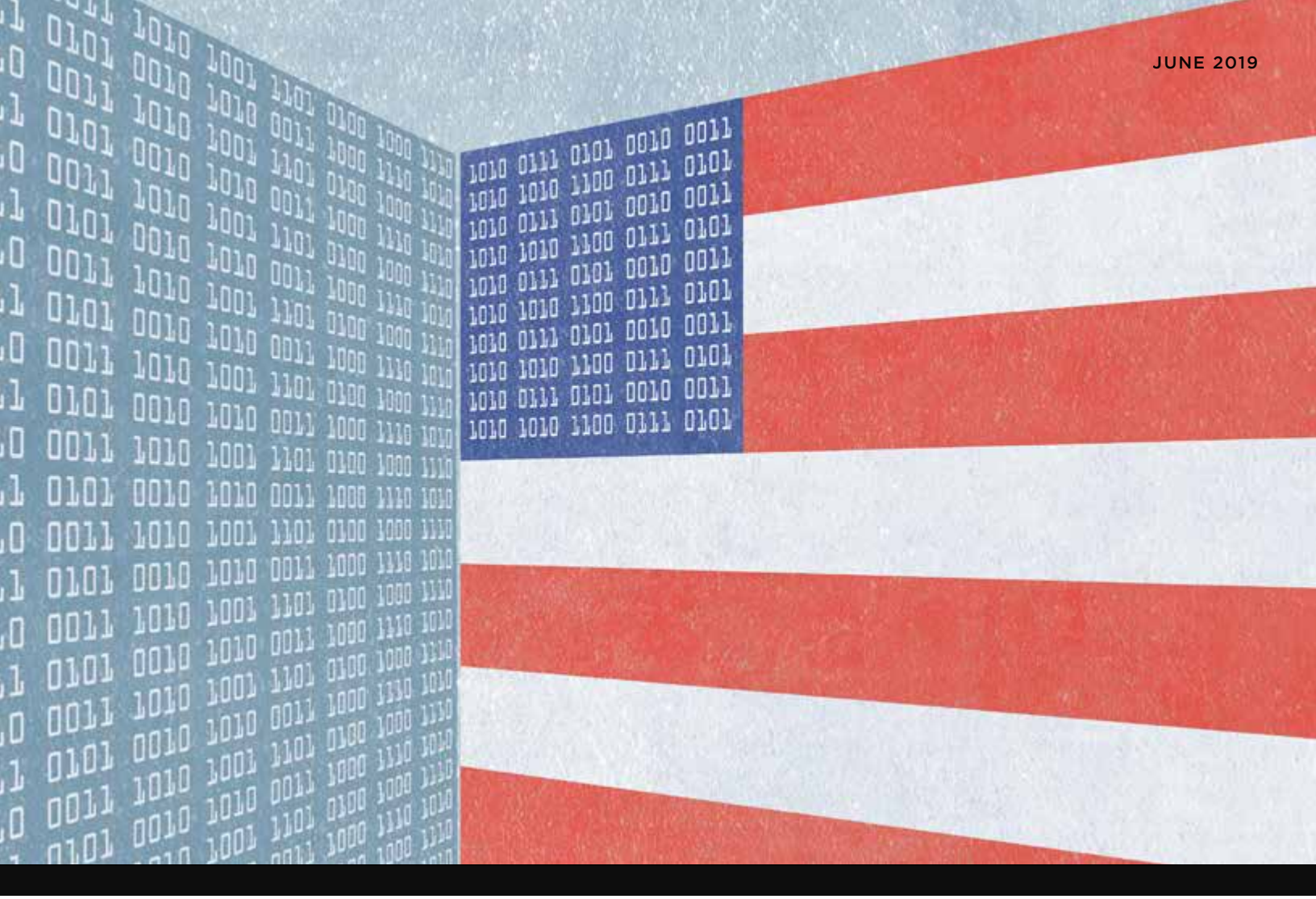

JUNE 2019

The New War of Ideas

Counterterrorism Lessons for the Digital Disinformation Fight

Kara Frederick

CNAS

About the Author

KARA FREDERICK is the Associate Fellow for the Technology and National Security Program at the Center for a New American Security (CNAS). Prior to joining CNAS, Kara helped create and lead Facebook's Global Security Counterterrorism Analysis Program. She was also the team lead for Facebook Headquarters' Regional Intelligence Team in Menlo Park, California. Prior to Facebook, she served as a senior intelligence analyst for a U.S. Naval Special Warfare Command and spent six years as a counterterrorism analyst at the Department of Defense. While at DoD, she deployed three times to Afghanistan in support of special operations forces, served as a briefer to the Assistant Secretary of Defense for Special Operations/Low Intensity Conflict, and acted as a liaison to the National Security Agency. She received her M.A. in War Studies from King's College London and her B.A. in Foreign Affairs and History from the University of Virginia.

Acknowledgments

The author is indebted to Paul Scharre for his critical insight, feedback, guidance, and innumerable reviews. Thank you to Anthony Cho, Megan Lamberth, and Ainikki Riikonen for their substantive contributions and research efforts. Special thanks to Ely Ratner for helping translate Silicon Valley colloquialisms into proper English, as well as structure the piece for impact. Maura McCarthy, Loren DeJonge Schulman, and Melody Cook provided superlative assistance in the editing and design of this report. Any errors of fact, omission, or analysis are the author's alone. Finally, CNAS would like to thank the Hewlett Foundation for its generous support of this project.

This report builds on prior published work by the author, particularly the War on the Rocks commentary entitled, "How to Defend Against Foreign Influence Campaigns: Lessons from Counter-Terrorism," published in October 2018.[1] Short excerpts from the text of this work, independently written and researched by the author, are cited throughout this report.

Cover Art
Melody Cook/CNAS

Executive Summary

A new battlespace emerged in the post-9/11 counterterrorism era, encompassing the halls of U.S. technology companies and the alleys of Raqqa alike. Today, the United States is engaged in an expansive conflict that requires solutions from the same key players—the private tech industry and the U.S. government. They cannot afford to waste the digital, organizational, and strategic lessons learned from nearly two decades of countering terrorism.

Learning from specific successes in tech sector and U.S. government counterterrorism efforts will optimize the United States' collective response to the digital disinformation challenges of the future. Private and public actors should consider five important lessons from countering terrorism: (1) improve technical methods for identifying foreign influence campaign content; (2) increase collaboration among companies; (3) build partnerships between government and the technology sector via public and private analyst exchanges; (4) maintain an offensive posture and devote the resources necessary to keep the adversary on the back foot; and (5) take advantage of U.S. allies' knowledge.

The following set of recommendations offers opportunities to apply these five lessons to combating foreign influence campaigns. The first two recommendations are aimed at the private technology industry; the third applies to both the tech industry and the U.S. government; and the final two recommendations are directed at U.S. government agencies.

Summary of Recommendations

- Tech companies should, over the long term, direct a sustainable percentage of engineering capacity to automating the identification of state-sponsored, malign influence campaigns. Companies can leverage existing practices and traditions, like Facebook "hackathons," to share engineering tasks, build prototypes, and seek new technical fixes for the disinformation problem.[2]
- Tech companies should create and fund an enduring disinformation-related consortium among willing companies, modeled after the Global Internet Forum to Counter Terrorism (GIFCT). The goal would be to move toward establishing industry standards on what constitutes disinformation and malign, foreign influence campaigns for U.S. companies.
- The Office of the Director of National Intelligence (ODNI), in coordination with the private sector, should appoint a body of interagency representatives to create and fund smaller, more forward-leaning fusion cells that integrate public and private sector analysts. Social media companies should lend their threat intelligence analysts (with intelligence agencies providing relevant all-source analysts) to this effort in an enduring dialogue at appropriate levels of classification. If this body meets certain standards of success, the U.S. government should explore appointing a standalone, high-level interagency task force to incorporate these cells and possess full responsibility for countering digital foreign influence operations.
- The executive branch should expand its Cybersecurity Strategy and U.S. Cyber Command's (CYBERCOM's) authorities to conduct offensive cyber operations that impose costs on foreign adversaries. However, expanding authorities should stop short of directives to conduct offensive *influence* operations in foreign countries.
- The United States should work with democratic allies to exchange best practices from their own efforts in countering foreign influence operations and conducting offensive cyber measures. The United States should use the same convening mechanism to institute a formal method of providing CYBERCOM with the results of this information-sharing and recommendations for action.

Senator Patrick Leahy (D-VT) questions representatives from Facebook, Twitter, and Google during a U.S. Senate Judiciary Subcommittee Hearing. The October 31, 2017, hearing "Extremist Content and Russian Disinformation Online: Working with Tech to Find Solutions" featured examples of Russian-purchased ads on Facebook. (Drew Angerer/Getty Images)

Introduction

The future of the world order hinges on influencing populations. While civilians have long been the currency of conflict—from insurgencies to terrorism to information operations—emerging technologies are revolutionizing the influence game. Advances in artificial intelligence, particularly machine learning, stand to weaponize information to exert social control at scale. Authoritarian regimes, such as China, have taken advantage of new tools to deepen their hold over their populations, using state-controlled social media accounts, automated bot networks, and facial recognition technology. Foreign actors are attempting to undermine and erode public trust in democratic processes through computational propaganda and microtargeting, and even non-state actors are stoking political tensions through the spread of misinformation online. Such developments, often aimed at the existing liberal order and the institutions that buttress it, portend potential geopolitical upheavals.

Yet an unlikely blueprint to resist this threat exists in the lessons of a different war. The post-9/11 counterterrorism fight offers a roadmap for both public and private organizations to respond to this new information battlespace. In recognition of the terrorist threat, the U.S. government and private businesses mobilized to contest it in both physical and digital landscapes. The degree of seriousness with which the U.S. government took the threat was reflected in its price tag. From 2002–2017, the global war on terrorism cost the United States approximately $2.8 trillion in related expenditures and made up almost 16 percent of discretionary spending during that timeframe.[3] This paid for a strategy to disrupt and deny threats before they struck home, as the U.S. military undertook operations to confront terrorists in their safe havens abroad.

