Chapter 7

# Social Media and Influence Operations Technologies

## Implications for Great Power Competition

*By Todd C. Helmus*

*Nation-states have increasingly been waging foreign propaganda campaigns on social media platforms such as Facebook and Twitter. Such campaigns are enticing because they are cheap and easy to execute; they allow planners to identify, target, and reach specific audiences; and the campaign's anonymity limits the associated political and foreign policy risks. Russia, China, and the so-called Islamic State are three key U.S. adversaries that have exploited online technologies for propaganda. This chapter reviews the aims, capabilities, and limitations of online propaganda for each of these entities. The chapter also highlights key recommendations that the United States should adopt in order to counter adversary use of online propaganda.*

As the world has entered a new era of Great Power competition over the past decade, nation-states have been increasingly waging foreign propaganda campaigns on social media platforms such as Facebook and Twitter, effectively turning such platforms into influence operations technologies.[1] A study from the University of Oxford documented that some 70 countries around the world are engaged in manipulating social media to serve domestic and foreign policy ends. This is up from 48 countries in 2018 and 28 countries in 2017. In particular, the study documented foreign propaganda campaigns conducted by Russia, China, India, Iran, Pakistan, Saudi Arabia, and Venezuela.[2]

Why are states increasingly relying on social media as a tool of foreign propaganda? It is cheap and easy to operate and allows campaign planners to identify, target, and reach specific overseas audiences, such as individuals, voter demographics, and ethnic groups. Governments also seek to engage in such campaigns anonymously, thereby limiting the associated political and foreign policy risks. The campaigns can also be conducted at scale, and they can be informed by a wealth of easy-to-access big data on target audiences.

States conduct online propaganda campaigns in a number of ways, including using "bot" and "troll" accounts. Bots are automated social media accounts, often on Twitter, that employ code to replicate human activity to promote a particular message. To enable more sophisticated interactions with other users, bot campaigns employ real people or trolls to monitor and control fake social media accounts. Campaigns employ these types of accounts in numerous ways. They can spread progovernment content, attack adversary positions, distract or divert conversations or criticism away from an issue, promote divisions and polarization, and suppress participation through attacks or harassment.[3]

This chapter offers a look at how three contemporary U.S. adversaries have used and are using online content and platforms to engage in foreign influence campaigns. It focuses on Russia, China, and the so-called Islamic State (IS). The first two are, as defined earlier in this volume, America's modern Great Power rivals. As noted in the 2018 U.S. National Defense Strategy, and discussed in detail in chapter 11, IS remains, despite major recent setbacks, a modern violent extremist organization with global reach and sustained influence that will challenge America into this Great Power era. For each case study, the chapter identifies the adversary's aims and objectives in using online technologies for influence operations and propaganda. It also identifies the capabilities and limitations for using online propaganda. In addition, because online platforms are not the only means of disseminating propaganda, the chapter briefly describes relevant offline mechanisms for influence. The chapter does not explicitly list U.S. Government aims, objectives, capabilities, or limitations for using social media and online technologies for external propaganda, instead offering an implicit assessment of these technologies in the final section on recommendations. This approach for the chapter has been selected in part because of the limited information available in open-source reporting.

## Russia

### Aims and Objectives

In a recent report on hostile social manipulation, RAND political scientist Mike Mazarr and his colleagues identified several key strategic aims for Russian online operations. First, they noted that Russia has long believed it is a target of adverse information operations, and Moscow may use its social manipulation efforts to counter these "disinformation" programs. Second, they noted that Russia uses social manipulation to pursue what it calls "discrete policy objectives" to influence a particular policy debate or foreign policy in order to suit its interests.[4] In addition, they noted that some analysts see an animus to push foreign societies to a "'posttruth' environment—one in which the distinction between fact and falsehood is immaterial, objectivity is unattainable, and reality is malleable."[5]

Diego Martin and Jacob Shapiro offered a glimpse of Russian influence objectives by analyzing a specially created database of influence campaigns waged between 2013 and 2018. The campaigns were waged by Russia, China, Saudi Arabia, and Iran and targeted 14 countries, including the United States, the United Kingdom, Australia, Germany, the Netherlands, and Ukraine.[6] Russia accounted for some 38 of 53 identified influence efforts, highlighting the obvious importance Russia places on this aspect of its foreign policy.

### Capabilities

First, we should note that Russia benefits from a broad set of capabilities for influencing overseas governments and publics. Elizabeth Bodine-Baron and colleagues specifically identified four key categories of capabilities.[7] The first category includes actors that are part of the Russian state, such as the Main Intelligence Unit (*Glavnoye razvedyvatel'noye upravleniye*) or Sputnik online media. Second is the RT international news network, which is a nonprofit news organization that is visibly supported by the Russian state. Third are those actors who knowingly work on behalf of the Russian government but whose connections to the state are concealed. This includes the Internet Research Agency (IRA; also known as the St. Petersburg troll factory) and patriotic Russian hackers and networks run by criminal oligarchs. Last, in the fourth category, are the various proxies and potential proxies. These include those actors who may or may not hold pro-Russian views but are nonetheless motivated to spread messages in line with Russian campaign objectives.

The media and messages produced by these different arms often work together in a seemingly systematic manner. Following the poisoning of former Russian spy Sergei Skripal, various channels, combined with official press statements and Russian bots and trolls, produced "a blizzard of falsehoods" designed to muddy the waters of international investigations and opinion on Russian blame for the assassination.[8]

The most famous example of Russian propaganda stems from its systematic campaign to target the U.S. 2016 election. Russia employed a high-volume array of social media content to include 10.4 million tweets, 1,000 YouTube videos posted on 17 accounts, 116,000 Instagram posts from 133 accounts, and 61,500 unique Facebook posts across 81 pages. These postings yielded 77 million engagements on Facebook, 187 million engagements on Instagram, and 73 million engagements on original Twitter content.

