No Silver Bullet

Fighting Russian Disinformation Requires Multiple Actions

Terry L. Thompson

These officials believe Russia is trying to create chaos in advance of the elections, giving President Trump the opportunity to promise stability as the law-and-order candidate.

With the November 2020 elections fast approaching, there is continuing concern about the effect of foreign interference affecting the voting process or outcomes of the election. For good reason. On October 21, 2019, in what could be an early indication of such interference, Facebook announced that it had taken down fifty Facebook and Instagram accounts that were associated with foreign entities. Although many posts were designed to build trust with like-minded social media participants, some focused directly on supporting the reelection of Donald Trump and disparaging Democratic candidates other than Bernie Sanders.[1] While these tactics are almost identical to those used in the Russian Internet Research Agency (IRA) disinformation campaign in 2016, the IRA continues to evolve, using new methods including recruiting American citizens to post its disinformation in social media.[2] In March 2020, US intelligence officials described Russian efforts to aggravate racial tensions by promoting white supremacist groups in private Facebook groups and anonymous message boards. These officials believe Russia is trying to create chaos in advance of the elections, giving President Trump the opportunity to promise stability as the law-and-order candidate. Or, in the words of a senior FBI official, "To put it simply, in this space, Russia wants to watch us tear ourselves apart."[3]

Like the United States, the European Union (EU) has experienced Russian disinformation in social media during elections, most recently in connection with the 2019 European Parliament elections and the 2017 French and German presidential elections.[4] More broadly, the EU and especially Baltic countries have felt the impact of Russian gaslighting, propaganda, and disinformation for decades, throughout the Soviet period and continuing in the post-Soviet era.[5]

The United States and EU have responded to these attacks on democracy by expanding monitoring efforts in social media and elsewhere, sharing threat information, and introducing regulatory measures. Europe developed an "Action Plan Against Disinformation" and a "Code of Practice on Disinformation," the latter a self-regulatory measure to encourage Facebook, Google, and Twitter to take responsibility for their platforms' content.[6] Some countries have introduced laws to disable local access to disinformation in social media.[7] The United States has taken a more operational ap-

Terry L. Thompson is a lecturer in cyber policy at the Johns Hopkins University and University of Maryland, Baltimore County. He transitioned to teaching after a forty-five-year professional career that included thirty years with the federal government and fifteen years at Booz Allen Hamilton, where he engaged in cybersecurity policy development for governments in the United States and six other countries.

proach, exemplified by US Cyber Command's blocking of IRA operatives in the 2018 midterm elections.[8] Outing Russian efforts in these ways has been only partially effective, however, and has not stopped their disinformation activities. The overall US effort to counter Russian influence operations has been inadequate. Without effective responses in multiple areas, Russia's efforts will not be deterred.[9]

The Fight against Disinformation

Many reports have described Russian cyber efforts to impact the 2016 election. The Intelligence Community Assessment of January 2017 summarized Russia's plan as one to "undermine public faith in the democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess that Putin and the Russian Government developed a clear preference for President-elect Donald Trump."[10] This report was bolstered by the comprehensive investigation of Special Counsel Robert Mueller and Congressional investigations in 2017 and 2018. Mueller's detailed report, together with the Department of Justice indictments it spawned, spelled out the tactics, techniques, and procedures used by the IRA in its attempt to interfere with the 2016 election.[11]

Despite continuing denials about the impact of Russian disinformation, including by President Trump himself, several studies assert that it did have an impact on the electorate, particularly on late deciders.[12] With a polarized electorate and controversial incumbent, nothing suggests that 2020 will be any different, particularly given the fact that many Americans still reject the idea that Russia interfered in 2016.[13]

The US government, despite Trump administration denials, has applied lessons learned from 2016 to develop a comprehensive approach to deal with election interference. The Cyber and Infrastructure Security Agency (CISA), established within the Department of Homeland Security by the Cybersecurity and Infrastructure Protection Act of 2018, launched several initiatives to help state and local election officials across the country identify and address election vulnerabilities. CISA established the Elections Interference Information Sharing and Analysis Center (EI-ISAC) to share election-related threat information nationwide.[14] To mitigate hacking of electronic voting systems, CISA provides "Albert" machines, deep-packet inspection technology that secures these systems' network connection points. CISA also supports tabletop exercises with state election officials to rehearse election interference response procedures.[15]

US Cyber Command (USCYBERCOM) has also improved its capabilities to counter election interference. Using new authorities in the 2017 National Security Strategy and the 2018 National Cyber Strategy, USCYBERCOM thwarted Russian attempts to meddle in the 2018 midterm elections by penetrating IRA computers, coming virtually face-to-face with operatives who generated disinformation in the 2016 election cycle.[16] The message was clear: any further attempts to interfere with US elections will be blocked.[17] USCYBERCOM has also trained National Guard cyber operators to support state and local officials' efforts to block election interference.[18]