In concert, the government launched major organizational, legislative, and policy reforms at the federal level. After the release of the 9/11 Commission Report in 2004, President George W. Bush and both the House and Senate instituted a breadth of changes aimed at restructuring the intelligence community to better warn of and respond to terrorist threats.[4] On the information-sharing front, the creation of the Office of the Director of National Intelligence and the National Counterterrorism Center (NCTC) were hallmarks of this reform. In 2005, ODNI began operations with a mission to lead and support intelligence integration within the intelligence community.[5] As a mission center within ODNI, NCTC fused foreign and domestic counterterrorism information, conducted terrorism analysis, shared "information with partners across the counterterrorism enterprise, and [drove] whole of government action to secure national counterterrorism objectives."[6] On top of newly improved indications and warnings, lawmakers and executives ratified numerous counterterrorism policies—some aimed at deterrence, others punitive. Most sought to target terrorist funding mechanisms, stem foreign fighter flows into the country, and interdict and prosecute threats to the homeland. Collectively, the USA Patriot Act in 2001, amendments to the long-standing 1978 Foreign Intelligence Surveillance Act, and the establishment of the Department of Homeland Security in 2002 increased penalties for terrorist activities, expanded surveillance measures, and tightened border security.[7] The Department of Justice did its part to try offenders under decades-old legislation like 18 U.S. Code 2339A and B, which prohibits the provision of material support to terrorists and designated organizations. From top to bottom, the federal government coordinated and organized for the fight.

The post-9/11 counterterrorism fight offers a roadmap for both public and private organizations to respond to this new information battlespace.

Social media companies followed suit in organizing to combat terrorism. The online distribution of an ISIS video depicting the beheading of U.S. journalist James Foley via YouTube and Twitter in 2014 opened up a new front at companies' doorsteps.[8] Against this backdrop and existing legislation aimed at stemming the terrorist advance, Facebook began meeting with other technology companies to discuss platform-based counterterrorism efforts around 2015.[9] In early 2016, White House and interagency officials flew to Silicon Valley to meet with tech leaders—including Apple CEO Tim Cook and representatives from Google, Facebook, Yahoo, and Twitter—to discuss solutions to the spread of terrorism-related content on the internet.[10] That year, Alphabet Inc.'s Jigsaw helped confront ISIS online messaging tactics and clean up content on YouTube.[11] By 2018, Facebook had hired 7,500 content moderators, a portion of whose job is dedicated to keeping terrorist content off the platform.[12] And in the three years since those initial discussions in 2015, Twitter permanently suspended 1.2 million accounts related to violations of the company's counterterrorism policies.[13]

The war was on, and tech companies actively worked to make their platforms hostile to terrorist actors. They hired talent to fill gaps in their counterterrorism expertise, created positions to coordinate and oversee global counterterrorism policy, convened relevant players in internal forums, and instituted a combination of technical measures and good old-fashioned analysis to root out offending users and content. Major and minor tech companies coordinated with each other and with law enforcement to share threat information, drafted policies around preventing terrorist abuse of their platforms, updated their community guidelines, and even supported counter-speech initiatives to offer alternative messaging to terrorist propaganda.

The blind transfer of counterterrorism practices to the battle against foreign influence operations would mean fighting yesterday's war. But certain lessons are critical enough to be repurposed for a different battlefield. Nearly two decades of countering terrorism taught the United States a great deal about how to approach this latest challenge. Five key lessons stand out:[14]

1. Improve technical methods for identifying foreign influence campaign content;
2. Increase collaboration among companies;
3. Build partnerships between the government and the private sector via analyst exchanges;
4. Maintain an offensive posture and devote the resources necessary to keep the adversary on the back foot; and
5. Take advantage of U.S. allies' knowledge.

These lessons provide the opportunity to fight back against malign foreign influence campaigns. But understanding the breadth and trajectory of the threat is critical to marshaling a response: Foreign attempts to propagate disinformation, amplify political polarization, disclose information, and hack elections persist. The ultimate goal of these actors is to influence the public discourse and undermine democratic institutions. A series of recommendations, aimed at thwarting digital attempts to undermine democracies, will help both social media companies and the U.S. government apply key technical, organizational, and tactical strategies learned in the years following 9/11 to foreign influence campaigns today.

Foreign Influence Efforts: Disinformation, Amplifying Political Polarization, Information Disclosures, and Election Hacking

To most Americans, the recent onslaught of influence operations at home may feel like a novel threat.[15] But disinformation and influence operations are not new. The hostile influence of foreign powers through information warfare has long menaced democratic integrity. From the Axis Powers in World War II to Russia in today's Ukraine, history is replete with foreign attempts to undermine and erode public trust in democratic processes and institutions through efforts like military intimidation, cyberattacks, energy coercion, and influence operations. The use of digital tools to weaponize information only raises the stakes in an otherwise familiar contest. Technologies that increase the efficiency, scalability, and diffusion of disinformation exacerbate vulnerabilities in U.S. society. Advances in technology make an old game especially pernicious.

FOREIGN INFLUENCE CAMPAIGNS AND DISINFORMATION

Influence campaigns—which can rely heavily on peddling disinformation—can be defined as the organized use of information to intentionally confuse, mislead, or shift the public opinion of a targeted population to achieve strategic aims.[16] This report defines disinformation as the intentional propagation of false or misleading information.[17] In order to combat their

effectiveness, particular attention should be paid to the agents (actors) and enablers (tools and techniques) of digital disinformation and foreign influence campaigns.

Agents

Researchers, media, and the general public continue to call attention to state-sponsored influence campaigns led by authoritarian powers ideologically opposed to democratic systems. Russian use of influence operations to undermine transatlantic solidarity is well documented. Leave out today's Saint Petersburg-based Internet Research Agency's (IRA's) Facebook incursions and consider the fake HIV/AIDS origin story from the Cold War. Dubbed Operation Infektion by their East German allies, Soviet operatives planted a narrative in a Russian-linked New Delhi newspaper in 1983 alleging that the U.S. military created the HIV/AIDS virus as a biological weapon.[18] The narrative took hold in the mid-1980s,

> **To most Americans, the recent onslaught of influence operations at home may feel like a novel threat. But disinformation and influence operations are not new.**

prompting a repudiation by the Reagan administration, but has since been cited by world leaders and pop culture figures alike.[19] China is also reportedly expanding its tactics to stifle democratic institutions in Taiwan by sowing discord in Taiwan's domestic politics.[20] These efforts appear to target popular support for the incumbent Tsai Ing-wen administration and insert discordant voices into the domestic arena with propaganda units, bots, co-opted journalists, and "content mills."[21] Another example includes the Philippines, where Duterte's Partido Demokratiko Pilipino Bayan (PDP-Laban) employs bot operators to tighten his grip on the population.[22] And Mexico offers another potential battleground, as RT en Espanol's coverage in advance of the 2018 Mexican presidential elections sought to widen a chasm between the United States and Mexico in support of populist President Andrés Manuel López Obrador.[23]

In addition to state actors, non-state actors like NGOs, local media, and authorities (often within the spheres of influence of malicious actors) play a role in foreign attempts to subvert democratic institutions.[24] In some instances, these actors have received training to incite physical violence and rioting against Western interests.[25] Other non-state actors are using online influence campaigns to challenge certain tenets of free, open societies, like dissent and the rule of law. These include contingents like Legion Holk, a self-organized grouping of online trolls originating in Mexico, which deliberately targets journalists and is linked to social media that promotes violence, looting, and general disorder within the region.[26]

Enablers

These actors can combine tactics such as amplification and microtargeting to maximize their effects.[27] A 2016 assessment of online bot activity by a U.S. cybersecurity firm concluded that bots make up over 50 percent of all online traffic.[28] Political bots target public opinion by amplifying damaging or distracting stories through "troll farms" (groups of online users coordinating their engagement with other users with intent to harass, mislead, or spread disinformation) and social media botnets (automated networks of fake accounts).[29] Actors can also mask their digital footprints via Internet Protocol spoofing, layering on obfuscation and compounding the anonymity offered by bots. And metadata generated by users of online platforms—often to paint a picture of consumer behavior for targeted advertising—can be exploited for disinformation purposes as well.[30] User data can be leveraged for microtargeting, in which personality assessments are used to tailor messages and content to specific cross-sections of the population.[31] In lieu of consumer ads, users are fed political ads based on their ideological preference, as determined by their online activity. Once users are identified as "left-leaning" or "right-leaning" on media platforms, political interest targeting can open the door for more malicious targeting efforts.[32]

Russian-linked operatives employed these techniques in the U.S. presidential election of 2016 to launch a state-sponsored influence campaign aimed at sowing discord within the United States. From at least 2016, Russians working for the Internet Research Agency used U.S.-based email accounts (linked to stolen online identities) and virtual private networks to provide secure, encrypted access while transmitting data via shared networks. These operatives also used servers to mask their St. Petersburg location in order to launder money through PayPal and cryptocurrency exchanges.[33] The IRA started on Twitter in 2013 and expanded its messaging to other social media platforms like Facebook and Instagram, reaching tens of millions of U.S. users by 2018.[34] Similarly, the Russian hacking group CyberBerkut uses a combination of hacking and disinformation

Outside the United States, Russian actors are seeking to undermine democratic alliances and penetrate electoral processes.

propagation through organizational doxing, a practice of hacking into the networks of a targeted organization to steal and publish or expose information.[35] This is typically aimed at confusing public perceptions of political issues.

