Stanford | Cyber Policy Center
Freeman Spogli Institute

SECURING AMERICAN ELECTIONS

Prescriptions for Enhancing the Integrity and Independence of the 2020 U.S. Presidential Election and Beyond

Michael McFaul, Editor

Stanford University
June 2019

TABLE OF CONTENTS

PREFACE

By Michael McFaul

In 2016, Russia attacked the United States. As the Special Counsel report stated, "The Russian government interfered in the 2016 presidential election in sweeping and systematic fashion."[1] More precisely, Russian President Vladimir Putin, his government, and his proxies deployed multiple strategies and instruments—media, doxing, covert operations, direct contacts with Trump associates, and cyber-attacks on U.S. electoral infrastructure—to influence the outcome of the 2016 U.S. presidential election, and more generally, to disrupt the electoral process. Although the Kremlin had intervened previously in the electoral processes of other countries and dabbled in influencing earlier American elections, the scale, scope, and sophistication of this Russian intervention in this American election were unprecedented.

In reaction to discoveries about Russia's election interference in 2016, many recommended the creation of a bipartisan, independent commission, similar to the commission established after the September 11th terrorist attacks, to investigate what happened, how the United States responded, and what policies should be adopted moving forward to prevent or at least minimize new attempts by Russia or other countries to interfere in American elections.[2] Unfortunately, that idea never took root. In May 2017, Deputy Attorney General Rod Rosenstein of the U.S. Justice Department instead appointed Robert Mueller as Special Counsel overseeing an investigation into the allegations of Russian interference in the 2016 U.S. presidential election and related matters. Mueller and his team have revealed detailed accounts of aspects of the Russian campaign and produced 34 indictments of both Americans and Russians, but his mandate was never to investigate all dimensions of the Russian operations.[3] Nor did he interrogate the Obama administration's responses to the Russian interference or offer policy prescriptions. Numerous Congressional committees have undertaken the challenge of investigating potentially illicit Russian activity—which some are continuing currently[4]—but none have thus far comprehensively examined the entirety of the Russian attack, or the American governmental and non-governmental responses (or lack thereof) to this foreign intervention. Moreover, the Mueller report lacks comprehensive policy recommendations for how to prevent foreign interventions in future U.S. elections. As discussed throughout this report, the executive branch has implemented several reforms to reduce the threat of foreign meddling in elections. The

U.S. Congress also has proposed several new bills to help the effort, many of which we endorse in this study. But the response so far does not meet the threat, which as FBI Director Christopher Wray warned in April 2019, remains very real.[5]

Outside of government, several books, articles, task forces, and non-governmental organizations have delivered critical insights regarding the Russian attack and proposed innovative policy prescriptions.[6] We endorse and amplify many of these ideas in our report. Nevertheless, the United States still has nothing on the shelf comparable to the 9/11 Commission Report, which contained not only analysis of what happened and why, but also significant policy prescriptions.

This study seeks to provide a partial substitute for such a commission report. Building on the abovementioned research and investigations, our report begins by summarizing in Chapter One what the Kremlin did in 2016 and why. Chapters Two through Eight then offer concrete prescriptions for protecting the integrity and independence of U.S. elections, focusing in particular on strengthening resiliency before the 2020 presidential election. Our recommendations are practical, concrete, and achievable before 2020—but they demand action now.

Our team of authors includes experts on cybersecurity, deterrence, Russia, social media companies, and American electoral regulations, as well as diplomacy, democracy and ethics.[7] Our view is that all of these disciplines must be brought to bear in order to develop a sophisticated, comprehensive, and successful strategy for repelling not only potential threats from Russia, but also attacks from other foreign and domestic actors seeking to disrupt the integrity of the U.S. electoral process. American voters must choose their leaders alone, without help or interference from outsiders. In this report, we suggest a strategy for enhancing the permissive conditions for just that—free and fair elections not shaped or undermined by the actions of foreign actors motivated by different aims or malign intentions. Our analysis and advice are non-partisan, animated by the belief that all Americans share a common interest in protecting the integrity and independence of the U.S. electoral process.

This report urges policymakers, in both government and the private sector, to act immediately in order to protect the integrity and independence of U.S. elections, particularly in the run-up to the 2020 presidential election, and recommends the following actions in order to do so:[1]

Increase the Security of the U.S. Election Infrastructure

2.1. Require that all vote-counting systems provide a voter-verified paper audit trail.

2.2. Require risk-limited auditing for all elections.

2.3. Assess the security of computerized election-related systems in an adversarial manner.

2.4. Establish basic norms regarding digital behavior for campaign officials.

2.5. Commit regular funding streams to strengthen the cybersecurity posture of the election infrastructure.

2.6. Retain the designation of election infrastructure as critical infrastructure.

2.7. Allow political parties to provide cybersecurity assistance to state parties and to individuals running for federal office and their campaigns.

Regulate Online Political Advertising by Foreign Governments and Nationals

3.1. Explicitly prohibit foreign governments and individuals from purchasing online advertisements targeting the American electorate and aimed at influencing U.S. elections.

3.2. Support the passage of the Honest Ads Act with several key amendments.

3.3. Strengthen self-regulation mechanisms for the major internet platforms.

Confront Efforts at Election Manipulation from Foreign Media Organizations

4.1. Require greater disclosure measures for FARA-registered foreign media organizations.

4.2. Mandate additional disclosure measures during pre-election periods.

4.3. Support existing disclosure measures of specific social media platforms.

Combat State-Sponsored Disinformation Campaigns from State-aligned Actors

5.1. Create standardized guidelines for labeling content affiliated with disinformation campaign producers.

5.2. Create norms for the media's handling of stolen information.

5.3. Limit the targeting capabilities for political advertising.

5.4. Expand transparency for paid and unpaid political content.

5.5. Improve the quality and scope of detection tools and reporting policies for social media platforms.

5.6. Build an industry-wide coalition to coordinate and encourage the spread of best practices.

5.7. Remove barriers to the sharing of information relating to disinformation, including changes to privacy and other laws as necessary.

5.8. Establish a Social Media ISAC/ISAO to improve communication between the U.S. government and social media companies about disinformation operations.

5.9. Increase overall transparency on social media platforms.

5.10. Carefully balance platform responsibility with individual freedoms.

5.11. Establish a norm among candidates to not use stolen data or manipulated content.

5.12. Emphasize digital literacy in educational curricula and focus public education on the knowledge that makes democracy more resilient to disinformation campaigns.

Enhance Transparency about Foreign Involvement in U.S. Elections

6.1. Mandate transparency in the use of foreign consultants and foreign companies in U.S. political campaigns.

6.2. Increase transparency about foreign business interests.

6.3. Disclose contacts with foreign nationals and governments.

6.4. Strengthen the norm of one government at a time.

Establish International Norms and Agreements to Prevent Election Interference

7.1. Fortify U.S. and international commitment to human rights.

7.2. Strengthen international norms protecting election infrastructures.

7.3. Create norms to deter the use of disinformation and hacked materials.

7.4. Lead international advocacy against foreign interference through disinformation.

7.5. Distinguish legitimate cross-border assistance from illicit or unlawful interventions.

7.6. Hold congressional hearings about policies to support free and fair elections internationally.

7.7. Promote cooperation among democracies focused on election protection.

7.8. Appoint a senior U.S. government representative on election interference.

7.9. Develop guidelines about platform cooperation with foreign governments.

Deter Foreign Governments from Election Interference

8.1. Recalibrate risk tolerances for actions in cyberspace.

8.2. Signal a clear and credible commitment to respond to election interference.

8.3. Maintain a visible position of U.S. capabilities, intentions, and responses.

8.4. Enact country-specific and timely responses that impose real, effective costs.

8.5. Promote collective engagement with international partners.

8.6. Conduct a continuous strategic disruption campaign against adversaries that seek to interfere with U.S. elections.

8.7. Pursue common interests in cyberspace where possible.

CHAPTER ONE

Understanding Putin's Intentions and Actions in the 2016 U.S. Presidential Election

By Michael McFaul and Bronte Kass

According to Russian President Vladimir Putin, the United States is a hostile power and a serious threat to Russian national interests. From his KGB days, Putin developed an analytical framework with regards to international politics, which cast the United States as the central enemy of the Soviet Union. His ideas evolved over time. After September 11, 2001, for instance, Putin pivoted towards greater cooperation with President George W. Bush in a common fight against terrorism. During Dmitry Medvedev's presidency, then Prime Minister Putin also allowed greater cooperation between the United States and Russia. Today, however, Putin has returned to his earlier ideas. Putin's animosity towards the United States has increased during his third and fourth terms in office, animated by a belief that the United States aims to undermine his rule and weaken Russia more generally.

Putin now is engaged in an international ideological struggle that he defines as a contest between conservative, Christian, sovereign values—which he embraces—and decadent, liberal, multilateral ideas championed by many Western governments, including first and foremost the United States. When given the opportunity, Putin seeks to weaken the United States and advance his ideology of 'Putinism'. The 2016 presidential election in the United States offered Putin one of those opportunities.

'Putinism' as a Transnational Ideology and International Campaign

Regarding international affairs, Putin increasingly has championed the sovereignty of great powers like Russia and criticized what he considers American hegemony.[2] In Putin's view, the liberal international order established after World War II serves American national interests at the expense of other countries. Putin also contends that the United States uses overt military power to violate the sovereignty of other countries, a claim backed by empirical evidence, including most recently, Serbia (1999), Afghanistan (2001), Iraq (2003), and Libya (2011). As Putin lamented in his speech before the 2007 Munich Security Conference, "Unilateral and frequently illegitimate actions have not resolved any problems. Moreover, they have caused new human tragedies and created new centers of tension… plunging the world into an abyss of permanent conflicts… One state and, of course, first and foremost the United States, has overstepped its

national borders in every way. This is visible in the economic, political, cultural, and educational policies it imposes on other nations. Well, who likes this? Who is happy about this?"[3] Other times, American presidents, according to Putin, deploy covert means to destabilize or overthrow regimes, be it in Serbia (2000), the Arab Spring (2011), Russia (2011-2012), Ukraine (2013-2014), or Venezuela today.[4]

It is Russia's mission, therefore, to resist and prevent American attempts at regime change as well as to weaken American power more generally in the international system. To achieve these objectives, Putin has been strategically investing in resources that strengthen his capacity to counter the United States. For example, Putin has increased military spending to modernize the Russian army, produce improved weapons, and better train soldiers. These increases in military capabilities were on display in Georgia in 2008, Ukraine in 2014, and Syria in 2015. Russian nuclear modernization, both of warheads and delivery vehicles, also has expanded during Putin's presidency. Putin also has invested heavily in Russia's cyber capabilities. In 2007, Putin launched what many consider 'the first cyber war' against Estonia, and then accompanied Russia's physical intervention into Georgia in August 2008 with cyber-attacks. Ukraine has similarly endured numerous cyber assaults since Russia's intervention in 2014.

In addition to expanding military and cyber capabilities, Putin and the Kremlin also have fostered ideological alliances around the globe, including within liberal democracies and countries formally aligned with the United States. Over the years, Putin has won over many sympathizers throughout Europe, including Prime Minister Viktor Orbán in Hungary, Marine Le Pen in France, Brexit champion Nigel Farage in the United Kingdom, Geert Wilders in the Netherlands, President Andrzej Duda in Poland, Deputy Prime Minister Matteo Salvini in Italy, and Prime Minister Andrej Babiš in the Czech Republic. The rise of these populist leaders has fostered a perception of a successful, coordinated, populist, illiberal global movement with Putin as its spiritual anchor.

In parallel, Putin and his proxies have enhanced ties between Russian and foreign non-governmental organizations with a shared ideology. Russian Houses have sprouted all over the world to propagate Putinism, and the Russian Orthodox Church has developed connections with conservative religious groups around the world, including in the United States. Moreover, strengthened Russian relations with non-governmental organizations, such as the National Rifle Association (NRA), are an important component of this global strategy to nurture ties with like-minded European and Americans.[5] At times, Russian actors have even provided direct financial resources to fellow ideological travelers.[6]

To further propagate his ideas abroad, Putin has allocated significant resources to developing several media outlets and social media platforms. In the Russian-speaking world, particularly in countries that gained independence after the Soviet collapse, the Kremlin has devoted massive resources to maintaining an influential expanse of Kremlin-controlled television networks, radio, and other media. To extend beyond the Russian-speaking world, the Kremlin started the media company Russia Today in 2005, later renamed RT to disguise its affiliation. With an

annual budget of over $300 million USD, RT now broadcasts in 6 languages and has claimed to be YouTube's most-watched media company with nearly 3 billion views (of which 1.5 billion are from its flagship English-language channel).[7] In 2014, the Russian government also created Sputnik, an organization that serves as a news agency, news website, and radio broadcast service. The Kremlin-controlled platform promotes a pro-Russian slant on politics, economics, and public opinion, which its regional bureaus gear specifically toward a non-Russian audience.

In parallel with these efforts, Putin and his proxies have invested in the means to circulate disinformation and shape political discourse on social media platforms, including most famously through the Internet Research Agency (IRA). As detailed in the Special Counsel report, the IRA orchestrated a multi-pronged intervention specifically during the 2016 U.S. presidential election, but notably, the IRA and other Russian agents have been conducting disinformation operations on social media platforms for several years in many countries around the world.[8] Other Russian actors in the digital world use social media platforms to push pro-Putin, anti-American ideas.

The Russian army and ethnic Russian separatists constitute a final blunt instrument of propagating 'Putinism'. Putin's annexation of Crimea in 2014 and intervention in eastern Ukraine later that year occurred in parallel with a massive ideological campaign to persuade ethnic Russians in these regions to embrace Putin's worldview. Putin's recent proposal to provide Russian citizenship to ethnic Russians living in eastern Ukraine, just as he did to residents in the Georgian territories of Abkhazia and South Ossetia, is another key attempt to undermine the sovereignty of a neighbor in the pursuit of his expansionist, ideological agenda.[9]

Putin's Preferences in the 2016 U.S. Presidential Election

By 2016, Putin's anti-American, anti-liberal, and anti-democratic perspective had crystalized, while simultaneously, his instruments for exporting and propagating his worldview were increasing substantially. Ideological intent and enhanced capability combined to produce the most comprehensive Russian interference campaign thus far in an American election.

Putin initially aimed to delegitimize the American electoral process and American democracy more generally. For years, Putin had endured what he believed were lectures from Western critics about the autocratic elements of Russia's system of government. Putin was particularly annoyed with Secretary of State Hillary Clinton's criticism of the lack of freeness and fairness of the electoral process in the December 2011 parliamentary election in Russia, an "attack" which Putin said publicly sent a signal to the Russian opposition to protest against his government.[10] Consequently, Putin wanted to sow division, disrupt processes, and more generally cast doubt about the integrity of the 2016 U.S. presidential election.

Putin also aimed to weaken Clinton's presidential candidacy and help Trump as another means for undermining the integrity of the 2016 election. The unexpected emergence of Trump as a viable candidate offered Putin more opportunities to advance his agenda against American democracy. Supporting Trump became a central part of Putin's strategy of delegitimization. Although easy to forget now, Trump was not considered a serious candidate at the beginning

of the campaign, as he was regarded as a provocateur and disrupter outside of the mainstream. Eventually, he would even directly challenge the legitimacy of the American democratic process himself, berating subjects such as the unfair primary process, "fake news", and the corrupting influence of money in politics. As Election Day approached, Trump even warned that the vote was going to be rigged.[11] Supporting such an unpredictable and oftentimes inflammatory candidate therefore served Putin's goal of undermining the integrity of American democracy.

In addition, as a candidate, Trump expressed many policy positions that Putin openly endorsed. For instance, candidate Trump pledged to look into lifting sanctions and recognizing Crimea as part of Russia.[12] Trump campaign representatives tried to change the Republican Party platform to eliminate support for lethal weapons for Ukraine. Trump frequently criticized the NATO alliance, while barely saying a word about democracy and human rights.[13] When asked about Putin's human rights abuses inside Russia, Trump defended Putin with a narrative of 'whataboutism', arguing, "Well, I think our country does plenty of killing also…."[14] After winning the election, he later pushed back on criticism of Putin by stating, "We have a lot of killers…you think our country is so innocent?"[15] On the campaign trail, Trump predicted, "We're going to have a great relationship with Putin and Russia."[16] Trump has also praised Putin personally and profusely,[17] describing him as "brilliant"[18] and a "genius",[19] and suggesting that he was a better leader than Obama, when he asserted, "I will tell you in terms of leadership [Putin] is getting an 'A', and our president is not doing so well…"[20] It was very rational, therefore, for Putin to want Trump to win, even if the Trump administration did not follow through on many of these pro-Putin campaign statements.[21] As the unclassified report by the Office of the Director of National Intelligence on Russian involvement in the 2016 U.S. presidential election concluded, "We assess Putin, his advisers, and the Russian Government developed a clear preference for President-elect Trump over Secretary Clinton."[22] Putin himself then affirmed this assessment of the American intelligence community. When asked point blank about his electoral preferences during the press conference at the summit in Helsinki in July 2018, Putin answered bluntly, "Yes. I wanted him to win, because he talked about the normalization of U.S.-Russia relations."[23]

Conversely, Putin loathed Clinton. Putin did not want to see continuity in American foreign policy. Well before becoming a presidential candidate, Clinton had earned a reputation in Putin circles as a hawk. As a candidate, she said nothing to dispel that image. On Russia, she advocated the opposite of Trump: recognition of Crimea as Ukrainian territory, increased sanctions, a need to strengthen NATO, and a commitment to advocating for greater freedom inside Russia. Ideologically, Clinton espoused liberal internationalism, the exact opposite of Putin's worldview. Putin also seemed to harbor personal animosity towards Clinton, beyond just policy differences or her criticism of the procedures in the 2011 parliamentary elections. As Clinton wrote in her latest memoir, "Our relationship has been sour for a long time."[24]

The Multi-Pronged Russian Intervention

Putin not only had a personal preference in the 2016 U.S. presidential election, but also greenlighted multiple efforts to help his preferred candidate win. Confirming what U.S. intelligence had assessed two years earlier, the Special Counsel investigation headed by Robert Mueller established that the Kremlin perceived it would benefit from a Trump presidency and thus worked diligently to secure that outcome. According to the Special Counsel report, "The Russian government interfered in the 2016 presidential election in sweeping and systematic fashion."[25] The unredacted portion of the Special Counsel report focused on two influential Russian operations: (1) computer-intrusion operations against the Clinton campaign and Democratic Party officials and (2) a social media campaign that favored candidate Trump and disparaged candidate Clinton.[26] The U.S. Department of Justice later determined that Russia's principal interference operations violated U.S. criminal law. Many of the individuals and entities involved in the social media campaign "have been charged with participating in a conspiracy to defraud the United States by undermining through deceptive acts the work of federal agencies charged with regulating foreign influence in U.S. elections, as well as related counts of identity theft."[27] Russian intelligence officers who carried out the hacking also have been charged for violating federal laws.

The overall Russian campaign, however, was wider than these two operations, and included traditional media messaging, offers of compromising materials on one candidate in support of another, possible counterintelligence efforts by Russian agents to create leverage over several individuals in Trump's orbit, and preparations to disrupt voter registration logs and even vote counts on Election Day.[28]

Publishing Stolen Information

All countries with the capacity to do so—including Russia—gather human intelligence (HUMINT) and signals intelligence (SIGINT). Regarding HUMINT collection, the Kremlin ran an aggressive campaign to build personal relationships with Trump campaign officials in 2016. Clinton and her team were considered a known entity to Moscow, but they knew significantly less about Trump and therefore vigorously cultivated contacts to learn more about the candidate and his advisors. As a good diplomat should, Russia's Ambassador to the United States, Sergey Kislyak, boldly reached out to and successfully met several key Trump advisors, including future National Security Advisor Michael Flynn, future Attorney General Jeff Sessions, and future White House senior advisor Jared Kushner. Kislyak mingled with VIPs at candidate Trump's one major address devoted to foreign policy, and he attended the Republican National Convention, while skipping the Democratic National Convention. Other Russian actors with close Kremlin ties cultivated relationships with Trump campaign advisors George Papadopoulos, Paul Manafort, and Carter Page.

Collecting intelligence is one thing; stealing it illicitly and publishing it extensively is quite another. In April 2016, Russian intelligence officers—i.e., the Main Intelligence Directorate of the General Staff of the Russian Army (commonly known as GRU)—hacked into the computer networks of the Democratic Congressional Campaign Committee (DCCC) and the Democratic National Committee (DNC) and stole hundreds of thousands of documents, including significant amounts of data pertaining to internal strategy documents, fundraising data, personal identifying and financial information, opposition research, and employee emails.[29] Two GRU military units were discovered to have facilitated the computer intrusions: Military Units 26165 and 74455.[30] Military Unit 26165 is a GRU cyber unit dedicated to targeting military, political, governmental, and non-governmental organizations outside of Russia.[31] Starting in March 2016, Unit 26165 had primary responsibility for hacking the DCCC and DNC, as well as email accounts of individuals affiliated with the Clinton campaign.[32] Military Unit 74455 is a related unit with multiple departments engaged in cyber operations, whose officers assisted in the release of documents stolen by Unit 26165, the promotion of those releases, and the publication of anti-Clinton content on social media accounts.