The European response, like that of NATO, has focused on the detection and publication of Russian interference efforts and on legislation to regulate social media companies. NATO, led by its Baltic members, established the Cooperative Cyber Defense Center of Excellence (CCDCOE) in Tallinn in 2008 and the Strategic Communications Center of Excellence (StratCom COE) in Riga in 2014. The CCDCOE

publishes studies of national cyber strategies, cybersecurity concepts, and other relevant topics for the cyber defense community. It also provides cyber defense training for NATO member countries.[19] The StratCom COE developed a seven-point deterrence checklist as part of a detailed study of election interference.[20] Creative responses such as those of the citizen-organized Baltic Elves and Lithuanian Elves have augmented government and NATO efforts, while the 2018 Prague Manual has credited Estonia, Latvia, and Lithuania as the three EU members most successful in responding to Russian disinformation.[21]

These efforts by the United States, EU, and NATO provide an improved deterrent against Russian disinformation. But the Russian effort to sow discord and mistrust is relentless. Inspired by President Vladimir Putin's desire to turn Americans against one another and armed with increasingly sophisticated cyber operators in the Russian military, Russian disinformation has become a powerful twenty-first-century information weapon that will not be easily defeated.[22] Russian tactics are constantly evolving, and rapid advances in artificial intelligence and deep-fake videos will make detecting disinformation and other active measures increasingly difficult in 2020 and beyond.

Disinformation Is Part of a Larger Problem

Actions taken by the United States, Europe, and NATO have not been fully effective for several reasons. First, Russia's disinformation campaign is part of a comprehensive set of "active measures" begun in the Soviet era. These measures are designed to divide the West through exacerbating societal and cultural tensions.[23] NATO's StratCom COE describes the larger context of election interference as follows: "Election interference aims to influence the outcome of an election, to undermine trust in the election, or to use the election to achieve other goals, such as undermining democracy, internal cohesion, or influencing how a country is perceived externally."[24] In the 2016 US election, disinformation in social media was just part of an overall active measures campaign, codenamed Project Lakhta, designed to "sow discord in the U.S. political system and to undermine faith in our democratic institutions."[25]

The US government lost focus on Russian active measures when it became enamored with "cyberwar" in the early 2000s. The situation was different in the 1990s, when US government agencies, think tanks, and academics began to understand the military implications of information and communications technologies in their focus on "information warfare." The Defense Science Board completed a major study on "Information Warfare—Defense" in 1996; the RAND Corporation published a related report in the same year; and Georgetown professor Dorothy Denning published her seminal work, *Information Warfare and Security*, in 1999.[26] However, although these studies acknowledged other aspects of information warfare, the major focus was the protection of Defense Department computer networks and the data they carried to support military operations.[27] Solving a technology problem was more attractive than dealing with the complexities of information warfare.

Concepts embedded in the term "information warfare," such as deception and perception management, were just too difficult for American strategists to handle. It was much easier to focus on hardware, software, and infrastructure—the physical components of cyberwar. Technology solutions always seemed possible, and industry was ready to provide those solutions. General Mike Hayden, former director of the

CIA and NSA, described the debates on this topic in 1996, when he commanded the Air Intelligence Agency (AIA). He and his staff struggled with adopting "information dominance" or "cyber dominance" to describe their evolving mission. AIA concluded that information dominance—including deception, public diplomacy, perception management, and psychological operations—was too risky in terms of the First Amendment and other constraints. In Hayden's colorful summary, AIA "stuck with door number 1: cyber dominance." The Russians, on the other hand, "opted for door number 2: information dominance."[28]

The second reason US and European efforts have failed to stop Russian disinformation is because they don't fully account for the evolving nature of Russia's military and security thinking. As the United States focused more on cyberwar, Russian strategists—wary of the internet's US origins and technology—began to focus on content and on using social media as a platform for disinformation. The turning point occurred when street protests erupted in Moscow in response to perceived election fraud in the 2011 Duma elections and Vladimir Putin's announcement that he would run for a third presidential term. Protest organizers communicated their activities on social media, leading Putin to believe the United States was behind the demonstrations.[29] Russia applied lessons learned from these protests when they used disinformation and other active measures in their annexation of Crimea in 2014, and these concepts were embedded in Russia's military doctrine in the same year.[30] The doctrine defines the main characteristics of modern conflict as "the coordinated application of military force and political, economic, *information* and other non-military measures, achieved with the *broad utilization of popular opposition* and special operations forces" (emphasis added).[31] Western observers characterize Russia's approach as "hybrid threats" or "hybrid warfare."[32]

Concepts embedded in the term "information warfare," such as deception and perception management, were just too difficult for American strategists to handle.