Outside the United States, Russian actors are seeking to undermine democratic alliances and penetrate electoral processes. For example, Russian-linked operatives weaved disinformation into a tranche of materials they hacked and made public during the 2017 French election. These agents targeted Emmanuel Macron's presidential campaign En Marche, hacked its network, extracted real information, and planted doctored documents within those materials.[36] The ultimate goal was to "expose" alleged dirty deeds in the campaign to the French public, like the falsified purchase of drugs by a Macron staffer.[37] Similarly, Russian-linked operatives flooded social media with fake news and forged documents during the 2016 debate over Sweden's military cooperation with NATO.[38]

Russia's Internet Research Agency, previously located in this building on Savushkina Street in St. Petersburg, was home to a government-linked troll farm, or group of online users coordinating their engagement with other users with intent to harass, mislead, or spread disinformation. (Charles Maynes/VOA)

AMPLIFYING POLITICAL POLARIZATION

The U.S. public is more ideologically divided than at any point in recent memory.[39] Gaps and disparities in educational attainment and income, as well as the rural-urban divide, have led to an environment that incentivizes tribal attitudes with a winner-take-all mentality.[40] This split supports and reinforces a hyperpartisan information ecosystem in traditional and social media.[41] Confirmation bias and conspiratorial thinking foster distrust in government institutions, the media, and other Americans, creating fertile soil for malicious state and non-state actors to sow further discord. It is precisely in this type of environment that "fake news" thrives, with social media as its breeding ground.

Social media's low barriers to entry make it easy for malicious actors to spread false, hyperpartisan content and propaganda to shape the information environment. Additionally, a 2018 study conducted by researchers from the Massachusetts Institute of Technology revealed that "falsehood diffused significantly farther, faster, deeper and more broadly" than truth on Twitter, especially regarding political news.[42] The researchers attributed this finding in part to the novelty and emotional reaction the tweets elicited in the humans who consumed them. Anonymity, new messaging technologies that enable microtargeting, and state and non-state actors with varying motivations further clutter this landscape. Confirmation bias and even radicalization are encouraged by algorithms serving up clickbait.[43] For instance, an investigation published in 2018 by *The Wall Street Journal* discovered that YouTube's recommendation algorithms point users to channels composed of "conspiracy theories, partisan viewpoints and misleading videos."[44] (YouTube has, as of January 2019, updated its recommendation algorithms to reduce "content that could misinform users in harmful ways."[45]) Taking advantage of this digital terrain, Russia devoted an entire apparatus to exploiting social media with a "Translator Project" and targeted the U.S. public through Facebook, Instagram, Twitter, and YouTube to maximize reach and impact, according to a February 16, 2018, U.S. grand jury indictment.[46]

Political polarization provides opportunities for foreign entities to further divide the U.S. public. For instance, in the wake of the 2018 Parkland high school shooting, Russia sought to inflame the ongoing U.S. domestic gun control debate by flooding Twitter with #guncontrolnow and incendiary hashtags designed to elicit emotional reactions.[47] As recently as May 2018, Russian-linked accounts weighed in on the U.S. National Football League national anthem controversy—on both

In the wake of the Salisbury, U.K., poisonings of Russian defector Sergei Skripal and his daughter Yulia, upwards of 2,800 Russian bots reached an estimated 7.5 million people in the United Kingdom when promulgating pro-Russian conspiracy theories. Some accounts cited Russian state-sponsored news outlet RT.com and used the hashtag #FalseFlag. (Screenshot @Piers Corbyn)

sides of the debate.[48] A report prepared in December 2018 for the Senate Select Committee on Intelligence noted that Russia's IRA targeted African Americans, Mexican Americans, and other specific demographic groups on Facebook and Instagram with messaging designed to stir distrust in U.S. political institutions.[49] An investigation by *USA Today* also found that more than half of the 3,500 IRA-created Facebook ads released in May 2018 as part of a U.S. House Permanent Select Committee on Intelligence investigation referenced race.[50] In similar efforts, terrorist groups like ISIS sought to exploit U.S. domestic fissures by exhorting their followers to stoke racial tensions within the United States as a way of contributing to America's ultimate destruction.[51] U.S. allies face similar Russian attacks. Upwards of 2,800 Russian bots reached an estimated 7.5 million people in the United Kingdom when promulgating pro-Russian conspiracy theories in the wake of the Salisbury poisonings.[52] Taken together, this landscape can cultivate the germs of democratic subversion by malicious foreign actors.

EMAIL HACKING AND INFORMATION DISCLOSURES

Real information can also be used as a weapon in foreign influence campaigns. Malign actors can subvert democratic institutions through hacking and information disclosures (of real information). Selective disclosures of hacked information can foster distrust and attempt to break down civil national discourse. With the American information landscape increasingly tribalized and fractured, a pervasive sense of mistrust in the system is a win for opponents of democracy. Methods of breaking down cohesion in this manner include campaign spearphishing and information disclosures.

Campaign Spearphishing

Spearphishing is characterized by attempts to trick a target into revealing information or installing malware by posing as a legitimate request via email. Digital phishing, like the email-based attack that victimized presidential candidate Hillary Clinton's campaign chairman John Podesta and the Democratic National Convention in 2016, is likely to continue for candidates, their staff, and even election administrators.[53] With the aid of AI-enabled information processing, these attacks will become more difficult to distinguish from legitimate inquiries. The ability to conduct automated spearphishing at scale will further increase the odds of an attacker's success.[54]

Information Disclosures

Seeding false information into a stream of hacked, real information can undermine trust in electoral candidates themselves. The 2017 French presidential election was a field-test of this technique, with Russian operatives reportedly forging documents to "prove" that a Macron staffer purchased drugs.[55] The Russians mixed in falsified documents with hacked authentic information, hoping to turn French public opinion against Macron and his team. Despite the French public's lack of a strong

During the 2017 French election campaign, Russian-linked operatives weaved disinformation into a tranche of materials they hacked and made public. These agents targeted Emmanuel Macron's presidential campaign En Marche, hacked its network, extracted real information, and planted doctored documents within those materials. (Axel Schmidt/Getty Images)

Election support specialists test Miami-Dade County's voting machines in Florida to ensure accuracy ahead of the U.S. 2018 midterm elections. As late as 2016, an estimated 43 states were using decade-old voting machines prone to malfunction and reliant on obsolete software. (Joe Raedle/Getty Images)

response to the fake documents, these hacking attempts bear implications for the highly polarized U.S. domestic arena. An adversary does not need Americans to believe false information to win, only for them to question the authenticity of real information. A fractured public may be more inclined to doubt the veracity of information from the targeted candidate or camp, especially if they are on opposing sides.

ELECTION INFRASTRUCTURE HACKING

Malign foreign actors also have sought to directly hack election infrastructure, such as voting machines. Malicious actors do not have to succeed in manipulating U.S. voting rolls or voter records to achieve their ends. To weaponize uncertainty, they simply need to undermine America's faith in the integrity of the process. However, an increasing reliance on electronic equipment for administering elections introduces clear digital vulnerabilities in the voting ecosystem. The infrastructure to support these local and national endeavors must be recreated and reimplemented due to varying election schedules. This infrastructure, which includes voter registration databases and day-of electronic pollbooks to record votes, is often held by third-party contractors and may be minimally secured.[56] Department of Homeland Security officials acknowledged that foreign adversaries targeted 21 states in the run-up to the 2016 presidential election and even succeeded in accessing some voting registration databases.[57] Officials did not indicate whether actual election results were impacted by these breaches.

Voting Machines & Ballot Counting

According to New York University's Brennan Center, an estimated 43 states were using decade-old voting machines prone to malfunction and reliant on obsolete software in 2016.[58] Other inspections revealed serious vulnerabilities with U.S. voting machines prior to the 2016 elections, including devices connected to a wireless network easily accessed with mobile phone connections and voting machines with potential vulnerabilities in their ballot counting processes.[59]

Other Attack Vectors

Voting registry vendors and other elements of the voting infrastructure offer opportunities for attackers to infiltrate the election process. Before the U.S. presidential election of 2016, Russian operatives targeted voter registration software supplier VR Systems, reportedly breaking into its servers and sending phishing emails to 122 state and local election-affiliated accounts in Florida.[60] Other companies and elements of the supply chain in the voting ecosystem are similarly at risk.

Election Readiness

A February 2018 Center for American Progress report indicated that since 2016, every state had undertaken security measures aimed at improving the administration of their 2018 midterm elections.[61] However, significant gaps and uneven progress remain. For instance, as of September 2018, only 1,100 out of 10,000 election jurisdictions are registered for the Department of Homeland Security's federal election threat alert system.[62]

Additionally, before the 2018 U.S. midterm elections, five states relied exclusively on electronic voting without paper back-ups—a major cyber vulnerability.[63]

> **Modern digital technologies present new vulnerabilities and open up new avenues for subversion—both cognitive and digital.**

Modern digital technologies present new vulnerabilities and open up new avenues for subversion—both cognitive and digital. But tech companies and the public sector already possess the muscle memory for identifying these attempts, restricting the space in which malicious actors operate, and fighting back against their initiatives. The counterterrorism experience created this muscle memory, which can be captured in five lessons.

Five Lessons

Lesson 1: Automate What You Can, When You Can[64]

First, social media companies should identify the tool-based methods that make their platforms "hostile" to terrorist content and then apply them to state-sponsored influence campaigns. Restricting the space in which bad actors can operate takes multiple forms, including identifying and removing content by using machine learning applications, mitigating the amplification of nefarious content, and reducing anonymity. These techniques can be applied directly to policing foreign influence campaigns on social media platforms, through their content and the behaviors that characterize them.