The content sought to promote wide-ranging themes specially targeted at different U.S. demographic groups. Targets included African-American communities to promote black separatism, inflame opinions toward police, and undermine confidence in the electoral system. Content engaged in voter suppression tactics included promoting third-party candidates, encouraging voters to stay home on election day, and creating confusion about voting rules. Beginning in the primaries and continuing through the election, the content promoted pro-Trump operations and countered Hillary Clinton.[9]

Many of these competing themes appeared to promote disunity among the American electorate. Campaigns sought to promote both Black Lives Matter and Blue Lives Matter themes to inflame opinions. Skillful manipulation of social media even proved successful at promoting dual street protests.[10] Other campaigns sought to promote secession by the state of Texas, anti-immigrant causes, gun rights, patriotism, Tea Party culture, and so forth.[11]

Russia has since engaged in a number of other online influence campaigns. For example, Russia supported the Brexit referendum in 2016, heavily promoted Catalonia's independence referendum in 2017, and sought to undermine the presidential election of Emmanuel Macron in France. Statistics tabulated by Martin and Shapiro suggest that Russia engaged in at least 28 campaigns in 2017 and 21 in 2018.[12]

Overall, Russia appears to demonstrate a relatively skilled approach to these information operations. First, we should note that Russia was one of the first countries to recognize the potential value of using social media for Great Power competition, and Russia's efforts to implement social media–based information operations have unfortunately paved the way for other nations, such as Iran and China, to follow suit. Second, by some accounts, Russia implemented the campaign with skill. IRA staffers visited the United States in order to conduct "market research." IRA social media accounts clustered around identity- or issue-based online communities and built sizable audiences—all without tipping off audiences (at least so far) to the Russian origin of the campaigns. Russian accounts were retweeted by political figures and news media. As Tom Uren and colleagues noted, the "IRA campaign displayed a clear understanding of audience segmentation, colloquial language, and the ways in which online communities framed their identities and political stances."[13]

Why is Russia so adept at using social media and other online channels of influence? Some analysts point to a 2013 article published on "ambiguous warfare" by the chief of the Russian general staff and general of the army, Valery Gerasimov, which led to some scholars believing that the Russian information campaigns are the result of an "elaborate strategy" developed and executed by Russian planners.[14] Sergey Sanovich, a researcher at Princeton's Center for Information Technology Policy, alternatively suggests that Russia's online propaganda tools were "conceived and perfected" in the liberal Russian economy and politics of the 1990s. After the 1990s, Russia proved unsuccessful at using its network of bots and trolls to curb domestic online discussions, and the government was unwilling to "ban the platforms outright." Consequently, it then adapted and stepped up its online international influence game.[15]

### Limitations

The Russian campaign may have been skilled, but was it effective? Clearly, audiences have seen and interacted with Russian content. However, clear scientific evidence is lacking on whether such social media campaigns helped Russia meet any particular campaign goals or change audience attitudes, behaviors, or beliefs in the ways that the Russian planners intended.[16]

Interestingly, one study assessed the IRA's impact on political attitudes and behaviors of American Twitter users in late 2017. The study identified users who interacted with IRA content on Twitter and analyzed whether outcomes of six distinctive measures of political attitudes and behavior changed over a 1-month period. The study found no such evidence of change and suggested that the Russian trolls might have failed because they directly targeted those who were already highly polarized in their attitudes and beliefs.[17]

Still, the campaign's ingenuity and scope have garnered it significant attention from politicians, journalists, researchers, and the American public. The social media campaign, combined with other elements of a broader Russian interference campaign—including hacking the Democratic National Committee (DNC) server and the release of DNC emails—has led at least some audiences to question the legitimacy of the 2016 election.[18] Such an outcome may well lead Russian planners and politicians to conclude that the campaign was a success.

One key limitation or challenge for Russia and other disinformation actors is that Facebook, Twitter, and other such platforms are now on the lookout for Russian content. Bots will need to be more sophisticated to overcome the various bot detectors that exist in the market. Russia will no longer be able to pay for advertisements with rubles or post content directly from IRA-affiliated computers.

An arms race will certainly ensue. Russians will likely adapt to any countermeasures Western governments or online platforms put in place. Evidence suggests this is already taking place. Russia has sought to test new disinformation tactics on the African continent. Instead of creating fake Facebook groups from the IRA offices in St. Petersburg, it has rented or purchased accounts already created and cultivated by locals. Russia also has created local media organizations in select African countries that post the content on behalf of Russia. The seemingly authentic nature of the content will make detection more difficult.[19]

## China

### Aims and Objectives

By documenting the expansion of the Communist Party media influence since 2017, analyst Sarah Cook identified several broad and overarching aims of the Chinese Communist Party (CCP) communication and influence strategy. First, she noted the government seeks to “promote a positive view of China and the CCP’s authoritarian regime.” By the same token, it also seeks to “marginalize, demonize, or entirely suppress anti-CCP voices” and other information that might cast a negative light on its government or leaders. China also seeks to promote nationalistic sentiment at home and abroad, promote the reunification of Taiwan with the mainland, and quell the protests in Hong Kong.[20]

### Capabilities

China has gained a strong reputation for effectively stifling and influencing online debate within its borders, and it has fostered a number of seemingly effective offline tools for international influence. However, China’s ability to use online tools to influence international policy and opinion remains in a relatively nascent state.