Russian disinformation activities take place in this broader context of their overall active measures capabilities. They have leveraged the low barriers to entry and low costs which make social media a useful attack surface for shaping public opinion and have applied deception to influence emotions. People are drawn to social media because it appeals to basic emotion and the need for social interaction. They share activities, pictures, articles, recipes, and other culturally significant topics with family and friends. As P.W. Singer and Emerson Booking describe in *Like War*, these characteristics provide psychic income when posts receive a "like" or are "shared" with others. Other factors like confirmation bias and believability strengthen the tendency of people to congregate online—as in real life—with others who think like them. These factors explain why false information spreads so quickly.[33] The emotional reactions invoked by social media are the main targets of Russian disinformation. Focusing on culture and identity exacerbates an already polarized society and lays the groundwork for the acceptance of fake news.[34]

A third reason that US and EU countermeasures against disinformation have been only partly successful is the reluctance of social media companies to identify and block or delete deceptive posts. Concerned employees at Facebook were "prevented from making any changes for fear of violating

People are drawn to social media because it appeals to basic emotion and the need for social interaction. ..... The emotional reactions invoked by social media are the main targets of Russian disinformation.

Facebook's 'objectivity,' as well as alienating conservative users and legislators."[35] In an apparent about-face, Facebook announced in October 2019 measures designed to prevent foreign interference in the 2020 elections.[36] These measures will take time, and their effectiveness is uncertain. Other social media companies are also taking action, but not quickly enough, and experts point out that dealing with disinformation requires a political response as well.[37] Meanwhile, Russian disinformation in social media continues to be a concern. As recently as February 2020, FBI Director Christopher Wray warned the House Judiciary Committee about Russia's ongoing "information warfare" against the United States.[38]

An Effective Response

Given that Russian disinformation is part of its larger concept of information warfare focused on culture and identity, additional measures are required to thwart interference in US and European elections. There is no simple solution. For one thing, the Russians and other foreign actors are continually improving their disinformation tactics and techniques.[39] Another complication is what one observer of democracy's response to the novel coronavirus pandemic calls "the inevitable chaos of pluralism and transparency."[40] Bringing about societal change in democracies is just plain hard.

Despite these difficulties, the following six approaches may bolster the defenses of the United States and EU against information warfare.

1. Acknowledge the Problem

Focusing on a national problem requires national leadership. The EU has countered Russia with measures like the "Code of Practice on Disinformation," while US senior leaders refuse to come to grips with Russia's malign activities.[41] Although the US government has made significant progress in documenting Russian disinformation and developing reasonable responses, there is no publicly available national strategy for dealing with social media disinformation or with Russia's culture war against the West.[42] There are, however, some positive developments. On Monday, March 2, 2020, the day before "Super Tuesday" primary elections, the Departments of Justice, State, Defense, and Homeland Security issued an unprecedented statement emphasizing the continuing threat of foreign efforts to influence American elections through false information and propaganda.[43] In addition, the US Congress, in the National Defense Authorization Act for Fiscal 2020 (2020 NDAA), recognized the need for a "whole of government strategy" to combat Russian "information warfare," "to detect and counter foreign influence operations," and to counter Russian cyber attacks against "electoral systems and processes in the United States."[44] And in March 2020, the Cyberspace Solarium Commission co-chaired by Senator Angus King (I-Maine) and Representative Mike Gallagher (R-Wisconsin) published an extensive report calling for increased national leadership attention on cyberspace, including dealing with foreign interference in elections.[45]

2. Increase Monitoring, Analysis, and Reporting

US and European efforts to identify and

communicate disinformation in social media have been effective and should be expanded.[46] US government reports and investigations are now augmented by companies, like Graphica, that focus on analyzing social media. These companies document and report culture- and identity-based deception in Russia-linked Twitter and Facebook accounts.[47] The government has also increased its efforts. In a Cyber Initiatives Group briefing on October 28, 2019, hosted by *Cipher Brief*, CISA director Christopher Krebs cited an increase in disinformation detection activities by the government and private sector as significant developments in advance of the 2020 election. Relatedly, the Air Force launched a new information warfare organization in 2019 to detect foreign deception efforts.[48] To encourage this trend, Congress in the 2020 NDAA addresses the need for " institutionalizing ongoing robust, independent, and vigorous analysis of data related to foreign threat networks within and across social media platforms" in order to "counter ongoing information warfare operations against the United States, its allies, and its partners." The 2020 NDAA also offers the Director of National Intelligence (DNI) the option of establishing a Social Media Data and Threat Analysis Center. The DNI's use of this authority could forge a coordinated government/industry effort to providing periodic reporting to Congress and the public.[49]

3. Expand Operational Responses

Technical and operational approaches must continue to augment publicizing threat information and analysis as part of an overall approach. USCYBERCOM actions to block Russian disinformation efforts that worked in 2018 will continue and will be improved.[50] Stopping disinformation before it appears in social media is highly effective. The October 2019 removal of fake accounts from Facebook and Instagram from Russia, Iran, and others indicate the increasing complexity of this challenge.