In the tech sector's current counterterrorism efforts, humans train machine "classifiers" to help identify content that violates that platform's terms of service.[65] Natural language processing, an application of machine learning used to help "understand text that might be advocating for terrorism," can be used against the spread of disinformation as well.[66] On Twitter, algorithms are already doing the heavy lifting in identifying accounts promoting terrorism: Machines flagged 93 percent of accounts that were suspended for promoting terrorism. Of those, three-quarters were taken down before launching a single tweet. Automation enables operations not only at larger scales but also in faster timelines, allowing for a speedy counter to influence operations.[67] Additionally, some social media companies identify and store common terms used by terrorism-related accounts and check new content against these banks as it is uploaded or posted. If these words match, content will be reviewed and possibly removed or featured less prominently ("downgraded") in users' feeds. Instead of terrorism-related words, a bank of words or characters that signal suspected misinformation, propaganda, or known disinformation campaigns can be instituted as a source of automated detection across platforms.

To restrict behaviors that characterize foreign influence campaigns, such as what Facebook terms "coordinated, inauthentic behavior," companies can adopt specific measures.[68] These include reducing anonymity, improving attribution by tightening verification processes (e.g., checking accounts that show signs of automation rather than human control), and increasing account integrity evaluation. Such methods, tested in the counterterrorism sphere to reduce the proliferation of malign networks, can be applied to reduce the number of fake accounts spreading disinformation.[69] Finally, the practice of identifying shared characteristics of suspicious accounts to detect terrorist clusters is an easily applicable methodology for detecting other malign networks.[70]

Facebook and Google are already implementing similar practices in the disinformation fight, such as de-ranking content flagged by third-party fact-checkers on their Newsfeeds and recalibrating search algorithms.[71] Social media companies have also come a long way in reducing the amplification of disinformation through botnet detection and removal, as well as troll tracking. Similarly, active use of detection algorithms can help reduce the spread of disinformation, like Twitter's suspension of 70 million accounts in May and June of 2018 and reported suspension of 9.9 million suspicious accounts a week, up from 3.2 million a week in September 2017.[72] As the volume and variety of data increases in the information environment, applying automation and machine learning to content mitigation, reducing amplification, and tightening attribution will only enhance these efforts.

RECOMMENDATION

Tech companies should, over the long term, direct a sustainable percentage of engineering capacity to automating the identification of state-sponsored malign influence campaigns. Companies can leverage existing practices and traditions, like Facebook "hackathons," to determine engineering tasks and build prototypes for this specific purpose. Companies should experiment with similar forums to seek new technical fixes for the disinformation problem.[73]

Former Acting Secretary of the U.S. Department of Homeland Security Elaine Duke delivers remarks at the first workshop of the Global Internet Forum to Counter Terrorism (GIFCT) in San Francisco in 2017. The GIFCT is an industry-led forum designed to disrupt and prevent terrorist use of member platforms. (Elijah Nouvelage/Getty Images)

Lesson 2: Increase Collaboration Among Companies

Industry cooperation has been essential to the counterterrorism fight. The hash-sharing consortium, introduced in 2016 between Facebook, YouTube, Twitter, Microsoft, and other companies, or the more formal Global Internet Forum to Counter Terrorism, provides a concrete model for this lesson.[74] The hash-sharing agreement created a shared industry database to automatically identify matching content—videos and images—that violates company policies. In other words, when one company detects terrorist content and inputs it in the database, future hits on the database should block this terrorist content before it is even posted to other platforms, precluding user engagement. Ultimately, this expanded into the GIFCT, an industry-led forum designed to disrupt and prevent terrorist use of its members' platforms. This initiative grew from purely large tech companies to one that includes smaller companies and partners with international government agencies, academics, and NGOs.

Different tech companies often face similar challenges in this new battlespace. Certain companies share each other's unique concerns: from creating policies for a majority of users outside the United States and Canada, like Facebook, to developing cutting-edge technologies that outpace traditional attempts to govern them. This overlap within industry is especially apparent when dealing with suspicious content and repeat offenders or recidivists.[75] Training and knowledge of each other's community guidelines can help streamline processes to detect content and recidivism in the disinformation fight. Just like industry cooperation helped to catch terrorist propaganda posts on YouTube before they were uploaded to Twitter, it can help prevent false state-sponsored narratives from spreading between platforms. Once identified, images and memes like those within the Internet Research Agency's 3,500 Facebook and Instagram posts released in May 2018 could be automatically prevented from distribution across platforms.[76]

As of mid-2018, tech companies are making major strides in collaborative efforts. Microsoft's "Defending Democracy" announcement in April 2018 cited partnerships between technology companies as part of countering the cyber-enabled interference threat.[77] In September 2018, Facebook's Chief Operating Officer Sheryl Sandberg told the Senate Select Committee on Intelligence that Facebook was working closely with industry peers to make progress on the problem of foreign influence operations.[78] Google, Facebook, and Twitter's pledge in the same month to work together to fight "fake news" in Europe can act as a test case for expanding this collaboration globally.[79] Recognizing that companies can effectively work together on these issues is critical, but these companies already have a ready-made, proven model within their own industry as a result of counterterrorism efforts. They should use and expand it.

Sheryl Sandberg, Facebook's Chief Operating Officer, testifies before the Senate Select Committee on Intelligence about Russian attempts to interfere in the 2016 U.S. presidential elections and social media companies' efforts to combat foreign influence operations. Jack Dorsey, CEO of Twitter, also testified in this session. (Drew Angerer/Getty Images)

RECOMMENDATION
Tech companies should create and fund an enduring disinformation detection consortium between willing companies, modeled after the GIFCT. The goal would be to not only increase automated detection of disinformation content between platforms, but to move toward establishing industry standards on what constitutes disinformation.[80] As with the hash-sharing consortium, the foundational element of this collaboration can be technical, with potential expansion to relevant cross-functional entities.

Lesson 3: Share Info and Analysts

A critical component of combating malign, foreign networks and actors is how the U.S. government organizes for the fight. Calls by experts for a body like the NCTC or an overarching structure like ODNI to coordinate information-sharing and streamline approvals processes for countering disinformation are rising.[81] These bureaucratic bodies are effective mechanisms for counterterrorism intelligence integration and authorities at a high, interagency level. However, effective collaboration is also needed "on the ground."[82] As established in the global war on terror, lower-level, peer-to-peer collaboration can generate immediate results. These interactions can also act as a testbed for the potential establishment of a new, overarching body whose remit is to counter and respond to digital foreign influence operations.

Under the philosophy that intelligence drives operations, after 9/11, Special Operations Command units were integrated at the analyst level through various mechanisms, one of which was the Joint Interagency Task Force (JIATF).[83] Subject matter experts specializing in social network and all-source intelligence analysis were in the same room as commanders leading the assault forces that would "operationalize" their analysis. This direct access

> **A critical component of combating malign, foreign networks and actors is how the U.S. government organizes for the fight.**

between "support" and the "action arm" not only cut out the middle man and saved valuable time, but also encouraged innovation within respective agencies. Young agency officers, often siloed within their respective organizations, not only shared threat intelligence for early indications and warning but traded best practices and brainstormed new solutions.

The National Counterterrorism Center, headquartered in northern Virginia, was founded in 2004 to improve information-sharing in order to better anticipate and respond to terrorist threats. Experts are calling for a similar body to combat foreign influence operations. (Mark Wilson/Getty Images)

Interagency information-sharing successes in the years following 9/11 can serve as a model for intelligence integration. The tech sector will be a key force multiplier in the wars of the future, and past successes can help bridge the public-private sector divide by putting ground-level experts from both sectors in the same room. These frameworks already exist, and proven systems of integration are in place. Creating smaller, more forward-leaning fusion cells that temporarily integrate public and private sector analysts at a more granular level of information-sharing can provide the agility needed for government and private companies to counter foreign information operations together. Social media companies are already integrating former practitioners into threat intelligence programs and other areas to sharpen responses to terrorist threats, especially in the case of imminent, "real-world" harm. Further, these companies are growing robust law enforcement response apparatuses that liaise with their federal government counterparts in the counterterrorism realm. But this is not enough to build a capability that offers proper

indications and warning for influence operations in the current information environment.

Such efforts should be expanded and refined for the disinformation fight. Tech company partnerships with academic and research institutions, like Google's partnerships with the National Cybersecurity Alliance and the Belfer Center for Science and International Affairs at the Harvard Kennedy School and Facebook's collaboration with the Atlantic Council, provide an important foundation from which to launch these efforts. Building on these partnerships to include government analysts who focus on intelligence value will help counter malign foreign influence campaigns on social media platforms. Entities like the FBI's Foreign Influence Task Force are a good start, but should be part of a broader effort that reaches to the analyst level, with U.S. government and tech company buy-in.[84]

U.S. intelligence agencies and major tech firms should co-locate their analysts on a voluntary basis to facilitate granular-level information sharing.[85] This would recreate the JIATF construct to include private sector analysts and formalize a public and private information-sharing mechanism. Private threat-intelligence analysts and government all-source analysts should be the initial focus of this effort. Voluntary, one-for-one analyst exchanges between the government and the tech sector, for predetermined time periods, are also an option. The goal is to generate momentum to respond quickly to the threat of foreign influence operations, and to create an enduring dialogue to share threat-oriented tactics and techniques at appropriate levels of classification.[86]

RECOMMENDATION

ODNI, in coordination with the private sector, should appoint a body of interagency representatives to create and fund smaller, more forward-leaning fusion cells that integrate public and private sector analysts on a voluntary basis. These fusion cells would reside under ODNI and serve as an unclassified testbed for exploring the appointment of a higher-level interagency body to tackle the threat of malign foreign influence campaigns in the digital realm. Social media companies should lend their threat intelligence analysts (with intelligence agencies providing relevant all-source analysts) to this effort in an enduring, persistent dialogue at the unclassified level.