### Censorship and Influence at Home

China uses both the “Great Firewall” and its “Golden Shield” to stifle dissent at home. The Great Firewall blocks access to restricted foreign Web sites. If a China-based user tries to access a restricted site, it will not load and the user will receive a time-out message.[21] Additionally, China uses its Golden Shield to regulate information on domestic sites. According to Gillian Bolsover at the University of Oxford, social media sites in China actively monitor user-generated content to ensure that posted information is not deemed illegal by the state. Examples of content often censored include information related to political scandals, political leaders, and efforts to organize protests.[22]

China also actively seeks to shape the social media–based conversations and discussions of its citizens. Starting in 2011, the Chinese government saw a need to do more than just censor online content; it engaged in political communication. The Central Party, state institutions, state-run media, and individual party cadres soon began setting up government social media accounts. By 2014, the government had created more than 100,000 official social media accounts on WeChat and 180,000 profiles on Sina Weibo.[23]

One potential tool for this internal information control is the use of 50-cent accounts. Academics and policy experts have written about an army of volunteers who are paid 50 cents per post to "attack critics and support the state" online and to do so in a way that appears these attacks come from ordinary people.[24] A 2017 Harvard paper studied a data leak associated with the 50-cent accounts. The authors estimate that the government fabricates and posts about 448 million social media comments a year. Instead of engaging in direct arguments with potential skeptics of the government, these bogus users often try to change the subject and engage in cheerleading for China and the CCP.[25] Much of this work is done by government employees who post part time outside their regular day jobs.

### Influence Abroad: "Offline" Capabilities

Although the focus of this chapter is online influence operations and propaganda technologies, China has built a robust and multimodel offline approach to influence overseas populations and governments. This approach was addressed earlier in chapter 3b but merits brief repetition here. First, China has built an expanding capacity for global media reach. China's most prominent state-owned media outlets offer an international presence.[26] The China Global Television Network (CGTN), for example, broadcasts in English, Spanish, French, Arabic, and Russian to every region in the world via satellite and cable. In addition, Chinese state media have distributed content associated with the *China Daily* and the *Washington Post* in newsstands in New York City and congressional offices in Washington. Diplomats and other key influencers draft various op-ed articles and assiduously work to build relationships with foreign journalists. China also often threatens to withhold access to its markets if representatives of various business interests do not toe the party line.[27]

In addition, China's state media organs have broadened their reach with the use of social media. The English-language Facebook pages for *China Daily*, the official Xinhua News Agency, and CGTN, according to disinformation researcher Renee DiResta, have amassed more than 75 million followers each, a sum two to three times greater than CNN or Fox News. DiResta argues that China's heavy use of paid social media advertisements played a key role in cultivating this large following.[28]

### Influence Abroad: Chinese Online Capabilities

China has attempted to use online tools, including fake social media accounts, to advance its Taiwan unification campaign and its efforts to counter the Hong Kong protests. China has engaged in several small-scale efforts at using social media to promote Taiwanese unification. In one interesting case, following a typhoon that disabled a bridge to Osaka's Kansai International Airport, a post on the Professional Technology Temple (PTT), a Taiwanese-focused bulletin board, falsely suggested that the Chinese consulate could evacuate Taiwan citizens from Osaka only if they identified themselves as Chinese citizens. Researchers traced the story on PTT to an account on the Chinese microblogging site Weibo and a "content farm" that posted on mainland media sites, where it was then picked up by PTT messaging.[29] The consequences were harmful: Taiwan's foreign ministry representative in Osaka committed suicide due to pressure stemming from his inability to aid Taiwanese citizens.

In another case, it was discovered that a large number of PTT accounts, some of which were deemed "influential," were purchased on an online auction site active in Taiwan and Southeast Asia. Many of these accounts switched their content from being pro-democratic to leaning pro-Chinese. The accounts posted at a time to allow the Taiwanese public to see the posts first thing in the morning.[30]

China has most recently been caught using sham Facebook and Twitter accounts in an attempt to counter the Hong Kong protests. On August 19, 2019, both Twitter and Facebook announced the discovery of the Chinese campaign. Twitter identified 936 accounts that originated within the People's Republic of China that were "deliberately and specifically attempting to sow political discord in Hong Kong, including undermining the legitimacy and political positions of the protest movement on the ground."[31] Fake accounts were also detected on Facebook and YouTube.[32]

Subsequently, the Australian Strategic Policy Institute (ASPI) released a detailed analysis of the archive of terminated Twitter accounts. The researchers discovered that the 940 false accounts had disseminated 3.6 million tweets and identified three key narrative themes of the accounts: condemnation of the protesters, support for the Hong Kong police and the "rule of law," and conspiracy theories about Western involvement in the protests.[33] The authors described the campaign as relatively small and "hastily assembled" and lacking in sophisticated advance planning. They observed that the accounts were cheaply acquired repurposed spam or marketing accounts. Prior account owners, for example, tweeted in Arabic, English, Korean, Japanese, and Russian on topics that ranged from British football to pornography.[34]

The researchers also observed that there was "little attempt to target online communities with any degree of psychological sophistication."[35] In contrast, they noted that carefully crafted and long-running influence operations on social media, such as those conducted by the Russian state, are often characterized by tight network clusters associated with key target audiences. Analysis of the Chinese database revealed no such network characteristics. They finally observed that the Chinese dialect in some of the tweets was a dead giveaway for Chinese mainland authors.[36]

Beyond the anti–Hong Kong protest campaign, the researchers at ASPI found evidence of relatively small campaigns targeting China's political opponents. The largest campaign targeted Guo Wengui, a Chinese businessman and bookseller now residing in the United States who has publicly levied allegations of corruption against senior members of the Chinese government. Over 38,000 tweets from 618 accounts targeted Wengui with vitriolic attacks on his character.[37] Two other smaller campaigns targeted two dissidents who had already been arrested in China.[38]

With the 2019–2020 outbreak of the novel coronavirus (COVID-19), China launched a new propaganda campaign partially aimed at avoiding blame for the virus and promoting its own relief efforts. First, China has pushed social media content arguing that the virus may not have originated from China. On March 7, for example, the Chinese embassy in South Africa tweeted, "Although the epidemic first broke out in China, it did not necessarily mean that the virus is originated from China, let alone 'made in China.'"[39] The tweet further speculated that the virus originated in the United States. Chinese media promoted a conspiracy theory that a U.S. military cyclist may have brought the disease to Wuhan from Fort Detrick, the location of the U.S. Army's premier biological laboratory. The spokesman and deputy director general of the Information Department of China's Foreign Ministry also speculated on Twitter that the United States secretly concealed COVID-19 deaths in its count of flu fatalities.[40]