GRU officers also sent hundreds of spear-phishing emails to the work and personal email accounts of Clinton campaign employees and volunteers.[33] Through a hacking operation, the GRU stole tens of thousands of emails from John Podesta, the chairman of Clinton's campaign. By April 2016, the GRU had gained access to the DCCC computer network using stolen credentials from a DCCC employee who had been successfully spear-phished. The GRU then traversed the network and continued to steal access credentials along the way, ultimately compromising approximately 29 computers. On April 18, 2016, the GRU gained access to the DNC network via a Virtual Private Network between the DCCC and DNC networks, compromising over 30 computers on the DNC network, including the mail server and shared file server.[34] Unit 26165 implanted two types of customized malware known as "X-Agent" and "X-Tunnel", a credential-harvesting tool, and a tool used to compile and compress materials for exfiltration onto the DCCC and DNC networks.[35]

Although unnerving, there is nothing unusual about either human or electronic data collection by the Russian government during the 2016 U.S. presidential election. The subsequent publication of this stolen data, however, was extraordinary and unprecedented. Russian agents carried out the anonymous release of this information through two fictitious online personas—DCLeaks and Guccifer 2.0—and later through third-party websites, including most importantly WikiLeaks. The GRU began posting stolen documents in June 2016.[36] While Russian cyber agents had compromised cybersecurity systems and stolen data from both the Republican and Democratic parties, the U.S. intelligence community discovered that they decided not to publish the data obtained from the Republican Party.

On June 14, 2016, the DNC and its cyber-response team announced the breach of the DNC network and suspected theft of DNC documents.[37] Guccifer 2.0 released thousands of stolen documents in a series of blog posts between June 15, 2016 and October 18, 2016.[38] According to

the Special Counsel report, "documents included opposition research performed by the DNC (including a memorandum analyzing potential criticisms of candidate Trump), internal policy documents (such as recommendations on how to address politically sensitive issues), analyses of specific congressional races, and fundraising documents. Releases were organized around thematic issues, such as specific states (e.g., Florida and Pennsylvania) that were perceived to be competitive in the 2016 U.S. presidential election."[39]

In order to expand their influence, the GRU units decided to transfer many of the documents to WikiLeaks. WikiLeaks founder Julian Assange had expressed opposition to candidate Clinton well before the first release of stolen documents.[40] His strong animosity stemmed in particular from then-Secretary of State Clinton's fierce condemnation of his role in facilitating "Cablegate"—WikiLeaks's controversial release of over 250,000 unredacted and previously classified U.S. diplomatic cables in 2010.[41]

In total, WikiLeaks released over 50,000 documents stolen from Podesta's personal email account.[42] On July 6, 2016, WikiLeaks contacted Guccifer 2.0 through Twitter's private messaging function, writing "if you have anything hillary related we want it in the next tweo [sic] days prefable [sic] because the DNC is approaching and she will solidify bernie supporters behind her after." The Guccifer 2.0 persona responded, "ok ... i see." WikiLeaks also explained, "we think trump has only a 25% chance of winning against hillary . . . so conflict between bernie and hillary is interesting."[43] As reports attributing the hacks to the Russian government emerged, WikiLeaks and Assange made several public statements to obscure the source of the released materials and continued similarly cryptic behavior after the U.S. intelligence community publicly announced its assessment that Russia was behind the hacking operation.

Trump and his campaign officials showed interest in WikiLeaks's releases of hacked materials during the summer and fall of 2016.[44] According to his former deputy campaign chairman Richard Gates, Paul Manafort expressed excitement, wanting to be kept apprised of developments and future releases.[45] Donald Trump Jr. had direct communications with WikiLeaks during the campaign period.[46] On October 12, 2016, WikiLeaks wrote to Trump Jr. that it was "great to see you and your dad talking about our publications. Strongly suggest your dad tweets this link if he mentions us wlsearch.tk."[47] WikiLeaks wrote that the link would help Trump in "digging through" leaked emails and stated "we just released Podesta emails Part 4."[48] Two days later, Trump Jr. publicly tweeted the wlsearch.tk link.[49] Candidate Trump encouraged Russia and WikiLeaks to do more, declaring on July 27, 2016, "Russia, if you're listening, I hope you're able to find the 30,000 emails that are missing. I think you will probably be rewarded mightily by our press." According to the Special Counsel report, "Trump made this request repeatedly, and [Michael] Flynn subsequently contacted multiple people in an effort to obtain the emails."[50] Within approximately five hours of Trump's statement, Unit 26165 officers targeted Clinton's personal office for the first time.[51]

WikiLeaks timed the publication of these emails and documents to maximize their disruptive effect. The stolen emails, accompanied by conservative commentary, generated a narrative of

unfair treatment of presidential candidate Bernie Sanders by the DNC. Supporters of Sanders were outraged, booed Clinton during the Democratic National Convention's opening ceremony and even picked up Trump's "lock her up" slogan during their protests. This scandal generated by Russian activity forced then-DNC Chair Debbie Wasserman Schultz to resign before she could open the party's convention. Beyond the specific allegations of DNC bias against Sanders, the publication of these emails fueled the more general narrative of Clinton being corrupt and insincere.

Strategic timing of this "doxing" campaign helped the Trump campaign to navigate potential pitfalls. On October 7, 2016, The Washington Post published an Access Hollywood video that captured candidate Trump using graphic language about women that was expected to adversely affect his campaign. Less than an hour after the video's publication, WikiLeaks released the first set of emails stolen from Podesta's account.[52] Print and broadcast media devoted considerable attention to the content of these stolen data.

Rather than criticizing the electoral interference, Trump encouraged the WikiLeaks operation, declaring "I love WikiLeaks" while on the campaign trail and calling on this foreign organization to continue publishing his opponent's private communications. By one count, Trump mentioned WikiLeaks over 160 times in the last month of the campaign.

Before 2016, no foreign government had ever attempted to steal data from American politicians and then publish this information as a means to significantly influence the electoral outcome. This element of Putin's strategy to influence the 2016 U.S. presidential election was the most impactful.[53]

Russian Media Campaigns, Disinformation Social Media Operations, and Physical Rallies

In parallel to publishing stolen data, the Kremlin orchestrated a multi-pronged media campaign within the United States designed to help Trump, hurt Clinton, and foster division within American society more generally. This campaign—part disinformation and part partisan commentary—was comprised of several methods.

One instrument of swaying American voter attitude was the use of traditional media. Russian state-controlled media produced pro-Trump and anti-Clinton content targeted at American voters. The Russian state-controlled television network RT broadcasted within the United States, appearing in 85 million households though cable bundles and as one of the most watched television channels on YouTube. For YouTube, RT produced a variety of anti-Clinton clips, claiming for instance that the Clinton Foundation paid for Chelsea Clinton's wedding, that Clinton created the conditions for ISIS, that Clinton and ISIS are funded by the same money, and that 100% of Clinton charity proceeds went to themselves. Sputnik also produced anti-Clinton, pro-Trump content, and then circulated these messages on multiple platforms, including Facebook and Twitter. When tweeting out #CrookedHillary, Sputnik made the Kremlin's preferences clear.

Second, Russian-operated Twitter and Facebook accounts then amplified the anti-Clinton, pro-Trump messaging. A key player in these social media activities was the IRA. Based in St. Petersburg with funding from Russian oligarch Yevgeniy Prigozhin, a close colleague of Putin, the IRA evolved from a generalized program designed in 2014 to undermine the integrity of the U.S. electoral system, into a targeted operation that by early 2016 was supporting candidate Trump and criticizing candidate Clinton. Its operations also included the purchase of political advertisements on social media in the names of fictitious U.S. persons and entities, as well as the staging of political rallies inside the United States.[54] In November 2017, a Facebook representative testified that Facebook had identified 470 IRA-controlled accounts that collectively made 80,000 posts between January 2015 and August 2017, reaching at least 29 million U.S. persons, but potentially an estimated 126 million persons overall.[55] According to Facebook, the IRA purchased over 3,500 advertisements, and the expenditures totaled approximately $100,000.[56] In January 2018, Twitter announced the identification of 3,814 IRA-controlled Twitter accounts and notified approximately 1.4 million individuals who may have been in contact with an IRA-controlled account.[57] According to recently published materials, Russian bots also retweeted Trump more than 470,000 times during the final months of election.[58] In addition, Russian-linked accounts were responsible for 48-73% of the retweets of WikiLeaks' tweets during the same time period.

Dozens of IRA employees, known as 'specialists', were responsible for operating accounts and personas on different social media platforms. By early 2015, the IRA began to create larger social media groups or public pages that claimed to be affiliated with U.S. political and grassroots organizations. In certain cases, the IRA designed accounts to mimic real U.S. organizations, but it more often created fictitious accounts, posing as anti-immigration groups, Tea Party activists, Black Lives Matter protestors, and other social and political activists. In November 2017, lawmakers released a collection of Russian-sponsored ads—featuring themes such as the Benghazi attack, border security, gun safety, the Black Lives Matter movement, and Texas secession—that were specifically aimed at U.S. Facebook and Instagram users.[59] IRA employees have acknowledged that their work focused on influencing the results of the 2016 U.S. presidential election.[60]

Throughout 2016, IRA accounts published an increasing number of materials supporting Trump and opposing Clinton. As early as March 2016, the IRA purchased advertisements that overtly opposed the Clinton campaign. The first known IRA advertisement explicitly endorsing the Trump campaign was purchased on April 19, 2016 as an advertisement on the Instagram account "Tea Party News" asking for help to "make a patriotic team of young Trump supporters" by uploading photos with the hashtag "#KIDS4TRUMP."[61] Dozens of advertisements supporting the Trump campaign were subsequently purchased, predominantly through the Facebook groups "Being Patriotic", "Stop All Invaders", and "Secured Borders."

Collectively, the IRA's social media accounts reached tens of millions of Americans through either operating accounts to pose as individual persons, or controlling a network of automated

accounts to amplify existing content.[62] Moreover, the IRA used social media platforms to organize protests in the United States and successfully encouraged tens of thousands of Americans to RSVP for their political events. According to the Special Counsel report, the IRA would recruit a real U.S. individual to serve as an event coordinator, promoting the event by contacting American media, and sharing videos or photographs of the event afterwards. The earliest evidence of a facilitated event was a "confederate rally" in November 2015.[63] In another example a year later, between 5,000 and 10,000 protesters in Manhattan attended a November 2016 anti-Trump protest organized by a Russian-linked group, seeking to capitalize on exacerbating racial tension.

The IRA continued to organize rallies even after the 2016 U.S. presidential election, although attendance varied. In addition, IRA employees were instructed to target specific American individuals that could be used to further advance their operational goals through amplifying IRA-posted content on social media platforms, such as persons whom they had successfully tasked with organizing rallies or taking photos with certain political messages.[64]

As per Robert Mueller's indictment of 13 Russians and 3 companies involved in interfering with the 2016 U.S. presidential election, "Defendants, posing as U.S. persons and creating false U.S. personas, operated social media pages and groups designed to attract U.S. audiences. These groups and pages, which addressed divisive U.S. political and social issues, falsely claimed to be controlled by U.S. activists when, in fact, they were controlled by Defendants. Defendants also used the stolen identities of real U.S. persons to post on [IRA]-controlled social media accounts. Over time, these social media accounts became Defendants' means to reach significant numbers of Americans for purposes of interfering with the U.S. political system, including the presidential election of 2016." The goal of the "troll factory", according to the indictment, was to sow discord in the U.S. political system, particularly during the 2016 U.S. presidential election.

Often referred to as the "translator project", the IRA's U.S. department is subdivided into different responsibilities, including operations on social media platforms, analytics, graphics, and IT.[65] The IRA's U.S. department is part of a larger set of interlocking operations known as 'Project Lakhta',[66] and employees were aware that Prigozhin was involved in the IRA's U.S. operations. In May 2016, IRA employees, claiming to be U.S. social activists and administrators of Facebook groups, boldly recruited Americans to hold signs (including one in front of the White House) that read "Happy 55th Birthday Dear Boss", as an homage to Prigozhin himself (whose 55th birthday was on June 1).[67]

Led by general director Mikhail Bystrov and executive director Mikhail Burchik, the IRA began hiding its funding and activities as early as the spring of 2014. The IRA's resources and budget were incredibly vast. According to Mueller's indictment, "The [IRA] employed hundreds of individuals for its online operations, ranging from creators of fictitious personas to technical and administrative support. The [IRA]'s annual budget totaled the equivalent of millions of U.S. dollars."[68] Russian journalists reported that by the summer of 2016, the IRA's U.S. department employed around 80-90 people, a mere one-tenth of the IRA's total workforce, and cost

approximately $1 million per year just in salaries alone. The monthly ad spend was approximately $5,000 for a total of $120,000 in two years. Thus, less than a hundred people were creating and posting approximately 1,000 pieces of content, which was seen by 20-30 million people every week. For example, in August 2016, 15 million people in the United States saw at least one IRA-created ad per week, and in October 2016 the number of weekly impressions had reached its height of 70 million people.

IRA employees even succeeded in traveling to the United States on intelligence-gathering missions. In June 2014, four IRA employees applied to the U.S. Department of State to enter the United States, while lying about the purpose of their trip and claiming to be four friends who had met at a party.[69] Ultimately, according to the Special Counsel report, two IRA employees named Anna Bogacheva and Aleksandra Krylova received visas and entered the United States on June 4, 2014.

Russian Offers of Business Opportunities and Kompromat

In addition to publishing stolen data and implementing an extensive media campaign to influence the outcome of the 2016 U.S. presidential election, the Russian government and its surrogates reached out directly to the Trump campaign through "business connections, offers of assistance to the Campaign, invitations for Campaign officials and representatives of the Russian government to meet, and policy positions seeking improved U.S.-Russian relations."[70]

Kremlin-connected individuals and media entities began showing interest in Trump's campaign shortly after he announced his candidacy in June 2015.[71] According to the Special Counsel report, early contact was made in connection with a Trump Organization real-estate project in Russia known as 'Trump Tower Moscow', for which candidate Trump signed a Letter of Intent by November 2015. In January 2016, Trump Organization executive Michael Cohen had emailed and spoken about the project with the office of Kremlin Press Secretary Dmitry Peskov. While negotiations were led by Cohen, Trump associate Felix Sater provided assistance and daringly suggested the project would increase candidate Trump's chance of being elected.[72] Ultimately, the Trump Organization pursued the project through at least June 2016, including the consideration of travel to Russia by Cohen and candidate Trump himself.[73]

In parallel with the Trump Tower Moscow project, the Trump Organization maintained numerous business contacts with Russian individuals and entities. These connections spanned a multitude of actors from the Kremlin and other associates of Putin, who had a natural interest in strengthening their relationships with Trump campaign team members—despite their varying degrees of closeness to Trump himself. In the unclassified sections of the Special Counsel investigation, however, none of these business interests were deemed to be illegal.

In late April 2016, campaign foreign policy advisor George Papadopoulos was told by London-based professor Joseph Mifsud, immediately after Mifsud's return from a trip to Moscow, that the Russian government had 'dirt' on Hillary Clinton in the form of thousands of emails. One week later, in May 2016, Papadopoulos suggested that the Trump campaign had received

indications from the Kremlin that it could assist the campaign through the anonymous release of information damaging to Clinton.[74] For several months thereafter, Papadopoulos worked with Mifsud and two Russian nationals to arrange a meeting between campaign officials and the Kremlin, which ultimately never took place.

Russian outreach continued into the summer of 2016. On June 9, 2016, Donald Trump Jr., campaign chairman Paul Manafort, and senior campaign advisor Jared Kushner met in Trump Tower with a visiting Russian delegation headed by Russian lawyer Natalia Veselnitskaya. Before traveling to New York, Veselnitskaya coordinated her talking points with Russian Prosecutor General Yuri Chaika, one of the most senior officials in the Russian government and a close associate of President Putin. According to the Special Counsel report, "The written communications setting up the meeting showed that the Campaign anticipated receiving information from Russia that could assist candidate Trump's electoral prospects."[75]

Robert Goldstone had arranged the meeting. During the 2013 Miss Universe pageant in Moscow, Goldstone first met Trump and later became an acquaintance after working as a publicist for Russian performer Emil Agalarov, the son of Aras Agalarov, who was Trump's partner in hosting the pageant. In an email from June 3rd titled, "Russia – Clinton – private and confidential", Goldstone informed Trump Jr. that Veselnitskaya was bringing compromising information on Clinton and her campaign, as part of the Kremlin's effort to assist Trump's campaign. In response, Trump Jr. wrote back within minutes, "If it's what you say, I love it."[76]

At the meeting, Veselnitskaya made claims that funds derived from illegal activities in Russia were provided to Hillary Clinton and other Democrats, although she was unable to provide evidence when pressed. (Bizarrely, Putin affirmed this same conspiracy during his press conference with President Trump at their Helsinki summit in July 2018 when Putin accused British businessman Bill Browder of laundering money out of Russia and then providing a portion of these funds to the Clinton campaign.)[77] She then turned to criticizing the Magnitsky Act, a 2012 statute that imposed financial and travel sanctions on Russian officials, which had triggered a retaliatory ban on the adoption of Russian children.[78] Although she seemingly provided nothing concrete in this meeting, Veselnitskaya appeared to be trading kompromat on Clinton in return for sanctions relief. Veselnitskaya made several targeted efforts to follow up on the meeting, but the Trump team did not engage.[79] However, one day after this meeting, Trump teased that he planned to give a major speech that would reveal very damaging information about Hillary Clinton and the Clinton Foundation. He never delivered such a speech.

Russian officials continued to hold numerous meetings with senior Trump advisors. By one count, during the campaign and transition period, Russians met with 12 Trump campaign officials and associates during the course of 19 in-person meetings and over 50 communications. Most mysteriously, in August 2016, Manafort met his long-time business associate Konstantin Kilimnik, who had requested the meeting in order to deliver a peace plan for Ukraine that Manafort later acknowledged as a 'backdoor' way for Russia to control part of eastern Ukraine.[80] They also discussed the status of the Trump campaign and Manafort's strategy for winning

Democratic votes in Midwestern states. Months before the August meeting, Manafort had instructed his campaign deputy Gates[81] to provide Kilimnik with internal polling data, which Manafort expected to be shared with others in Ukraine and with Russian oligarch Oleg Deripaska.[82] Furthermore, Manafort met Kilimnik twice in the United States during the campaign period and conveyed campaign information, such as the strategic discussion of "battleground" states, which Manafort identified as Michigan, Wisconsin, Pennsylvania, and Minnesota.[83]

The Special Counsel investigation evaluated a series of additional links between Russian actors and the Trump campaign: outreach to two of Trump's then-recently named foreign policy advisors, dealings with a D.C.-based think tank that specializes in Russia and has connections with the Kremlin, events at the Republican National Convention, post-Convention contacts between Trump campaign officials and Kislyak, and other contacts through Manafort, who had previously worked for a Russian oligarch and a pro-Russian political party in Ukraine. Notably, the Special Counsel investigation established that "several individuals affiliated with the Trump Campaign lied to the Office and the U.S. Congress about their interactions with Russian-affiliated individuals and related matters… materially impair[ing] the investigation of Russian election interference."[84] The reasons for all of these meetings remains a mystery.

These meetings, usually initiated by Russian officials, produced subsequent suspicion about the intentions of Trump campaign officials and family members. While Putin explicitly wanted Trump to win, a Trump team delegitimized by multiple contacts with Russian officials—contacts that the Kremlin and Russian intelligence agents of course knew that American intelligence agencies would be monitoring closely—also served Putin's interests. The counterintelligence portion of the Special Counsel investigation has not been published and is most likely still ongoing.

Hacking of U.S. Electoral Infrastructure

Most disturbingly, Russian intelligence agents probed the U.S. electoral infrastructure in 2016. In June 2017, Samuel Liles, the Acting Director of the Department of Homeland Security's Office of Intelligence and Analysis Cyber Division, testified to the Senate Intelligence Committee that "Internet-connected election-related networks, including websites, in 21 states were potentially targeted by Russian government cyber actors."[85] Beyond probing, the Special Counsel report specifically identified Russia's successful penetration of computers of one county government in Florida as well as successful placement of malware within VR Systems, a company that supplies Florida counties with voter registration systems.[86] VR Systems was also the provider of electronic poll books that malfunctioned in Durham Country, North Carolina in 2016.[87] Thankfully, Director Liles noted that there was no evidence that any hacking attempts in 2016 affected actual operations or outcomes, but implanted malware could still remain on these network systems and computers.

