called in 2015, now seems to be the information warfare branch he openly admitted to. This army of professional trolls' mission is to fight online. The Russian trolls have a variety of state resources at their disposal, including a vast intelligence network to assist their cyber warriors. The additional tools available to Russia also include RT (Russia Today) and Sputnik, the Kremlin-financed television news networks broadcasting in multiple languages around the world. Before the trolls begin their activities on social media, the cyber warrior hackers first provide hacked information to Wikileaks, which, according to CIA director Mike Pompeo, is a "non-state hostile intelligence service abetted by state actors like Russia."[40] In intelligence terms, WikiLeaks operates as a "cutout" for Russian intelligence operations—a place to spread intelligence information through an outside organization—similar to the Soviets' use of universities to publish propaganda studies in the 1980s.[41] The trolls then take command of the trend to spread the hacked information on Twitter, referencing WikiLeaks and links to RT news within their tweets. These Russian efforts would be impossible without an existing network of American true believers willing to spread the message. The Russian trolls and the bot accounts amplified the voices of the true believers in addition to inserting propaganda into that network. Then, the combined effects of Russian and American Twitter accounts took command of the trend to spread disinformation across networks.

The cyber trolls produced several hoaxes in the United States and Europe, like the Louisiana hoax, according to Adrian Chen in his article "The Agency" in the *New York Times Magazine*.[42] Protests of police departments throughout the United States during the summer of 2015 provided several opportunities to manipulate narratives via social media, and it is likely Russian trolls hijacked some of the Black Lives Matter–related

trends to spread disinformation and accuse journalists of failing to cover important issues.[43] The Russian trolls said the idea was to spread fear, discrediting institutions—especially American media—while making President Obama look powerless and Russian president Vladimir Putin more favorable.[44]

Several hijacked hashtags in 2015 attempted to discredit the Obama administration while spreading racist memes and hoaxes aimed at the African American community. In other words, the Russian trolls seemed to target multiple groups to generate anger and create chaos. One particularly effective Twitter hoax occurred as racial unrest fell on the University of Missouri campus that fall.

#PrayforMizzou

On the night of 11 November 2015, #PrayforMizzou began trending on Twitter.[45] The trend was a result of protests at the University of Missouri campus over racial issues; however, "news" slowly started developing within the hashtag that altered the meaning and soon shot the hashtag to the top of the trend list. The news was that the KKK was marching through Columbia and the Mizzou campus. One user, display name "Jermaine" (@Fanfan1911), warned residents, "The cops are marching with the KKK! They beat up my little brother! Watch out!" Jermaine's tweet included a picture of a black child with a severely bruised face; it was retweeted hundreds of times. Additionally, Jermaine and a handful of other users continued tweeting and retweeting images and stories of KKK and neo-Nazis in Columbia, chastising the media for not covering the racists creating havoc on campus.

Looking at Jermaine's followers, and the followers of his followers, one could observe that the original tweeters all followed and retweeted each other. Those users also seemed to be retweeted automatically by approximately 70 bots. These bots also used the trend-distribution technique, which used all of the trending hashtags at that time within their tweets, not just #PrayforMizzou. Spaced evenly, and with retweets of real people who were observing the Mizzou hashtag, the numbers quickly escalated to thousands of tweets within a few minutes. The plot was smoothly executed and evaded the algorithms Twitter designed to catch bot tweeting, mainly because the Mizzou hashtag was being used outside of that attack. The narrative was set as the trend was hijacked, and the hoax was underway.

The rapidly spreading image of a bruised little boy was generating legitimate outrage across the country and around the world. However, a quick Google image search for "bruised black child" revealed the picture that "Jermaine" attached to the tweet was a picture of an African American child who was beaten by police in Ohio over one year earlier. The image and the narrative were part of a larger plot to spread fear and distrust. It worked.

The University of Missouri student body president tweeted a warning to stay off the streets and lock doors because "KKK members were confirmed on campus." National news networks broke their coverage to get a local feed from camera crews roaming Columbia and the campus looking for signs of violence. As journalists continued to search for signs of Klan members, anchors read tweets describing shootings, stabbings, and cross burnings. In the end, the stories were all false.

Shortly after the disinformation campaign at Mizzou, @Fanfan1911 changed his display name from Jermaine to "FanFan" and the profile picture of a young black male changed to the image of a German iron cross. The next few months, FanFan's tweets were all in German and consisted of spreading rumors about Syrian refugees. Russian active measures in Europe around this time were widely reported, and the account that previously tweeted disinformation regarding Mizzou now focused on messages that were anti-Islamic, anti–European Union, and anti-German Chancellor Angela Merkel. His tweets reached a crescendo after reports of women being raped on New Year's Eve 2016. Some of the reports were false, including a high-profile case of a 13-year-old ethnic-Russian girl living in Berlin who falsely claimed that she was abducted and raped by refugees.[46] Once again, Russian propaganda dominated the narrative.[47] Similar to previous disinformation campaigns on Twitter, the Russians trolls were able to spread the information because of an underlying fear and an existing narrative that they were able to exploit. The trolls used trend-hijacking techniques in concurrence with reporting by Russian state-funded television network Russia Today. To attempt to generate more attention to the Russian anti-Merkel narrative in European media, Russian foreign minister Sergey Lavrov accused German authorities of a "politically correct cover-up" in the case of the Russian teen.[48] Because of the Russian propaganda push, the anti-immigration narrative began spreading across traditional European media.[49] In fact, a magazine in

Poland devoted an entire issue to the topic of Muslim immigration with a disturbing cover photo entitled "Islamic Rape of Europe."[50]

In addition to the German tweets, FanFan began tweeting in English again in the spring of 2016. His tweets and the tweets of other Russian trolls were spreading in America. The narrative they spread was developing a symbiotic relationship with American right-wing news organizations like Breitbart and its followers on social media—a group of true believers in the Russian propaganda narrative.