Second, China has promoted its domestic and international response to COVID-19. In February, Chinese state-run media began running social media advertisements that praised Secretary General Xi Jinping for his leadership in containing the virus.[41] On March 9, the official account of China's Ministry of Foreign Affairs tweeted, "China's endeavor to combating the epidemic has bought time for [international] preparedness."[42] China also promoted its international relief efforts. State-run media pushed advertisements that promoted stories of countries such as Italy and Serbia expressing gratitude to China for supporting them with medical supplies.[43] Pro-China bots pushed out tweets promoting Chinese medical relief efforts in Italy with two hashtags: #forzaCinaeItalia, which means "Come on China and Italy," and #grazieCina, which means "Thank you, China." Chinese diplomatic Twitter accounts also used these hashtags.[44]

### Limitations

The discovered Chinese online propaganda campaigns targeting Taiwan and protesters in Hong Kong suggest that China has struggled to weaponize social media to influence audiences abroad. China clearly has had success at home in terms of effectively censoring illicit content on the Web and shaping online conversations. The control it enjoys domestically over the Internet is not so easily replicated abroad, where it must contend with competing narratives that cannot be suppressed.[45]

China will likely learn its lesson. On the same August 2019 day that Twitter announced China's suspensions, China's Internet regulator put out notice for a contract to help it "operate and grow" overseas social media accounts on platforms such as Facebook. The project sought a team of experts who could "tell China's stories with multiple angles, express China's voice, and get overseas audience recognition and support for Jinping Thought." The state news agency, China News Services, also announced that it has started a new project to build its social media presence overseas. It specifically seeks to increase Twitter followers on its 2 accounts by 580,000 within 6 months. It wants at least 8 percent of the accounts to come from North America, Australia, and New Zealand. Overall, China is spending more than $1 million on both accounts.[46]

Further aiding China will be its investment in artificial intelligence, which, if effectively integrated in highly scaled social media campaigns, could prove a serious social media threat.[47] China's stake in the rapidly growing TikTok social media application could also help further the country's message. Suspicions have already arisen about China using the application to promote censorship and manipulation. Growing access to a widening public could be an information advantage for the Chinese and give them a new platform for influence.

## The So-Called Islamic State and Social Media

### Aims and Objectives

According to a leaked strategy document, IS had three main aims for its information operations campaign: recruitment, governance, and media.[48] First, IS sought to increase the recruitment of local and foreign fighters into the organization. Second, IS developed a plan that included a sophisticated information and intelligence apparatus designed to help IS expand and maintain control over its territory. Finally, IS's well-crafted media system sought to empower its recruitment and governance efforts while strengthening its embrace of atrocities intended to deter opponents and energize supporters with maximum psychological impact.

Other studies have sought to understand IS information objectives and aims by examining the content of its propaganda campaigns. Researchers in a RAND study isolated a community of ardent IS members and supporters on Twitter and lexically analyzed the content. They found that IS appeared to demonstrate "a more self-aware social media strategy" than any of the other groups, with disproportionately high usage of social media terms such as *spread*, *link*, *breaking news*, and *now released*.[49] In addition, themes of religion and belonging resonated strongly. In reference to violent IS activities, users employed noble phrases such as *lions of the Islamic State* and *mujahideen* and coopted the trappings of real states by using terms such as *army* and *soldiers of the Caliphate*.[50]

## Capabilities

To understand IS capabilities for using online tools in radicalization and recruitment, it is important to first understand the evolution of extremist radicalization and recruitment. Al Qaeda and other militants in places such as Bosnia, Chechnya, and the Palestinian territories used to disseminate propaganda content via DVD and cassette videos. Many of these videos featured depictions of atrocities that were meant to inflame opinions and sermons of religious leaders who sought to lay the intellectual and spiritual groundwork for terrorist actions. Recruitment into militant groups was often done through small social groups. For example, gatherings at private homes or mosques targeted Saudi recruits for Iraq and served as a venue where a "harmless discussion about Islam" turned to the U.S. war in Iraq and U.S.-committed atrocities.[51]

This approach to extremist propaganda and recruitment began to evolve slowly as al Qaeda turned to the Internet to aid in recruitment efforts. After initially disseminating speeches on al Jazeera, Osama bin Laden and his deputy, Ayman al-Zawahiri, began posting long and dry speeches. Anwar al-Awlaki, a key al Qaeda ideologue, gained particular fame through sermons posted to YouTube. His success as a propagandist led to him being targeted by U.S. forces in Yemen.[52] During the Iraq War, al Qaeda gained notoriety by posting videos of improvised explosive device attacks on American troops.[53] Throughout this process, al Qaeda and other groups used the Internet primarily as a broadcast tool, but limited effort was placed into harnessing social media platforms or the social aspects of online life.

IS helped revolutionize how extremist groups used the Internet and its social media platforms. IS decentralized its propaganda production and dissemination, used a multilayered set of media centers to produce its official media publications, and then leveraged a network of supporters in order to distribute its message. It also learned how to use direct messaging capabilities to reach out and connect to prospective recruits. A range of outlets helped IS produce its official propaganda. Official outlets Al-Furqan Media and Al-Hayat Media produced and released top-level messaging, such as the sermons of Abu Bakr al-Baghdadi and issues of the sleek English-language magazine *Dabiq*. Various "provincial" media outlets also produced an assortment of content and propaganda videos.