In addition, the Special Counsel report revealed that GRU officers also targeted election administrators and officials, including "U.S. state and local entities, such as state boards of elections (SBOEs), secretaries of state, and county governments, as well as individuals who worked for those entities… [and] private technology firms responsible for manufacturing and administering election-related software and hardware, such as voter registration software and electronic polling stations."[88] By the summer of 2016, GRU officers were seeking access to state and local computer networks by exploiting known software vulnerabilities on the websites of state and local governmental entities. Through techniques such as "SQL injection", malicious code was sent to the state or local website in order to run commands, e.g., exfiltrating the database contents.

According to the Special Counsel report, "In one instance in approximately June 2016, the GRU compromised the computer network of the Illinois State Board of Elections by exploiting a vulnerability in the SBOE's website. The GRU then gained access to a database containing information on millions of registered Illinois voters, and extracted data related to thousands of U.S. voters before the malicious activity was identified."[89] Russian intelligence agents also sent spear-phishing emails to public officials involved in election administration and personnel at companies involved with voting technology.[90]

Despite having the capacity to do so, Putin and his agents decided not to try to disrupt these machines on Election Day itself. President Obama personally warned Putin about the consequences of Russian disruption of Election Day activities; perhaps this deterrence worked. Nonetheless, the mere fact that Russian cyber actors successfully penetrated and accessed the U.S. election infrastructure is highly concerning for its potential to undermine confidence in electoral outcomes in the future.

Measuring the Impact of the Russian Intervention

Russian activities played only a marginal role in influencing the outcome of the 2016 U.S. presidential election. Multiple other structural, institutional, and campaign factors were clearly more dominant in deciding the presidential election.[91] Furthermore, additional proximate events, such as pronouncements and non-pronouncements about ongoing FBI investigations, were influential on the final vote count. Without question, tens of millions of American voters cast their ballots for Trump or Clinton with no influence whatsoever from Russian actions. In the vast sea of variables determining voter preferences, precisely measuring the independent causal influence of Russia's efforts during the 2016 U.S. presidential election is impossible.[92] Several Russian actions, after all, amplified the campaign activities of the Trump team and his surrogates, making the task of isolating a Russian causal role even harder. But small effects in the tightly contested election could have made a difference, despite being impossible to prove. Even if Russian interference played only a marginal role, this election was won in the margins–78,000 votes in only three states: Michigan, Pennsylvania, and Wisconsin.

Some correlations seem probative. Putin made his biggest impact on the 2016 campaign by

stealing and then publishing DNC and Podesta emails, an operation that sparked a major rift between Sanders and Clinton supporters. In post-election surveys, twelve percent of Sanders's supporters in the Democratic primaries reported that they voted for Trump in the general election.[93] Many Sanders supporters also decided to instead stay home. Approval ratings of Clinton as a qualified candidate decreased significantly in October 2016 after the WikiLeaks publication of Podesta emails.[94]

Moreover, Russian disinformation operations sought to suppress voter turnout.[95] In some swing states, especially among the African-American population, turnout among Democratic voters was significantly lower in 2016 (59.6%) than 2012 (66.2%). Targeted efforts by the Kremlin sought to explicitly and implicitly discourage African-Americans voters from going to the polls, as other Russian-backed efforts bolstered white extremism online.[96]

Russian efforts also actively promoted third-party candidates.[97] Votes cast for third-party candidates were significantly higher in 2016 than in 2012, including in several swing states.[98] Green Party candidate Jill Stein won 31,072 votes in Wisconsin (four times as many votes as she garnered in 2012), ten thousand more votes than Clinton lost to Trump by (22,748) in that state. Similarly, in Michigan, Stein won 51,463 votes; Clinton lost to Trump by 10,704. In Pennsylvania, Stein won 49,463 votes; Clinton trailed Trump there by 44,292.

Again, it is impossible to say for certain that Russian actions played a decisive role in any of these outcomes. But to suggest that Russian intervention played no role seems implausible. That the Kremlin tried to influence the outcome of the 2016 U.S. presidential election is without question—and that the Kremlin should influence even the outcome of one voter in 2020 should not be permitted to happen.

Future Foreign Threats

Future online election interference will likely take three tracks: (1) the spread of disinformation intended to discredit political candidates and the political process, discourage and confuse voters from participating in elections, and influence the online discussion of political topics; (2) the use of information operations to disrupt election infrastructure during the electoral cycle, on the day of the election, and immediately afterward during vote tallying and result certification—including, but not limited to, changing vote records and tallies, interfering with the operation of voting machines, impeding communications between precincts and election operations centers, and providing disinformation that misdirects voters to the wrong polling place or suggests long wait times, incorrect ID requirements, or precinct closures that do not actually exist; and (3) the undermining of public confidence in electoral processes after the election takes place.[99]

Additional actors also should be expected to join Russia in future attempts to influence political discourse online, as the barriers to mounting disinformation campaigns will depend less on available computing power and technical skill, and more on the ability to quickly iterate among strategies, produce text in naturalistic English or another targeted native language, and identify psychological vulnerabilities in a target segment of the electorate.

Furthermore, new technologies, including deepfakes, AI text-generation engines, and more sophisticated networks of bots on Twitter and other sites that permit pseudonymous accounts, will continue to be used to spread disinformation, discredit candidates, confuse voters, and influence the discussion of divisive political topics. Notably, these technologies need not be fully convincing, nor capable of deceiving digital forensic auditors. A faked image or video that is convincing at first glance but later revealed to be a forgery will cast suspicion on other low-resolution or thinly-sourced images and video, and will ultimately serve to imbue the political process with doubt and resignation over the truth of any piece of political media. The spread of a viral hoax also can serve to push users off associated platforms, as seen in recent pushback against YouTube content aimed at children, which thereby narrows the channels through which information, including politically motivated information, is received and disseminated.

In testifying before Congress on his agency's preparations for the 2020 presidential elections, FBI Director Christopher Wray stated bluntly, "Make no mistake: The threat just keeps escalating and we're going to have to up our game to stay ahead of it…"[100] Wray is right, but it will take more than just the FBI upping their game to enhance the security and integrity of our next presidential election. Many other government agencies, the U.S. Congress, state governments, media and social media companies, the candidates and their campaigns, and all American voters more generally must also be involved. The remainder of this report offers concrete suggestions for how to do so.

Increasing the Security of the U.S. Election Infrastructure

By Herbert Lin, Alex Stamos, Nate Persily, and Andrew Grotto

The Problem

The existing technical infrastructure for facilitating U.S. elections includes computer-based electronic systems for both voter registration and vote casting. Although these systems are the primary focus of this chapter, other important parts of the entire electoral ecosystem include electronic poll books, vote tabulation systems, election night reporting systems on which news services rely, and auditing systems. This ecosystem is vast, decentralized in many places, and varies tremendously in its resilience to attack, therefore requiring substantial upgrades to advance its overall security.

In accordance with the Help America Vote Act (HAVA) of 2002, systems for voter registration are centralized at the state level.[1] The administration of voter registration databases entails a number of large-scale tasks, including (1) maintaining the correct status of individuals who are properly registered to vote and their relevant information on voter registration lists, (2) removing individuals who are no longer eligible to vote (e.g., those who have moved out of the jurisdiction) off registration lists, and (3) delivering precinct-by-precinct registration lists to the individual precincts where in-person voting occurs (e.g., creating and delivering paper-based or electronic poll books). By contrast, vote casting systems are decentralized down to the county level. Each county within the same state can use a different electronic voting system, which must include the following: (1) electronic voting systems that record ballots cast by citizens in person at individual precincts, (2) tabulation systems that record absentee ballots via postal mail, and (3) programs that tabulate vote totals at levels higher than the precinct.

Given the complexities of both systems, opportunities for internal error and hostile outside intervention abound. Small errors or deliberate disruptions can easily erode voter confidence in the electoral system. Vote casting systems and voter registration systems are components of a larger election ecosystem that includes political parties and candidate campaigns, traditional and non-traditional news media, poll workers, pollsters, and engaged citizens. Partisan stakeholders, who by definition want their candidates to win, add further complexity since they might be tempted to promote systems for voter registration and vote casting that favor their particular party or candidates and also are less secure than others available.

During the 2016 U.S. presidential election, a number of elements of the U.S. electoral infrastructure came under attack. The Special Counsel report described in detail these attacks carried out by the Main Intelligence Directorate of the General Staff of the Russian Army (GRU) on behalf of the Russian government.

> [I]n addition to targeting individuals involved in the Clinton Campaign, GRU officers also targeted individuals and entities involved in the administration of the elections. Victims included U.S. state and local entities, such as state boards of elections (SBOEs), secretaries of state, and county governments, as well as individuals who worked for those entities... The GRU also targeted private technology firms responsible for manufacturing and administering election-related software and hardware, such as voter registration software and electronic polling stations.[2]

Moreover, the Special Counsel report specifically highlights:

> GRU officers... targeted state and local databases of registered voters using a technique known as 'SQL injection,' by which malicious code was sent to the state or local website in order to run commands (such as exfiltrating the database contents) ... In one instance in approximately June 2016, the GRU compromised the computer network of the Illinois State Board of Elections by exploiting a vulnerability in the SBOE's website. The GRU then gained access to a database containing information on millions of registered Illinois voters, and extracted data related to thousands of U.S. voters before the malicious activity was identified.

GRU officers also "sent spearphishing emails to public officials involved in election administration and personnel at companies involved in voting technology." As the Special Counsel report detailed, "In August 2016, GRU officers targeted employees of... a voting technology company that developed software used by numerous U.S. counties to manage voter rolls, and installed malware on the company network." Furthermore, "In November 2016, the GRU sent spearphishing emails to over 120 email accounts used by Florida county officials responsible for administering the 2016 U.S. Election. The spearphishing emails contained an attached Word document coded with malicious software (commonly referred to as a Trojan) that permitted the GRU to access the infected computer... The FBI was separately responsible for this investigation. We understand the FBI believes that this operation enabled the GRU to gain access to the network of at least one Florida county government."[3]

Thankfully, there is no evidence that any votes were actually changed and that no lasting damage was done to voter registration databases. Nonetheless, these incidents should be viewed as precursors or dress rehearsals for similar attacks against the 2020 U.S. presidential election. As FBI Director Christopher Wray remarked in comparing the 2018 midterm elections to

the 2020 presidential race, "We recognize that our adversaries are going to keep adapting and upping their game… So we are very much viewing 2018 as just kind of a dress rehearsal for the big show in 2020…."[4]

Guaranteeing the integrity of the vote count is instrumental to a healthy democracy. Candidates and their campaigns have strong incentives to sway or portray the electoral processes in partisan terms, and thus those running elections, particularly election administrators, must do everything in their power to maximize the public's trust in their work. In a 2005 report still relevant today, the National Research Council asserted:

> [T]rusted election processes should be regarded as the gold standard of election administration, where a trusted election process is one that works, that can be shown to have worked after the election has been held, that can be shown to have not been manipulated and to have not led to a large number of mistaken or lost votes, and that can be shown to reflect the intent of the voters. Trusted election processes increase the likelihood that elections will be regarded as fair, even by the losing side and even in a partisan political environment.[5]

Because the majority of technology infrastructure supporting elections is computer-based, robust cybersecurity of the infrastructure is an essential element for assuring American voters that an election was conducted fairly. Providing such assurance is nevertheless complicated by three key challenges. First, all voters have a right to cast their ballots in secret, which cannot be compromised by election audits. Imagine, for example, the difficulty of developing a financial audit procedure for a bank in which particular monetary transactions of customers could not be associated with specific customers.

Second, an election must always produce a winner, even when only a few votes separate the results. A small number of fraudulent, improperly cast, miscounted, manufactured, lost, or otherwise invalid ballots can thus sway an election. Because small manipulations are simultaneously easier to perpetrate and inherently harder to detect than large ones are, the risk of election fraud is greatest when the electorate is evenly divided and vote counts are close, as has been the case recently for a number of American presidential elections.[6]

Third, the value of cybersecurity measures in many other computer-based systems can often be justified in cost-benefit terms, e.g., by comparing the cost of a particular security measure to the expected loss if the measure is not taken. In an election in a democracy, however, how does one measure the supposed value of a single vote? (Autocracies don't have to worry about such issues.) Budgets for cybersecurity are finite, thereby placing constraints on election administrators who must subsequently undertake careful assessment and evaluation of the security issues of the electoral infrastructure—both as a whole and for individual components.

Cybersecurity Considerations for the Overall Electoral Infrastructure

An unfortunate reality of information technology (IT) is that system testing can identify defects, including security vulnerabilities or software bugs, but no reasonable amount of system testing can prove that an IT-based system is completely free of defects. When a system is deployed for actual use, security becomes further complicated. The process of system certification can only evaluate the software and hardware that the vendor presents but cannot take into account how the system is actually operated and maintained when in use. It is even difficult to prove that the software running on a given machine in the infrastructure is the same as that which was presented for certification.

In addition, all software, including software for electoral infrastructure systems, contains bugs and other vulnerabilities that will be discovered after initial deployment, implying that a system that repairs any vulnerabilities known today may well be discovered to have vulnerabilities tomorrow. The assurance of security is therefore an ongoing process that requires searching for vulnerabilities proactively and fixing them immediately. This attribute of all software undergirds two necessary elements of electoral cybersecurity.

First, the assurance of security by checklist compliance—a requirement of the certification process—provides a baseline level of security, but by itself is known to be inferior to security assessed through an adversarial process. The best such process is an independent white-hat attack,[7] or a test attack conducted by white-hat teams that attempt everything real attackers would try by taking advantage of technological or procedural flaws in the system's security posture or the human infrastructure in which the technology is embedded. Security flaws uncovered by white-hat attacks are then forwarded to responsible parties for repairing.

Another type of adversarial process is an independent examination of the physical hardware and software of the system in question. Such examination will yield information about the system's ability to resist attack. Inspections before systems are deployed provide an opportunity for discovering the potential for bad behavior. However, vendors, who provide the hardware and software for elections, generally resist third party inspection of source code on the grounds that allowing outsiders such access compromises their intellectual property.

Second, "security by obscurity" is a poor security practice of relying predominantly on the secrecy of the system's design or implementation as the main method for ensuring its security.[8] By contrast, the responsible disclosure of discovered vulnerabilities is usually recommended, in order to provide strong incentives for system owners to address and fix them. (Under the practice of responsible disclosure, the system owner or vendor is notified of a vulnerability when it is discovered to ensure a quick resolution, and the vulnerability is publicly disclosed after a period of time that is deemed sufficient for repairing it.)

A few misconceptions about election cybersecurity also need to be briefly addressed. Many people commonly believe that the security of a computer can be assured by not connecting the computer to the internet. Although many attacks on computer systems are delivered through the internet, the lack of an internet connection does not guarantee security. For

example, an individual's computer could be compromised prior to ownership or while being updated, e.g., through using outdated operating systems with existing vulnerabilities, installing new programs or operating systems with additional files (e.g., backdoors or trojans that share information with a hacker), disabling an anti-virus or anti-malware program, or even monitoring power consumption.

Moreover, election officials themselves may compromise the election infrastructure, either wittingly or unwittingly, as cybersecurity is not solely a technical issue. Because human beings are intimately involved in all electoral operations, human vulnerabilities can certainly be exploited. Looking at the resilience of the electoral infrastructure as only or even primarily a technical issue is therefore a profound mistake, as many of the most harmful attacks on computer systems originate with an attacker targeting a human being.

Cybersecurity Considerations for Vote Casting Systems

For the acquisition of vote casting systems, election officials often rely on a process established by the Election Assistance Commission (EAC) certifying that a vendor's voting system meets the Commission's Voluntary Voting Systems Guidelines (VVSG), the latest of which were issued in 2015.[9] This certification is provided by any one of a number of voting system testing laboratories, which are accredited by the EAC and receive fees from vendors for their work in qualifying a system.

Because these standards include criteria related to security, election officials often view certification as complete assurance that a system's security is sufficient. Although the certification does confirm that the vendor paid attention to required security protocols, certification does not necessarily denote an adequate security posture. Moreover, even in states where verifiable systems are used, oftentimes a check on a voting system's functionality and accuracy does not take place.

A number of independent research efforts have demonstrated the ease with which individual electronic voting stations can be compromised by simply using the paltry resources available to university research teams.[10] Hostile foreign governments would be able to deploy orders of magnitude more resources to this task. In addition, these actors would have no qualms about attacking vulnerabilities or weaknesses that would yield higher leverage—in other words, engaging in vendor-level attacks such as installing damaging software or infiltrating outdated operating systems, as opposed to targeting specific machines to modify individual votes.

Verifying the security afforded by a given system's certification level is the first step in assuring overall election security. A second measure is to ensure that the properly certified system is the actual system deployed for use by voters, and not one that has been tampered with after its certification. Tampering opportunities occur at two stages: when the vendor loads software onto voting machines before they are shipped to precincts, and while voting machines sit in storage after delivery but before deployment and use.

Finally, a secure process must be established to address additional security risks when communicating the results from individual polling stations to a central tabulation authority. The received ballot totals must match those recorded at the precinct level. Such communication can be performed manually, by electronic transmission (e.g., over the internet or a phone line), or by physically carrying computer-readable media containing precinct-level vote totals to the tabulation authority's physical location. The security risks of each method can be mitigated with proper attention and even using more than one in parallel.

Types of vote casting systems currently vary from state to state.[11] Several states only allow vote by mail (e.g., Washington, Oregon, and Colorado), or paper ballot only (e.g., Michigan, Massachusetts, New York, and Virginia, among others). However, many have previously employed Direct Recording Electronic (DRE) voting machines without using a Voter Verified Paper Audit Trail (VVPAT) (e.g., Louisiana, Georgia, and South Carolina), or had mixed paper ballots and DREs without using VVPAT (e.g., Texas, Florida, Pennsylvania, Indiana, and Kentucky.) In total, fourteen states did not use VVPAT as their polling place equipment as of November 2018. This practice is dangerous.

Following the spark of public anger over Russian interference, states seeking to upgrade their vote casting systems have been caught between funding shortages, litigation challenges within procurement processes, or political deadlock. Despite these barriers, it appears that only Louisiana, South Carolina, and the majority of New Jersey, along with dozens of counties, will be using paperless voting machines in the 2020 U.S. presidential election.[12]

Nevertheless, it is still unclear whether the upgrades that have taken place thus far truly solve vote casting problems or simply create further security considerations, disguised by trust in new systems that lack thorough evaluation. For example, with the introduction of ballot-marking devices (BMDs),[13] a voter can use a touchscreen to vote, review a printed version of the ballot for verification and insert it into an optical scanner that counts and saves it in a secure lockbox. This paper trail consequently allows election officials to audit the election. Two primary concerns about the rollout of BMDs have been raised, however.[14] First, the system's printer and scanner share the same path, so if any races are left blank by voters, the machine could autofill the races—and neither election administrators nor voters themselves would be able to verify the change. Second, voters can opt to not review their ballot and send the vote directly to the scanner, thereby circumventing the exact process designed to confirm accuracy between the voter's intention and the actual counted ballot. It is also inevitable that future issues with BMDs would be dismissed or considered user error, leaving manipulation largely undetected. The New York State Board of Elections is reviewing certification due to these issues, but other jurisdictions, which have chosen to implement BMDs, are not.

In addition to the use of aging or unreliable vote casting machines, it should be noted that shortages of both physical equipment and human resources are likely, as resources for updating vote casting systems continue to be inadequate for effectively addressing future challenges.

Strengthened support must be provided to states and counties across the country that continue to conduct elections through vulnerable vote casting machines with insufficient ballot verification.

Cybersecurity Considerations for Voter Registration Systems

Voter registration systems differ from vote casting systems in a number of ways that affect their security posture. Most importantly, voter registration systems are centralized at the state level, giving the attacker the ability to have a bigger impact on manipulating or disrupting an election by compromising just a few voter registration systems, rather than the many voting machines that are not connected to a centralized system. Moreover, some voter registration systems rely on information from other databases, such as departments of motor vehicles, departments of correction, or departments of vital statistics, to confirm voter eligibility. Compromises in these databases, such as the alteration or erasure of key data, in turn could produce ripple effects on the accuracy of voter registration databases. Security issues with other databases could adversely affect the overall integrity of voter registration databases.

Voter registration systems also entail relatively straightforward computerized functionality that is present in many commercial database systems. Because the underlying software of voter registration systems is typically proven through applications to multiple problem domains and exercised repeatedly, they are less likely to be successfully hacked, but potentially more destructive in causing harm if ultimately compromised. By contrast, vote casting systems are niche products, put into operational use only sporadically, rendering them more vulnerable to concealed or undetected attacks that take place.

Finally, apart from requirements imposed by HAVA, voter registration databases are not required to conform to any set of national standards or guidelines for cybersecurity, thereby leaving the development and testing of such systems to each state. Although HAVA was the first U.S. law under which the federal government developed policies and provided funding for state and local elections, it lacks sufficient provisions with respect to uniform collection, reporting, and transparency of election-related data.[15] Nor does it mandate standards for voting technology and vote casting protocols.

Recommendations

In 2018, the National Academies released a consensus report entitled *Securing the Vote: Protecting American Democracy.*[16] This report made a number of recommendations intended to harden the election infrastructure of the United States against external attack and to safeguard its integrity and credibility. The authors incorporate all of these recommendations by reference, underscore the importance of several of them by mentioning them below, and go further by making a number of additional recommendations.