Additionally, the troll network already seeded various social media platforms with pages designed for spreading disinformation.[51] Seemingly patriotic American Facebook pages linked articles to RT, legitimate American news sources advocating a right-leaning perspective, Breitbart, right-wing conspiracy sites like InfoWars, and non-factual "news" sites like the Conservative Tribune and Gateway Pundit. The Facebook pages also linked to Russia-run sites with nothing but false news stories. Based on anti-Obama sentiment, the Facebook pages were popular among conservative users but not getting broad exposure. Before 2016, Russian active measures were also used in European elections, most notably the "Brexit" campaign. One European expert on Russia quoted in the *Atlantic* article "War Goes Viral" summarized Putin's intent as "not to make you love Putin"; instead "the aim is to make you disbelieve anything. A disbelieving, fragile, unconscious audience is much easier to manipulate."[52] Active measures enable manipulation. Smearing political candidates, hacking, the spread of disinformation, and hoaxes all contribute to a breakdown of public trust in institutions.

As the 2016 US presidential campaign began in earnest, much of the online animosity was now directed at Obama's potential successor: Hillary Clinton. She became a rallying cry for Trump supporters and a force-multiplying tool for the Russian trolls.

Influencing the 2016 Presidential Election

According to the Office of Director of National Intelligence (ODNI) Report on Russian Influence during the 2016 presidential election, "Moscow's influence campaign followed a messaging strategy that blends covert intelligence operations—such as cyber activity—with overt efforts by Russian Government agencies, state funded media, third-party intermediaries, and paid social media users, or 'trolls.' "[53] In the case of the 2016 election, Russian propaganda easily meshed with right-wing

networks known as the "alt-right" and also with supporters of Senator Bernie Sanders in the left wing of the Democratic Party. Hillary Clinton had been a target of conservative groups since she first came into the national spotlight as first lady in the 1990s.[54] Thus, groups on the left and right presented strong opposition to her candidacy in 2016, which meant Russian trolls already had a narrative to build upon and a network of true believers on social media to spread their propaganda.

In a September 2016 speech, Clinton described half of candidate Trump's supporters as "deplorables." She went on to say that the other half of Trump's supporters were just people who felt the system had left them behind, who needed support and empathy. Clearly, she was not referring to all of Trump's supporters as deplorable, but the narrative quickly changed after social media users began referring to themselves as "Deplorable" in their screen names.

Before the "basket of deplorables" comment, the trolls primarily used an algorithm to rapidly respond to a tweet from Donald Trump. Those tweets were prominently displayed directly under Trump's tweet if a user clicked on the original. Those users became powerful voices with large followings; Trump himself frequently retweeted many of those users.[55] However, after the Clinton speech, a "people search" on Twitter for "deplorable" was all one needed to suddenly gain a network of followers numbering between 3,000 and 70,000. Once again, FanFan's name changed—this time to "Deplorable Lucy"—and the profile picture became a white, middle-aged female with a Trump logo at the bottom of the picture. The FanFan follower count went from just over 1,000 to 11,000 within a few days. His original network from the Mizzou and European campaigns changed as well: tracing his follower trail again led to the same groups of people in the same network, and they were all now defined by the "Deplorable" brand. In short, they were now completely in unison with a vast network of other Russian trolls, actual American citizens, and bot accounts from both countries on Twitter. With a large network consisting of Russian trolls, true believers, and bots, it suddenly became easier to get topics trending with a barrage of tweets. The Russian trolls could employ the previously used tactics of bot tweets and hashtag hijacking, but now they had the capability to create trends.

Besides creating trends, the trolls could relay strategy under the radar using Twitter. That is to say, a message could be delivered in the form of a picture that did not include any words. The lack of words would

spread the message to the followers in a timeline, but retweets would not develop any trends—only that network of followers or someone actively observing the network saw the messages. Often, anonymous users discussed the tactics behind the trend creation on the social media site 4Chan or on the bulletin board called "/pol/" and subsequently coordinated the trend within the Deplorable Network on Twitter. The most effective trends derived from this strategy came in the days following the release of the "Access Hollywood" tape from 2005 in which Trump had made vulgar remarks.[56] The Deplorable Network distributed the corresponding strategy throughout the network to drown out negative attention to Trump on Twitter. Coinciding with the implementation of the strategy to mask anti-Trump comments on Twitter, WikiLeaks began releasing Clinton campaign chairman John Podesta's stolen emails.[57] The emails themselves revealed nothing truly controversial, but the narrative that the trending hashtag created was powerful. First, the issue of hacked emails developed into a narrative conflating Podesta's emails to the issue of Clinton's use of a private email server while she was secretary of state. The Clinton server was likely never hacked, but the problem of email loomed over her candidacy.