4. Employ Active Countermeasures

The most aggressive option would be for the United States to engage in active measures to counter foreign disinformation. Such "active countermeasures" are risky and have historically been avoided because of First Amendment and related legal and ethical issues.[51] However, language in the 2020 NDAA indicates that such measures are under consideration. In extraordinary detail, the law requires the DNI to provide a comprehensive review of Russian president Vladimir Putin's "legitimately and illegitimately obtained assets" inside and outside Russia as well as "the methods used by Vladimir Putin or others acting at his direction" to acquire and conceal said wealth.[52] The purpose of gathering all this information is clear: to prepare for possible disinformation or other active measures against the Russian president.

5. Regulate Social Media Companies

In addition to its "Action Plan for Disinformation" and "Code of Practice" for social media companies, the EU is using the new General Data Protection Regulation to apply pressure on Facebook and Google with fines for privacy violations.[53] Yet in the US, regulation is more of a long-term solution, given the time required to pass new legislation affecting one of America's biggest industries. Self-regulation and efforts to identify and delete disinformation by social media companies offer better, more effective solutions, and Congress should put more pressure on companies to expand current self-regulatory activities.[54] This would be a welcome change considering the historic resistance of these companies to deal with the problem because of potential impacts on their bottom line.

6. Employ More Innovative Approaches

Several creative ideas have also been offered to identify disinformation in social media. Mike Hayden suggests that part of the answer lies in collaboration between tech companies in Silicon Valley and the film industry in Hollywood. These global technology centers could create practical solutions to identify and publicize disinformation efforts that threaten American democracy, similar to how crowdsourced sites like Rotten Tomatoes help shape public judgments about movies.[55] Former General Stanley McChrystal has suggested a nonmilitary form of mandatory national service to bring together people from various groups to bridge social and cultural gaps and blunt the effects of polarization in social media.[56] Ben Brostoff, a graduate of Johns Hopkins University's Information Security Institute, suggests that an "active measure risk management framework"—modeled on NIST's Cyber Security Framework—could categorize information threat types and recommend security controls to address them.[57]

The Russians have continued their disinformation activities in social media even after their efforts in the 2016 election were exposed. They are not deterred by traditional Western responses focused on government investigations and legal measures. Russia's approach to active measures and disinformation is constantly evolving, and more creative thinking is required to confront their aggression in cyberspace.

These global technology centers could create practical solutions to identify and publicize disinformation efforts that threaten American democracy, similar to how crowdsourced sites like Rotten Tomatoes help shape public judgments about movies.

Looking Forward

There is no single solution—no silver bullet—that will effectively address the organized, well-funded, and efficient Russian deception and disinformation operations or their broader campaign of active measures directed against US and European elections. Expanding efforts by governments, think tanks, social media companies, and the growing social media analysis industry will help to detect, publicize, and respond to disinformation. The authorities granted by the 2020 NDAA will go a long way toward addressing the problem of information warfare directed against the United States. But a much harder challenge will be overcoming political and cultural polarization and Americans' love of social media. Absent a comprehensive national effort involving all elements of government and society, the United States will continue to struggle with foreign interference. The 2020 election will demonstrate whether US actions to date are enough to thwart Russian disinformation in the election process.

Notes

1. "Removing More Coordinated Inauthentic Behavior from Iran and Russia," Facebook, accessed April 16, 2020, https://newsroom.fb.com/news/2019/10/removing-more-coordinated-inauthentic-behavior-from-iran-and-russia/. See also Donnie O'Sullivan, "Facebook: Russian Trolls Are Back. And They're Here to Meddle with 2020," CNN Business, last updated October 22, 2019, https://www.cnn.com/2019/10/21/tech/russia-instagram-accounts-2020-election/index.html.
2. For a detailed summary of Russian disinformation activities during the 2016 election cycle, see Robert S. Mueller III, *The Mueller*

Report: The Final Report of the Special Counsel into Donald Trump, Russia, and Collusion (New York: Skyhorse, 2019). For more general studies of Russian disinformation in social media, see Bret Schafer, "A View from the Digital Trenches: Lessons from Year One of Hamilton 68," *Alliance for Securing Democracy* no. 33 (2018), last updated November 9, 2018, https://securingdemocracy.gmfus.org/a-view-from-the-digital-trenches-lessons-from-year-one-of-hamilton-68/; and Philip N. Howard et al. "The IRA, Social Media, and Political Polarization in the United States, 2012–2018," University of Oxford Computational Propaganda Research Project, https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/12/Appendices-for-The-IRA-Social-Media-and-Political-Polarization.pdf; Davey Alba, "How Russia'sTroll Farm Is Changing Tactics before the Fall Election," *New York Times*, March 29, 2020, https://www.nytimes.com/2020/03/29/technology/russia-troll-farm-election.html?searchResultPosition=1.