2.1. Require that all vote-counting systems provide a voter-verified paper audit trail.

New federal legislation should require that all vote casting systems must have the capability to provide a VVPAT for federal elections (NRC recommendation 4.11). Current guidelines for vote casting systems do not impose such a requirement, although existing regulations do provide specifications to which a VVPAT must conform if such a capability is used.

2.2. Require risk-limited auditing for all elections.

Legislation should require risk-limited auditing (NRC recommendation 5.8).[17] Through requiring voter-verified paper ballots, manual counting, and risk-limiting audits, the Protecting American Votes and Elections (PAVE) Act, introduced by Senators Ronald Wyden, Kirsten Gillibrand, Elizabeth Warren, Patricia Murray, Edward Markey, and Jeffrey Merkley, marks a positive step in this direction.[18] It would not only strengthen structures for risk-limiting audits and "provide the voter with an opportunity to correct any error on the paper ballot before the permanent voter-verified paper ballot is preserved", but also improve access to voting systems for individuals with disabilities and make funding available to enhance the analysis and testing of accessible paper ballot verification mechanisms for "the regularly scheduled election for Federal office in November 2020, and for each subsequent election for Federal office."[19] It is recommended that similar legislation be introduced and enacted in a timely matter.

2.3. Assess the security of computerized election-related systems in an adversarial manner.

The security of computerized election-related systems should be addressed through a combination of white-hat attacks and independent code inspection. Without third-party examination or review of the systems' security, a key aspect of protecting U.S. election infrastructure will be neither publicized nor subject to independent scrutiny.

Legitimate concerns about intellectual property protection can be addressed through the use of carefully crafted non-disclosure and/or non-compete agreements. The former would permit public discussion of security flaws found but also specify details that could not be disclosed. Non-compete agreements would provide vendors with assurances that allowing code inspection would not enable those viewing code to become competitors. Findings from reports derived from white-hat attacks and code inspection could therefore be widely publicized to pressure vendors and election administrators to fix the problems without delay. Bug bounties, which incentivize individuals to report vulnerabilities through receiving recognition and compensation, should also be offered to encourage regular testing.

2.4. Establish basic norms regarding digital behavior for campaign officials.

In order to ensure the widespread adoption of improved cybersecurity practices during electoral cycles in particular, campaign officials should establish and uphold basic norms with regards to their own digital behavior.[20] For example, multi-factor or dual authentication is an easy practice to implement for confirming a user's claimed identity and strengthening

information security overall. In addition, improved processes for threat-intelligence sharing and disclosure of vulnerabilities would contribute to the development of digital behavior norms. Such efforts would illustrate that campaign officials not only take cybersecurity issues seriously, but are also raising overall levels of awareness and related action in the United States.

2.5. Commit regular funding streams to strengthen the cybersecurity posture of the election infrastructure.

Certain measures related to the organizations surrounding election infrastructure would enhance resilience and increase public confidence in the conduct of an election, and all of these measures will require increased funding. These include:

- The implementation of specific training programs for election administrators and their staff on basic cybersecurity practices (NRC Recommendation 5.2).[21]
- Extension of the voting period so that voters are able to cast their ballots over a period of time (e.g., several days). Entirely apart from making the voting process more convenient, it is simply a reality that technical problems often appear in complex computer-based equipment when placed into widespread operation with real users, and attempting to deploy fixes on a time scale of a few hours is often infeasible. An extended voting period would provide an opportunity to fix problems that appeared early, and voters unable to cast votes because of such problems would be given the opportunity to return after those problems had been fixed.
- Ongoing efforts to enhance the resilience of electoral infrastructure—both technical and organizational (NRC Recommendation 5.4). As technology advances, more vulnerabilities will occur and a continuing (as opposed to a one-time) effort will be needed to address them.

To address the issue of partisanship, the administration of elections should be undertaken by nonpartisan officials, and both vote casting and voter registration systems should be acquired from vendors whose senior leadership is scrutinized and demonstrably nonpartisan.[22]

2.6. Retain the designation of election infrastructure as critical infrastructure.

In 2017, the Department of Homeland Security designated election infrastructure as critical infrastructure, thus making operators of election infrastructure eligible for a variety of its cybersecurity services. Election infrastructure was defined as "storage facilities, polling places, and centralized vote tabulations locations used to support the election process, and information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and report and display results on behalf of state and local governments."[23] The designation of election infrastructure as critical infrastructure gives priority to the systems involved as a matter of national security—quite appropriately

given the role of that infrastructure in supporting the foundations of the nation's democracy (NRC Recommendation 5.1).

2.7. Allow political parties to provide cybersecurity assistance to state parties and to individuals running for federal office and their campaigns.

Currently, Federal law (52 U.S.C. 30116) limits the amount of financial support that political campaigns can receive from national political parties. Without legislative relief, cybersecurity assistance must be treated as an "in-kind donation", and thus would count against those limits and reduce the amount of direct financial support a campaign could otherwise receive. As of the date of this writing, there is at least one bill in draft form that provides for such relief; in any case, legislation to this effect should be enacted with all due haste.

CHAPTER THREE

Regulating Online Political Advertising by Foreign Governments and Nationals

By Nate Persily and Alex Stamos

The Problem

Agents of the Russian government purchased a significant amount of digital advertising during the 2016 U.S. presidential election. The scale of the paid advertising effort and the exact amounts of foreign spending on digital ads remain unknown and may never be known. However, it is now well understood that, alongside "organic" social media content, paid advertising by Russian nationals helped push messages about candidates and issues relevant to the 2016 election campaigns.

Facebook's investigation of Russian spending on its platform, as well as the indictments and report from Special Counsel Robert Mueller and his team, provide most of what is known about Russian paid-advertising throughout the campaigns.[1] Through 470 inauthentic accounts, Russians spent over $100,000 (some in rubles) on over 3,500 advertisements on Facebook and Instagram between June 2015 and May 2017, in addition to unspecified amounts through Google and Twitter.[2] As is often true for advertisement spending even by domestic actors, the impact of these communications is hard to quantify.[3]

The online ads run by Russian organizations and agents contained a variety of messages with varying connections to the presidential campaign. Some contained explicit messages of endorsement or opposition to a candidate, containing phrases such as "Support Hillary", "Save American Muslims", "Make America Great Again!", or "Join Florida Trump Rallies". Others mentioned the candidates but did not use charged language of endorsement or opposition. According to the Special Counsel report:

> During the U.S. presidential campaign, many IRA-purchased advertisements explicitly supported or opposed a presidential candidate or promoted U.S. rallies organized by the IRA (discussed below). As early as March 2016, the IRA purchased advertisements that overtly opposed the Clinton Campaign. For example, on March 18, 2016, the IRA purchased an advertisement depicting candidate Clinton and a caption that read in part, "If one day God lets this liar enter the White House as a president - that day would be a real national tragedy." Similarly, on April 6, 2016, the IRA purchased advertisements for its account "Black Matters" calling for a "flashmob" of U.S. persons to "take a photo

> with #HillaryClintonForPrison2016 or #nohillary2016." IRA-purchased advertisements featuring Clinton were, with very few exceptions, negative. IRA-purchased advertisements referencing candidate Trump largely supported his campaign. The first known IRA advertisement explicitly endorsing the Trump Campaign was purchased on April 19, 2016. The IRA bought an advertisement for its Instagram account "Tea Party News" asking U.S. persons to help them "make a patriotic team of young Trump supporters " by uploading photos with the hashtag "#KIDS4TRUMP." In subsequent months, the IRA purchased dozens of advertisements supporting the Trump Campaign, predominantly through the Facebook groups "Being Patriotic," "Stop All Invaders," and "Secured Borders."[4]

The lion's share of Russian-sponsored ads, however, did not directly reference the candidates, but instead addressed divisive political issues, including gun rights, immigration, police brutality, or terrorism. Some of these ads went so far as to encourage Americans on both sides of an argument to actively join groups or attend rallies. Judging by the content of their ad buys on social media platforms, the Russians engaged in the 2016 U.S. presidential election had two goals—support Trump by disparaging Clinton, and amplify existing polarization in American society.

These critical distinctions matter both for existing law and the constitutional restrictions that might govern certain proposed reforms. To date, digital campaign spending is largely unregulated, notwithstanding two key exceptions: (1) a ban on electioneering communications sponsored by foreign nationals and (2) disclosure requirements for all advertisements of candidate-advocacy placed for a fee on another person's website. Many of the Russian ads violated these laws, but the majority did not. To prevent similar foreign spending in future elections requires policy innovations tailored to the unique opportunities that online environment offers malicious actors and the unique challenges that this environment presents to regulatory agencies in charge of promoting transparency in campaign spending.

To successfully confront the exploitation of digital political advertising platforms by foreign actors, several significant obstacles must be overcome. In particular, the 2016 campaign revealed how the internet facilitates anonymous campaign spending and how the law's limited reach to candidate-related advocacy can be easily avoided by foreigners spending money on issue advocacy. Although serious constitutional constraints rightly limit available options, any new regulation that seeks to address the problems discovered in 2016 must deal with these two problems: anonymity and issue advocacy. Disclosure represents the necessary first step for any reform. However, capturing the relevant universe of ads deemed "political" and requiring disclosure presents serious challenges.

Similar challenges and concerns exist apart from the special case of online foreign intervention in U.S. elections. Reformers have long advocated for greater disclosure in political

advertising and greater regulation of "issue advertising". Indeed, the litigation surrounding the McCain-Feingold campaign finance law, otherwise known as the Bipartisan Campaign Reform Act (BCRA), often focused on whether the law swept in too much speech by banning corporate-sponsored advertising beyond "express advocacy" or communication promoting the election or defeat of candidates. BCRA banned corporate-sponsored advertising on "electioneering communications" or satellite communications made within sixty days of the general election or thirty days before the primary that refer to a clearly identified candidate for federal office and were targeted to the relevant electorate. In *Citizens United v. FEC*, the Supreme Court struck down that provision as unconstitutional. Because independent spending by individuals did not pose a threat of corruption and was protected by the First Amendment, the Court reasoned, similar spending by corporations from their treasury funds was equally protected. Given the dramatic result of *Citizens United*, fewer people paid attention to the part of the opinion that upheld, on an 8 to 1 vote, the law's disclosure provisions. The ultimate result of *Citizens United*, then, was suspicion of limits on spending, but general deference to disclosure.

Neither BCRA's "electioneering communication" definition, nor its disclosure provisions, cover messaging beyond candidate-related advertising. Although ads can influence voter perceptions of candidates without directly mentioning a candidate's name, regulating election-related speech beyond words or images, which refer clearly to candidates, has always proven conceptually and constitutionally difficult. In today's political climate, virtually any issue can become politicized, from general topics such as immigration and civil rights to features of daily life such as sports and entertainment. Defining ex ante a universe of "issues" relevant to elections or politics is challenging, if not impossible. Attempts to do so rely on vague phrases, such as "issues of national legislative importance", and place a great responsibility on administrators—or in the case of the proposed Honest Ads Act, on a social media platform—to define the phrase's meaning in application.

Regardless of how the universe of ads requiring disclosure or disclaimers is defined, any adequate disclosure regime must specify who is required to disclose, and how disclosure will properly reveal the identity of the person or entity behind the ad. With respect to foreign election interference in particular, the regime of disclosure must be tailored so that the true entity behind the ad, rather than a front organization or pass-through, is made public. With the exception of RT and Sputnik, Russian advertisements or internet communications during the 2016 U.S. presidential election largely operated through fabricated organizations to disguise the original identity of the advertiser.

Of course, the issue of ambiguous or non-transparent funding behind campaign ads is not new nor limited to the issue of foreign interference. So-called "dark money" is a longstanding problem that has accelerated in importance with the rise of prominent Super PACs and 501(c)(4) organizations involved with the independent funding of campaign-related advocacy. In contrast to the obligations placed on candidates and parties, the law places incomplete disclosure

responsibilities on Super PACs and 501(c)(4) organizations, allowing them either to evade disclosure for many expenditures or merely to disclose non-human entities, such as corporations or other associations. The law never requires disclosure for pure issue advocacy for any entity.

Most existing disclosure regimes fail to capture the original financial source of an expenditure. If the regulation merely requires an organization's name to be included in a disclaimer or in a filing with an election authority, then sponsors can create groups with innocuous, patriotic-sounding names, such as "Americans for America". Consequently, any system of disclosure that seeks to avoid the cloaking of money in intermediary organizations must require the identification of an individual who either manages the organization or contributes money to the organization above a certain threshold. If the disclosure is limited to the name of a corporation or association, then the actual source of the money—whether foreign or domestic—can easily remain concealed.

Finally, any regime that addresses either express or issue advocacy must have special provisions for the media. Journalists and the companies they work for spend money on "communications" that refer to candidates and have a sizeable impact on election coverage and results. Media coverage of campaigns is more ubiquitous and influential than paid online communication, such as advertisements. As compared to news and other unpaid commentary, advertising represents only a tiny share of voters' exposure to information sources relevant to campaigns. A disclosure regime, or any campaign finance regulation for that matter, that covers expenditures on politically relevant communication must draw a line between legitimate media organizations and other forms of paid communication. All existing campaign finance regulations do so, but defining the media in the age of the internet is challenging given that anyone can blog, post, or Tweet. YouTube celebrities often have followings comparable to established media organizations. Interest groups regularly create their own webpages and news-like sites in order to appear similar to journalistic institutions. Although any "media exception" for campaign finance regulation will inevitably exclude some legitimate journalists and include some illegitimate ones, the designers of such regulations need to carefully consider the impact on free speech from roping legitimate media into definitions of paid electoral communication.

Existing Proposals

Since the 2016 U.S. presidential election, social media platforms and members of Congress have explored different proposals for increasing transparency related to political advertising, particularly regarding expenditures by foreign nationals. Proposed by Senators Mark Warner and Amy Klobuchar, the Honest Ads Act[5] is the most advanced legislative proposal thus far. A similar proposal, titled the New York State Democracy Protection Act, was signed into law by Governor Andrew Cuomo in April 2018.[6]

The Honest Ads Act would require a public archive of all election-related advertisements, both candidate-related and on issues of national legislative importance. Maintained by the FEC, the

archive would contain a digital copy of the ad, a description of the target audience, the number of views or impressions, and the rate charged for the ad buy. In addition, clear disclaimers revealing the name of the organization or individual who paid for the ad would be required.

In the wake of the 2016 U.S. presidential election and in the shadow of potential legislation, several social media platforms have developed new transparency regimes for political advertising that include a similar public library of political advertising, including the ad's sponsor, frequency, and how much was spent.[7] Facebook already has created a searchable archive for all political ads—both candidate-related and those determined as on "issues of national legislative importance"—for its platform and Instagram. All ads will stay in the archive for at least seven years and include information on the number of impressions or views by gender, age, and state. Facebook users can search the archive on keywords and select ads from specific sponsors. Similarly, Google presents candidate-related advertisements in its public library. Google also notes the demographics of individuals targeted by the advertiser and the total amount spent, whereas Facebook only tracks and records the viewers themselves. In addition, Twitter's archive for political advertisements is searchable by Twitter account, as well as targeted and actual audience, including characteristics such as age, gender, language, or location by state and city.

None of these archives or libraries are optimized for the kind of research that is necessary to trace with accuracy the flows of money from outside groups to the platforms. They vary greatly in the search features they provide (especially whether ads can be organized by date) as well as the clarity with which they identify spenders. Facebook, for example, identifies spenders according to Facebook pages, which can change, as opposed to an FEC-identified account, which would be crucial both to measure legal compliance and to trace spending across platforms. Google does not provide information on political candidates' advertisements in state elections or advertisements on political issues. The shortcomings of the ad archives led a group of scholars connected to Mozilla to issue a helpful letter describing to the platforms what an effective ad archive would look like.[8]

Recommendations

3.1. Explicitly prohibit foreign governments and individuals from purchasing online advertisements targeting the American electorate and aimed at influencing U.S. elections.

The prohibition on electioneering activity by foreign nationals should be clarified to make explicit a ban on any foreign-sponsored online advertisements that target the American electorate and are intended to influence a U.S. election. The ban should apply to any advertisement that mentions or features a candidate or party within sixty days of an election, as well as advertisements on issues of national legislative importance during that time period. Because such issue ads are difficult to identify *ex ante*, the FEC should develop a list of such issues for which the ban would apply.

3.2. Support the passage of the Honest Ads Act with several key amendments.

The Honest Ads Act represents an important first step in bringing online advertising within the regulatory ambit of existing law. At a minimum, the U.S. Congress must pass and President Trump must then sign into law the Honest Ads Act to establish fair and reasonable guidelines for online advertising in political campaigns, including the regulation of foreign actors in this domain. But more could be done; this legislation could be strengthened with several amendments to more effectively increase the transparency of online political advertisements.

Currently, the most significant drawback of the Honest Ads Act is that the draft legislation places the critical responsibility of defining a political ad or an "issue of national legislative importance" entirely with the social media platforms themselves. Disclosure of issue advocacy represents a dramatic shift in the law, and it is too significant to trust private companies with defining which issues rise to the level of warranting advertising disclosure. As Facebook has moved in this direction, the firm has run into an array of line-drawing problems, including (1) addressing media organizations that boost news stories; (2) potentially designating charitable activity as political if, for example, its advertisements are related to health; or (3) managing product ads that touch on politics, such as a recent Nike ad featuring Colin Kaepernick, a Budweiser ad mentioning immigration, or an Amazon ad promoting a political book. Strong arguments could be made in favor of disclosure in all or just some of these cases, but such decisions should not depend on an individual company's definition. Instead, the Honest Ads Act should be amended to make the FEC responsible for declaring for a given election cycle what issues require ad transparency, along the lines described in the ban on foreign advertising described above.

The second drawback of the proposed legislation concerns the disclosure of targeting information. While the Honest Ads Act is premised on a conception of targeting in which advertisers specify demographic categories and/or geographic regions, targeted online advertising has moved beyond categories of users to individual lists of users. The most sophisticated political consultants and parties now curate lists of individuals, along with email addresses to identify them, so as to send individualized messages to them. These lists are then turned over to Facebook and Google who promise to deliver the advertisement to a list of people (a "custom audience") representing a large share of the targets. Moreover, Facebook also has provided "lookalike audiences", which is a Facebook audience similar to the one originally targeted. Exposing individuals' names rather than larger group-targeting categories, such as suburban white women between the age of 30 and 40, raises serious privacy issues.

Data regarding who was exposed to an ad is equally if not more important than targeting information. As targeting increasingly moves away from categories and towards individuals, advertisers or platforms cannot be expected to reveal the names of people who are targeted by the ad. "Exposure disclosure" should instead be required at a smaller level, such as zip code, census block, precinct level, or even at the county or district level. Talented enterprising analysts—and opposing campaigns—may still be able to identify some individuals from this geographical data,

but the specific characteristics of these individuals would remain concealed. Although platforms tend to balk at such micro-level disclosure because it reveals the "secret sauce" of advertisers, the innate surgical precision of effective individual-level targeting remains a key problem with digital advertising, and exposure disclosure is the only way to truly understand the dynamics of modern campaigning. At a minimum, policy makers and the platforms should consider calibrating disclosure to the level of ad targeting, in order to ensure that the more micro targeted an ad, the greater the disclosure obligation on the spender.

A third challenge with the Honest Ads Act concerns the current requirement of a library for the "creatives" or the actual advertisements delivered to targets. By combining artificial intelligence with advertising, modern campaigns in some instances have created hundreds of thousands of variations on a given ad that are A-B tested with targets. Subsequently, the platforms have taken the logical position that no matter how minor the variation, each creative is then presented as its own advertisement in the library. To maximize efficiency, however, analysts should classify advertising and spending by candidate or group, so that the library could organize creatives into groups derived from a core advertisement, and the universe of ads and their collective targets can be analyzed and evaluated more coherently.

Finally, new regulations of online political advertising provide an opportunity to address the challenge of "dark money" or front organizations that place advertisements funded by individuals and groups wishing to evade disclosure. Compared to television or other media, the internet affords greater capacity for foreign and domestic actors to participate in surreptitious activity to influence elections. By revealing the individuals who sponsor advertisements, both disclosure and disclaimers can effectively uncover the original source of the money. Therefore, advertisers and platforms should be required to disclose the names of responsible individuals and entities to the FEC, and each online ad should be identified by the FEC code of its purchaser. In practice, this recommendation would likely require, on the face of an ad or with one click-through, a list of the top five individuals who fund an organization (e.g., Super PAC), the CEO of a corporation funding ad, or the leader of a union funding an ad. Certainly, this requirement will not solve all problems, because shell corporations can be established to ensure that the CEO is not truly "responsible" for the advertisement. But this mandated change would represent a significant step in the right direction for increasing campaign transparency.