Secondly, the Podesta email narrative took routine issues and made them seem scandalous. The most common theme: bring discredit to the mainstream media. Podesta, like any campaign manager in modern politics, communicated with members of the press. Emails communicating with reporters were distributed via trending tweets with links to fake news websites. The fake news distorted the stolen emails into conspiracies of media "rigging" of the election to support Hillary Clinton. The corruption narrative also plagued the Democratic National Committee (DNC), which experienced a hack earlier in the year, by Russian sources and revealed by WikiLeaks.[58]

A month after the election, a man drove from his home in North Carolina to Washington, DC, to uncover the truth behind another news story he read online. He arrived at Comet Ping-Pong, a pizza restaurant, with an AR-15, prepared to free children from an underground child sex trafficking ring in the restaurant. After searching the store, he found no children. The story was a hoax. One of the emails stolen from John Podesta was an invitation to a party at the home of a friend that promised good pizza from Comet Ping Pong and a pool to entertain the kids. Fake news sites reported the email as code for a pedophilic sex party; it

was widely distributed via the trending #PodestaEmail hashtag and an associated new hashtag, #PizzaGate.

The #PizzaGate hoax, along with all of the other false and quasi-false narratives, became common within right-wing media as another indication of the immorality of Clinton and her staff. Often, the mainstream media would latch onto a story with unsavory backgrounds and false pretenses, thus giving more credibility to all of the fake news; however, the narrative from the #PizzaGate hoax followed the common propaganda narrative that the media was trying to cover up the truth and that the government failed to investigate the crimes. Ultimately, that is what drove the man to inquire into the fake news for himself.[59]

Finally, the stolen emails went beyond sharing on social media. The trend became so sensational that traditional media outlets chose to cover the Podesta email story, which gave credibility to the fake news and the associated online conspiracy theories promulgated by the Deplorable Network. The WikiLeaks release of the Podesta emails was the peak of Russian command of the trend during the 2016 election. Nearly every day #PodestaEmail trended as a new batch of supposedly scandalous hacked emails made their way into the mainstream press.

By analyzing the followers of a suspected Russian troll, a picture emerges regarding the structure of the network that was active during the 2016 election. The core group in the Deplorable Network consisted of Russian trolls and popular American right-wing accounts like Jack Posobiec, Mike Cernovich, and InfoWars editor Paul Joseph Watson. The Network also consisted of two bot accounts while the remaining nodes are individual accounts likely consisting of human-managed accounts. In total, the Deplorable Network was approximately 200,000 Twitter accounts consisting of Russian trolls, true believers, and bots. Based on my analysis, the bot network appeared to be between 16,000 and 34,000 accounts.[60] The cohesiveness of the group indicates how a coordinated effort can create a trend in a way that a less cohesive network could not accomplish. To conduct cyberattacks using social media as information warfare, an organization must have a vast network of bot accounts to take command of the trend. With unknown factors like the impact of fake news, the true results of the Russian influence operation will likely never be known. As Ellul said, experiments undertaken to gauge the effectiveness of propaganda will never work because the tests "cannot reproduce the real propaganda situation."[61] The concept itself

is marred by the fact that much of the social media support Trump received was through real American true believers tweeting. However, two numbers will stand out from the 2016 election: 2.8 million and 80,000. Hillary Clinton won the popular vote by 2.8 million votes, and Donald Trump won the electoral vote via a combination of just over 80,000 votes in three key states. One could easily make the case—as many on the left have done—that Clinton lost because of the Russian influence.[62] Conversely, one could also argue she was destined to lose because of a botched campaign combined with a growing sense of disenchantment with the American political system. However, one cannot dispute the fact that Russia launched a massive cyberwarfare campaign to influence the 2016 presidential election.[63]

For the most part, the Russian trolls became savvier with their techniques as they adapted to the influence operation in the United States. However, some users, like FanFan, were sloppy with their tradecraft and were obvious to anyone monitoring. The trolls were occasionally sloppy with their IP address locations as well. Following the first presidential debate, the #TrumpWon hashtag quickly became the number one trend globally. Using the TrendMap application, one quickly noticed that the worldwide hashtag seemed to originate in Saint Petersburg, Russia. Russian trolls gave obvious support to Donald Trump and proved that using social media could create chaos on a massive scale, discredit any politician, and divide American society.

Adrian Chen, the *New York Times* reporter who originally uncovered the troll network in Saint Petersburg in 2015, went back to Russia in the summer of 2016. Russian activists he interviewed claimed that the purpose of the trolls "was not to brainwash readers, but to overwhelm social media with a flood of fake content, seeding doubt and paranoia, and destroying the possibility of using the Internet as a democratic space."[64] The troll farm used similar techniques to drown out anti-Putin trends on Russian social media in addition to pumping out disinformation to the United States.

A Congressional Research Service Study summarized the Russian troll operation succinctly in a January 2017 report: "Cyber tools were also used [by Russia] to create psychological effects in the American population. The likely collateral effects of these activities include compromising the fidelity of information, sowing discord and doubt in the

American public about the validity of intelligence community reports, and prompting questions about the democratic process itself."[65]

For Russia, information warfare is a specialized type of war, and modern tools make social media the weapon. According to a former Obama administration senior official, Russians regard the information sphere as a domain of warfare on a sliding scale of conflict that always exists between the US and Russia.[66] This perspective was on display during a Russian national security conference "Infoforum 2016." Andrey Krutskih, a senior Kremlin advisor, compared Russia's information warfare to a nuclear bomb, which would "allow Russia to talk to Americans as equals," in the same way that Soviet testing of the atomic bomb did in 1949.[67]

Table 3. Russia case study analysis in 2016 election

Types	Examples
Propaganda narratives	• Anything discrediting to Hillary Clinton • News media hides information • Politicians are rigging the system • Global elite trying to destroy the world • Globalism is taking jobs and destroying cultures • Refugees are terrorists • Russian foreign policy is strong on antiterrorism • Democrats and some Republicans want WWIII with Russia
True believers	Alt-right, some Bernie Sanders supporters, followers of InfoWars and Breitbart, 4Chan and /pol/ users.
Cyber warriors	Hackers and professional trolls
Bot network	Large, sophisticated network that leveraged cyber warriors and true believer accounts to create the "Deplorable Network."