Lesson 4: Keep the Pressure On

Policymakers should apply a counterterrorism philosophy – sustained pressure to create a non-permissive operating environment— to today's disinformation fight. This type of persistent presence is analogous to the concept of "tactical friction" laid out in the March 2018 Command Vision for U.S. Cyber Command.[87] Policymakers should embrace the concept of tactical friction and the "continuous engagement" that "imposes strategic costs on our adversaries, compelling them to shift resources to defense and reduce attacks."[88] This type of "defend forward" mentality in the physical realm served as a general framework for the counterterrorism policy community, arguably helping reduce the territory controlled by ISIS since 2014 down to 1 percent of what it previously controlled in Syria.[89] So far, the application of this concept to the cyber realm, especially in the social media age of content takedowns, has been mixed. The United States' 2016 operation to disrupt ISIS propagandists online, Operation Glowing Symphony, left little of an enduring mark, as terrorists simply recycled their content on other platforms.[90]

> **On the private side, tech companies can follow suit by aggressively prioritizing and resourcing their efforts against influence operations, just like they did with counterterrorism.**

More pressure is needed. Despite the good work the government and tech companies are doing, terrorists continue to find new and creative ways to abuse social media platforms, and social media companies continue to hire terrorism analysts and reviewers to keep up.[91] While the transferability of these counterterrorism tactics and techniques is a useful start, the disinformation problem, with its broader implications for democratic institutions, requires an increasingly proactive posture.

The United States should take initiative to shape the decisionmaking of its adversaries to reset conditions of deterrence in cyberspace. This includes imposing costs on offenders who use cyber-related social media operations to peddle the subversion of democratic institutions, developing preemptive techniques, and undertaking disruptive activities. The September 2018 Department of Defense Cybersecurity Strategy and CYBERCOM's fall 2018 operations targeting individual Russians to deter the spread of disinformation are steps in the right direction.[92] By giving DoD the authority to "defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict," the U.S. is resetting conditions to make deterrence possible.[93] Presidential Policy Directive-20

revisions by the current administration also offer a potential mechanism for imposing costs on would-be sponsors of foreign influence operations.[94] Yet the U.S. government can still do more to complement these efforts. Efforts with a lighter touch, like government cooperation with internet service providers to rethink internet access for attackers, are easy ways to start.[95] On the private side, tech companies can follow suit by aggressively prioritizing and resourcing their efforts against influence operations, just like they did with counterterrorism.

There are obvious pitfalls to a more aggressive approach, to include frustrating allies with any missteps and escalating cyber conflict to the physical realm. Applying greater force must be tempered by these trade-offs. Specifically, the United States should take care to avoid conducting offensive *influence* operations. Its track record of attempting to influence electoral outcomes, from the Cold War to Iran in 1953 and Serbia in 2000, is poor.[96] More recent information operations conducted by the United States against the Taliban in Afghanistan during the war on terror yielded mixed results at best and revealed critical weaknesses in its counter-messaging capabilities in the process.[97] Further, a legitimacy question exists when the United States engages in the behavior it would seek to deter in other countries. Overall, the bad is likely to outweigh the good if America intends to remain a credible voice against election meddling worldwide.

But even more important than the efficacy (or lack thereof) of such efforts is the dangers they would pose to the free system upon which the United States depends. The United States possesses an asymmetric advantage over authoritative regimes: the truth. While lies, disinformation, and influence campaigns benefit dictatorships, which rule by power and fear, free societies like the United States use truth as a touchpoint, a disinfectant against corruption and tyranny. Certain regimes must cultivate false realities—like the "harmonious" society of North Korea or the fist of order China brandishes internally—to survive. But in democracies, the public has access to the truth, warts and all. Authoritarian regimes need lies to retain their grip on power. This makes the truth a powerful weapon against repression, and the United States should not surrender such an advantage. When the truth prevails, democracy wins.

U.S. Cyber Command conducted operations in the fall of 2018, in a similar timeframe to the November 2018 U.S. midterm elections, targeting individual Russians to deter the spread of disinformation. (Chip Somodevilla/Getty Images)

RECOMMENDATION

The executive branch should expand on its Cybersecurity Strategy and CYBERCOM's authorities to conduct expeditious, offensive cyber operations that impose costs on foreign adversaries. It should invest in convening democratic allies to exchange best practices from their own forays into loosening restrictions on offensive cyber measures and provide CYBERCOM with the results. However, expanding authorities should stop short of directives to conduct offensive *influence* operations in foreign countries.

Lesson 5: Leverage Allies[98]

This complementary line of effort and component of a pressure-driven strategy rests in a largely untapped advantage: U.S. democratic allies. NATO contributions to the war on terror enhanced intelligence collection and drove operations in Operation Enduring Freedom in Afghanistan. At peak levels, the International Security Assistance Force in Afghanistan included troops from 51 partner nations, with multiple countries acting as the battlespace owners of Regional Commands.[99] Separately, the NATO Alliance became an official member of the Global Coalition to Defeat ISIS in May 2017 and soon established a Terrorism Intelligence Cell for information sharing at its headquarters in Brussels.[100] Today, 38 nations in addition to the United States supply troops to Operation Resolute Support in Afghanistan to counter the terrorist threat.[101]

As with terrorism, the United States can leverage our NATO partners' long experience as victims of disinformation campaigns (for example, Estonia in 2007, the United Kingdom in 2016, France in 2017, and Germany in 2017) to enhance its own initiatives.[102] The United States' common investment with its democratic partners in systems of governance and values (e.g., free press, open society, rule of law, etc.) provides similar

Defense chiefs from NATO member states, like Chairman of the U.S. Joint Chiefs of Staff USMC General Joe Dunford and his United Kingdom counterparts, can leverage NATO partners' long experience as victims of disinformation campaigns to enhance U.S. initiatives. (James. K. McCann/Department of Defense)

environments to test use cases of successful cyber operations that keep the pressure on or technically frustrate enemies of democracy. And given the extensive investigation of the Internet Research Agency's "Translator Project" and the Russian hacking group CyberBerkut, the United States has an idea of how tomorrow's enemy will operate against Western systems. The French are already codifying lessons learned from their 2017 presidential elections and Macron leaks, and Germany expanded its legal framework to potentially include offensive cyber measures.[103] Using the know-how of U.S. friends and re-orienting the intent to actively seek out similar enemies will move the United States in the right direction.[104]

RECOMMENDATION

The United States should convene democratic allies to exchange best practices from their own experience countering foreign influence campaigns and their forays into loosening restrictions on offensive cyber measures. The United States should use the same convening mechanism to institute a formal method of providing CYBERCOM with the results of this information-sharing and recommendations for action.

Conclusion

Information operations are not new. But the growth of emerging technologies threatens to disrupt and overwhelm the fixes that social media companies and governments already have in place.[105] Conflicts of the future will heighten the efficiency of disinformation campaigns, make fake information almost indistinguishable from reality, and target specific segments of the electorate for electoral influence at scale.

The counterterrorism analogy is valuable but has limitations. Key features of the U.S. counterterrorism strategy—preventing terrorist groups from controlling territory, uprooting them from safe havens, and removing enemy combatants from a physical battlespace—can align conceptually, but do not perfectly translate to a murkier, digital information battlespace. Additionally, disinformation campaigns play heavily on the susceptibility of humans to manipulation and subversion. Enemies of democracy are striking at the heart of public confidence in the entire system. The United States must mobilize many aspects of society to confront them. Technology, political, legal, and economic actors must collaborate to retain the faith in democratic institutions that disinformation purveyors are seeking to undermine. Already, signs point to this conviction fraying.[106] Combined with technology that exacerbates these doubts, the situation threatens grave geopolitical consequences. The United States possesses a toolkit with which to meet this challenge. It should use it.

Endnotes

1. Kara Frederick, "How to Defend Against Foreign Influence Campaigns: Lessons from Counter-terrorism," *War on the Rocks*, October 19, 2018, https://warontherocks.com/2018/10/how-to-defend-against-foreign-influence-campaigns-lessons-from-counter-terrorism/.

2. David Zax, "Secrets of Facebook's Legendary Hackathons Revealed," *Fast Company*, November 9, 2012, https://www.fastcompany.com/3002845/secrets-facebooks-legendary-hackathons-revealed.

3. Laicie Heeley, Amy Belasco, Mackenzie Eaglen, Luke Hartig, Tina Jonas, Mike McCord, and John Mueller, "Counterterrorism Spending: Protecting America While Promoting Efficiencies and Accountability," Stimson Study Group on Counterterrorism Spending (Stimson Center, May 2018); and Aaron Mehta, "Here's how much the US has spent fighting terrorism since 9/11," *Defense News*, May 16, 2018, https://www.defensenews.com/pentagon/2018/05/16/heres-how-much-the-us-has-spent-fighting-terrorism-since-911.

4. The prevailing logic of the U.S. government was that such reforms could help prevent or mitigate the impact of similar terrorist threats to the United States. As of 2019, the mission centers of ODNI include NCTC and the Cyber Threat Intelligence Integration Center, the National Counterproliferation Center, and the National Counterintelligence and Security Center.

5. Office of the Director of National Intelligence, "Who We Are," ODNI.gov, https://www.odni.gov/.

6. The National Counterterrorism Center, "Who We Are," ODNI.gov, https://www.odni.gov/index.php/nctc-home.

7. Department of Justice, "The USA Patriot Act: Preserving Life and Liberty," Justice.gov, https://www.justice.gov/archive/ll/highlights.htm.

8. SITE Staff, "IS Supporters React to James Foley Beheading Video," INSITE Blog, August 20, 2014, http://news.siteintelgroup.com/blog/index.php/categories/jihad/entry/238-is-supporters-react-to-james-foley-beheading-video; and Seamus Hughes, "Whose Responsibility is it to Confront Terrorism Online?" Lawfare, April 27, 2018, https://www.lawfareblog.com/whose-responsibility-it-confront-terrorism-online. While concerns over terrorist use of online platforms as propaganda was discussed in 2007 and earlier, the online amplification of Foley's 2014 murder increased the visibility of the problem for U.S. lawmakers.