IS sought to disseminate this content not only on various Internet sites but also through a variety of social networking applications, including Facebook, Instagram, Tumblr, Ask.fm, and, most famously, Twitter. These channels allowed IS to enlist a worldwide army of supporters in both propaganda creation and dissemination. In addition to disseminating its own content on the Internet, IS welcomed supporters and members taking the initiative to create their own unofficial propaganda. In her 2014 study of tweets posted by 29,000 accounts belonging to Western IS foreign fighters, Jytte Klausen found that disseminators outside the conflict zone, including a handful of particularly influential women, played a key role in this effort to "build redundancy by spreading the material, often posting and reposting material provided by the feeder accounts belonging to organizations and fighters based in Syria."[54]

IS also worked with individual fighters who had their own Twitter, Instagram, or Tumblr accounts. IS worked to coordinate and synchronize the postings of fighters. These tales describing life and success on the battlefield gained a wide following.[55] In addition, a report by the International Centre for the Study of Radicalisation and Political Violence emphasized the role of disseminators based primarily in the West, arguing that many foreign fighters informed themselves about the conflict by following unofficial disseminators rather than official IS channels.[56]

IS also used social media to support its recruitment efforts. IS enlisted "units of specialized recruiters operating around the clock from Internet cafes in Iraq and Syria, interacting on an individual level with prospective recruits."[57] Individuals who liked, retweeted, or positively commented on IS social media accounts self-identified themselves as potentially suitable targets for recruitment. Recruiters could then make contact using private communications such as direct messaging on Twitter or Facebook. The two-way dialogue allowed the recruiter to groom the target and promote action (be it conducting attacks in the West or emigrating to IS territory). As J.M. Berger notes, such recruitment efforts became increasingly important as IS sought to recruit from lands farther than Iraq and Syria.[58]

Overall, these efforts appeared successful. IS gained significant media exposure and notoriety for the conduct of its social media campaign. Ultimately, it recruited over 40,000 people (32,809 men, 4,761 women, and 4,640 children) to join its ranks. Over 5,900 foreign fighters joined from Western Europe and 753 joined from the Americas.[59] IS operatives also launched various deadly attacks, most notably the Brussels airport and subway bombings of March 22, 2016, which killed 32 individuals, and the Paris attacks of November 13, 2015, which resulted in 130 fatalities. IS-inspired attacks also took place in the United States, Canada, Australia, Tunisia, Turkey, and Egypt.[60]

## Limitations

IS success with social media did not last. In 2015, Twitter and other social media firms initiated an effort to suspend IS social media accounts based on terms of service violations. IS in turn worked diligently to overcome these suspensions. As soon as Twitter suspended one IS supporter's account, the supporter was supposed to move to a backup account.[61] However, even under the best of circumstances, such remediation efforts could not maintain the previous breakneck pace of propaganda dissemination.[62] Soon the platforms created new artificial intelligence tools that could detect and terminate accounts in near real time. In the first 6 months of 2017, Twitter took down nearly 300,000 terrorist accounts.[63] As a result, Maura Conway and colleagues wrote in their research on Twitter takedowns that "the costs for most pro-IS users of engaging on Twitter (in terms of deflated morale, diffused messages, and persistent effort needed to maintain a public presence) now largely outweigh the benefits. This means that the IS Twitter community is now almost nonexistent."[64]

IS has since sought new online territory from which to recruit and radicalize. For some time, IS turned to Telegram, an application that, while lacking the unique broadcast capability of Twitter, allowed IS a secure way to "communicate with likeminded supporters across the world, disseminate official and unofficial [IS] media, and provide instructional material for operations."[65] However, a series of account suspension efforts by Telegram, mostly recently conducted in collaboration with Interpol in late 2019, has left IS once again looking for more friendly territory.

## Recommendations

The growing use of social media as a technology tool for strategic influence operations and nation-state propaganda represents a significant threat to U.S. interests as America moves into a new era of Great Power competition. While Russian social media may not have decisively impacted the U.S. election of 2016, it is clear the campaign likely negatively impacted American trust in that election. Additionally, it seems clear that such attacks will continue against the United States, its allies, and other nations' democratic elections. As demonstrated by its assertive social media activities during 2020 to shape a factually suspect COVID-19 narrative, Beijing has targeted the United States and its allies with online propaganda. Clearly, the United States needs to safeguard the authority, legitimacy, and respect of American norms, values, and institutions from such adversaries.

Numerous documents and reports lay out an array of recommendations for how the United States can best counter this threat.[66] Reviewing the long lists of recommendations is beyond the scope of this chapter; however, it is useful to briefly consider some broad approaches that the United States could undertake to limit the threat.

### Track, Highlight, and Block Adversarial Content

The U.S.-led and Western campaign against IS propaganda proved successful largely because social media platforms were able and willing to identify IS content and terminate IS social media accounts. Overall, the platforms seem uniquely able to identify and target such content in part because extremists clearly branded their campaigns for driving terrorist recruitment. The U.S. Government should continue to work with Twitter, Facebook, and other platforms to ensure suspensions of extremist accounts. The challenge is much greater for nation-state campaigns, which wage stealth propaganda using fake accounts and targeting a litany of causes. An arms race is already taking place between those charged with planning and executing online propaganda and those seeking to detect and remove such campaigns. The U.S. Government will need to work closely with technology firms and the academic community to support this arms race and enable new approaches for detecting campaigns.

### Build Resilience of At-Risk Populations

It will be crucial to help audiences be more critical consumers of social media. Doing so means giving audiences the skills and capabilities to identify fake news, consider the credibility of sources on social media, and recognize their role in countering such content or limiting its propagation. Media literacy campaigns represent one potential avenue for this resilience-building, and efforts are under way to develop and implement relevant educational curriculums in the United States and elsewhere. Governments should also warn citizens when they detect or other otherwise suspect that adversaries are targeting such citizens with online influence campaigns.