From 2015 to 2016, Russian trolling modus operandi took a logical path from small stories designed to create panic and sow seeds of doubt to a social media machine that IS could only imagine. In warfare strategy, narrative manipulation through social media cyber operations is the current embodiment of taking the fight directly to the people. The 2016 election proved that using social media to influence political outcomes, as opposed to violence or Cold War–like posturing, is a highly effective strategy in modern information warfare—a strategy that will likely continue as technology continues to develop and adapt to the ever-growing social media landscape as more actors gain the ability to take command of the trend.

The Future of Weaponized Social Media

Smear campaigns have been around since the beginning of politics, but this article illustrated novel techniques recently employed by a terrorist group and foreign state actor, with each attack gaining popularity and credibility after trending on Twitter. The attacks, often under the guise of a "whistleblower" campaign, make routine political actions seem scandalous. Additionally, WikiLeaks advertises that it has never published anything requiring retraction because everything it posts is supposedly authentic stolen material. Just like the Podesta email releases, several politicians and business leaders around the world have fallen victim to this type of attack.

Recall the 2015 North Korean hacking of Sony Studios. Lost in the explosive nature of the hacking story is that the fallout at the company was not because of the hacking itself but from the release of embarrassing emails from Sony senior management, as well as the salaries of every employee at Sony. The uproar over the content of the emails dominated social media, often fed by salacious stories like the RT headline: "Leaked Sony emails exhibit wealthy elite's maneuvering to get child into Ivy League school." Ultimately, Sony fired a senior executive because of the content of her emails.[68]

In another example from May 2017, nine gigabytes of email stolen from French presidential candidate Emmanuel Macron's campaign were released online and verified by WikiLeaks. Subsequently, the hashtag #MacronLeaks trended to number one worldwide. It was an influence operation resembling the #PodestaEmail campaign with a supporting cast of some of the same actors. During the weeks preceding the French election, many accounts within the Deplorable Network changed their names to support Macron's opponent, Marine LePen. These accounts mostly tweet in English and still engage in American political topics as well as French issues.[69] Some of the accounts also tweet in French, and a new network of French-tweeting bot accounts uses the same methods as the Deplorable Network to take command of the trend.

In his book *Out of the Mountains*, David Kilcullen describes a future comprising large, coastal urban areas filled with potential threats, all connected.[70] The implications of his prediction are twofold. First, networks of malicious nonstate actors can band together to hijack social media using a template similar to IS. Although these groups may not have the power to create global trends, they can certainly create chaos

with smaller numbers by hijacking trends and creating local trends. With minimal resources, a small group can create a bot network to amplify its message. Second, scores of people with exposure to social media are vulnerable to online propaganda efforts. In this regard, state actors can use the Russian playbook.

Russia will likely continue to dominate this new battlespace. It has intelligence assets, hackers, cyber warrior trolls, massive bot networks, state-owned news networks with global reach, and established networks within the countries Russia seeks to attack via social media. Most importantly, the Russians have a history of spreading propaganda. After the 2016 elections in the United States, Russian trolls again worked toward influencing European elections. Currently, Russian trolls are active in France, the Balkans, and the Czech Republic using active measures and coercive social media messages.[71] It is clear that other countries are attempting to build capabilities to match the Russian cyber troll influence.

Already, Turkey, Iran, and Venezuela are noted as having bot networks and cyber warriors similar to Russian trolls.[72] With these other states, a popular use for the trolls in the social media battlespace is to stoke nationalism and control the narrative within their own borders. For example, the fake Twitter followers of Venezuelan president Nicolás Maduro number so many that he is now the "third-most-retweeted public figure in the world, behind only the king of Saudi Arabia and the pope."[73]

With a large enough bot network, states can also control messages outside of social media using similar techniques. Manipulating search engines is called "search engine optimization," which uses bot accounts to increase the number of clicks to a particular web page after performing a search. The search engine algorithm then prioritizes that page in response to subsequent searches using the same keyword. A Google search for "ODNI Report" is illustrative: in March 2017, the top Google results were RT articles lambasting the intelligence assessment that named the Russian government as the perpetrators behind the 2016 election interference.

Techniques like search engine optimization and command of the trend will become common in future wars to sow discord and spread false information, with the aim of causing the other side to change its course of action. These online weapons should frighten every leader in a democracy. Perhaps most frightening is the Oxford Internet Institute Unit for Propaganda discovery that "hundreds of thousands of 'sleeper bots' exist

on Twitter."[74] These bots are accounts that are active but have not yet started tweeting. Researchers do not know who owns the accounts or what will trigger them. The ease of use and large numbers of active bots and sleeper bots indicate a high likelihood of social media continuing to be used for propaganda, especially as more and more state and nonstate organizations realize the impact they can make on an adversary.