3.3. Strengthen self-regulation mechanisms for the major internet platforms.

Tackling foreign interference in U.S. elections requires new effort from both government and the private sector. The 2020 presidential campaign is already underway and most of the applicable restrictions on foreign spending come from legislation drafted in the pre-internet age. In addition, given the pace of technological change, foreign adversaries (like domestic political entrepreneurs) will always be one step ahead of any regulatory regime the U.S. Congress designs. The major internet platforms, therefore, must together confront the problem of foreign sponsored advertising, as they should foreign election manipulation through other means.

Such coordinated action may require a specific exception to the antitrust laws or a congressionally blessed industry self-regulatory body akin to the Financial Industry Regulatory Authority. However such coordination is achieved, preventing foreign interference should demand the same kind of collective industry response that was engendered by terrorist recruitment and child endangerment. In those domains, the industry has found a way to trade information and develop best practices to confront common problems. Foreign election meddling is another such issue. All efforts should be made by social media and other internet companies to present a common front against foreign election interference in the run-up to the 2020 U.S. presidential elections.

CHAPTER FOUR

Confronting Efforts at Election Manipulation from Foreign Media Organizations

By Nate Persily, Megan Metzger, and Zachary Krowitz

The Problem

Much of the analysis of Russian intervention in the 2016 U.S. presidential election has focused on covert forms of internet-based influence generated through clandestine social media campaigns and advertising. However, not all efforts by the Russian government or its affiliated entities were done in secret. Some attempts at influence were open and notorious, such as the stories broadcasted, posted, and promoted by Russian media organizations RT and Sputnik. Policy prescriptions for how the U.S. government or social media companies should confront efforts by foreign governments to influence U.S. elections through official media organizations, however, raise complex questions regarding the rights of those organizations, as well as the government's regulatory capacity to distinguish between authentic journalism, government-sponsored propaganda, and election manipulation.

As discussed in Chapter One, the Russian government created Russia Today in 2005. Although formally modeled after the BBC, RT was later renamed and evolved into an effective propaganda outlet for transmitting the values and objectives of the Russian government across the world. As the Kremlin's response to Western criticism of its anti-democratic efforts, RT uses an international, multiple-language, 24-hour television service and associated website to promote Russian policies and attack the values and policies of Western governments, especially those of the United States.[1] With a budget of approximately $300 million, RT is available on Comcast, Cox, Charter, DirecTV, and Fios, and claims that it "reaches more than 644 million people worldwide."[2] As mentioned earlier, RT also claims to be the number one watched "news" channel on YouTube.[3] Sputnik, for its part, is "a brash Russian-government-run news and commentary site that models itself on BuzzFeed."[4]

In addition to adopting a name change to obscure its connection to the Russian government, RT America operates through a complex network of financial arrangements to create fictional distance between the media organization and the Russian government. The Russian government finances RT through a parent company, TV Novosti, which in turn transfers money to a production company, T&R Productions, to underwrite RT America. This convoluted web

of funding is tailored towards demonstrating formal independence, despite clear control and financial responsibility by the Russian government. RT editor-in-chief Margarita Simonyan has spoken frequently about the instrumental role her organization plays in advancing Russian state interests, at times even implying that RT is as important to the Russian state as the Russian Armed Forces.[5] Statements from those who have left both RT and Sputnik confirm the lack of journalistic independence from the state.[6] Controversial coverage by RT of the Russian military intervention in Ukraine in 2014 resulted in one of its anchors, Liz Wahl, resigning while on-air.[7]

In some respects, however, RT and Sputnik are functionally indistinguishable from a host of similar media organizations within and beyond the United States. While the overwhelming majority of RT's stories are true, others are barely news at all, but instead clickbait used to acquire a sizeable audience. They often feature controversial figures, such as Nigel Farage when he was championing Brexit,[8] 9/11 truthers, or those who believe Osama bin Laden's death was staged.[9] Simonyan also has explicitly stated that part of Russia and RT's strategy is to build audiences through lighter entertainment shows and soft news during less volatile times, but then to target them with political messages during more critical or vulnerable moments.[10]

The U.S. intelligence community's report following the 2016 U.S. presidential election described how RT and Sputnik had "contributed to the influence campaign by serving as a platform for Kremlin messaging to Russian and international audiences."[11] RT coverage of the campaign followed what is now acknowledged as the larger Russian strategy of sowing discord, diminishing Hillary Clinton, and facilitating mixed but generally more positive coverage of Donald Trump.[12] RT and Sputnik segments focused on Clinton's health,[13] discussed alleged corruption,[14] and called her the "Queen of War."[15] Additionally, RT focused its election coverage on significantly highlighting Senator Bernie Sanders in a positive light in the primary.[16] In the general election, RT devoted considerable coverage to third-party candidates, especially Green Party candidate Jill Stein. In 2015, Stein attended an anniversary gala for RT's 10th anniversary, where she was seated at the head table with Putin. In 2016, RT interviewed Stein several times, focused considerable attention on events such as the Green Party convention, and explicitly suggested Stein was a better choice for the American left.[17] Third-party debates were even hosted on RT between multiple Green Party candidates and between Stein and Gary Johnson, who were excluded from the major candidate debates. RT was therefore a substantial source of Stein's television coverage in the 2016 U.S. presidential election.

Concrete data on RT's reach are hard to find, but circumstantial evidence suggests that RT succeeded in effectively reaching many American internet users during the campaign period. By 2017, views of its flagship channel alone were similar to CNN's, with over 2 billion views,[18] and an interview on the U.S. elections with Julian Assange in November 2016 was one of RT's most popular videos the following year, with over 2 million views alone.[19]

RT trails mainstream media considerably in terms of followers on Twitter and Facebook. While RT's YouTube viewership at times has rivaled and surpassed CNN's, RT is far behind CNN on Twitter, with 2.6 million compared to 38.1 million followers respectively.[20] And yet, in

2016 RT was the 30th most shared news source on Twitter for election-related stories,[21] placing it just below Vox and ABC News and above Time Magazine and Slate. In other words, RT's reach on Twitter was similar to sources that would be considered fairly mainstream in the United States. Although the numbers are unavailable for how many of those viewers were located in the United States, recent research[22] during the 2018 elections found RT to have a similar ranking among users geo-located in the United States, putting its reach just between Vox and The Huffington Post in the week before the midterms.

RT and Sputnik pose difficult conceptual and regulatory challenges for U.S. government officials and executives at social media companies who seek to reduce Russian influence over the American electorate. And more generally, well beyond these specific Russian media organizations, distinguishing good from bad actors and manipulation from quality journalism presents intractable line-drawing issues that no regulatory regime can specify *ex ante*. In addition, the U.S. treatment of foreign media organizations generally and Russian companies in particular cannot be considered in a vacuum. As discussed in detail in Chapter Seven, when the United States seeks to promote democracy worldwide, some foreign governments accuse the American government of meddling in their internal affairs. Therefore, active U.S. regulation of foreign media organizations targeting American audiences could trigger retaliation in Moscow and elsewhere against both publicly sponsored (e.g., Voice of America or Radio Free Europe) and private U.S. media entities. Russia already has taken steps to retaliate against several U.S.-based media organizations by labeling them as foreign agents.[23]

In considering reform measures to address foreign election manipulation, it should be recognized that the "foreign-ness" of a media organization exists along a continuum, and is often far from a black and white distinction. At one time, for example, News Corp, which owned Fox News, The New York Post, and the Wall Street Journal, was an Australian corporation and had an Australian CEO, Rupert Murdoch, who later became a U.S. citizen. The Korean Unification movement leader Sun Myung Moon founded The Washington Times, which was owned by a corporation he had founded until 2010. Additionally, WikiLeaks transmits a sizeable amount of content in the United States, but has been registered as a library in Australia, a foundation in France, and a newspaper in Sweden, in addition to using two U.S.-based non-profit 501c3 organizations for funding purposes.[24]

Further along the spectrum, foreign governments own or control many international media organizations based outside the United States, such as RT with its well-established connection to the Russian government. A variety of media organizations, however, exist with less direct connection to foreign governments and with greater or lesser connection to the United States. Should BBC America be treated differently than BBC, for example? Should RT be treated differently than the BBC, Deutsche Welle (DW), France24, China Central Television, or Al Jazeera? Moreover, the conceptual and regulatory challenges become increasingly complex in the online environment, given the multiplicity of online sources of news, as compared to the limited number of broadcast and cable stations. Even defining or characterizing a news or media

organization for the online environment has proven difficult, let alone the degree of foreign ownership or influence over organizational operations that lead it to cross a legally relevant line drawn to identify foreign media sources.

Assuming the law can identify the requisite degree of "foreign-ness" of media outlets, the question of delineating propaganda and election manipulation from standard news or campaign coverage remains. RT does present "news", as well as what is sometimes described as "disaster porn", referring to viral stories of natural disasters, criminal incidents, and bizarre mishaps. In between these stories, which help develop its audience, RT weaves in opinion that promotes Russian government policy. RT is distinctive, not because of the unique substance of its coverage, but because of the identity of its sponsor, its intent, and its role as an instrument in pursuing Putin's foreign policy objectives. Because of its mix of news and propaganda, however, it poses a unique challenge for First Amendment law. Foreign governments or their agents are not protected by the First Amendment, but a law that might ban such media from internet platforms accessible to an American audience would pose unprecedented constitutional questions. As dangerous or effective as foreign sponsored propaganda might be, it will be difficult, as a constitutional matter, to control Americans' access to such communication on the worldwide web.

Recent Measures and Existing Proposals

In response to Russian election manipulation efforts in 2016, the U.S. government compelled RT and Sputnik to register under the Foreign Agents Registration Act (FARA).[25] FARA was passed in 1938 in response to a large group of American non-citizen residents being paid to disseminate propaganda on behalf of foreign governments and parties, including the German Nazi Party.[26] Initially, FARA required "each agent of a foreign principal to register with the government and disclose certain information," but it did not limit expenditures by those agents.[27] In 1966, Congress amended FARA "to prohibit any person acting under the direction or control of a foreign principal from knowingly making any contribution 'in connection with an election to any political office.'"[28] FARA defines an "agent of a foreign principal" as "any person who acts as an agent, representative, employee . . . or any person who acts in any other capacity at the order . . . of a foreign principal" who also engages in political activity for the foreign principal in the United States or "acts within the United States as a public relations counsel, publicity agent, information-service employee or political consultant for . . . such foreign principal."[29] The law exempts any newspaper, press service or association organized if it is at least 80% owned by American citizens of the United States, and the policies are not controlled, financed, or otherwise determined by a foreign principal.[30]

FARA requires foreign agents to register with the Attorney General[31] by disclosing the agent's name, a description of the agent's business, and any actions taken "as an agent of a foreign principal", the "nature and amount" of contributions given by the principal to the agent in the last sixty days, written and oral agreements between the agent and principal, a "detailed statement

of every activity which the registrant is performing for anyone other than a foreign principal . . . which requires registration" under FARA, and "[s]uch other statements, information, or documents pertinent to the purposes" of FARA.[32] The law then bars foreign agents who transmit "informational materials" to do so "without placing in such informational materials a conspicuous statement that the materials are distributed by the agent on behalf of the foreign principal."[33] Furthermore, the law requires every foreign agent to "keep and preserve . . . books of account and other records with respect to all his activities" that can be inspected by U.S. Justice Department officials.[34] Thus, FARA currently has three different requirements for foreign principals: registration, disclosure, and record keeping.[35]

Prior to 1995, FARA referred to political propaganda, rather than informational materials. It considered political propaganda to be communication that is reasonably adapted to indoctrinate, convert, or in any other way influence a recipient with reference to the political or public interests, policies, or relations of a foreign government or political party.[36] When faced by a First Amendment challenge to this seemingly vague provision, the Supreme Court nevertheless upheld the definition of propaganda, a decision that remains important for considering contemporary reform options.[37]

Before the government forced RT and Sputnik to register under FARA, only the media organizations NHK Cosmomedia and China Daily had been previously required to register.[38] Not surprisingly, RT opposed the FARA designation, arguing that the law's disclosure obligations would interfere with its journalism, for example by requiring the disclosure of confidential sources. Nevertheless, the U.S. Department of Justice required RT and Sputnik, as well as RT's parent company T&R Productions, to register as foreign agents.

In its FARA filing, T&R Productions noted that "the Russian Federation finances ANO TV-Novosti [the nonprofit, nongovernmental organization that oversees RT] to a substantial extent."[39] In its press release about the registration of T&R Productions as a foreign agent, the U.S. Justice Department wrote that T&R registered "as an agent for ANO TV-Novosti, the Russian government entity responsible for the worldwide broadcasts of RT Network."[40] Moreover, Acting Assistant Attorney General Dana J. Boente explained the move as an attempt to show Americans "who is acting in the United States to influence the U.S. government or on behalf of foreign principals."[41] Because T&R was ultimately labeled a foreign agent, RT lost its credentials for covering Congress-related news.

Independent of U.S. government action, social media platforms have taken several measures to reduce the reach of Russian government-sponsored media. In October 2017, Twitter announced that RT and Sputnik will no longer be allowed to advertise on the platform.[42] The company also pledged to use previously earned revenues from these organizations to fund research on the 2016 U.S. presidential election.[43] Google and YouTube also have begun to provide context when results from RT are displayed. Below all RT videos, YouTube currently states, "RT is funded in whole or in part by the Russian government" and provides a Wikipedia link with more information. YouTube has started to include similar disclaimers for other foreign-sponsored media

organizations as well, albeit with slight variations. For example, BBC videos are accompanied by the message "BBC is a British public broadcast service." In addition, after announcing the "deranking" of RT and Sputnik in its search results in order to combat misinformation, Google removed RT from its preferred news lineup, a group of news providers who receive access to additional revenue from premium advertisers.[44] Facebook recently suspended several pages linked to RT and demanded a disclosure of affiliation, citing the need for users "connecting with pages [not to] be misled about who's behind them."[45]

Recommendations

Less democratic governments would likely respond to the challenge posed by RT by banning it from the airwaves and blocking it on the internet altogether. For the same reasons justifying the registration of RT under FARA, the United States government may have the authority to do so as well. But banning RT and Sputnik would present constitutional questions concerning the right of American audiences to hear and view content from foreign media entities. An outright ban of these Russian propaganda agents also would likely trigger retaliation against legitimate, independent American media companies in Russia and other autocracies around the world. Short of a direct ban, therefore, we recommend a series of disclosure measures by social media platforms and the U.S. government as a strategy to help temper and mediate the most aggressive propaganda efforts of foreign media organizations.

4.1. Require greater disclosure measures for FARA-registered foreign media organizations.

Foreign media organizations registered under FARA should be required by law to present disclaimers attesting to their registration as a foreign agent. In practice, this restriction could include a disclaimer at the bottom of RT broadcasts and internet videos that simply identifies the station either as an "agent of the Russian government" or "sponsored by the Russian government". The same should be required, to the extent possible, for online texts and images. This regulation should apply specifically to the foreign agent itself, but it could also apply, if practicable, to the cable provider or platform hosting the content.

4.2. Mandate additional disclosure measures during pre-election periods.

If requiring foreign agents to disclose their FARA registration all the time is deemed too speech-restrictive, then more minimally, all foreign media organizations registered under FARA should be obligated to run such disclaimers in pre-election periods. As with the electioneering restrictions under the Bipartisan Campaign Reform Act, the pre-election period could be defined as sixty days before the general election and thirty days before the primary. Because these periods are when foreign-sponsored propaganda are likely to have the most electorally-relevant impact and damaging influence, clear signals for the broadcast's origin and likely intent of its sponsor can help viewers contextualize the presented information.

4.3. Support existing disclosure measures of specific social media platforms.

Companies such as YouTube, Twitter, and Facebook should voluntarily adopt measures—as some already have done—to promote these disclaimers to the extent possible. Undoubtedly, much of the content promoted by RT, Sputnik, or similar organizations will appear on the internet without disclaimers, particularly when forwarded by individual users or retweeted. Propaganda efforts can be mitigated by tagging the shared content with similar disclaimers, at least during the pre-election period. Moreover, steps to demote content by FARA registrants and prohibit their advertising (even nonpolitical advertising and "boosting" of posts) in the pre-election period should be encouraged.

If such a body of law and practice were to be developed as a supplement to FARA registration, the stakes of being labeled a foreign agent would become much higher, and thus, the United States could expect more intense objections to such designations, as well as an increase in retaliatory measures against American media organizations. Nevertheless, with respect to broadcasting to their own populations, authoritarian and semi-authoritarian regimes are quick to do much more than force disclosures on U.S. media organizations, even in cases without cause or evidence. As an example, both Voice of America and Radio Free Europe/Radio Liberty have only recently been labeled foreign agents in Russia, but have been "banned from broadcasting in the country since 2014 and 2012, respectively."[46]

As regulations expand beyond designating media organizations as foreign agents to monitoring foreign media organizations in general, the potential sweep would be quite broad. However, as foreign propaganda efforts through official government-sponsored media—whether from Russia, China, or anywhere else—become increasingly common, it may be necessary to adopt a bright line of disclosure during the pre-election period for foreign media organizations, irrespective of FARA registration. If such efforts become warranted, then even foreign media organizations that do not engage in propaganda activities on par with RT also might be required to run disclaimers indicating that the channel, video, or news item comes from a source supported by a given foreign government.

The abovementioned recommendations for regulation cannot fully prevent foreign-sponsored content from appearing on the internet or influencing American voters during election and non-election periods. "Information wants to be free", as the old adage goes, and content from international sources will continue to make its way onto American screens regardless of security efforts. Nonetheless, disclaimer regulations can serve the crucial purpose of un-packaging RT from the seemingly innocuous brand name it has adopted. Foreign instruments of state propaganda will continue to seek to influence the American electorate. Therefore, foreign agents should always be identified as what they are and where they come from. Whether the transmitted propaganda will ultimately persuade the American voter presents a challenge to democratic theory and decision-making—one that law in a free society may be incapable of preventing comprehensively and effectively.

CHAPTER FIVE

Combatting State-Sponsored Disinformation Campaigns from State-aligned Actors

By Alex Stamos, Sergey Sanovich, Andrew Grotto, and Allison Berke

The Problem

As documented in great detail in the Special Counsel report, the publication of stolen documents, purposively provocative and divisive misinformation, and disinformation dissemination through social media platforms by Russian government agents and their proxies constituted one of the most impactful methods of Russian government interference in the 2016 U.S. presidential election. Social media companies were unaware of the scale and scope of the malicious activities happening on their platforms as they occurred, and downplayed the potential impact for too long. Eventually, after significant pressure and criticism from lawmakers and the press, the companies began to take action. The U.S. government, and the FBI in particular, also did not communicate in a timely manner with social media companies about information they were collecting on Russian disinformation operations. Cooperation between the public and private sector on disinformation was almost non-existent before the 2016 U.S. presidential election, a situation that has improved only slightly since.

Several social media companies have taken measures to reduce the influence of foreign-government content producers on their platforms. Google, Facebook, and Twitter have created teams to find and shut down organized disinformation actors, although these shutdowns have not always been publicly disclosed. One known operation against Russian groups occurred in April 2018 when Facebook's team removed 70 Facebook accounts, 65 Instagram accounts, and 138 Facebook pages controlled by the IRA.[1] Additional takedowns of a variety of actors, including accounts operating from Iran, Pakistan, and India, have followed.[2]

As highlighted in Chapter Three, the most tangible progress in preventing online disinformation to date has been restrictions on the use of paid advertisements to spread disinformation on social media platforms. For instance, in the summer of 2018, Facebook, Twitter, and Google implemented new requirements for political ads, including ads on "social issues", to be labeled with "Paid for by" disclaimers. In the United States, these ads can only be run by verified residents of the U.S. and are stored in public archives along with particular targeting and reach data. Anecdotal evidence suggests that this approach may deter certain known players

in information warfare. For example, In the NOW, a video-focused RT outlet with over 3 million Facebook followers, attempted to run an advertisement on the site in early June 2018 for its story on poverty in America, but the advertisement was removed due to its lack of a "Paid for by" label. Deciding not to disclose the source of its funding, In the NOW chose to not run further ads before being banned outright in February 2019.

The ban and its subsequent reinstatement also illustrate the inconsistent implementation of labeling across platforms. While In the NOW videos on YouTube were being labeled as "funded in whole or in part by the Russian government," the same videos on Facebook were not. After a CNN report, the page was banned by Facebook, then required to reveal its source of funding under a new policy, then reinstated. The entire process was closely covered by both Russian and American media, which ultimately raised the page's profile and popularity while rendering Facebook vulnerable to censorship charges.[3]

To successfully combat state-sponsored disinformation campaigns, further efforts must be undertaken. In part, the solution requires implementing previously adopted solutions in a more comprehensive and coordinated manner, particularly with regards to paid content and advertising on social media.

A second line of work must focus on improving tools and strengthening policies to support efforts to identify and neutralize existing and emerging types of organic content used for disinformation purposes, as well as hacked or leaked documents. In addition to the recommendations provided in Chapter Three regarding the regulation of paid advertisements from foreign-government content producers, additional measures should be taken to reduce the impact of disinformation and stolen material spread from foreign government-aligned actors seeking to influence American voters. Most of these actions could be taken by private companies and need not be mandated through government regulation or new laws.