9. Monika Bickert and Brian Fishman, "Hard Questions: Are We Winning the War on Terrorism Online?" Facebook, press release, November 28, 2017, https://newsroom.fb.com/news/2017/11/hard-questions-are-we-winning-the-war-on-terrorism-online; 18 U.S.C. § 2339A, "Providing Material Support to Terrorists," https://www.justice.gov/jm/criminal-resource-manual-15-providing-material-support-terrorists-18-usc-2339a; and 18 U.S.C. § 2339B, "Providing Material Support to Terrorists," https://www.justice.gov/jm/criminal-resource-manual-16-providing-material-support-designated-terrorist-organizations.

10. Aarti Shahani, "U.S. Officials, Tech Leaders Meet To Discuss Counterterrorism," NPR, January 8, 2016, https://www.npr.org/sections/alltechconsidered/2016/01/08/462385985/u-s-tech-industry-leaders-hold-meeting-on-counterterrorism.

11. Austin Carr, "Can Alphabet's Jigsaw Solve Google's Most Vexing Problems?" *Fast Company*, October 22, 2017, https://www.fastcompany.com/40474738/can-alphabets-jigsaw-solve-the-internets-most-dangerous-puzzles.

12. Alexis C. Madrigal, "Inside Facebook's Fast-Growing Content-Moderation Effort," *The Atlantic*, February 7, 2018, https://www.theatlantic.com/technology/archive/2018/02/what-facebook-told-insiders-about-how-it-moderates-posts/552632.

13. "Twitter bans 270,000 accounts for 'promoting terrorism,'" *The Guardian*, April 5, 2018, https://www.theguardian.com/technology/2018/apr/05/twitter-bans-270000-accounts-to-counter-terrorism-advocacy.

14. This section draws from previously published work by the author, namely: Kara Frederick, "How to Defend Against Foreign Influence Campaigns: Lessons from Counter-terrorism," *War on the Rocks*, October 19, 2018, https://warontherocks.com/2018/10/how-to-defend-against-foreign-influence-campaigns-lessons-from-counter-terrorism/.

15. Frederick, "How to Defend Against Foreign Influence Campaigns: Lessons from Counter-terrorism."

16. Tim Hwang, "Digital Disinformation: A Primer," (Atlantic Council, September 2017); and Herb Lin, "Developing Responses to Cyber-Enabled Information Warfare and Influence Operations," Lawfare, September 6, 2018, https://www.lawfareblog.com/developing-responses-cyber-enabled-information-warfare-and-influence-operations.

17. Hwang, "Digital Disinformation: A Primer"; and Lin, "Developing Responses to Cyber-Enabled Information Warfare and Influence Operations."

18. James. M. Ludes and Mark R. Jacobson, "Shatter the House of Mirrors: A Conference Report on Russian Influence Operations," (Pell Center for International Relations and Public Policy, October 2017), 6; and Linda Qiu, "Fingerprints of Russian Disinformation: From AIDS to Fake News," *The New York Times*, December 12, 2017, https://www.nytimes.com/2017/12/12/us/politics/russian-disinformation-aids-fake-news.html.

19. Qiu, "Fingerprints of Russian Disinformation: From AIDS to Fake News."

20. Peter Mattis, "Contrasting China's and Russia's Influence Operations," *War on the Rocks*, January 16, 2018, https://warontherocks.com/2018/01/contrasting-chinas-russias-influence-operations.

21. J. Michael Cole, "Will China's Disinformation War Destabilize Taiwan?" National Interest, July 30, 2017, http://nationalinterest.org/feature/will-chinas-disinformation-war-destabilize-taiwan-21708; and Gerry Shih, "Taiwanese president quits party leadership after pro-China rivals claim ballot landslide," *The Washington Post*, November 25, 2018, https://www.washingtonpost.com/world/taiwanese-president-quits-party-leadership-after-pro-china-rivals-claim-ballot-landslide/2018/11/25/46ce7fa4-f078-11e8-9236-bb94154151d2_story.html?noredirect=on&utm_term=.e0f564a3817d.

22. Jonathan Corpus Ong and Jason Vincent A. Cabañes, "Architects of Networked Disinformation: Behind the Scenes of Troll Accounts and Fake News Production in the Philippines," (The Newton Tech4Dev Network, February 2018), https://newtontechfordev.com/wp-content/uploads/2018/02/ARCHITECTS-OF-NETWORKED-DISINFORMATION-FULL-REPORT.pdf.

23. "El Negocio Detrás de las Noticias Falsas [The Business Behind the False News]," Expansion, November 3, 2017, https://expansion.mx/tecnologia/2017/11/03/las-mentiras-politicas-son-un-negocio; David Salvo and Stephanie De Leon, "Russian Influence in Mexican and Colombian Elections," German Marshall Fund of the United States, January 4, 2018, https://securingdemocracy.gmfus.org/russian-influence-in-mexican-and-colombian-elections/; Jonathan Head, "Myanmar conflict: Fake photos inflame tension," BBC, September 2, 2017, https://www.bbc.com/news/world-asia-41123878; and Vladimir Rouvinski, "Understanding Russian Priorities in Latin America," Kennan Cable No. 20 (Wilson Center, February 2017).

24. John Lough, Orysia Lutsevych, Peter Pomerantsev, Stanislav Secrieru, and Anton Shekhovtsov, "Russian Influence Abroad: Non-state Actors and Propaganda," (Chatham House, October 24, 2014), https://www.chathamhouse.org/sites/default/files/field/field_document/20141024RussianInfluenceAbroad.pdf.

25. Ludes et al., "Shatter the House of Mirrors," 5.

26. Andalusia Knoll Soloff, "Mexico's Troll Bots Are Threatening the Lives of Activists," *Motherboard*, March 9, 2017, https://motherboard.vice.com/en_us/article/mg4b38/mexicos-troll-bots-are-threatening-the-lives-of-activists; Tanya O'Carroll, "Mexico's misinformation wars: How organized troll networks attack and harass journalists and activists in Mexico," *Medium*, January 24, 2017, https://medium.com/amnesty-insights/mexico-s-misinformation-wars-cb748ecb32e9; and Pepe H. and Hayes Brown, "Meme Factories Are Fighting Over Who Gets Credit For A School Shooting in Mexico," *BuzzFeed News*, January 19, 2017, https://www.buzzfeednews.com/article/josehernandez/this-is-what-we-know-about-the-facebook-group-that#.xhmE7nbnX.

27. This section draws on the author's previously published, and independently conducted, research contained in the CNAS report, "Artificial Intelligence and International Security." Michael Horowitz, Gregory C. Allen, Edoardo Saravalle, Anthony Cho, Kara Frederick, and Paul Scharre, "Artificial Intelligence and International Security" (Center for a New American Security, July 2018), 5-6.

28. Adrienne Lafrance, "The Internet Is Mostly Bots," *The Atlantic*, January 31, 2017, https://www.theatlantic.com/technology/archive/2017/01/bots-bots-bots/515043/; Igal Zeifman, "Bot Traffic Report 2016," (Imperva Incapsula, January 24, 2017), https://www.incapsula.com/blog/bot-traffic-report-2016.html.; Horowitz et al., "Artificial Intelligence and International Security," 5; and Onur Varol, "Online Human-Bot Interactions: Detection, Estimation and Characterization," paper presented at International AAAI Conference on Web and Social Media, Montreal, May 2017, 1.

29. Horowitz et al., "Artificial Intelligence and International Security," 5-6.

30. Hwang, "Digital Disinformation: A Primer," 7.

31. Toomas Hendrik Ilves, "Guest Post: Is Social Media Good or Bad for Democracy?" Facebook Newsroom, January 25, 2018, https://newsroom.fb.com/news/2018/01/ilves-democracy.

32. Google, "Security and Disinformation in the U.S. 2016: What We Found," October 30, 2017, https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/google_US2016election_findings_1_zm64A1G.pdf.

33. Robert McMillan, Deepa Seetharaman, and Georgia Wells, "Russian Influence Operation Allegedly Ran Like a Propaganda Startup," *The Wall Street Journal*, February 17, 2018, https://www.wsj.com/articles/russian-influence-operation-allegedly-ran-like-a-propaganda-startup-1518872400; Del Quentin Wilber and Aruna Wiswanatha, "Russians Charged With Interfering in U.S. Election," *The Wall Street Journal*, February 16, 2018, https://www.wsj.com/articles/russians-charged-with-interfering-in-u-s-election-1518804495; and Department of Justice, *Internet Research Agency Indictment*.

34. Philip N. Howard, Bharath Ganesh, Dimitra Liotsiou, John Kelly, and Camille François, "The IRA, Social Media and Political Polarization in the United States, 2012-2018," (University of Oxford, December 2018), 18-19.

35. Bruce Schneier, "How Long Until Hackers Start Faking Leaked Documents?" *The Atlantic*, September 13, 2016, https://www.theatlantic.com/technology/archive/2016/09/hacking-forgeries/499775/.

36. Adam Hulcoop, John Scott-Railton, Peter Tanchak, Matt Brooks, and Ron Deibert, "Tainted Leaks," *The Citizen Lab,* May 25, 2017, https://citizenlab.ca/2017/05/tainted-leaks-disinformation-phish/.

37. Andy Greenberg, "Russian Hackers Are Using 'Tainted' Leaks to Sow Disinformation," *Wired*, May 25, 2017, https://www.wired.com/2017/05/russian-hackers-using-tainted-leaks-sow-disinformation/; and Adam Nossiter, David E. Sanger, and Nicole Perlroth, "Hackers Came, but the French Were Prepared," *The New York Times*, May 9, 2017, https://www.nytimes.com/2017/05/09/world/europe/hackers-came-but-the-french-were-prepared.html.

38. Neil MacFarquhar, "A Powerful Russian Weapon: The Spread of False Stories," *The New York Times*, August 28, 2016, https://www.nytimes.com/2016/08/29/world/europe/russia-sweden-disinformation.html.