3. Julien E. Barnes and Adam Goldman, "Russia Trying to Stoke US Racial Tensions before Election, US Officials Say," *New York Times*, March 10, 2020, https://www.nytimes.com/2020/03/10/us/politics/russian-interference-race.html?referringSource=articleShare.
4. Michael Birnbaum and Craig Timberg, "EU: Russians Interfered in Our Elections, Too" *Washington Post*, June 14, 2019, https://www.washingtonpost.com/technology/2019/06/14/eu-russians-interfered-our-elections-too/; Nicole Perlroth, "Russian Hackers Who Targeted Clinton Appear to Attack France's Macron," *New York Times*, April 24, 2017, https://www.nytimes.com/2017/04/24/world/europe/macron-russian-hacking.html?search Result-Position=1; Adam Satariano, "Russia Sought to Use Social Media to Influence EU Vote, Report Finds," *New York Times*, June 14, 2019, https://www.nytimes.com/2019/06/14/business/eu-elections-russia-misinformation.html?searchResultPosition=1refs. Beginning in March 2020, foreign disinformation efforts began to focus on spreading rumors about the novel coronavirus. See: Zeke Miller and Colleen Long, "US Officials: Foreign Disinformation is Stoking Coronavirus Fears," *Washington Post*, March 16, 2020, https://www.washingtonpost.com/politics/us-officials-foreign-disinformation-stoking-virus-fears/2020/03/16/5d58c2d4-679b-11ea-b199-3a9799c54512_story.html. See also Satnam Narang, "COVID-19: Novel Coronavirus Becomes Hotbed for Misinformation, Scams, and Fake Cures," Tenable, March 19, 2020, https://www.tenable.com/blog/covid-19-novel-coronavirus-becomes-hotbed-for-misinformation-scams-and-fake-cures.
5. Terry Thompson, "Countering Russian Dis-Information the Baltic Nations' Way," The Conversation, January 9, 2019, https://theconversation.com/countering-russian-disinformation-the-baltic-nations-way-109366; for a synopsis of gaslighting against Baltic nations, see Gatis Krumins, "Soviet Economic Gaslighting of Latvia and the Baltic States," *Defence Strategic Communications*, 4 (Spring 2018): 49–78, DOI: 10.30966/2018.RIGA.4.2,https://www.stratcomcoe.org/gatis-krumins-soviet-economic-gaslighting-latvia-and-baltic-states.
6. In October 2018 the EU launched a new code against disinformation that provided guidelines for social media companies to help in self-regulation. See "Code of Practice on Disinformation," European Commission, September 26, 2018, https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation. Several months later, the EU asked member nations to increase efforts to identify and remove disinformation in social media prior to the 2019 EU parliamentary elections. See "Code of Practice against Disinformation," European Commission, January 29, 2019, https://ec.europa.eu/commission/news/code-practice-against-disinformation-2019-jan-29_en. These efforts appear to be only partially effective. See Matt Apuzzo, "Europe Build a System to Fight Russian Meddling. It's Struggling," *New York Times*, July 6, 2019, https://www.nytimes.com/2019/07/06/world/europe/europe-russian-disinformation-propaganda-elections.html?searchResultPosition=1.
7. Shibani Mathani, "Singapore Introduced Tough Laws against Fake News. Coronavirus Has Put Them to the Test," *Washington Post*,

March 16, 2020, https://www.washingtonpost.com/world/asia_pacific/exploiting-fake-news-laws-singapore-targets-tech-firms-over-coronavirus-falsehoods/2020/03/16/a49d6aa0-5f8f-11ea-ac50-18701e14e06d_story.html. While these laws have been invoked to prevent fake news about coronavirus, they can also be applied to election interference.