Thus far, the United States response has been relatively weak. For one, the US government does not prioritize information operations the way it once did during the Cold War. When President Eisenhower started the United States Information Agency (USIA), the objective was to compete with Soviet propaganda around the world. The mission statement of USIA clarified its role: "The purpose of the United States Information Agency shall be to submit evidence to peoples of other nations by means of communication techniques that the objectives and policies of the United States are in harmony with and will advance their legitimate aspirations for freedom, progress, and peace."[75]

Knowing what we know now about Russian disinformation active measures, USIA was never truly equipped to fight an information war. The agency became a public diplomacy platform with a positive message rather than a Soviet-style campaign of negative smear tactics. Accordingly, several questions arose: should USIA spread propaganda? Should it seek out and attempt to remove negative publicity about the US? Should it slander opponents? Most importantly: should it do any or all of these things when the American public could be influenced by a message intended for an international audience?[76]

Those problems persist today because the government lacks a centralized information authority since the mission of USIA was relegated to the Department of State. Several failed attempts to counter IS on Twitter show the US government's weakness when trying to use social media as a weapon. One example is the Center for Strategic Counterterrorism Communications, created in 2010, which started the program "Think Again, Turn Away." The State department awarded a $575,046 contract to a Virginia-based consulting firm to manage the project.[77] The intent was to curb the appeal of IS by creating a counternarrative to the IS message on social media. Unfortunately, the Twitter campaign had undesirable consequences after the account sent tweets arguing the finer points of the Islamic faith with IS sympathizers. Rita Katz best summarized the failure: "In order to counter a problem, one must first study it

before adopting a solution. Had the people behind 'Think Again, Turn Away' understood jihadists' mindsets and reasons for their behavior, they would have known that their project of counter-messaging would not only be a waste of taxpayer money but ultimately be counterproductive."[78]

In the end, the "Think Again, Turn Away" campaign was almost comical as it could not communicate effectively with any audience and severely discounted the importance of its message. Jacques Ellul noted that democracies were prone to having problems with outward communication through propaganda. Because democracies rely on presenting an image of fairness and truth, "propaganda made by democracies is ineffective, paralyzed, mediocre."[79] The United States was ill equipped to combat Soviet active measures during the Cold War, and it remains unable to compete using social media as an influence operation.

Unfortunately, countering Russian influence operations has taken a partisan slant within the United States. Many downplay the Russian role in the 2016 election while others appear to be so blinded by the Russian operation that they cannot see the underlying conditions that allowed for the spread of that narrative in the first place.[80] With the two parties unable to reach a consensus on what happened or the impact of the operation, they fail to realize that as technology improves and proliferates around the world, disinformation campaigns and influence operations will become the norm. The attack in a future information war could be toward either political party and come from any of the several countries attempting to build an online army in the mold of Russia's trolls and bot network.

Conclusion

In the 1987 book *Truth Twisters*, Richard Deacon laments the future of independent thinking, as computers "could become the most dangerous hypnotic influence in the future. . . . [T]he effect of a reliance on computerology, of allowing oneself to be manipulated and controlled by it, is certainly hypnotic in that the mind allows itself to accept whatever the computer tells it."[81] He believed that such technology could lead one to commit treason without realizing any manipulation. Propaganda is a powerful tool, and, used effectively, it has been proven to manipulate populations on a massive scale. Using social media to take command of the trend makes the spread of propaganda easier than ever before for both state and nonstate actors.

Fortunately, social media companies are taking steps to combat malicious use. Facebook has been at the forefront of tech companies taking action to increase awareness of fake news and provide a process for removing the links from the website.[82] Also, although Facebook trends are less important to information warfare than Twitter trends, the website has taken measures to ensure that humans are involved in making the trends list. Furthermore, Twitter has started discreetly removing unsavory trends within minutes of their rise in popularity. However, adversaries adapt, and Twitter trolls have attempted to regain command of the trend by misspelling a previous trend once it is taken out of circulation. Still, even if the misspelled word regains a spot on the trend list, the message is diminished.

The measures enacted by Facebook and Twitter are important for preventing future wars in the information domain. However, Twitter will also continue to have problems with trend hijacking and bot networks. As demonstrated by #PrayforMizzou and #WorldCup2014, real events happening around the world will maintain popularity as well-intending users want to talk about the issues. In reality, removing the trends function could end the use of social media as a weapon, but doing so could also devalue the usability of Twitter. Rooting out bot accounts would have an equal effect since that would nearly eliminate the possibility of trend creation. Unfortunately, that would have an adverse impact on advertising firms that rely on Twitter to generate revenue for their products.

With social media companies balancing the interests of their businesses and the betterment of society, other institutions must respond to the malicious use of social media. In particular, the credibility of our press has been put into question by social media influence campaigns—those groups should respond accordingly. For instance, news outlets should adopt social media policies for their employees that encourage the use of social media but discourage them from relying on Twitter as a source. This will require a culture shift within the press and fortunately has gathered significant attention at universities researching the media's role in the influence operation. It is worth noting that the French press did not cover the content of the Macron leaks; instead, the journalists covered the hacking and influence operation without giving any credibility to the leaked information.

Finally, our elected officials must move past the partisan divide of Russian influence in the 2016 election. This involves two things: first, both parties must recognize what happened—neither minimizing nor overplaying Russian active measures. Second, and most importantly, politicians must commit to not using active measures to their benefit. Certainly, the appeal of free negative advertising will make any politician think twice about using disinformation, but the reality of a foreign influence operation damages more than just the other party, it damages our democratic ideals. Senator John McCain summarized this sentiment well at a CNN Town Hall: "Have no doubt, what the Russians tried to do to our election could have destroyed democracy. That's why we've got to pay . . . a lot more attention to the Russians."[83]

This was not the cyber war we were promised. Predictions of a catastrophic cyberattack dominated policy discussion, but few realized that social media could be used as a weapon against the minds of the population. IS and Russia are models for this future war that uses social media to directly influence people. As technology improves, techniques are refined, and internet connectivity continues to proliferate around the world, this saying will ring true: He who controls the trend will control the narrative—and, ultimately, the narrative controls the will of the people. SSQ

Notes

1. Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.," *New York Times*, 11 October 2012, http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?mcubz=0/.