39. "Political Polarization in the American Public," Pew Research Center, June 12, 2014, http://www.people-press.org/2014/06/12/political-polarization-in-the-american-public.

40. Avi Tuschman, "Why Americans Are So Polarized: Education and Evolution," *The Atlantic*, February 28, 2017, https://www.theatlantic.com/politics/archive/2014/02/why-americans-are-so-polarized-education-and-evolution/284098; Katherine J. Cramer, *The Politics of Resentment: Rural Consciousness in Wisconsin and the Rise of Scott Walker* (Chicago: University of Chicago Press, 2016); and Lazaro Gamio, "Urban and rural America are becoming increasingly polarized," *The Washington Post*, November 17, 2016, https://www.washingtonpost.com/graphics/politics/2016-election/urban-rural-vote-swing.

41. Lee Drutman, "We need political parties. But their rabid partisanship could destroy American democracy." Vox, September 5, 2017, https://www.vox.com/the-big-idea/2017/9/5/16227700/hyperpartisanship-identity-american-democracy-problems-solutions-doom-loop.

42. Soroush Vosoughi, Deb Roy, and Sinan Aral, "The spread of true and false news online," *Science*, 359 no. 6380 (March 2018), 1146-1151.

43. Zeynep Tufekci, "YouTube, the Great Radicalizer," *The New York Times*, March 10, 2018, https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html.

44. Jack Nicas, "How YouTube Drives People to the Internet's Darkest Corners," *The Wall Street Journal*, February 7, 2018, https://www.wsj.com/articles/how-youtube-drives-viewers-to-the-internets-darkest-corners-1518020478.

45. The YouTube Team, "Continuing our work to improve recommendations on YouTube," YouTube Official Blog, January 25, 2019, https://youtube.googleblog.com/2019/01/continuing-our-work-to-improve.html.

46. Department of Justice, *Internet Research Agency Indictment*, (February 16, 2018); and Brian Barrett, "For Russia, Unraveling US Democracy Was Just Another Day Job," *Wired*, February 17, 2018, https://www.wired.com/story/mueller-indictment-internet-research-agency.

47. Erin Griffith, "Pro-Gun Russian Bots Flood Twitter After Parkland Shooting," *Wired*, February 15, 2018, https://www.wired.com/story/pro-gun-russian-bots-flood-twitter-after-parkland-shooting.

48. Donnie O'Sullivan and Aaron Kessler, "Why Russian trolls may be more excited that the NFL is back than you are," CNN, September 8, 2018, https://money.cnn.com/2018/09/08/technology/nfl-national-anthem-russia-trolls.

49. Howard et al., The IRA, Social Media and Political Polarization in the United States, 2012-2018," 18-19.

50. Nick Penzenstadler, Brad Heath, and Jessica Guynn, "We read every one of the 3,517 Facebook ads bought by Russians. Here's what we found," *USA Today,* May 11, 2018, https://www.usatoday.com/story/news/2018/05/11/what-we-found-facebook-ads-russians-accused-election-meddling/602319002/.

51. Brendan I. Koerner, "Why ISIS Is Winning the Social Media War," *Wired*, April 2016, https://www.wired.com/2016/03/isis-winning-social-media-war-heres-beat.

52. Deborah Haynes, "Skripal attack: 2,800 Russian bots 'sowed confusion after poison attacks," *The Times*, March 24, 2018, https://www.thetimes.co.uk/edition/news/2-800-russian-bots-sowed-confusion-after-poison-attacks-zf6lvb3nc. In March 2018, Russian defector Sergei Skripal and his daughter were poisoned in Salisbury, United Kingdom, by suspected Russian agents, likely in retaliation for Skripal's defection.

53. University of Massachusetts Amherst, "Phishing: Fraudulent Emails, Text Messages, Phone Calls & Social Media," UMass.edu, https://www.umass.edu/it/security/phishing-fraudulent-emails-text-messages-phone-calls; Eric Lipton, David E. Sanger, and Scott Shane, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.," *The New York Times*, December 13, 2016, https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html; and Ellen Nakashima and Shane Harris, "How the Russians hacked the DNC and passed its emails to WikiLeaks," *The Washington Post*, July 13, 2018, https://www.washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78_story.html.

54. Horowitz et al., "Artificial Intelligence and International Security," 4; and John Seymour and Philip Tully, "Weaponizing data science for social engineering: Automated E2E spear phishing on Twitter," https://www.blackhat.

com/docs/us-16/materials/us- 16-Seymour-Tully-Weaponizing-Data-Science-For-Social-Engineering-Automated-E2E-Spear- Phishing-On-Twitter-wp.pdf.

55. Nossiter et al., "Hackers Came, but the French Were Prepared."

56. Meredith Berger et al., "The State and Local Election Cybersecurity Playbook," Defending Digital Democracy (Harvard Kennedy School, February 15, 2018), 22.

57. Nicole Lee, "Russians accessed US voter registration records before 2016 election," Engadget, February 7, 2018, https://www.engadget.com/2018/02/07/russians-successfully-gained-access-to-us-voter-registration-rec; Grant McCool, ed., "Russians compromised election systems in seven states: NBC News," Reuters, February 27, 2018, https://www.reuters.com/article/us-usa-trump-russia-election/russians-compromised-election-systems-in-seven-states-nbc-news-idUSKCN1GC01E.

58. "Election Infrastructure: Vulnerabilities and Solutions," (Center for American Progress, September 11, 2017); Lawrence Norden and Christopher Famighetti, "America's Voting Machines at Risk," (Brennan Center for Justice, 2015), 4; and Lawrence Norden and Ian Vandewalker, "Securing Elections from Foreign Interference," (Brennan Center for Justice, 2017).

59. Pam Fessler, "Vulnerable Voting Machine Raises Questions About Election Security," NPR, April 16, 2015, https://www.npr.org/sections/itsallpolitics/2015/04/16/399986331/hacked-touchscreen-voting-machine-raises-questions-about-election-security; Ben Wofford, "How to Hack an Election in 7 Minutes," *Politico*, August 5, 2016, https://www.politico.com/magazine/story/2016/08/2016-elections-russia-hack-how-to-hack-an-election-in-seven-minutes-214144; and Brian Barrett, "America's Electronic Voting Machines Are Scarily Easy Targets," *Wired*, August 2, 2016, https://www.wired.com/2016/08/americas-voting-machines-arent-ready-election.

60. Sam Biddle, "A Swing-State Election Vendor Repeatedly Denied Being Hacked By Russians. The New Mueller Indictment Says Otherwise," *The Intercept*, July 13, 2018, https://theintercept.com/2018/07/13/a-swing-state-election-vendor-repeatedly-denied-being-hacked-by-russians-new-mueller-indictment-says-otherwise.

61. Danielle Root, Liz Kenedy, Michael Soza, and Jerry Parshall, "Election Security in All 50 States: Defending America's Elections," (Center for American Progress, February 2018), https://cdn.americanprogress.org/content/uploads/2018/02/21105338/020118_ElectionSecurity-report11.pdf.

62. Kevin Collier, "If There Is Meddling with the Midterms, Local Voting Officials May Be to Blame," *BuzzFeed News*, September 23, 2018, https://www.buzzfeednews.com/article/kevincollier/local-governments-voting-security.

63. Eric Geller, "States slow to prepare for hacking threats," *Politico*, July 18, 2018, https://www.politico.com/story/2018/07/18/hackers-states-elections-upgrades-729054.

64. This section of the report builds on the author's original "Lessons 1-5," as conceived and published in the previously cited *War on the Rocks* commentary: Frederick, "How to Defend Against Foreign Influence Campaigns: Lessons from Counter-Terrorism."

65. Verification of content that may violate terms of service can include a combination of digital and non-digital methods with a transparent standard, to include the use of third-party fact checkers. Identifying content for review signifies that a human reviewer will interact with that content after it is flagged.

66. Bickert et al., "Hard Questions: How We Counter Terrorism," Facebook, press release, June 15, 2017, https://newsroom.fb.com/news/2017/06/how-we-counter-terrorism.

67. Twitter, "Twitter Rules enforcement," January-June 2018, https://transparency.twitter.com/en/twitter-rules-enforcement.html; and Twitter, "Twitter transparency report," https://transparency.twitter.com/.

68. Nathaniel Gleicher, "Removing Coordinated Inauthentic Behavior from Russia," Facebook Newsroom, January 17, 2019, https://newsroom.fb.com/news/2019/01/removing-cib-from-russia/.

69. "reCAPTCHA v3," Google, https://www.google.com/recaptcha/intro/v3beta.html.

70. Monika Bickert, Head of Product Policy and Counter-terrorism at Facebook, "Testimony of Monika Bickert," Hearing before the United States Senate Committee on Commerce, Science, & Transportation, U.S. Senate, January 17, 2018.

71. "Google to 'derank' Russia Today and Sputnik," BBC, November 21, 2017, https://www.bbc.com/news/technology-42065644.

72. "Update: Russian interference in the 2016 US presidential election," Twitter, press release, September 28, 2017, https://blog.twitter.com/official/en_us/topics/company/2017/Update-Russian-Interference-in-2016--Election-Bots-and-Misinformation.html; Nick Pickles, Senior Strategist, Public Policy at Twitter Inc., "Statement of Nick Pickles," Statement before the Committee on the Judiciary, U.S. House of Representatives, July 17, 2018; and Craig Timberg and Elizabeth Dwoskin, "Twitter is sweeping out fake accounts like never before, putting user growth at risk," *The Washington Post,* July 6, 2018, https://www.washingtonpost.com/technology/2018/07/06/twitter-is-sweeping-out-fake-accounts-like-never-before-putting-user-growth-risk.

73. Zax, "Secrets of Facebook's Legendary Hackathons Revealed." These groups should be composed of cross-functional teams within each company, like finance, information security, legal, etc.