8. Julian E. Barnes, "US Begins First Cyber Operation against Russia Aimed at Protecting Elections," *New York Times*, October 23, 2018, https://www.nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html?searchResultPosition=1.
9. The US Congress has recognized the need for more direct and comprehensive actions to thwart influence operations and disinformation. The National Defense Authorization Act for Fiscal 2020 (2020 NDAA) directs the executive branch to take many specific actions to counter the Russian threat. See below for more details.
10. "Background to 'Assessing Russian Activities and Intentions in Recent US Elections': The Analytic Process and Cyber Incident Attribution," National Intelligence Council, January 6, 2017, https://www.intelligence.senate.gov/sites/default/files/documents/ICA_2017_01.pdf.
11. Robert S. Mueller III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, vol. 1 of 2 (Washington, DC: US Department of Justice, 2019). Reports by the House and Senate intelligence committees provided additional details and examples of Russian disinformation targeted at the election. See "Exploring Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements," US House Permanent Select Committee on Intelligence, last accessed April 16, 2020, https://intelligence.house.gov/social-media-content/; "Report of the Select Committee on Intelligence on Russian Active Measures Campaigns and Interference in the 2016 Election, Volume 2: Russia's Use of Social Media," US Senate Permanent Select Committee on Intelligence, last accessed April 16, 2020, https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf. See also Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Cambridge, MA: Harvard University Press, 2020), 211–39.
12. John Fritze and David Jackson, "Donald Trump Acknowledges Russia Helped Him Get Elected In 2016, Then Backtracks," *USA Today*, May 30, 2019, https://www.usatoday.com/story/news/politics/2019/05/30/donald-trump-acknowledges-russia-helped-his-election-then-backtracks/1221107001/. In presentations I have given to several voting-age groups in Maryland and Florida and in a webinar sponsored by the NSA's Centers of Academic Excellence program, audience members tend to accept the "fact of" Russian interference, but strongly deny that Russian disinformation affected the election's outcome; Kathleen Hall Jamieson, *Cyber War: How Russian Hackers and Trolls Helped Elect a President* (Oxford: Oxford University Press, 2018). Other studies about the impact of disinformation on the election are cited in Buchanan, *Hacker and the State*, 233.
13. Kathy Frankovic, "Republicans Still Not Convinced of Russian Election Meddling," YouGov, August 10, 2018, https://today.yougov.com/topics/politics/articles-reports/2018/08/10/republicans-still-not-convinced-russian-election-m. See also "The Senate Has Rejected the Constitution," *Washington Post*, February 4, 2020, https://www.washingtonpost.com/opinions/the-senate-has-rejected-the-constitution/2020/02/04/15656960-46b1-11ea-91ab-ce439aa5c7c1_story.html
14. Housed at the Center for Internet Security, the EI-ISAC, like other ISACs, provides a mechanism for sharing of threat intelligence between the federal government, state, local, tribal, and territorial governments, and private sector critical infrastructure companies. There are currently twenty-five ISACs across multiple industry sectors. See "Join Your Sector's ISAC Today," National Council of iSACs, last accessed April 16, 2020, https://www.nationalisacs.org/.
15. "Election Infrastructure Security," Cybersecurity and Infrastructure Security Agency, last updated February 21, 2020, https://www.cisa.gov/election-security.

16. "A New National Security Strategy for a New Era," The White House, December 18, 2017, https://www.whitehouse.gov/articles/new-national-security-strategy-new-era/; "President Trump Unveils America's First Cybersecurity Strategy in 15 Years," The White House, September 20, 2018, https://www.whitehouse.gov/articles/president-trump-unveils-americas-first-cybersecurity-strategy-15-years/. For background on USCYBERCOM's more aggressive approach, see Paul M. Nakasone, "A Cyber Force for Persistent Operations," *Joint Forces Quarterly*, 1st Quarter (2019): 4–9, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92.pdf.
17. Ellen Nakashima, "Pentagon Launches First Cyber Operation to Deter Russian Interference in Midterm Elections," *Washington Post*, October 23, 2018, https://www.washingtonpost.com/world/national-security/pentagon-launches-first-cyber-operation-to-deter-russian-interference-in-midterm-elections/2018/10/23/12ec6e7e-d6df-11e8-83a2-d1c3da28d6b6_story.html.
18. Mark Pomerleau, "Air Force Creates New Information Warfare Organization, Revamps Cyber Command Teams," Fifth Domain, September 18, 2019, https://www.fifthdomain.com/dod/air-force/2019/09/19/air-force-creates-new-information-warfare-organization-revamps-cyber-command-teams/.
19. NATO Cooperative Cyber Defence Center of Excellence, last accessed April 16, 2020, https://ccdcoe.org/.
20. The entire checklist is conduct a comprehensive threat analysis, focus on resilience building according to the threat analysis, consider deterrence factors, establish coordination and cooperation mechanisms, establish early warning and detection mechanisms, invest in education and training, and establish strategic communications framework—from deterrence to crisis communication. See Sebastian Bay and Guna Snore, "Protecting Elections: A Strategic Communications Approach," NATO Strategic Communications Centre of Excellence, June 2019, https://www.stratcomcoe.org/protecting-elections-strategic-communications-approach.
21. Jakob Willemo, "Trends and Developments in the Malicious Use of Social Media," NATO Strategic Communications Centre of Excellence, August 2019, https://stratcomcoe.org/trends-and-developments-malicious-use-social-media. The StratCom COE continues to publish useful documents on "Disinformation as a Global Problem—Regional Perspectives" (February 7, 2020); and "Decoding Crimea. Pinpointing the Influence Strategies of Modern Information Warfare" (January 31, 2020). Visit https://www.stratcomcoe.org/ for access to these and other publications; Veronika Vichova et al., *The Prague Manual: How to Tailor National Strategy Using Lessons Learned from Countering Kremlin's Hostile Subversive Operations in Central and Eastern Europe*, Kremlin Watch Report (Prague: European Values Think-Tank, 2018), https://www.europeanvalues.net/wp-content/uploads/2018/07/Prague-Manual.pdf.
22. For an excellent analysis of Putin's motives to turn Americans against one another, see David VonDrehle, "Vladimir Putin's Virus: How the Russian President Has Infected Our National Trust." *Washington Post*, March 2, 2020, https://www.washingtonpost.com/opinions/2020/03/02/did-vladimir-putin-turn-america-itself/?arc404=true. See also Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (New York: Doubleday, 2019) for a penetrating summary of hacking operations carried out by the GRU, Russia's main intelligence directorate.
23. "Disinformation" in the context of Russian active measures is best defined in a 1984 book as the "non-attributed or falsely attributed communication containing false, incomplete or misleading information (frequently combined with true information) to deceive, misinform, and/or mislead the target." See Richard H. Shultz and Roy Godson, *Dezinformatsia: Active Measures in Soviet Society* (Pergamon-Brasseys, 1984), 195.
24. Bay and Snore, "Protecting Elections."
25. "Russian National Charged with Interfering in U.S. Political System," US Department of Justice, October 19, 2018, https://www.jus