2. Jeremy Scott-Joynt, "What Myspace Means to Murdoch," BBC News Analysis, 19 July 2005, http://news.bbc.co.uk/2/hi/business/4697671.stm.

3. Sitaram Asur, Bernardo A. Huberman, Gabor Szabo, and Chunyan Wang, "Trends in Social Media: Persistence and Decay" (unpublished manuscript, submitted to Cornell University Library arXiv 7 February 2011), 1, https://arxiv.org/abs/1102.1402?context=physics.

4. "Blog" is short for "web log." A blog is a way to share your thoughts via the internet. A microblog is a blog with a character limit to the text.

5. Rani Molla, "Social Studies: Twitter vs. Facebook," *Bloomberg Gadfly*, 12 February 2016, https://www.bloomberg.com/gadfly/articles/2016-02-12/social-studies-comparing-twitter-with-facebook-in-charts.

6. Carole Cadwalladr, "Robert Mercer: The Big Data Billionaire Waging War on the Mainstream Media," *Guardian*, 26 February 2017, https://www.theguardian.com/politics/2017/feb/26/robert-mercer-breitbart-war-on-media-steve-bannon-donald-trump-nigel-farage.

7. Gabriel Weimann, *Terrorism in Cyberspace: The Next Generation* (Washington, DC: Woodrow Wilson Center Press, 2015), 138.

8. Alex Lubben, "Twitter's Users Are 15 Percent Robot, but That's Not Necessarily a Bad Thing," VICE News, 12 March 2017, https://news.vice.com/story/twitters-users-are-15-percent-robot-but-thats-not-necessarily-a-bad-thing.

9. Jacques Ellul, *Propaganda: The Formation of Men's Attitudes* (New York: Knopf, 1965), 6.

10. Eric Hoffer, *The True Believer: Thoughts on the Nature of Mass Movements* (New York: Harper and Row, 1951), 105.

11. Thomas Rid, *Cyber War Will Not Take Place* (New York: Oxford University Press, 2013), 132.

12. Ellul, 85.

13. Daniel Kahneman, *Thinking, Fast and Slow* (New York: Farrar, Straus and Giroux, 2011), 87.

14. Christopher Paul and Miriam Matthews, *The Russian "Firehose of Falsehood" Propaganda Model*, RAND Report PE-198-OSD (Santa Monica, CA: RAND, 2016), 4, https://www.rand.org/pubs/perspectives/PE198.html.

15. Garth Jowett and Victoria O'Donnell, *Propaganda & Persuasion*, 5th ed. (Thousand Oaks, CA: SAGE, 2012), 159.

16. Katerina Eva Matsa and Kristine Lu, "10 Facts about the Changing Digital News Landscape," Pew Research Center, 14 September 2016, http://www.pewresearch.org/fact-tank/2016/09/14/facts-about-the-changing-digital-news-landscape/.

17. Jowett and O'Donnell, *Propaganda & Persuasion*, 300.

18. Tom Hashemi, "The Business of Ideas Is in Trouble: Re-injecting Facts into a Post-truth World," *War on the Rocks*, 9 December 2016, https://warontherocks.com/2016/12/the-business-of-ideas-is-in-trouble-re-injecting-facts-into-a-post-truth-world/.

19. Asur, Huberman, Szabo, and Wang, "Trends in Social Media," 1.

20. *Merriam-Webster Dictionary Online*, s.v. "lede," accessed 10 October 2017, https://www.merriam-webster.com/dictionary/lede. "The introductory section of a news story that is intended to entice the reader to read the full story."

21. Tess Townsend, "The Bizarre Truth behind the Biggest Pro-Trump Facebook Hoaxes," Inc.com, 21 November 2016, https://www.inc.com/tess-townsend/ending-fed-trump-facebook.html.

22. Craig Silverman, "This Analysis Shows How Viral Fake Election News Stories Outperformed Real News on Facebook," BuzzFeed News, 16 November 2016, https://www.buzzfeed.com/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook?utm_term=.qwWdA0G8G#.fcEv1Qono.

23. Art Swift, "Americans' Trust in Mass Media Sinks to New Low," Gallup, 14 September 2016, http://news.gallup.com/poll/195542/americans-trust-mass-media-sinks-new-low.aspx.

24. Andrea Peterson, "Three Charts that Explain how U.S. Journalists Use Social Media," *Washington Post*, 6 May 2014, https://www.washingtonpost.com/news/the-switch/wp/2014/05/06/three-charts-that-explain-how-u-s-journalists-use-social-media/?utm_term=.9cdd82cb8fa7.

25. Weimann, *Terrorism in Cyberspace*, 138.

26. Audrey Kurth Cronin, "ISIS Is Not a Terrorist Group," *Foreign Policy* (March/April 2015), https://www.foreignaffairs.com/articles/middle-east/isis-not-terrorist-group.

27. Stephen M. Walt, "ISIS as Revolutionary State," *Foreign Policy* (November/December 2015): 42, https://www.belfercenter.org/publication/isis-revolutionary-state.

28. Caliphate is defined as "a form of Islamic government led by a—a person considered a political and religious successor to the Islamic prophet, Muhammad, and a leader of the entire Muslim community. Source: Wadad Kadi and Aram A. Shahin, "Caliph, caliphate," in *The Princeton Encyclopedia of Islamic Political Thought*, ed. Gerhard Bowering, Patricia Crone, Wadad

Kadi, Devin J. Stewart, Muhammad Qasim Zaman, and Mahan Mirza (Princeton, NJ: Princeton University Press, 2013), 81–86, http://www.jstor.org/stable/j.ctt1r2g6m.8.