74. "Update on the Global Internet Forum to Counter Terrorism," Google, press release, December 4, 2017, https://www.blog.google/around-the-globe/google-europe/update-global-internet-forum-counter-terrorism.

75. Bickert et al., "Hard Questions: Are We Winning the War on Terrorism Online?"

76. Issie Lapowsky, "House Democrats Release 3,500 Russia-Linked Facebook Ads," *Wired*, May 10, 2018, https://www.wired.com/story/house-democrats-release-3500-russia-linked-facebook-ads.

77. "Announcing the Defending Democracy Program," Microsoft, press release, April 13, 2018, https://blogs.microsoft.com/on-the-issues/2018/04/13/announcing-the-defending-democracy-program.

78. Sheryl Sandberg, Chief Operating Officer at Facebook, "Testimony of Sheryl Sandberg," Hearing before the United States Senate Select Committee on Intelligence, U.S. Senate, September 5, 2018.

79. Natalia Drozdiak, "Google, Facebook and Twitter Agree to Fight Fake News in the EU," Bloomberg, September 25, 2018, https://www.bloomberg.com/news/articles/2018-09-25/google-facebook-and-twitter-agree-to-fight-fake-news-in-eu.

80. Just as private technology companies exchange views with peer companies to grapple with definitions of "terrorism," they can use those same companies as sounding boards to help define disinformation and debate the value of an industry standard.

81. Robert J. Butler, Senior Vice President, Critical Infrastructure Protection Operations, AECOM Adjunct Senior Fellow, Center for a New American Security, "Countering Russian Influence in the United States Elections Process," Testimony before the Cyber Subcommittee, Senate Armed Service Committee, U.S. Senate, February 13, 2018, 3.

82. U.S. Congress, Senate, Committee on Armed Services, Subcommittee on Cybersecurity, *Hearing to Receive Testimony on the Department of Defense's Role in Protecting Democratic Elections*, 115th Cong., 2nd sess., 2018, 1-65.

83. Christopher Lamb, "Global SOF and Interagency Collaboration," *Journal of Strategic Security*, 7 no. 2 (2014), 8-20.

84. "The FBI Launches a Combating Foreign Influence Webpage," Federal Bureau of Investigation, press release, August 30, 2018, https://www.fbi.gov/news/pressrel/press-releases/the-fbi-launches-a-combating-foreign-influence-webpage.

85. This paragraph is composed of selected portions of the author's original language from "Lesson 3" of the previously cited *War on the Rocks* commentary: Frederick, "How to Defend Against Foreign Influence Campaigns: Lessons from Counter-Terrorism."

86. Frederick, "How to Defend Against Foreign Influence Campaigns: Lessons from Counter-Terrorism."

87. Patrick Tucker, "Trump's Pick for NSA/CyberCom Chief Wants to Enlist AI For Cyber Offense," Defense One, January 9, 2018, https://www.defenseone.com/technology/2018/01/how-likely-next-nsacybercom-chief-wants-enlist-ai/145085.

88. "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command," (United States Cyber Command, March 23, 2018).

89. Linda Qiu, "Can Trump Claim Credit for a Waning Islamic State?" *The New York Times*, October 17, 2017, https://www.nytimes.com/2017/10/17/us/politics/trump-islamic-state-raqqa-fact-check.html.

90. Ellen Nakashima, "U.S. military cyber operation to attack ISIS last year sparked heated debate over alerting allies," *The Washington Post*, May 9, 2017, https://www.washingtonpost.com/world/national-security/us-military-cyber-operation-to-attack-isis-last-year-sparked-heated-debate-over-alerting-allies/2017/05/08/93a120a2-30d5-11e7-9dec-764dc781686f_story.html.

91. Eric Schmitt, "ISIS May Be Waning, but Global Threats of Terrorism Continue to Spread," *The New York Times*, July 6, 2018, https://www.nytimes.com/2018/07/06/world/middleeast/isis-global-terrorism.html.

92. Summary: The Department of Defense Cyber Strategy, (September 2018), https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF; David E. Sanger, "Pentagon Puts Cyberwarriors on the Offensive, Increasing the Risk of Conflict," *The New York Times*, June 17, 2018, https://www.nytimes.com/2018/06/17/us/politics/cyber-command-trump.html; Mark Pomerleau, "Cyber Command granted new, expanded authorities," *Defense News*, February 28, 2018, https://www.defensenews.com/dod/cybercom/2018/02/28/cyber-command-granted-new-and-expanded-authorities/?utm_source=Twitter&utm_medium=Socialflow; and Julian E. Barnes, "U.S. Begins First Cyberoperation Against Russia Aimed at Protecting Elections," *The New York Times*, October 23, 2018, https://www.nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html.

93. Summary: The Department of Defense Cyber Strategy, (September 2018), https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

94. Mark Pomerleau, "Cyber Command granted new, expanded authorities," *Defense News*, February 28, 2018, https://www.defensenews.com/dod/cybercom/2018/02/28/cyber-command-granted-new-and-expanded-authorities/; Dustin Volz, "Trump, Seeking to Relax Rules on U.S. Cyberattacks, Reverses Obama Directive," *The Wall Street Journal*, August 15, 2018, https://www.wsj.com/articles/trump-seeking-to-relax-rules-on-u-s-cyberattacks-reverses-obama-directive-1534378721; and Erica D. Borghard and Shawn W. Lonergan, "What Do the Trump Administration's Changes to PPD-20 Mean for U.S. Offensive Cyber Operations?" Council on Foreign Relations, September 10, 2018, https://www.cfr.org/blog/what-do-trump-administrations-changes-ppd-20-mean-us-offensive-cyber-operations.

95. Michael Sulmeyer, "How the U.S. Can Play Cyber-Offense," *Foreign Affairs*, March 22, 2018, https://www.foreignaffairs.com/articles/world/2018-03-22/how-us-can-play-cyber-offense.

96. Peter Beinart, "The U.S. Needs to Face Up to Its Long History of Election Meddling," *The Atlantic*, July 22, 2018, https://www.theatlantic.com/ideas/archive/2018/07/the-us-has-a-long-history-of-election-meddling/565538/; Frud Bezhan, "Aftershocks of Iran's 1953 Coup Still Felt Around the World, 60 Years Later," Rferl.org, August 15, 2013, https://www.rferl.org/a/iran-coup-mossadegh-cia-60th-anniversary/25076552.html; and Michael Dobbs, "U.S. Advice Guided Milosevic Opposition," *The Washington Post*, December 11, 2000, https://www.washingtonpost.com/archive/politics/2000/12/11/us-advice-guided-milosevic-opposition/ba9e87e5-bdca-45dc-8aad-da6571e89448/?utm_term=.de123efd6335.

97. Arturo Munoz, "U.S. Military Operations in Afghanistan: Effectiveness of Psychological Operations 2001-2010," No. MG-1060-MCIA (RAND Corporation, 2012); https://www.rand.org/pubs/monographs/MG1060.html.

98. This section includes short excerpts of the author's original language from "Lesson 5" in the previously cited *War on the Rocks* commentary: Frederick, "How to Defend Against Foreign Influence Campaigns: Lessons from Counter-Terrorism."

99. Jens Stoltenberg, "Press conference by NATO Secretary General Jens Stoltenberg following the meeting of the North Atlantic Council at the level of Defence Ministers," NATO, June 29, 2017, https://www.nato.int/cps/en/natohq/opinions_145385.htm; and "ISAF's mission in Afghanistan (2001-2014)(Archived)," NATO, September 1, 2015, https://www.nato.int/cps/en/natohq/topics_69366.htm.

100. Jens Stoltenberg, "Press conference by NATO Secretary General Jens Stoltenberg following the meeting of the North Atlantic Council at the level of Defence Ministers," NATO, June 29, 2017, https://www.nato.int/cps/en/natohq/opinions_145385.htm; and "Countering terrorism," NATO, July 17, 2018, https://www.nato.int/cps/ua/natohq/topics_77646.htm.

101. NATO, Resolute Support Mission (RSM): Key Facts and Figures, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_09/20180903_2018-09-RSM-Placemat.pdf.

102. Constanze Stelzenmüller, Robert Bosch Senior Fellow, Foreign Policy at Brookings Institution, "The impact of Russian interference on Germany's 2017 elections," Testimony to the Senate Select Committee on Intelligence, U.S. Senate, June 28, 2017.

103. Jean-Baptiste Jeangène Vilmer, "Successfully Countering Russian Electoral Interference," CSIS Briefs (Center for Strategic & International Studies, June 2018).

104. Pomerleau, "Cyber Command granted new, expanded authorities."

105. Chris Meserole and Alina Polyakova, "Disinformation Wars," *Foreign Policy*, May 25, 2018, https://foreignpolicy.com/2018/05/25/disinformation-wars.

106. Gerald F. Seib, "If Faith in Democracy Ebbs, Danger Rises," *The Wall Street Journal*, July 2, 2018, https://www.wsj.com/articles/if-faith-in-democracy-ebbs-danger-rises-15305357.

About the Center for a New American Security

The mission of the Center for a New American Security (CNAS) is to develop strong, pragmatic and principled national security and defense policies. Building on the expertise and experience of its staff and advisors, CNAS engages policymakers, experts and the public with innovative, fact-based research, ideas and analysis to shape and elevate the national security debate. A key part of our mission is to inform and prepare the national security leaders of today and tomorrow.

CNAS is located in Washington, and was established in February 2007 by co-founders Kurt M. Campbell and Michèle A. Flournoy.

CNAS is a 501(c)3 tax-exempt nonprofit organization. Its research is independent and non-partisan. CNAS does not take institutional positions on policy issues. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the authors.

1152 15th Street, NW Suite 950 Washington, DC 20005
t. 202.457.9400 | f. 202.457.9401 | info@cnas.org | cnas.org

Bold. Innovative. Bipartisan.