### Support Allies Targeted by U.S. Adversaries

The United States should help its allies stand up against online propaganda. For example, Russia has been engaged in a near-persistent propaganda campaign against the government of Ukraine as well as other Eastern European countries. The United States should work with the targeted countries to give them the necessary capabilities to withstand and counter these campaigns. The specific policy prescriptions will vary, but efforts may include training local governments in better communication strategies, improving training for journalists, providing funds to support outing adversary propaganda, and establishing media literacy campaigns.

### Better Organize to Counter Adversary Propaganda

The U.S. Government must ensure it is properly organized to fight online disinformation. The Intelligence Community will need the necessary capabilities and funding to help detect foreign influence campaigns before or as they occur. Interagency coordination will be critical as the Department of Homeland Security, Department of State, and Department of Defense will each be responsible for countering a particular component of adversary campaigns.[67] Coordination should continue down to the state level to help states prepare for elections and address locally targeted campaigns. It is critical that the United States and social media firms work closely together in an information-sharing capacity to ensure communication of threats and adversary campaigns and to coordinate on counterpropaganda activities.

## Notes

[1] This chapter uses the terms *propaganda* and *disinformation*. Merriam-Webster defines *propaganda* as “Ideas, facts, or allegations spread deliberately to further one’s cause or to damage an opposing cause.” *Disinformation* is considered a type of propaganda. Christina Nemr and William Gangware describe disinformation as including authentic material used in a deliberately wrong context to make a false connection as well as fake news sites, manipulated sites, or outright false information shared through graphics, images, and videos. See Christina Nemr and William Gangware, *Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age* (Washington, DC: Park Advisors, 2019).

[2] Samantha Bradshaw and Philip N. Howard, *The Global Disinformation Order: 2019 Global Inventory of Organized Social Media Manipulation*, Working Paper No. 2019.3 (Oxford, UK: Project on Computational Propaganda, 2019).

[3] Ibid., 1, 13.

[4] Michael J. Mazarr et al., *Hostile Social Manipulation: Present Realities and Emerging Trends* (Santa Monica, CA: RAND, 2019).

[5] Ibid., 61.

[6] Diego A. Martin and Jacob N. Shapiro, *Trends in Online Foreign Influence Efforts*, Working Paper Version 1.2 (Princeton: ESOC Publications, 2019).

[7] Elizabeth Bodine-Baron et al., *Countering Russian Social Media Influence* (Santa Monica, CA: RAND, 2018).

[8] Joby Warrick and Anton Troianovski, "Agents of Doubt: How a Powerful Russian Propaganda Machine Chips Away at Western Notions of Truth," *Washington Post*, December 10, 2019, available at <www.washingtonpost.com/graphics/2018/world/national-security/russian-propaganda-skripal-salisbury/>.

[9] Robert S. Mueller III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, vols. 1 and 2 (Washington, DC: Department of Justice, 2019).

[10] Claire Allbright, "A Russian Facebook Page Organized a Protest in Texas. A Different Russian Page Launched the Counterprotest," *Texas Tribute* (Austin), November 1, 2017, available at <www.texastribune.org/2017/11/01/russian-facebook-page-organized-protest-texas-different-russian-page-l/>.

[11] Renee DiResta et al., *The Tactics and Tropes of the Internet Research Agency* (New York: New Knowledge, 2018), available at <https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1003&context=senatedocs>.

[12] Martin and Shapiro, *Trends in Online Foreign Influence Efforts*.

[13] Tom Uren, Elise Thomas, and Jacob Wallis, *Tweeting Through the Great Firewall: Preliminary Analysis of PRC-Linked Information Operations Against the Hong Kong Protests*, Issues Paper Report No. 25/2019 (Canberra: Australian Strategic Policy Institute, 2019), 5, available at <https://www.aspi.org.au/report/tweeting-through-great-firewall>.

[14] Sergey Sanovich, *Computational Propaganda in Russia: The Origins of Digital Misinformation*, Working Paper No. 2017.3 (Oxford, UK: Computational Propaganda Research Project, 2017), available at <http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Comprop-Russia.pdf>.

[15] Ibid., 15.

[16] Looking at the Russian campaign targeted at the U.S. 2016 elections, it appears that Russia's ad-targeting efforts were not focused on the battleground states critical to Presidential victory. Russia spent less than $2,000 on advertisements in Wisconsin, Pennsylvania, and Michigan, suggesting the campaign was not decisive in changing votes associated with the Electoral College. See Nemr and Gangware, *Weapons of Mass Distraction*.

[17] Christopher A. Bail et al., "Assessing the Russian Internet Research Agency's Impact on the Political Attitudes and Behaviors of American Twitter Users in Late 2017," *Proceedings of the National Academy of Sciences* 117, no. 1 (January 2020), 243–250.

[18] Matthew Nussbaum, "Worries About Trump's Legitimacy Resurface with Russia Indictment," *Politico*, February 16, 2018, available at <www.politico.com/story/2018/02/16/muller-indictment-trump-election-legitimacy-416163>.

[19] Davey Alba and Sheera Frenkel, "Russia Tests New Disinformation Tactics in Africa to Expand Influence," *New York Times*, October 30, 2019, available at <www.nytimes.com/2019/10/30/technology/russia-facebook-disinformation-africa.html>.

[20] Sarah Cook, *Beijing's Global Megaphone: The Expansion of Chinese Communist Party Media Influence Since 2017*, Special Report (Washington, DC: Freedom House, 2020), available at <https://freedomhouse.org/sites/default/files/2020-02/01152020_SR_China_Global_Megaphone_with_Recommendations_PDF.pdf>.

[21] Gillian Bolsover, *Computational Propaganda in China: An Alternative Model of a Widespread Practice*, Working Paper No. 2017.4 (Oxford, UK: Computational Propaganda Research Project, 2017), available at <https://blogs.oii.ox.ac.uk/politicalbots/wp-content/uploads/sites/89/2017/06/Comprop-China.pdf>.

[22] Ibid.