Moreover, legal and cultural changes need to be made to enhance cooperation between social media companies and between the private sector and the government to thwart disinformation campaigns. Tackling this issue involves addressing the larger question of data privacy. After a series of privacy scandals over the last several years, consumers justifiably want greater accountability from the companies that hold their private data, especially when this data might be used to influence their voting preferences. The U.S. Congress has started to debate the contours of a new federal consumer privacy law, prodded in part by California's consumer privacy law passed in 2018.[4] Tradeoffs between privacy and safety will frame this debate, which should include discussions of which parties are responsible for certain areas of election protection and what data are necessary for them to fulfill those responsibilities.

Social media companies will be far more effective against disinformation campaigns if they can coordinate and cooperate, and if they can partner with other large journalistic outlets to agree on norms around spreading and citing manipulated or stolen content. To do so, however, requires that information sharing about these threats be lawful. For example, it is debatable how

information posted publicly but subsequently taken down by a platform should be handled under the Electronic Communications Privacy Act (ECPA).

Exceptions to privacy requirements should be just that—exceptional. On the other hand, if the U.S. Congress wants to incentivize private companies to take more action against disinformation, it may have to pass new legislation to lower or eliminate those legal barriers now in place for doing so.

Recommendations

5.1. Create standardized guidelines for labeling content affiliated with disinformation campaign producers.

Social media companies and other online platforms need to develop and publicize industry-wide guidelines for labeling content from producers engaged in disinformation and information warfare. They also need to maintain a database of entities, which are actively employed in delivering disinformation. While the link between RT and In the NOW was never concealed, it is likely that under increasing pressure, future producers of disinformation will become progressively adept and creative in hiding their true identities.

A good initial step would be unified standards and language around government-aligned or government-sponsored media. Care would have to be taken to avoid false equivalence between outlets, which are editorially independent from governments but receive funding from them, such as the BBC and PBS, and outlets more closely aligned with their governments' policies, such as RT and the Xinhua News Agency. An appropriate labeling regime that applies to individual pieces of content would inform users of the source of information without unduly harming legitimate journalistic outlets with government ties.

5.2. Create norms for the media's handling of stolen information.

A significant component of the GRU's portion of the Russian campaign was the manipulation of the U.S. mass media, most notably well-respected print and television news outlets.[5] This manipulation occurred both in private via emails and private messages to reporters,[6] and in public via mass dumps of stolen information.

Previous industry-wide norms of ethics and conduct have been established for media and news organizations to avoid publishing material that is truthful but that could result in violence, gratuitous emotional harm, and other disproportionate harms. For instance, most media outlets currently do not publish photos of military casualties, the names of crime victims whose next of kin have not been notified, detailed descriptions of suicide methodologies, or the names of mass shooting suspects who were motivated by notoriety.[7] To date, journalists and media executives have taken the initiative to define, coordinate, and enforce these norms.

These same actors, not the government or lawmakers, should take the initiative regarding this new frontier of ethical behavior and endorse new norms around hacked documents and other content that has been leaked for political purposes. This norm should hold in particular when

journalists believe that intelligence services or organized groups are behind strategic leaks. To be sure, leaked information is a key component of journalism that brings accountability to powerful actors. But norms around the amount of coverage given to strategic leaks, the fact-checking that goes into stories, and the context in which leaks are reported—including the source of the leak—can reduce the chance that responsible media outlets will be used by autocrats to undermine democracy.

Because journalistic reporting and social media platforms are amplification tools for disinformation and for leaked documents, the absence of their cooperation will pose a serious challenge to malicious actors in reaching a broad audience with their preferred narrative. Furthermore, the precedent of previous norms intended to protect victims or potential victims can be easily used to lend credibility to the need to protect hacking victims and subjects of manipulated content like deepfakes. Although the relationship between the American major media and multinational social media organizations is often strained, synchronizing responses to U.S. adversaries should be possible and could be determinative of whether a future attempt along the lines of DCLeaks is effective.

5.3. Limit the targeting capabilities for political advertising.

Social analytics and advertising tools serve as a "finely tuned disinformation machine for the precision propagandist."[8] Of all of the opportunities for message amplification provided by the major social media products, advertising poses the greatest risks. First, it allows for amplification limited only by the budget of the attacker. Second, it allows an information warfare actor to put content in front of citizens who did not ask to see it. Most importantly, online advertising platforms allow adversaries to target individuals and groups that are most vulnerable to their specific message. Such targeting played a key role in the IRA's audience building campaign.

While there are equivalent capabilities for individualized targeting with more traditional campaign techniques, such as direct mail, the combination of low per-unit cost and the ease of targeting online creates a need for online political ads to be monitored more aggressively. The social media companies have already created voluntary standards for defining political advertisements; they can and should voluntarily choose to limit targeting capabilities for those ads as well. The current standards have been created by a handful of large companies; existing self-regulatory groups such as the Internet Advertising Bureau[9] should be utilized to establish standards that apply to the thousands of companies involved in the internet advertising ecosystem. With or without external interference, it is important for the health of American democracy that malicious actors be limited in their ability to target very narrowly defined subgroups of Americans with advertising specifically designed to appeal to a unique concern or base instinct.[10]

5.4. Expand transparency for paid and unpaid political content.

Several large online advertisers already have created online archives for political advertisements. These archives can be improved in several ways, such as by updating the archives in near-real time and providing detailed engagement metrics.[11] This information needs to be available through an open application programming interface (API).

Social media companies also should create content archives and disclose audience information for known disinformation actors and hacked documents. Preferably, social media platforms could provide access to this information and other data through an API meeting basic standards of thoroughness, transparency, and timeliness.[12] Facebook already provides much of the relevant information via its commercial social media data offering, CrowdTangle.[13] Unfortunately, the usefulness of this platform is undermined by the immediate removal of violating content. This approach could help not only to guide fact-checkers and other counter-disinformation efforts, but also to identify the trends and, more importantly, the goals and targets of disinformation.

Existing transparency measures have been voluntary, and only a handful of companies are providing any transparency into online political ads. The U.S. Congress needs to act to set compulsory standards for online ad archives and to create a privacy safe harbor for tech platforms to share content from disinformation actors with responsible researchers.

5.5. Improve the quality and scope of detection tools and reporting policies for social media platforms.

Social media companies should also develop additional tools and formats to identify disinformation and hacked content more rapidly and remove it with higher precision, removing content before harm is done. To achieve this objective, they should draw on existing academic research in the area[14] and make the tools they develop open for verification and oversight.[15] Social media and content platforms also need to strengthen their investment in developing technology to detect new and different ways in which entities are disseminating disinformation, such as peer-to-peer messaging apps, or using machine learning-written text and inauthentic pictures, audio, and video, including deepfakes. Hosting providers with significant traffic or business operations in the United States can be incentivized to remove disinformation and hacked documents upon coordination with law enforcement and victims, similar to measures that are taken to remove explicit sexual content or copyright-infringing content. Establishing regular searches for, and removal of, this content will disrupt channels that hackers use to disseminate leaked documents, and will provide the perception that this content, in the few places where it can be found, is untrustworthy or potentially discrediting to host or possess. It is therefore critical to enforce industry-wide norms or legislation with regard to this issue.

As we have witnessed already, when social media platforms institute policies that could result in the removal of user content, they must be mindful of the high costs of false positives, i.e., unjustified removals. This error matters not only with regards to freedom of expression from the individual user's point of view, but also as a factor of legitimacy for the justified removals. Platforms, therefore, cannot rely on artificial intelligence (AI) alone, but must employ competent moderators—who are familiar with the local environment and know the language they are working with—as well as establish efficient appeal procedures. Instead of making these decisions inside a black box, social media platforms should provide transparency for the reasoning behind these decisions, perhaps assisted by third-party councils. This openness and clarity will help both personal and institutional users navigate relevant rules and build trust in the platform's decision-making.[16]

To both increase public awareness of disinformation threats and improve the accountability of social media platforms, platforms must develop policies for disclosing their ongoing disinformation campaigns, as well as producing regular "community health reports", including statistics on the percentage of anonymous, inauthentic, and automated accounts active in the system, and engagement metrics for the categories of accounts relative to authenticated human activity and labeled bots.[17]

5.6. Build an industry-wide coalition to coordinate and encourage the spread of best practices.

As major social media platforms become more serious about policing their platforms, disinformation may move to smaller, less prepared, and more niche platforms. Major tech companies therefore must make tools and best practices on fighting disinformation available to these less equipped companies. Moreover, the implementation of these best practices should be tied to the ability to access other important industry-wide resources such as those used to identify copyright infringement or other forms of harmful content.

There have been several successful examples of this kind of coordination. The first is the model known as the Information Sharing and Analysis Center/Organization (ISAC/ISAO).[18] These are industry-wide, non-profit organizations that provide various levels of services to their members, ranging from facilitating discussions and lightweight information sharing to operating completely independent and well-staffed intelligence functions. While the Multi-State ISAC has been an important component of securing election systems, there is no designated ISAC or ISAO for the consumer internet companies and no natural home for coordination on measures meant to prevent online disinformation.

The major companies, namely Google, Facebook, and Twitter, have a responsibility to create such an organization and to utilize it to encourage sharing among themselves, with smaller competitors to help build their capacity, and with government agencies when appropriate under the law.

5.7. Remove barriers to the sharing of information relating to disinformation, including changes to privacy and other laws as necessary.

Signed by President Obama in December 2015, the Cybersecurity Information Sharing Act (CISA) of 2015 reduced legal barriers to sharing cybersecurity threat indicators among technology companies, and between the private sector and the U.S. government, by establishing a blanket exception for such sharing under American privacy and surveillance laws. Although CISA does not require or guarantee that private companies share the information, it eliminates numerous legal constraints as a barrier to action.

As social media platforms, civil society, and government work to address disinformation threats, they should consider whether similar exceptions are necessary in order to effectively counter these threats. When conducting information operations, adversaries routinely exploit multiple platforms to disseminate their malign content. Because action by one platform to address malign content does not guarantee that other platforms become aware of the threat, the content typically persists, which enables the adversary to adapt their strategies in order to better evade future detection.

At the moment, access to the content used by disinformation actors is generally restricted to analysts who archived the content before it was removed or governments with lawful request capabilities. Few organizations have been able to analyze the full paid and unpaid content created by Russian groups in 2016, and the analysis we have is limited to data from the handful of companies who investigated the use of their platforms and were able to legally provide such data to Congressional committees. Congress was able to provide that content and metadata to external researchers, an action that is otherwise proscribed by U.S. and European law.[19]

Congress needs to establish a legal framework within which the metadata of disinformation actors can be shared in real-time between social media platforms, and removed disinformation content can be shared with academic researchers under reasonable privacy protections.

5.8. Establish a Social Media ISAC/ISAO to improve communication between the U.S. government and social media companies about disinformation operations.

Before 2020, the U.S. intelligence community must implement plans to assist social media companies in thwarting disinformation and influence campaigns from foreign governments through rapid declassification of technical indicators and regular updates on potential threats. Social media companies must be willing to engage as well with the U.S. government. Tighter coordination between U.S. agencies and tech platforms might be facilitated by third-party oversight, which would enhance the credibility of these interactions.

The U.S. tech industry currently lacks a coordinating body to facilitate data sharing and provide a single interface to U.S. agencies working to protect our elections. These companies need to create such a body, following the model of effective coordination centers already

established by the finance and power industries.[20] A new organization representing all social media companies could then act as an intermediary between the tech industry and the intelligence community for discussion of these national security issues.

5.9. Increase overall transparency on social media platforms.

More generally, social media platforms need to provide more transparency for their users in cases when content was produced or promoted using automation or AI tools. Existing user interface features and platforms' content delivery algorithms need to be utilized as much as possible to provide contextualization for questionable information and help users escape echo chambers. In addition, social media platforms should provide more transparency around users who are paid to promote certain content.

One area ripe for innovation is the automatic labeling of synthetic content, such as videos created by a variety of techniques that are often lumped under the term "deepfakes". While there are legitimate uses of synthetic media technologies, there is no legitimate need to mislead social media users about the authenticity of that media. Automatically labeling content, which shows technical signs of being modified in this manner, is the minimum level of due diligence required of the major video hosting sites.

Bots that attack other users (trolling bots) and hijack coordination tools to render them ineffective (dumping bots) have received the most attention thus far. But bots that amplify certain messages and cheerlead certain users must be carefully analyzed as well for having a serious negative impact on our elections.[21] In particular, social media platforms need to prevent bots from "following", "liking", "sharing", and "retweeting" to ensure that only organic human activity is reflected in various measures of popularity, authority, and influence on social media.

5.10. Carefully balance platform responsibility with individual freedoms.

The U.S. Congress also should consider new guidelines on the obligations of major social media platforms to their users regarding freedom of expression. Because demotion, shadow bans, and outright bans of certain kinds of content are already becoming the subject of litigation, continued efforts to resist disinformation campaigns are likely to provoke further legal disputes.

Several groups have proposed changes to the critical protections provided by Section 230 of the Communications Decency Act. The U.S. Congress needs to carefully balance the need to protect the freedom of speech and the integrity of social media platforms while also defending the country from disinformation campaigns. A good first step would be legislation encouraging transparency on how social media companies interpret their own guidelines, and standardized reports on content moderation statistics.

5.11. Establish a norm among candidates to not use stolen data or manipulated content.

Prodded by the Daily Beast in February 2019, candidates running for the Democratic Party nomination for the 2020 U.S. presidential election have pledged not to use data about other candidates obtained illegally.[22] This norm should be codified in a formal document drafted by the Democratic National Committee and then signed by all candidates. The Republican National Committee should do the same for its candidates in 2020, including President Trump.

5.12. Emphasize digital literacy in educational curricula and focus public education on the knowledge that makes democracy more resilient to disinformation campaigns.

Many of the most successful disinformation campaigns, including the one perpetrated by the Russian government against the United States in 2016, involved technically trivial, easily preventable hacking of private data. The amount of sensitive data that could be easily weaponized by a disinformation campaign will only increase and will be located far beyond the electoral campaign headquarters, including across various government and corporate entities that routinely store the personal data of millions of their patrons and clients. Building a robust defense against high-end attacks on the most critical platforms is essential, but raising awareness and developing skills among much larger groups of people who will manage people's data is also urgent. Equipping the general public with common sense digital safety skills will further increase the costs and reduce the agility of any attack.

The most powerful weapon against a disinformation campaign is a public that is curious about the sources of information, can assess their credibility,[23] and most importantly, is capable of thinking critically about the information received.[24] This means that narrowly defined digital and media literacy could serve only as the foundation for the educational programs that need to teach how to put information in context and perspective. To effectively confront disinformation campaigns perpetrated by autocracies against democracies, a teaching curriculum needs to build on serious theoretical and empirical work that uncovers the role of information in both modern autocracies[25] and democracies.[26] Emerging research in this area points to emphasizing the difference between the political and policy outcomes of the democratic process (which are legitimate goals in electoral competition) and the universal right of people and coalitions of people to participate in it (which is supposedly sacred but might require additional training to be perceived as such).[27]

To this end, the U.S. Congress should mandate the Department of Education to convene a task force on making existing[28] and new information security and media literacy curricula available to educational programs at all levels, from the primary education to lifelong learning, including tailored versions for keepers of personal data in the commercial sector, government employees, PR professionals, and other critical groups, as well as teachers who will teach these skills. The

task force should provide its recommendations following an open and transparent process of public consultation, meeting with educators at all levels and engaging different communities at the state and local level by offering opportunities to run pilot programs, whose results would undergo rigorous evaluation. To ensure that the best-performing curriculum is selected at the national level and students' progress is monitored, media literacy would need to become a part of national standardized testing as well as comparative studies such as PISA.[29]

Because empirical research suggests that older Americans are particularly vulnerable to fake news on social media,[30] public education in this area cannot exclusively focus on the younger generation currently in school or college. The task force would need to assess existing research in this area and develop, in collaboration with academic and civil society stakeholders, learning tools suitable for older audiences who are already in the workforce or in retirement.

CHAPTER SIX

Enhancing Transparency about Foreign Involvement in U.S. Elections

By Michael McFaul, Andrew Grotto, and Alex Stamos

The Problem

Our Founding Founders worried a lot about possible foreign meddling in the domestic affairs of the new United States of America. In particular, they were concerned that powerful European actors would use their wealth to corrupt elected officials in the new American democracy.[1] The Federalist papers are filled with expressions of concern about foreigners exercising influence over the conduct of American politics. More specifically, the Emoluments Clause was included in Article I of the Constitution precisely to reduce foreign influence over elected officials, declaring "no Person holding any Office of Profit or Trust under them, shall, without the Consent of the Congress, accept of any present, Emolument, Office, or Title, of any kind whatever, from any King, Prince, or foreign State."

Over time, concern about foreign influence in American politics and elections has varied, sometimes with negative results for democratic practices. The Alien and Sedition Acts were signed into law by President John Adams in 1798 in the context of undeclared armed hostilities with France, ostensibly to protect against French interference, but were used by the government to suppress political dissidents until the relevant portions of the law expired in 1800. In the run up to World War II, Congress passed the Foreign Agents Registration Act in 1938 in response to growing Nazi influence in the United States, a law that has served to enhance transparency regarding foreign lobbying efforts, but also, some believe, invoked to criminalize legitimate interactions between foreigners and Americans.[2] And most certainly, fears of foreigners meddling in American politics spun tragically out of control during World War II when Americans of Japanese descent were rounded up and forcible removed to internment camps or when Senator McCarthy launched his crusade against alleged American communists. In seeking greater transparency about foreign influence in our elections, we obviously must avoid repeating these tragic chapters in American history.

The involvement of foreigners—Russian government agents in particular—in the 2016 U.S. presidential election did expand substantially compared to recent other presidential elections.

The Mueller Report documented in detail a vast range of contacts between Russian officials, Russian business people, and Russian non-governmental leaders with American officials involved directly or indirectly in the Trump campaign. Most strikingly, Russian government officials and their proxies aggressively pursued contacts with as many Trump campaign officials as they could make, oftentimes with successful results. As discussed in Chapter One, some of these meetings involved direct offers of assistance to the Trump campaign, offers that would have worried our Founding Fathers. According to one careful count, "Donald J. Trump and 18 of his associates had at least 140 contacts with Russian nationals and WikiLeaks, or their intermediaries, during the 2016 campaign and presidential transition…."[3] Notably, the Kremlin and WikiLeaks–also a foreign non-governmental organization–showed no interest in pursuing meetings with the Clinton campaign.

Another kind of foreign involvement in the 2016 U.S. presidential election involved prospective business deals with American candidates, including Donald Trump in particular. As illustrated in Chapter One, during the 2016 presidential campaign, Trump and his colleagues actively pursued a major business deal in Russia—the construction of a Trump Tower in Moscow—and deliberately hid these negotiations first from voters and later from investigators on the Special Counsel team at the U.S. Department of Justice. The full extent of other business ventures with foreigner partners by either the Trump or Clinton campaigns—or any campaign in recent memory, for that matter—has not been disclosed.

In addition to in-person meetings, several foreign companies and consultants were paid to participate in the 2016 U.S. presidential elections. The Trump campaign hired a British firm, Cambridge Analytica, to work directly for their organization. Other Republicans candidates hired the British firm, Orbis Business Intelligence, to collect compromising materials on Trump relationships with Russian individuals and organizations. When these Republicans dropped out of the race, the Clinton campaign contracted with the American company Fusion GPS to collect opposition research on Trump, and Fusion GPS in turn hired again Orbis Business Intelligence to continue its research on Trump, a contract that eventually produced the "Steele Dossier".[4] As documented in the Special Counsel report, people close to the Trump campaign also interacted directly with another foreign organization, WikiLeaks, allegedly to coordinate the dissemination of compromising materials on candidate Clinton and her campaign.

Foreigners also made illicit donations to the Trump inauguration committee. For example, political consultant W. Samuel Patten plead guilty in 2018 to steering $50,000 from a Ukrainian politician to the inaugural committee.[5] In addition, it was reported that weeks after being placed on notice by watchdog groups, the Trump campaign had continued to solicit illegal donations from foreign individuals—including members of foreign governments at their official email addresses.[6]

Many of these contacts clearly stretch the boundaries of propriety, and several of them were considered illegal, but to date, no American has been charged with conspiracy regarding

foreign contacts during the 2016 U.S. presidential campaign. In fact, most of these contacts were legal—but should they be? Our answer is no. But even if not legally criminalized, the American voters have a right to know about presidential candidates' business and political activities with foreign individuals and companies before they go the polls on Election Day. Consequently, greater transparency is needed to ensure that voters will be able to make informed decisions for themselves about the appropriateness of these contacts and business deals with foreigners.

Recommendations

6.1. Mandate transparency in the use of foreign consultants and foreign companies in U.S. political campaigns.

Foreign consultants and companies seeking to provide advice or assistance to candidates should be required to register with the Federal Election Commission, with criminal and civil penalties for failing to register. In addition, candidates should be required to disclose their use of foreign consultants and foreign companies in political campaigns. The U.S. Congress should mandate these requirements in legislation.