29. Graeme Wood, "What ISIS Really Wants," *Atlantic*, March 2015, 3, https://www.theatlantic.com/magazine/archive/2015/03/what-isis-really-wants/384980/.

30. Dabiq is also the name of the ISIS magazine, which is available electronically and spread via social media.

31. Walt, "ISIS as Revolutionary State," 43.

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

33. Ibid.

34. "Terrorist Use of Social Media: Policy and Legal Challenges," roundtable forum (Washington, DC: Council on Foreign Relations, 14 October 2015).

35. Berger, "How ISIS Games Twitter."

36. Carleton English, "Twitter Continues to Wage its Own War against ISIS," *New York Post*, 21 March 2017, http://nypost.com/2017/03/21/twitter-continues-to-wage-its-own-war-against-isis/.

37. United States Department of State, report, *Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986–87* (Washington, DC: Bureau of Public Affairs, 1987), viii.

38. Natasha Bertrand, "It Looks Like Russia Hired Internet Trolls to Pose as Pro-Trump Americans," *Business Insider*, 27 July 2016, http://www.businessinsider.com/russia-internet-trolls-and-donald-trump-2016-7.

39. Vladimir Isachenkov, "Russia Military Acknowledges New Branch: Info Warfare Troops," AP News, 22 February 2017, https://www.apnews.com/8b7532462dd0495d9f756c9ae7d2ff3c.

40. Richard Gonzalez, "CIA Director Pompeo Denounces WikiLeaks as 'Hostile Intelligence Service,'" NPR, 23 April 2017, http://www.npr.org/sections/thetwo-way/2017/04/13/523849965/cia-director-pompeo-denounces-wikileaks-as-hostile-intelligence-service.

41. Malcolm Nance, *The Plot to Hack America: How Putin's Cyberspies and WikiLeaks Tried to Steal the 2016 Election* (New York: Skyhorse Publishing, 2016), Kindle edition, 1,839.

42. Adrian Chen, "The Agency," *New York Times Magazine*, 2 June 2015, https://www.nytimes.com/2015/06/07/magazine/the-agency.html. On 11 September 2014, the small town of St. Mary Parish, Louisiana, was thrown briefly into a panic when residents began hearing reports through text, social media, and on local television stations that a nearby chemical plant fire was spreading toxic fumes that would soon endanger the whole town. The entire narrative was based on falsified—but very real looking—online news stories, hashtag manipulation, and mass texts (SMS) to various numbers with the local area code and dialing prefix. The actual source for the news was not the chemical factory; it was a nondescript building in St. Petersburg, Russia, where an army of online cyber-warrior trolls seeks to distribute false information.

43. Statement of Clint Watts, Foreign Policy Research Institute fellow, in "Disinformation: A Primer in Russian Active Measures and Influence Campaigns," testimony before the Senate Intelligence Committee, 115th Cong., 1st sess., 30 March 2017, https://www.intelligence.senate.gov/sites/default/files/documents/os-cwatts-033017.pdf.

44. Chen, "The Agency."

45. Because of the Adrian Chen article, I observed particular tweeting patterns of certain individuals involved in a hoax on the campus of the University of Missouri that seemed to match the methods of the Russian trolls interviewed by Chen. I mention only one particular user in this article, but I also monitored a dozen or so accounts that contributed to that hoax. Each account followed a pattern that also happened to align with noted Russian influence operations in Europe and eventually in the US presidential election. I describe that transition in the article. From those accounts, I built a database of suspected Russian bot accounts to build a network map. The

Mizzou hoax was a trend hijacking effort launched by actors who later proved to match the Russian modus operandi of using cyber trolls originally observed by Adrian Chen and confirmed by the Office of the Director of National Intelligence (ODNI) report and Foreign Policy Research Institute fellow Clint Watts in his testimony before the Senate Intelligence Committee (note 43).

46. Nadine Schmidt and Tim Hume, "Berlin Teen Admits Fabricating Migrant Gang-Rape Story, Official Says," CNN, 1 February 2016, http://www.cnn.com/2016/02/01/europe/germany-teen-migrant-rape-false/index.html.

47. Judy Dempsey, "Russia's Manipulation of Germany's Refugee Problems," Carnegie Europe, 28 January 2016, http://carnegieeurope.eu/strategiceurope/?fa=62611.

48. Schmidt and Hume, "Berlin Teen Admits Fabricating Migrant Gang-Rape Story."

49. Barbara Tasch, "'The Aim Is to Weaken the West': The Inside Story of How Russian Propagandists Are Waging War on Europe," *Business Insider*, 2 February 2017, http://www.businessinsider.com/russia-propaganda-campaign-weakening-europe-2017-1?r=UK&IR=T.

50. Harriet Sherwood, "Polish Magazine's 'Islamic Rape of Europe' Cover Sparks Outrage," 18 February 2016, https://www.theguardian.com/world/2016/feb/18/polish-magazines-islamic-of-europe-cover-sparks-outrage.

51. Chen, "The Agency."

52. Robinson Meyer, "War Goes Viral: How Social Media Is Being Weaponized across the World," *Atlantic*, 18 October 2016, https://www.theatlantic.com/magazine/archive/2016/11/war-goes-viral/501125/.