[23] Hauke Gierow, Karsten Luc, and Kristin Shi-Kupfer, "Governance Through Information Control: China's Leadership Struggles with Credibility in Social Media Staged Propaganda, Everyday Tips, Lack of Interactivity," *China Monitor* 26 (January 19, 2016), available at <https://www.merics.org/sites/default/files/2019-08/China_Monitor_No_26_Social_Media_EN.pdf>.

[24] Bolsover, *Computational Propaganda in China*.

[25] Gary King, Jennifer Pan, and Margaret E. Roberts, "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument," *American Political Science Review* 111, no. 3 (2017), 484–501.

[26] Cook, *Beijing's Global Megaphone*. China has also exerted significant influence on Hollywood by granting select films access to Chinese markets. The films *Martian* and *Gravity* received significant praise in the Chinese market for giving Chinese astronauts key roles in saving beleaguered American astronauts. See Gus Lubin, "18 Hollywood Films That Pandered to China's Giant Box Office," *Business Insider*, October 14, 2016, available at <www.businessinsider.com/hollywood-movies-in-china-2016-10#cloud-atlas-removed-nearly-30-minutes-from-its-chinese-cut-largely-plotlines-and-scenes-with-controversial-sexual-relations-3>.

[27] Such was learned when Daryl Morey, the general manager of the Houston Rockets, published his now-deleted tweet: "Fight for freedom, Stand with Hong Kong." He quickly deleted the tweet, apologized, and the National Basketball Association worked overtime to avoid alienating itself from the lucrative Chinese basketball market. See Theodore Yu, "One Tweet, a Week of Turmoil: NBA Steps Out of Bounds with China and Pays the Price," *Sacramento Bee*, October 13, 2019, available at <www.sacbee.com/sports/nba/sacramento-kings/article235933242.html>.

[28] Renee DiResta, "For China, the 'USA Virus' Is a Geopolitical Ploy," *The Atlantic*, April 11, 2020, available at <www.theatlantic.com/ideas/archive/2020/04/chinas-covid-19-conspiracy-theories/609772/>.

[29] Gary Schmitt and Michael Mazza, *Blinding the Enemy: CCP Interference in Taiwan's Democracy* (Washington, DC: Global Taiwan Institute, October 2019).

[30] Ibid., 8–9.

[31] Twitter Safety, "Information Operations Directed at Hong Kong," *Twitter*, August 19, 2019, available at <https://blog.twitter.com/en_us/topics/company/2019/information_operations_directed_at_Hong_Kong.html>.

[32] Nathaniel Gleicher, "Removing Coordinated Inauthentic Behavior from China," *Facebook*, August 19, 2019, available at <https://about.fb.com/news/2019/08/removing-cib-china/>; Chris Welch, "YouTube Disabled 210 Accounts for Spreading Disinformation About Hong Kong Protests," *The Verge*, August 22, 2019, available at <www.theverge.com/2019/8/22/20828808/youtube-hong-kong-protests-china-disabled-accounts-suspension-disinformation>.

[33] Uren, Thomas, and Wallis, *Tweeting Through the Great Firewall.*

[34] Ibid., 4.

[35] Ibid.

[36] Ibid., 11.

[37] Ibid., 14.

[38] Ibid., 22.

[39] Bethany Allen-Ebrahimian, "Beijing's Coronavirus Propaganda Blitz Goes Global," *Axios*, March 11, 2020, available at <www.axios.com/beijings-coronavirus-propaganda-blitz-goes-global-f2bc610c-e83f-4890-9ff8-f49521ad6a14.html>.

[40] DiResta, "For China, the 'USA Virus' Is a Geopolitical Ploy."

[41] Ibid.

[42] Allen-Ebrahimian, "Beijing's Coronavirus Propaganda Blitz Goes Global."

[43] DiResta, "For China, the 'USA Virus' Is a Geopolitical Ploy."

[44] Bethany Allen-Ebrahimian, "Bots Boost Chinese Propaganda Hashtags in Italy," *Axios*, April 1, 2020, available at <www.axios.com/bots-chinese-propaganda-hashtags-italy-cf92c5a3-cdcb-4a08-b8c1-2061ca4254e2.html>.

[45] Echo Huang, "No Little Red Guidebook: Why China Isn't as Skillful at Disinformation as Russia," *Quartz*, September 19, 2019, available at <https://qz.com/1699144/why-chinas-social-media-propaganda-isnt-as-good-as-russias/>.

[46] "China's Propaganda Machine Is Spending Over $1 Million to Buy Influence on Foreign Social Media," *Quartz*, August 21, 2019, available at <https://finance.yahoo.com/news/china-propaganda-machine-spending-over-150453611.html>.

[47] Christopher Paul and Marek Posard, "Artificial Intelligence and the Manufacturing of Reality," *RAND Blog*, January 20, 2020, available at <www.rand.org/blog/2020/01/artificial-intelligence-and-the-manufacturing-of-reality.html>.

[48] See Linda Robinson et al., *Modern Political Warfare: Current Practices and Possible Responses* (Santa Monica, CA: RAND, 2018); Shiv Malik, "IS Papers: Leaked Documents Show How IS Is Building Its State," *Guardian*, December 7, 2015, available at <www.theguardian.com/world/2015/dec/07/leaked-isis-document-reveals-plan-building-state-syria>.

[49] Elizabeth Bodine-Baron et al., *Examining IS Support and Opposition Networks on Twitter* (Santa Monica, CA: RAND, 2016), available at <https://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1328/RAND_RR1328.pdf>.

[50] Another study analyzed the content of IS propaganda magazines *Dabiq* and *Rumiyah*. Common themes associated with the articles in the magazines included IS theological justification and inspiration for violence; descriptions of community, belonging, and meaning; stories of progress or heroism; establishment of a common enemy, that is, the West and Muslim "apostates"; and instructional and inspirational articles empowering individual violent action. See Tyler Welch, "Theology, Heroism, Justice, and Fear: An Analysis of IS Propaganda Magazines *Dabiq* and *Rumiyah*," *Dynamics of Asymmetric Conflict* 11, no. 3 (2018), 186–198.