tice.gov/opa/pr/russian-national-charged-interfering-us-political-system. Although the US government has dropped charges against two Russian companies mentioned in the indictment, the case against Khusyaynova is still being pursued. See Katie Benner and Sharon LaFraniere, "Justice Dept. Moves to Drop Charges against Russian Firms Filed by Mueller," *New York Times*, March 16, 2020, https://www.nytimes.com/2020/03/16/us/politics/concord-case-russian-interference.html?searchResult Position=1.

26. "Report of the Defense Science Board Task Force on Information Warfare—Defense," Defense Science Board, Office of the Under Secretary of Defense for Acquisition and Technology (November 1996), https://apps.dtic.mil/dtic/tr/fulltext/u2/a319571.pdf; Roger C. Molander, Andrew S. Riddle, and Peter A. Wilson, "Strategic Information Warfare: A New Face of War," RAND report MR-661-OSD, 1996, https://www.rand.org/pubs/monograph_reports/MR661.html; Dorothy E. Denning, *Information Warfare and Security* (Boston: Addison-Wesley, 1999).
27. Denning, *Information Warfare and Security* chap. 5, Molander et. al, "Strategic Information Warfare."
28. Michael V. Hayden, *The Assault on Intelligence: American National Security in an Age of Lies* (London: Penguin Press, 2018), 191.
29. Andrei Soldatov and Irina Borogan, *The Red Web: The Kremlin's Wars on the Internet* (New York: Public Affairs, 2015).
30. Jolanta Darczewska, "The Anatomy of Russian Information Warfare: The Crimean Operation, a Case Study," *Point of View* 42 (May 2014), Centre for Eastern Studies, https://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf.
31. Author's translation and emphasis added. Russia's 2014 military doctrine (in Russian) can be found on the CCDCOE website, https://ccdcoe.org/library/strategy-and-governance/.
32. For a detailed explanation and discussion of hybrid threats, see Ben Heap et al. "Hybrid Threats: A Strategic Communications Perspective," NATO Strategic Communications Centre of Excellence, last accessed April 16, 2020, https://www.stratcomcoe.org/hybrid-threats-strategic-communications-perspective. A RAND report defines "hybrid warfare" as "the use of assertive policies, information operations, and covert and overt military and nonmilitary tactics (including cyber attacks) by Russia and other countries to advance conflicting interests or territorial claims." See Stephen J. Flanagan et al., "Deterring Russian Aggression in the Baltic States through Resilience and Resistance," RAND Corporation, 2019, https://www.rand.org/pubs/research_reports/RR2779.html.
33. P. W. Singer and Emerson T. Booking, *Like War: The Weaponization of Social Media* (Boston: Houghton, Mifflin, Harcourt, 2018), 123–27.
34. Michael Jensen, "Russian Trolls and Fake News: Information or Identity Logics?," *Journal of International Affairs* Special Issue 71, no. 1.5 (2018).
35. Singer and Booking, *Like War*, 240–41.
36. "Helping to Protect the 2020 US Elections," Facebook, accessed April 16, 2020, https://newsroom.fb.com/news/2019/10/update-on-election-integrity-efforts/. Increasing transparency by identifying posting individuals or organizations, labeling state-controlled media, and adding labels to posts debunked by fact checkers are some of these measures. Facebook is also investing $2 million to support media literacy projects.
37. In a March 2020 survey, 89 percent of experts in the *Washington Post*'s "Technology 202 Network" said that social media companies haven't done enough to prevent voter manipulation in 2020. They note the need for Congressional action to supplement technology company activities. See Cat Zakrzewski, "The Technology 202: Social Networks Haven't Done Enough to Prevent Voter Manipulation, Tech Leaders Say," *Washington Post*, March 10, 2020, https://www.washingtonpost.com/news/powerpost/paloma/the-technology-202/2020/03/10/the-technology-202-social-networks-haven-t-done-enough-to-prevent-voter-manipulation-tech-leaders-say/5e667771602ff10d49ac68f4/.
38. See, for example, Amanda Seitz and Barbara Ortutay, "Report: Russian Social Accounts Sow Elec-

tion Discord – Again," AP News, March 5, 2020, https://apnews.com/0db953743c56cd6fd6e4ef73e02f120c.