6.2. Increase transparency about foreign business interests.

Candidates should not be forced to divest from all investments abroad or business deals with foreigners and their companies. Instead, candidates should make public their business interests abroad and then let the voters decide whether there are conflict of interests. The easiest way to make such information available to the voters would be for candidates to publish their tax returns. The U.S. Congress should mandate this practice in legislation.

6.3. Disclose contacts with foreign nationals and governments.

Beginning in 2020, all non-incumbent presidential candidates should pledge to document all meetings and other substantive interactions with foreign nationals, especially foreign governments, and to make public this information. To incentivize transparency, the U.S. Congress should establish information handling guidelines, including a tailored exemption for this information under the Freedom of Information Act. Many government agencies already require such disclosures, and the same practice should apply for campaigns. The significance of requiring candidates and their campaign officials to report contacts with foreign nationals attempting to coordinate, make campaign donations, or offer information and services is echoed in the Foreign Influence Reporting in Elections (FIRE) Act—recently introduced by Senator Mark Warner—although the requirements of the FIRE Act go beyond the recommendations in this report.

Moreover, some basic norms about engagement with foreigners should also be embraced proactively by all presidential candidates and their campaigns. For example, all candidates should avoid contact with foreigners to obtain compromising material on their opponents. In addition, they should not encourage foreign governments to steal property from their opponents and then promote the widespread dissemination of that illicit material.

6.4. Strengthen the norm of one government at a time.

Prior to Election Day, the president-elect and the incoming executive branch team should pledge to abstain from meeting with foreign government officials during their transition period, unless such a meeting has been approved and preferably attended by outgoing administration officials. This commitment would demonstrate high levels of transparency and accountability during a critical time of the electoral process, and would allow for appropriate transition planning while demonstrating that only one administration represents the United States at a time.

CHAPTER SEVEN

Establishing International Norms and Agreements to Prevent Election Interference

By Eileen Donahoe, Toomas Ilves, Chris Painter, Sergey Sanovich, Larry Diamond, Andrew Grotto, and Megan Metzger

The Problem

The United States is not the only country in the world to experience malicious, foreign interference during an election. Cyber interference in electoral processes and digital disinformation operations surrounding elections are an international phenomenon.[1] American policymakers rightly are focused on threats to election integrity in the United States in the run-up to the 2020 presidential vote, but these threats are part of a much larger, ongoing challenge to democracies everywhere. Because the problem is global, the American response must be both domestic *and* international. American government officials as well as the American private sector must recognize and underscore the global dimension of the threat and assume a leadership role in developing defenses against efforts to erode confidence in democracy. Reinforcement of international democratic governance norms in the digital context is vital. International law and other multilateral commitments already provide a substantial normative basis for action.[2]

One of the most important international norms of the post-World War II era is the right of the people of every country to freely choose their own government and determine their own future, enshrined in Article 21, Section 3 of the Universal Declaration of Human Rights (UDHR),[3] as well as in Articles 1 and 25 of the International Covenant on Civil and Political Rights (ICCPR).[4] Following these multilateral treaties, democratic norms and principles have subsequently been further codified in numerous regional and international agreements and declarations, including those of the Organization of American States (OAS), the Organization for Security and Co-operation in Europe (OSCE), the European Union (EU), and the African Union (AU). Most recently, over 100 countries signed the Warsaw Declaration, a founding document of the Community of Democracies that defines global democratic norms and principles.

The world's democracies, including the United States, must reaffirm these principles and then translate and update them for the digital age. A range of stakeholders have undertaken important work to rearticulate and further develop norms for the cyber context. The U.S. government must now provide leadership and engage more systematically in developing and asserting these principles in the cyber realm.

Previous efforts in updating international norms for the digital age include the Tallinn Manual[5] and Tallinn Manual 2.0,[6] both of which were early efforts to support the application of existing international law to new cyber challenges, particularly relating to warfare. The Freedom Online Coalition was formed in 2011 and now includes 30 governments committed to reinforcing fundamental human rights principles in the digital realm.[7] In 2012, the United Nations Human Rights Council passed a consensus resolution affirming the applicability of fundamental human rights law in the digital space.[8] The United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) also took steps to identify and promote international norms in the cyber realm. In a 2013 report, the UN GGE critically asserted that existing international law should be applied to cyber space and in its 2015 report, it articulated a list of eleven voluntary norms of state behavior. Unfortunately, the UN GGE process broke down in 2017 and was unable to reach a consensus. Though both a new GGE and an "Open Ended Working Group" on cyber issues will be launched in the UN this year, prospects for further substantive progress are uncertain. However, none of these prior efforts have dealt explicitly with issues around election interference.

Following the 2016 U.S. presidential election, a surge of individuals and groups[9] have joined the process of identifying norms to protect the integrity of elections, including the important work of articulating the distinction between legitimate efforts to promote democracy and illegitimate interference in the democratic processes of other countries.[10] Some stakeholders have argued that previous democracy promotion efforts of the U.S. and EU in other countries leave Americans and Europeans in a poor position to criticize the disruptive attempts of non-democratic countries.[11] We strongly disagree. There are important, identifiable differences between democracy promotion and unacceptable election interference. Democracy promotion is about ensuring that elections and other democratic processes reflect the will of the people; interference involves distorting the connection between the will of the people and representative government. Compelling analysis detailing these distinctions is beginning to emerge.[12]

This report has articulated dozens of concrete policy recommendations for enhancing the integrity and independence of the American electoral process in the run-up to the 2020 presidential vote. We believe that utilizing international norms more effectively can contribute both to the domestic American mission of protecting elections, while simultaneously building an international coalition dedicated to elections free of outside interference around the world.

Recommendations

7.1. Fortify U.S. and international commitment to human rights.

U.S. policymakers should begin by emphasizing the importance of existing international human rights law and norms. As noted in the UDHR and the ICCPR, as well as in numerous regional covenants and the Warsaw Declaration, these ratified agreements forbid states, groups, or persons from using any means to interfere with or subvert the ability of the people of a country

to choose their representatives and government through open and fair elections that are "free of fraud and intimidation."[13] Moreover, the President of the United States and senior leaders from both dominant political parties should forcefully denounce any attempt to subvert the sovereign right of the people to elect their representatives, through digital or any other means.

7.2. Strengthen international norms protecting election infrastructures.

The Group of Twenty (G20) and the UN GGE have both endorsed the U.S.-sponsored norm that "state[s] should not conduct or knowingly support ICT activity… that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public."[14] In 2016, the Secretary of Homeland Security formally designated electoral infrastructure as critical infrastructure.

The President of the United States and senior leaders from both dominant political parties should now emphasize the importance of existing norms on protecting critical infrastructure, which can be extended and reinforced in a digital context in several ways. As a starting point, all democracies should be encouraged to similarly acknowledge the obvious: that their election infrastructure, including the digital machinery of voter registration, vote casting, and other aspects of electoral administration, is critical infrastructure in accordance with their national critical infrastructure frameworks.

Furthermore, in line with the Transatlantic Commission on Election Integrity's pledge and the Global Commission on the Stability of Cyber Space's proposed norm protecting election systems, political leaders should assert that any effort to hack or otherwise infringe upon a country's electoral administrative and technical infrastructure—or any of its subnational electoral administrative jurisdictions—is illegitimate. This assertion would include any illicit effort to enter, view, or modify digital systems for voter registration, vote casting, or other aspects of electoral administration.

7.3. Create norms to deter the use of disinformation and hacked materials.

By definition, democracies already value and uphold strong norms against using violence and fraud to sway voters. As a form of fraud, disinformation campaigns thus violate fundamental democratic norms by producing, using, or spreading data and materials that were stolen, falsified, fabricated, illegally accessed, or doxed. Similarly, any effort to generate or knowingly distribute false information for the purposes of influencing an election should not be tolerated.

Consequently, political parties and candidates for office in democracies around the world should forge compacts agreeing to adhere to new norms about the production, use, or dissemination of such materials. For example, the Transatlantic Commission on Election Integrity has crafted a pledge and launched a process to seek widespread political recognition and support for such norms.[15] As discussed earlier in this report, both the Democratic and Republican parties, as well as their candidates and campaigns, should lead by example and pledge to strictly uphold these norms. Political parties in democracies around the world should similarly make a public commitment.

7.4. Lead international advocacy against foreign interference through disinformation.

The United States should lead international advocacy in support of a norm against any organized fraudulent effort by a foreign entity—including by disguising the true source and nature of the intervention—to engage in, shape, stimulate, or inflame social media discourse for the purpose of distorting public opinion or political discourse, in particular during an election period.

7.5. Distinguish legitimate cross-border assistance from illicit or unlawful interventions.

The distinction between legitimate forms of cross-border assistance to strengthen democratic electoral processes, including all aspects of electoral administration and the political environment for campaigning and voting, and illegitimate cross-border interventions to distort and subvert democratic electoral processes, must be clarified in the digital context and defended by democratic institutions. The UDHR recognizes that "the will of the people", as "expressed in periodic and genuine elections...with free voting procedures …shall be the basis of the authority of government."[16] Because states have an obligation to respect the sovereignty of other countries and sovereignty resides in the people of the country, free and open elections are an indispensable means for determining "the will of the people." Democratic states have not only a right, but also an obligation to assist other peoples to express their will through free and fair elections.

The U.S. State Department, in parallel with similar institutions providing democratic assistance, should clearly articulate the following principles that differentiate legitimate from illegitimate engagement in this realm:

Democratic Intent: Any cross-border engagement with the electoral processes of another country should be done for the purpose of supporting the right to self-determination of the people of that country and to strengthen the integrity of electoral processes, so that universally accepted norms, as stipulated by the UDHR and by regional intergovernmental organizations, such as the OSCE, AU, and OAS, can be better realized.

Transparency: Cross-border engagement with the electoral processes of another country should be openly reported, with the exception of rare instances in which the personal safety of democratic actors is at risk. Furthermore, any involvement by a foreign government or non-state actor should be clearly disclosed by that entity. Engagement should be defined as any action that could affect the opinions or actions of citizens in favor of, or in opposition to, any candidate or party; the decision to participate or abstain from electoral participation; or the belief or confidence in elements of democratic governance.

Commitment to Trustworthy Information and Honest-Minded Discourse: State and non-state actors should refrain from propagating false or misleading information or producing fraudulent, inauthentic social media activity for the purpose of distorting or polarizing public opinion or

online political discourse, particularly during an election period. At the same time, state and non-state actors should strengthen the capacity of democratic media, parties, institutions, and organizations to detect, expose, and counter existing disinformation and manipulation of social media.

7.6. Hold congressional hearings about policies to support free and fair elections internationally.

The U.S. Congress should hold a series of hearings on U.S. government policies and programs to support free and fair elections internationally. Hearings would bring transparency to U.S. government efforts to promote democracy and help sharpen distinctions between appropriate and illegitimate behavior. Greater understanding of best practices to support free and fair elections internationally, including a discussion of efforts of other democracies beside the United States, could help to broaden more public support for these activities.

7.7. Promote cooperation among democracies focused on election protection.

Democratic countries should forge an international coalition to develop, support, and enforce universal norms of appropriate state behavior relating to non-interference in elections, as well as appropriate responses to illegitimate interference in elections. The coalition should establish one or more multilateral centers for sharing diagnostic information and intelligence, developing rapid situational analysis, and distributing this analysis in real time. The centers could be organized either as virtual organizations or brick and mortar institutions. Through the development of multilateral centers, democratic governments can strengthen both bilateral and multilateral forms of cooperation to identify and respond to digital threats to electoral integrity. They should also develop digital literacy initiatives for citizens and share effective strategies for building public resilience against disinformation. Moreover, government leaders from democratic states should meet at an annual summit to review disinformation trends and identify avenues for deepening existing methods of collaboration.

International cooperation is an essential element of the U.S. strategy to combat disinformation and establish new norms preventing electoral interference, as well as to reinforce the validity of previously articulated principles. States that respect the rule of law must cooperate[17] and collaborate[18] in addressing these issues.

7.8. Appoint a senior U.S. government representative on election interference.

The U.S. State Department should designate a senior-level official (ambassador-rank) to serve as the U.S. government lead for building coalitions with other countries to combat election interference and for developing and promoting overall norms on this topic. This official should work in coordination with American law enforcement, intelligence and other agencies to ensure adequate information sharing with foreign counterparts about disinformation campaigns and other malign interference with democratic processes. This official could be an existing official

with a compatible portfolio, such as the official charged with carrying out cyber policy, assuming that he or she is at least of ambassador rank.

7.9. Develop guidelines about platform cooperation with foreign governments.

The U.S. Department of Justice should prepare a legal opinion on the appropriate responses of digital and social media platforms if they are pressured by foreign governments to facilitate censorship, disseminate disinformation, or violate users' privacy. In addition, the U.S. Department of Justice should work with technology and human rights experts to establish community norms and guidelines for the acceptable level of cooperation between major social media platforms and foreign governments that engage in disinformation campaigns. The U.S. State Department should seek to synchronize such guidelines with the EU, other democratic countries, and relevant international bodies, and subsequently advocate for global recognition and enforcement of these guidelines to support platform integrity and to protect users' rights under international law.

Deterring Foreign Governments from Election Interference

By Herbert Lin, Chris Painter, and Andrew Grotto

The Problem

In deciding to interfere in the 2016 U.S. presidential election, Russian President Vladimir Putin calculated that the potential rewards were greater than potential costs. Given continued Russian interference, it is clear that American efforts to date have not changed his calculus. The U.S. government must impose timely, tailored, consistent and credible costs on Russia for aggression that both adequately penalize past conduct and serve as a deterrent for future interference. In so doing, the United States will help to deter other foreign governments from undertaking similar cyber actions both during the 2020 presidential election and more broadly.

The United States has taken some actions in response to Russian interference. For example, both the Obama and Trump administrations have imposed economic sanctions on Russian individuals and companies.[1] Secretary of State Mike Pompeo has asserted that the Trump administration has warned the Russian government about the negative consequences of future meddling, but the content of those threats has never been specified—making them impossible to assess—and their credibility is consistently undercut by contradictory messaging from the President.[2] There is news reporting about Cyber Command operations against Russian infrastructure, which we applaud in principle because they disrupt malicious activity and impose fleeting costs on Russia.[3] However, they are no substitute for a comprehensive, sustained campaign aimed at deterring interference from the Russian government or other foreign actors.

The lack of consistent and forceful U.S. action has had the opposite effect of deterrence, serving instead as a signal to Russia and other potential attackers that this is a relatively cost-free enterprise and encouraging more, not less, malicious activity.[4] The United States must do far more. Specifically, a deterrence strategy must be developed and executed to prevent foreign adversaries from intervening in American elections. To be effective and ultimately successful, a deterrence strategy must convince an adversary that the costs of taking a specific action will outweigh the benefits in a way that persuades that adversary to choose not to take that specific action.[5] Because deterrence concerns not only the objective facts of intentions, capabilities, and potential responses, but also the subjective perceptions of these facts by adversaries, the

consistency, credibility, and clarity of communication about one's intentions, capabilities, and potential responses are crucial. U.S. leaders must signal clearly the expected consequences in response to election interference and then commit credibly to taking that course of action before meddling occurs.

However, American leaders have thus far not signaled consistently, credibly, nor clearly about American intentions, capabilities, or potential responses to election interference. Most damagingly, President Trump has not even acknowledged the previous Russian attack, let alone denounce it, or outline clearly how he intends to deter future interventions. A recent report indicates that the President's Chief of Staff explicitly told Kirstjen Nielsen in the months before her resignation as Secretary of Homeland Security to refrain from discussing with the President preparations for new and different forms of interference by Russia in the 2020 election.[6]

Much of the theoretical discussion on deterrence originated during the Cold War, as researchers and policymakers sought to understand mechanisms for deterring adversaries from launching a nuclear attack. Bernard Brodie, Thomas Schelling, and Herman Kahn were among the most prominent theorists who articulated theories that rational adversaries can be deterred if they assess that the costs of a course of action exceed the benefits.[7] A critical element of these theories is that the adversary must believe in the credibility of claims about those costs. These ideas underpinned Cold War nuclear doctrine and remain more-or-less implicit in much of American nuclear posture up to the present, despite some valid criticism of their strength and legitimacy in light of newer findings about decision-making in cognitive psychology.[8] Deterrence theory also shapes Russian nuclear doctrine considerably. However, less well understood is the extent to which a variety of direct actions short of war—be they clandestine, covert, cyber, cyber-enabled, psychological, or propaganda—taken by one nuclear power against another might be effectively deterred.

The United States has acknowledged the necessity of deterrence in cyberspace and taken several related actions. In the 2011 International Strategy for Cyberspace, the United States stated that it would use the full range of tools, including diplomatic, economic (including sanctions), law enforcement, cyber, and even kinetic military actions to respond to appropriate cyberattacks.[9] President Obama signed an executive order authorizing the use of economic sanctions against actors assessed to have participated in malicious cyber actions against critical infrastructure and other targets, while the U.S. Congress and the Trump administration have issued sanctions regimes to deal with election interference. The U.S. State Department's May 2018 "Recommendations to the President on Deterring Adversaries and Better Protecting the American People From Cyber Threats" call for a new policy "for when the United States will impose consequences", a menu of "swift, costly, and transparent" consequences, and better policy planning and international partnerships to impose these consequences.[10] If effectively implemented, these steps could be successful and further strengthened by consistent, high-level messaging regarding the explicit threat of cost imposition asymmetrically and across domains. To succeed, however, these threats must be credible.

As noted earlier, U.S. Cyber Command reportedly conducted operations aimed at knocking the Internet Research Agency (IRA) offline on the day of the 2018 midterm elections, though the U.S. government has not publicly acknowledged this action. [11] Although this particular operation, if accurately reported as being focused on disrupting operations during Election Day, was a good start, it nevertheless was too little and too late. As discussed in other chapters, the IRA engages in medium- to long-term propaganda efforts that weaponize social media to undermine public trust in Western institutions, amplify societal polarization, and destabilize perception vis-à-vis truth and factual evidence. If the IRA were operating in the 2018 U.S. midterm elections, as it did during the 2016 U.S. presidential elections, significant damage would have already been inflicted prior to Election Day.[12] Rather than conducting similarly limited operations, the United States needs to impose costs in a strategic way, acting together, when possible, with allies and partners.

Moreover, U.S. government activity in cyberspace often appears to be too quiet to deliver a deterrent message. There clearly is a place for concealed activity with regard to disruption–especially if such disruption is to sow confusion in the adversaries' ranks. But if the purpose is, even in part, deterrence, then the United States should be more willing to claim responsibility, even if it is after the fact. If the United States communicates either privately or publicly to the adversary that it is taking action, it demonstrates both a willingness and capability to act (helping to deter future conduct) and opens up potential channels of de-escalation through clear military, intelligence, and diplomatic communications channels.

Recommendations

8.1. Recalibrate risk tolerances for actions in cyberspace.

To be more successful in deterring adversary behavior, the United States must begin by increasing its willingness to accept greater risk of adversary retaliation, including retaliation in the cyber domain. Today, U.S. opponents are counting on American aversion to cyber risk in order to deter U.S. responses.[13] When risk-aversion dominates policymaking, the choice to take no action is privileged. What is necessary instead is a long-term strategy that frames the costs of inaction in terms of both the present and future malicious adversary behavior that inaction enables.

8.2. Signal a clear and credible commitment to respond to election interference.

From the top down, and including most importantly from the President, the U.S. government must demonstrate a clear, credible, and consistent commitment in response to future attempts at election interference.[14] U.S. leaders should detail specifically what costs will be imposed on attacking adversaries and, when election interference occurs, actually impose those costs. The worst of all outcomes is drawing red lines without delivering on them. Clear, credible, and consistent commitments to respond and follow-through are crucial to deterrence; in their absence, an adversary is more likely to gamble and believe that the United States is bluffing.

Among other conditions, mandatory response regimes, similar but not necessarily identical to the one contemplated in the DETER Act calling for mandatory sanctions to be imposed upon a determination by the Director of National Intelligence that a foreign power had interfered in a U.S. federal election, should be enacted and implemented.[15]

8.3. Maintain a visible position of U.S. capabilities, intentions, and responses.

Deterrent responses from the United States should not be entirely concealed from the adversary, but this requirement does not imply necessarily that the American response must be made public. Specifically, if the intent of a response to penalize meddling or deter future meddling, the adversary must understand that the United States is responding (or has responded) to meddling and that penalties will continue unless the adversary's behavior changes. It should also be signaled or communicated to the adversary that penalties will cease when its behavior changes. Clear signaling can be conveyed publicly or privately, during presidential summits, calls, and written communications or private meetings between diplomats or intelligence officers. Actions can also send signals, though care must be taken to ensure that the adversary actually gets the message. The mode of signaling should be calibrated to maximize impact while minimizing retaliatory and other risks—private signaling might allay the domestic political need for an adversary leader to respond to a perceived threat from the United States and serve as a means of de-escalation if needed. The U.S. State Department's proposed new policy on transparent deterrence responses should be fleshed out and released swiftly,[16] as should incorporate asymmetric and cross-domain responses recommended below.