53. Office of the Director of National Intelligence (ODNI), Intelligence Community Assessment Report, *Assessing Russian Activities and Intentions in Recent US Elections*, 6 January 2017, ii, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

54. Hanna Rosin, "Among the Hillary Haters," *Atlantic*, 1 March 2015, 63, https://www.theatlantic.com/magazine/archive/2015/03/among-the-hillary-haters/384976/.

55. K. Thor Jensen, "Inside Donald Trump's Twitter-Bot Fan Club," *New York Magazine*, 15 June 2016, http://nymag.com/selectall/2016/06/inside-donald-trumps-twitter-bot-fan-club.html.

56. David A. Farenthold, "Trump Recorded Having Extremely Lewd Conversation about Women in 2005," *Washington Post*, 8 October 2016, https://www.washingtonpost.com/politics/trump-recorded-having-extremely-lewd-conversation-about-women-in-2005/2016/10/07/3b9ce776-8cb4-11e6-bf8a-3d26847eeed4_story.html.

57. "The Podesta Emails," Politico LiveBlog, accessed 6 December 2016, http://www.politico.com/live-blog-updates/2016/10/john-podesta-hillary-clinton-emails-wikileaks-000011.

58. ODNI Report, 2.

59. Faiz Siddiqui and Susan Svrluga, "N.C. Man Told Police He Went to D.C. Pizzeria with Gun to Investigate Conspiracy Theory," *Washington Post*, 5 December 2017, https://www.washingtonpost.com/news/local/wp/2016/12/04/d-c-police-respond-to-report-of-a-man-with-a-gun-at-comet-ping-pong-restaurant/?utm_term=.c33057f66007.

60. This count is based on analysis of the followers of followers of suspected troll accounts and bots. The study was conducted 15 March 2016. The number of accounts appears to have reduced dramatically since May, following the French election, implying that Twitter suspended some of the accounts. Unfortunately, software limitations prevent this analysis from being more accurate. Additionally, it is nearly impossible to derive the exact number of Russian accounts from that network using my available resources.

61. Ellul, *Propaganda*, 6.

62. Many on the left have mischaracterized the attack as "Russian hacking of the election," which has in turn conflated the issue of the John Podesta email theft with a hacking of the

actual election systems. To be clear: there is no evidence of any sort of hack on any ballot-counting systems, only evidence outlined in this paper of two hacks (Democratic National Committee and Podesta) combined with an influence/information operation.

63. ODNI Report, 1.

64. Adrian Chen, "The Real Paranoia-Inducing Purpose of Russian Hacks," *New Yorker*, 27 July 2016, https://www.newyorker.com/news/news-desk/the-real-paranoia-inducing-purpose-of-russian-hacks.

65. Catherine Theohary and Cory Welt, "Russia and the U.S. Presidential Election," CRS Report no. IN10635 (Washington, DC: Congressional Research Service, 2017).

66. David Ignatius, "Russia's Radical New Strategy for Information Warfare," *Washington Post*, 18 January 2017, https://www.washingtonpost.com/blogs/post-partisan/wp/2017/01/18/russias-radical-new-strategy-for-information-warfare/?utm_term=.da53e31d7aaa.

67. Ibid.

68. "Ex-Sony Chief Amy Pascal Acknowledges She Was Fired," NBCNews.com, 12 February 2015, https://www.nbcnews.com/storyline/sony-hack/ex-sony-chief-amy-pascal-acknowledges-she-was-fired-n305281.

69. The political left in the United States seems to have a large group of bot accounts forming around the "Resist" movement. It is unclear whether those accounts are foreign cyber warriors or bots, but external actors can certainly feed off the underlying narratives and tap into existing networks of true believers.

70. David Kilcullen, *Out of the Mountains: The Coming Age of the Urban Guerrilla* (New York: Oxford University Press, 2013), 231.

71. Anthony Faiola, "As Cold War Turns to Information War, a New Fake News Police Combats Disinformation," *Washington Post*, 22 January 2017, 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?utm_term=.7c99cc2fadd5.

72. Meyer, "War Goes Viral."

73. Ibid.

74. Cadwalladr, "Robert Mercer: The Big Data," 1.8.

75. Malcolm Mitchell, *Propaganda, Polls, and Public Opinion: Are the People Manipulated?* (Englewood Cliffs, NJ: Prentice-Hall, 1977), 12.

76. Ibid., 13.

77. Rebecca Carroll, "The State Department Is Fighting with ISIL on Twitter." Defense One, 25 June 2014, http://www.defenseone.com/technology/2014/06/state-department-fighting-isil-twitter/87286/.

78. Rita Katz, "The State Department's Twitter War with ISIS Is Embarrassing," *Time*, 16 September 2014, http://time.com/3387065/isis-twitter-war-state-department/.

79. Ellul, *Propaganda*, 241.

80. Adrian Chen, "The Propaganda about Russian Propaganda," *New Yorker*, 1 December 2016, https://www.newyorker.com/news/news-desk/the-propaganda-about-russian-propaganda.

81. Richard Deacon, *The Truth Twisters* (London: Macdonald, 1987), 95.

82. Michelle Castillo, "Facebook Found Fake Accounts Leaking Stolen Info to Sway Presidential Election," CNBC.com, 27 April 2017, https://www.cnbc.com/2017/04/27/facebook-found-efforts-to-sway-presidential-election-elect-trump.html.

83. Eric Bradner, "At CNN Town Hall, McCain and Graham Give Their View of Trump's Presidency so Far," CNN, 2 March 2017, http://www.cnn.com/2017/03/01/politics/john-mccain-lindsey-graham-town-hall/index.html.