39. Oxford University's computational propaganda project is doing excellent work on foreign disinformation. For a book-length summary of their research, see Samuel C. Woolley and Philip N. Howard, *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media* (New York: Oxford University Press, 2019). Dario Cristiani, "Italy's Coronavirus Experience and the Challenge by Extreme Crises to Liberal Democracies," German Marshall Fund of the United States, March 20, 2020, http://www.gmfus.org/blog/2020/03/20/italys-coronavirus-experience-and-challenge-extreme-crises-liberal-democracies.
40. Dario Cristiani.
41. "Code of Practice on Disinformation"; and "Code of Practice Against Disinformation."
42. A recent study by the RAND Corporation suggests that the US "needs an updated framework for organizing its thinking about the manipulation of infospheres by foreign powers determined to gain competitive advantage." See Michael J. Mazarr et al., "Hostile Social Manipulation: Present Realities and Emerging Trends," RAND Corporation, 2019, https://www.rand/org/pubs/research_reports/RR2713.html/.
43. "Joint Statement from DOJ, DOS, DOD, DHS, ODNI, FBI, NSA, and CISA on Preparations for Super Tuesday," US Department of Justice, March 2, 2020, https://www.justice.gov/opa/pr/joint-statement-doj-dos-dod-dhs-odni-fbi-nsa-and-cisa-preparations-super-tuesday.
44. The 2020 NDAA includes many related actions to address the growing problem of "malign foreign influence." See *National Defense Authorization Act of 2020*, HR 2500, 116th Congress, sec. 5323 & 6504, https://congress.gov/bill/116th-congress/senate-bill/1790/text.
45. The Cyberspace Solarium Commission was established by the 2019 National Defense Authorization Act. The report's more than seventy-five recommendations include enhancing CISA's role in cybersecurity, modernizing campaign regulations to emphasize cybersecurity, reforming online political advertising to defend against foreign election interference. See "Report: Our Strategy," US Cyberspace Solarium Commission, March 2020, https://www.solarium.gov/report.
46. For example, in January 2020 NATO's StratCom COE published a comprehensive study: Rachel Lim, "Disinformation as a Global Problem—Regional Perspectives." NATO Strategic Communications Centre of Excellence, January 2020, https://stratcomcoe.org/disinformation-global-problem-regional-perspectives.
47. See, for example, *Graphika*, last updated 2019, https://www.graphika.com/. The UK firm Bellingcat is a global leader in investigating disinformation efforts by Russia and other governments. See, *Bellingcat*, last updated 2020, https://www.bellingcat.com/.
48. Lori A. Bultman, "Air Force Integrates Missions, Strengthens Information Warfare Capabilities," US Air Force, October 11, 2019, https://www.af.mil/News/Article-Display/Article/1987970/air-force-integrates-missions-strengthens-information-warfare-capabilities/. See also Pomerleau, "Air Force Creates."
49. 2020 NDAA, Section 5323. Among many related actions, the 2020 NDAA tasks the DNI, in collaboration with other federal agencies, to submit to Congress "an assessment of security vulnerabilities in state election systems" 180 days prior to any federal election and to notify Congress of any "significant foreign cyber intrusions or active measures campaign intended to influence an upcoming election for federal office" when such activity can be attributed to a foreign government.
50. Recent reporting suggests USCYBERCOM is continuing its offensive cyber operations by implanting malicious software in Russia's electrical grid. See David E. Sanger and Nicole Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid," *New York Times*, June 15, 2019, https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html?searchResultPosition=1.
51. Hayden, *Assault on Intelligence*.
52. Walter Pincus identified this language in a

draft of the NDAA. See Walter Pincus, "Why You Should Pay Close Attention to the Intelligence Authorization Bill," *The Cipher Brief*, July 23, 2019, https://www.thecipherbrief.com/column/fine-print/why-you-should-pay-close-attention-to-the-intelligence-authorization-bill. For the final text in the law, see 2020 NDAA, Section 5502.

53. See, for example, Sean Keane, "GDPR: Google and Facebook Face Up To $9.3B in Fines on First Day of New Privacy Law," CNET, May 25, 2018, https://www.cnet.com/news/gdpr-google-and-facebook-face-up-to-9-3-billion-in-fines-on-first-day-of-new-privacy-law/.
54. Facebook has a detailed plan to prevent inauthentic content and manipulative posts from interfering with elections. See "Preventing Election Interference," Facebook, last accessed April 16, 2020, https://about.fb.com/actions/preventing-election-interference/.
55. Hayden, *Assault on Intelligence*, 241.
56. Clint Watts, *Messing with the Enemy: Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News* (New York: Harper, 2018), 251.
57. Benjamin J. Brostoff, "Developing a National Cyber Disinformation Threat Response Network," *Cybersecurity Quarterly* (Summer 2019), https://issuu.com/cybersecurityquarterly/docs/csq_volume_3_issue_2.