[51] Thomas Hegghammer, *Saudi Militants in Iraq: Backgrounds and Recruitment Patterns* (Kjeller: Norwegian Defence Research Establishment, February 5, 2007), available at <https://www.ffi.no/en/publications-archive/saudi-militants-in-iraq-backgrounds-and-recruitment-patterns>; Alexandria Zavis, "Foreign Fighters in Iraq Seek Recognition, U.S. Says," *Los Angeles Times*, March 17, 2008, available at <www.latimes.com/world/la-fg-iraq17mar17-story.html>.

[52] "The Propaganda Wars Since 9/11," *Washington Post*, May 8, 2015, available at <www.washingtonpost.com/graphics/national/propaganda/>; Scott Shane, "The Lessons of Anwar al-Awlaki," *New York Times*, August 27, 2015, available at <www.nytimes.com/2015/08/30/magazine/the-lessons-of-anwar-al-awlaki.html>.

[53] Edward Wyatt, "Anti-U.S. Attack Videos Spread on Web," *New York Times*, October 6, 2006, available at <www.nytimes.com/2006/10/06/technology/06tube.html>.

[54] Jytte Klausen, "Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq," *Studies in Conflict & Terrorism* 38, no. 1 (October 2014), 1–22.

[55] Ibid.

[56] Joseph Carter, Shiraz Maher, and Peter Neumann, *#Greenbirds: Measuring Importance and Influence in Syrian Foreign Fighter Networks* (London: International Centre for the Study of Radicalisation and Political Violence, 2014), 5.

[57] Landon Shroder, "The Islamic State's Propaganda War: Advertisers and Marketers Weigh in on the World's Angriest Ad Campaign," VICE News, July 14, 2015, available at <www.vice.com/en_us/article/8x3nnv/the-islamic-states-propaganda-war-advertisers-and-marketers-weigh-in-on-the-worlds-angriest-ad-campaign>.

[58] J.M. Berger, "Tailored Online Interventions: The Islamic State's Recruitment Strategy," *Combating Terrorism Center Sentinel* 8, no. 10 (October 2015), available at <https://www.ctc.usma.edu/posts/tailored-online-interventions-the-islamic-states-recruitment-strategy>.

[59] Joana Cook and Gina Vale, *From Daesh to Diaspora: Tracing the Women and Minors of the Islamic State* (London: International Centre for the Study of Radicalisation, 2018).

[60] Karen Yourish, Derek Watkins, and Tom Giratikanon, "Where IS Has Directed and Inspired Attacks Around the World," *New York Times*, March 22, 2016, available at <www.nytimes.com/interactive/2015/06/17/world/middleeast/map-isis-attacks-around-the-world.html>.

[61] As one IS supporter urged in a blog, "To counter suspensions, you must support each other. Don't make the brothers and sisters ask for a shout out. If someone you recognize has followed you after a suspension, tell your followers to follow them." See "Blog Post Suggests Ways for IS Supporters to Boost Social Media Effectiveness," SITE Intelligence Group, July 17, 2015.

[62] J.M. Berger and Heather Perez, *The Islamic State's Diminishing Returns on Twitter: How Suspensions Are Limiting the Social Networks of English-Speaking IS Supporters*, Occasional Paper (Washington, DC: Program on Extremism at George Washington University, 2016).

[63] Madhumita Murgia, "Twitter Takes Down 300,000 Terror Accounts as AI Tools Improve," *Financial Times*, September 19, 2017, available at <www.ft.com/content/198b5258-9d3e-11e7-8cd4-932067fbf946>.

[64] Maura Conway et al., "Disrupting Daesh: Measuring Takedown of Online Terrorist Material and Its Impacts," *Studies in Conflict & Terrorism* 42, nos. 1–2 (2019), 141–160.

[65] Bennett Clifford and Helen Powell, *Encrypted Extremism: Inside the English-Speaking Islamic State Ecosystem on Telegram* (Washington, DC: Program on Extremism at George Washington University, 2019), available at <https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/EncryptedExtremism.pdf>.

[66] See, for example, Todd C. Helmus et al., *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe* (Santa Monica, CA: RAND, 2018), available at <https://www.rand.org/pubs/research_reports/RR2237.html>; Bodine-Baron et al., *Countering Russian Social Media Influence*; Alina Polyakova and Daniel Fried, *Democratic Defense Against Disinformation 2.0* (Washington, DC: Atlantic Council, 2019), available at <https://www.atlanticcouncil.org/wp-content/uploads/2019/06/Democratic_Defense_Against_Disinformation_2.0.pdf>; Paul Barret, Tara Wadhwa, and Dorothée Baumann-Pauly, *Combating Russian Disinformation: The Case for Stepping Up the Fight Online* (New York: NYU Stern Center for Human Rights, 2018), available at <https://issuu.com/nyusterncenterforbusinessandhumanri/docs/nyu_stern_cbhr_combating_russian_di?e=31640827/63115656>.

[67] There is no single U.S. agency or government entity leading the work to counter foreign propaganda and influence. See *Homeland Security Advisory Council Interim Report of the Countering Foreign Influence Subcommittee* (Washington, DC: Department of Homeland Security, June 2019), 10, available at <https://www.dhs.gov/sites/default/files/publications/ope/hsac/19_0521_final-interim-report-of-countering-foreign-influence-subcommittee.pdf>; Melissa Dalton et al., *By Other Means—Part II: U.S. Priorities in the Gray Zone* (Lanham, MD: Rowman & Littlefield, 2019), 6–11, available at <https://csis-prod.s3.amazonaws.com/s3fs-public/publication/Hicks_GrayZone_II_full_WEB_0.pdf>.