8.4. Enact country-specific and timely responses that impose real, effective costs.

American policymakers should take appropriate deterrence responses, which are not only country-specific and timely, but also impose real costs on adversaries. Cost imposition need not be in the same domain—U.S. decisionmakers should consider responding in a domain unrelated to the one in which the original incident occurred. In addition to more traditional diplomatic sanctions, law enforcement, and cyber tools, response options can span the full range of dealings between the United States and the country at issue and could include anything from trade to immigration—as long as it places at risk something the adversary wants until their behavior changes.[17]

Examples of responsive actions that could be considered, subject to the caveats below, include more targeted economic sanctions on the adversary, restrictions on travel to the United States, or targeted economic sanctions on the adversary's agents and close friends.[18] Various kinds of covert action could also be considered, including targeted action against the financial holdings of the key individuals responsible for meddling. With respect to the Russian government, publication of true information about corruption or illicit financial dealings is another instrument of deterrence to maintain in the American arsenal.

U.S. decisionmakers must also keep in mind that a meaningful response from the United States is likely to provoke a counterreaction, and therefore insights of the intelligence community regarding such counterreactions should be sought and taken into account in determining the wisdom of taking such actions in the first place. In other words, concerns about the scope and nature of a likely counterreaction should not deter the United States from responding (see recommendation 1), but the United States should proceed knowing to the extent possible the risks from any given U.S. response.

Furthermore, U.S. actions to impose costs for bad behavior must be accompanied by credible promises to cease cost imposition activities once bad behavior has terminated. Otherwise, the adversary will have no particular incentive to stop its own aggressive behavior.

8.5. Promote collective engagement with international partners.

Deterrence is more effective and impactful when done collectively rather than acting alone. Perceptions of credibility and commitment to take substantial and significant actions in response to election interference are strengthened when they come from a coalition of countries and multilateral organizations working in solidarity. Building a coalition of countries to take collective action is a stated goal of the State Department's deterrence initiative and should be fully resourced and supported. Although there has been some success in joint attribution efforts with respect to Russian and North Korean malicious cyber activity, the practice of "naming and shaming" those countries is unlikely to change their malign behavior absent cost imposition. Achieving collective cost imposition, however, will require more than diplomacy and coalition building. Among other things, information sharing with partners will need to be improved to enable those partners to act and get needed political-level buy-in for taking action. Partners will also need to expand their ability to impose substantial costs.[19] In addition, as discussed in greater detail in Chapter Seven, the international community must come together to establish norms against electoral interference. The next step would be to transparently agree on cost-imposing responses to those countries who violate these norms.

8.6. Conduct a continuous strategic disruption campaign against adversaries that seek to interfere with U.S. elections.

At its most effective level, election interference is not so much an event as an ongoing adversary activity. Accordingly, the United States must conduct its counter-interference efforts as a strategic campaign rather than as a one-time response. Strategic campaigns are, of course, defined by consistent effort over time and coherent strategy, and should be directed specifically against the offending actors (i.e., those individuals and organizations most closely involved with the interference activities). Note, however, that in conducting such a campaign, the United States should be aware that conducting cyber operations unilaterally in non-adversary space can place at risk partnerships with those countries that might otherwise be willing to take future collective action.

8.7. Pursue common interests in cyberspace where possible.

As highlighted in the beginning of this chapter, the United States has failed to impose costs on Russia adequate to deter meddling in U.S. elections, and so the previous recommendations propose various measures to increase costs to Russia as a consequence of continuing interference. Such actions also will deter other foreign actors. Nevertheless, the necessity of taking such measures should not blind the United States to the reality that the United States and Russia must have communication channels and do have common interests that are worth exploring despite the adversarial relationship between the two nations. Eventually, not unlike nuclear arms control negotiations during the Cold War, we must be able to credibly deter and to establish some rules of the road for preventing catastrophic outcomes at the same time. First, the United States should ensure that there are adequate formal and informal communication channels—military, intelligence, and diplomatic—to allow for appropriate signaling and de-escalation as the deterrence strategy is being implemented. Such channels also can help to avoid misperception or misattribution in the event of a third-party cyber operation seeking to provoke further conflict or escalate tensions between the two nations. For example, working and technical level talks to make sure the U.S.-Russia cyber hotline is operational and tested would ensure that this communication channel is available when needed.

In addition, the United States, when appropriate, should support the establishment of working groups between the two nations and encourage unofficial Track 2 dialogues to explore the shape and nature of carefully scoped common interests. For example, both nations share commitments to fight child pornography and human trafficking, activities that rely in large measure on cyber-enabled communications. Neither nation wants the other nation to suffer cyberattacks that increase the likelihood of accidental nuclear conflict. Discussions about such topics (or others—these are merely illustrative) could lead to mutual actions that serve the interests of both the United States and Russia, and as importantly could help to establish and sustain channels of communication that would prove valuable in the future.

Of course, in commissioning any formal government discussions, the United States must be careful not to inadvertently signal to Russia or the rest of the world that it has simply forgiven Russia's past and continuing election meddling and other malicious cyber conduct. Russia has long sought to re-establish the high-level, political cyber dialogue (that was suspended, like other such dialogues, following Russia's incursions into Ukraine), in part, for this very purpose. Unless and until there are significant commitments by Russia and substantial changes in Russia's actions, any high-level cyber dialogue is at best premature and at worst simply a public relations coup that would be seen as rewarding them for their disruptive conduct. And even if such a dialogue on cyber issues starts again in the future, the United States must continue to deter Russia's belligerent behavior in other domains, including first and foremost in Europe in general and Ukraine in particular.[20] During the Cold War, U.S. administrations managed to engage their

Soviet counterparts on nuclear arms control issues, while simultaneously containing the Soviet Union on other fronts. Regarding cyber issues and other confrontational areas of the current U.S.-Russian agenda, we can pursue a similarly sophisticated, dual track strategy of engagement and containment again.

PREFACE

1 Special Counsel Robert S. Mueller, III., "Report On The Investigation Into Russian Interference In The 2016 Presidential Election: Volume I," *U.S. Department of Justice*, March 2019, Page 1.

2 Thomas H. Kean et al., "The 9/11 Commission Report," https://www.9-11commission.gov/report.

3 Bart Jansen, Tom Vanden Brook, Kevin Johnson, and William Cummings, "Mueller's investigation is done. Here are the 34 people he indicted along the way," *USA Today,* March 25, 2019, https://www.usatoday.com/story/news/politics/2019/03/25/muellers-russia-report-special-counsel-indictments-charges/3266050002/.

4 Sonam Sheth and Pat Ralph, "The House Intel Committee report on its controversial Russia investigation is out — here are the big points," *Business Insider,* April 27, 2018, https://www.businessinsider.com/house-intel-committee-report-russia-investigation-2018-4.

5 Julian E. Barnes and Adam Goldman, "F.B.I. Warns of Russian Interference in 2020 Race and Boosts Counterintelligence Operations," *The New York Times,* April 26, 2019, https://www.nytimes.com/2019/04/26/us/politics/fbi-russian-election-interference.html.

6 The authors acknowledge that this report draws from and builds on research and insights produced by the following studies: "A Guide to Cyber Attribution," Office of the Director of National Intelligence, September 14, 2018; "A multi-dimensional approach to disinformation: Report of the independent High level Group on fake news and online disinformation," European Commission, 2018; "A White Paper on the Key Challenges in Cyber Threat Intelligence: Explaining the 'See it, Sense it, Share it, Use it' approach to thinking about Cyber Intelligence," Office of the Director of National Intelligence, October 2018; Alice Marwick and Rebecca Lewis, "Media Manipulation and Disinformation Online," Data & Society Research Institute; Ann M. Ravel, Samuel C. Woolley, and Hamsini Sridharan, "Principles and Policies to Counter Deceptive Digital Policies," MapLight, February 2019; Ben Judah and Nate Sibley, "Countering Russian Kleptocracy," Hudson Institute, April 2018, https://s3.amazonaws.com/media.hudson.org/files/publications/CounteringRussianKleptocracy.pdf; "Building Blocks of Cyber Intelligence," Office of the Director of National Intelligence; Christopher Paul and Miriam Matthews, "The Russian 'Firehose of Falsehood' Propaganda Model: Why It Might Work and Options to Counter It," RAND Corporation, 2016, https://www.rand.org/pubs/perspectives/PE198.html; David P. Fidler, "The U.S. Election Hacks, Cybersecurity, and International Law," Indiana University, Maurer School of Law, 2017; Dipayan Ghost and Ben Scott, "Digital Deceit II: A Policy Agenda to Fight Disinformation on the Internet," Harvard Kennedy School, Shorenstein Center on Media, Politics and Public Policy, September 2018; Dipayan Ghost and Ben Scott, "#DigitalDeceit: The Technologies Behind Precision Propaganda on the Internet," Harvard Kennedy School, Shorenstein Center on Media, Politics and Public Policy, January 2018; "Disinformation and 'fake news': Final Report," House of Commons: Digital, Culture, Media and Sport Committee, February 18, 2019; Gordon Ramsay and Sam Robertshaw, "Weaponising news: RT, Sputnik and targeted disinformation," King's College London, the Policy Institute, Centre for the Study of Media, Communication & Power; John W. Kelly, "Briefing for the United States Senate Select Committee on Intelligence," Graphika, August 1, 2018; Margaret Roberts, "Testimony before the U.S.-China Economic and Security Review Commission, Hearing on China's Information Controls, Global Media Influence, and Cyber Warfare Strategy," May 4, 2017; "Draft Charter: An Oversight Board for Content Decisions," Facebook; "Midterm Assessment: the Trump Administration's Foreign and National Security Policies," Foundation for Defense of Democracies, edited by John Hannah and David Adesnik, January 2019; Erik Brattberg and Tim Maurer, "Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks," Carnegie Endowment for International Peace, May 2018; "Examining Foreign Interference in U.S. Elections," Campaign Legal Center, January 2018; "Fighting Fake News: Workshop Report," The Information Society Project, the Floyd Abrams Institute for Freedom of Expression; "Forbidden Feeds: Government Controls on Social Media in China," PEN America, March 13, 2018; Geir Haugen, "Manipulation and Deception with Social Bots: Strategies and Indicators for Minimizing Impact," Norwegian University of Science and Technology, May 2017; Greg Miller, The Apprentice: Trump, Russia and the Subversion of American Democracy (New York: HarperCollins, 2018); Kathleen Hall Jamieson, How Russian Hackers and Trolls Helped Elect a President (Oxford: Oxford University Press, 2018); "International Security and Estonia: 2018," Estonian Foreign Intelligence Service; Jamie Fly and Laura Rosenberger, "The Mueller Report Shows Politicians Must Unite to Fight Election Interference," German Marshall Fund, April 22, 2019, http://www.gmfus.org/commentary/mueller-report-shows-politicians-must-unite-fight-election-interference; Jamie Fly, Laura Rosenberger, and David Salvo, "The ASD Policy Blueprint for Countering Authoritarian Interference in Democracies," German Marshall Fund, June 26, 2018, http://www.gmfus.org/publications/asd-policy-blueprint-countering-authoritarian-interference-democracies; Joshua A. Tucker, Andrew Guess, Pablo Barberá, Cristian Vaccari, Alexandra Siegel, Sergey Sanovich, Denis Stukal, and Brendan Nyhan, "Social

Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature," William and Flora Hewlett Foundation, March 2018; Laura Galante and Shaun Ee, "Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Enabled Incidents," Atlantic Council, the Brent Scowcroft Center for Strategy and Security, September 2018; Laura Rosenberger, "Statement of Laura Rosenberger, Alliance for Securing Democracy, the German Marshall Fund of the United States, Before the United States Senate Select Committee on Intelligence Concerning 'Foreign Influence Operations and their use of Social Media Platforms'", United States Senate Select Committee on Intelligence, August 1, 2018; "'Make Germany Great Again': Kremlin, Alt-Right and International Influences in the 2017 German Elections," London School of Economics, Institute of Global Affairs, Institute for Strategic Dialogue; Malcolm Nance, The Plot to Destroy Democracy: How Putin and His Spies Are Undermining America and Dismantling the West (New York: Hachette, 2018); Michael Isikoff and David Corn, Russian Roulette: The Inside Story of Putin's War on America and the Election of Donald Trump (New York: Twelver 2018); Michael McFaul, "Testimony of Ambassador Michael McFaul, Putin's Playbook: the Kremlin's Use of Oligarchs, Money and Intelligence in 2016 and Beyond," U.S. House Permanent Select Committee on Intelligence, March 28, 2019; "Online and On All Fronts: Russia's Assault on Freedom of Expression," Human Rights Watch, 2017; Paul M. Barrett, "Tackling Domestic Disinformation: What the Social Media Companies Need to Do," NYU Stern, Center for Business and Human Rights, March 2019; Paul M. Barrett, Tara Wadhwa, and Dorothé Baumann-Pauly, "Combating Russian Disinformation: The Case for Stepping Up the Fight Online," NYU Stern, Center for Business and Human Rights, July 2018; 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, Computational Propaganda Research Project; Philip N. Howard, "Testimony of Philip N. Howard, Oxford University, 'Foreign Influence on Social Media Platforms: Perspectives from Third-Party Social Media Experts,'" United States Senate Select Committee on Intelligence, August 1, 2018; Renee DiResta, Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Jonathan Albright, and Ben Johnson, "The Tactics & Tropes of the Internet Research Agency," New Knowledge; Richard Fletcher, Alessio Cornia, Lucas Graves, and Rasmus Kleis Nielsen, "Measuring the reach of 'fake news' and online disinformation in Europe," University of Oxford, Reuters Institute for the Study of Journalism, February 2018; "Robotrolling: Issue 1," NATO Strategic Communications Centre of Excellence, 2017; "Robotrolling: Issue 2," NATO Strategic Communications Centre of Excellence, 2017; Samantha Bradshaw and Philip N. Howard, "Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation," University of Oxford, Computational Propaganda Research Project; Seth Abramson, Proof of Collusion: How Trump Betrayed America (New York: Simon and Shuster, 2018); "SSCI Research Summary December 1, 2018: An assessment of the Internet Research Agency's U.S.-directed activities in 2015-2017 based on platform-provided data," New Knowledge; Timothy Garton Ash, Robert Gorwa, and Danaë Metaxa, "GLASTNOST! Nine ways Facebook can make itself a better forum for free speech and democracy: An Oxford-Stanford Report," University of Oxford, Reuters Institute for the Study of Journalism; Todd C. Helmus, Elizabeth Bodine-Baron, Andrew Radin, Madeline Magnuson, Joshua Mendelsohn, William Marcellino, Andriy Bega, and Zev Winkelman, "Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe," Rand Corporation; Todd C. Helmus, "Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe: Testimony before the Senate Select Committee on Intelligence," Rand Corporation, August 1, 2018; Whitney Phillips, "The Oxygen of Amplification: Better Practices for Reporting on Extremists, Antagonists, and Manipulators Online," Data & Society Research Institute; "Who Said What? The Security Challenges of Modern Disinformation: Highlights from the Workshop," Canadian Security Intelligence Service, February 2018.

7 In addition to the authors of the chapters, I am deeply grateful to Bronte Kass and Kimberly Renk for their editorial and research assistance in completing this report.

SUMMARY OF RECOMMENDATIONS

1 Authors of individual chapters clearly support the recommendations in their chapters but do not necessarily endorse the recommendations in other chapters.

CHAPTER ONE

1 Additional thanks to Anya Shkurko and Anna Manafova for their research contributions to this chapter.

2 For a deeper elaboration of 'Putinism', see Michael McFaul, "Putinism and the 2016 U.S. Presidential Election," (Working Paper, February 2019), https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/putinisn2016election-3-10-19_1.pdf.

3 "Speech and the Following Discussion at the Munich Conference on Security Policy," *The Kremlin,* February 10, 2007, http://en.kremlin.ru/events/president/transcripts/24034.

4 For elaboration, see: ВРЕМЕННАЯ КОМИССИЯ СОВЕТА ФЕДЕРАЦИИ ПО ЗАЩИТЕ ГОСУДАРСТВЕННОГО СУВЕРЕНИТЕТА И ПРЕДОТВРАЩЕНИЮ ВМЕШАТЕЛЬСТВА ВО ВНУТРЕННИЕ ДЕЛА РОССИЙСКОЙ ФЕДЕРАЦИИ: СПЕЦИАЛЬНЫЙ ДОКЛАД ПО ИТОГАМ ПРЕЗИДЕНТСКИХ ВЫБОРОВ В РОССИЙСКОЙ ФЕДЕРАЦИИ (2018 г.) С ТОЧКИ ЗРЕНИЯ ПОКУШЕНИЙ НА РОССИЙСКИЙ ЭЛЕКТОРАЛЬНЫЙ СУВЕРЕНИТЕТ, http://council.gov.ru/media/files/2uQuCAAwoWu0B8tiDeDExn5x9CtBkTDV.pdf. In this final report, issued by "The interim commission of the council of federation for the protection of state sovereignty and prevention of the interference in the internal affairs of the Russian Federation", the authors claim that in addition to interfering with the affairs of other sovereign states, the United States has been meddling in Russian affairs since the dissolution of the USSR through undermining the Russian government and dividing Russian society, whether acting directly in the country or indirectly through third countries or organizations. The authors of the report claim that Americans are funding Russian civil society organizations, think tanks, non-governmental organizations, journalists, and even individual activists to undermine Russian sovereignty from within. Simultaneously, they assert that in partnership with NATO member countries, the United States actively participated in destabilizing the situation in the Middle East and Northern Africa during the "Arab Spring", just around the time of Russian elections of 2011-12.

5 Gillian Edevane, "NRA Admits Accepting Money from 12 Russia-Linked Donors," *Newsweek,* April 11, 2018, https://www.newsweek.com/nra-admits-accepting-money-23-russia-linked-donors-882310.

6 Paul Sonne, "A Russian bank gave Marine Le Pen's party a loan. Then weird things began happening," *The Washington Post,* December 27, 2018, https://www.washingtonpost.com/world/national-security/a-russian-bank-gave-marine-le-pens-party-a-loan-then-weird-things-began-happening/2018/12/27/960c7906-d320-11e8-a275-81c671a504-22_story.html?utm_term=.d38f1372ea01.

7 Edward Delman, "When is a TV Channel a Foreign Agent?" *The Atlantic*, April 22, 2015, https://www.theatlantic.com/international/archive/2015/04/rt-lobbyist-russia-putin-media/390621/. For a deeper analysis of RT efforts on YouTube, see Robert Orttung and Elizabeth Nelson, "Russia Today's strategy and effectiveness on YouTube," *Post-Soviet Affairs* 35, no. 2 (2019): 77-92.

8 For background, see Sergey Sanovich, "Russia: The Origins of Digital Misinformation," in *Computational Propaganda: Political Parties, Politicians and Political Manipulation on Social Media*, ed. Samuel Wooley and Philip Howard (Oxford: Oxford University Press, 2019), 21-40.

9 Neil MacFarquhar, "Outrage Grows as Russia Grants Passports in Ukraine's Breakaway Regions," *The New York Times,* April 25, 2019, https://www.nytimes.com/2019/04/25/world/europe/russia-citizenship-ukraine.html.

10 For details, see Michael McFaul, *From Cold War to Hot Peace: An American Ambassador in Putin's Russia* (Houghton Mifflin Harcourt, May 2018), 239-63.

11 Blair Miller, "Trump election fraud commission wants personal information from Colorado, US voter rolls," *The Denver Channel,* June 29, 2017, https://www.thedenverchannel.com/decodedc/for-trump-supporters-election-fraud-is-a-real-fear.

12 Tyler Pager, "Trump to Look at Recognizing Crimea as Russian Territory, Lifting Sanctions," *Politico,* July 27, 2016, http://www.politico.com/story/2016/07/trump-crimea-sanctions-russia-226292.

13 Carol Morello and Adam Taylor, "Trump Says U.S. Won't Rush to Defend NATO Countries if They Don't Spend More on Military," *The Washington Post,* July 21, 2016, https://www.washingtonpost.com/world/national-security/trump-says-us-wont-rush-to-defend-nato-countries-if-they-dont-spend-more-on-military/2016/07/21/76c48430-4f51-11e6-a7d8-13d06b37f256_story.html?tid=a_inl&utm_term=.c864abc4ab0c. Candidate Trump actually argued inaccurately that NATO allies were not paying enough to the United States. NATO does not operate that way. For elaboration, see Michael McFaul, "Mr. Trump, NATO Is an Alliance, Not a Protection Racket," *The Washington Post*, July 25, 2017, https://www.washingtonpost.com/opinions/global-opinions/mr-trump-nato-is-an-alliance-not-a-protection-racket/2016/07/25/03ca2712-527d-11e6-88eb-7dda4e2f2aec_story.html?utm_term=.4f2db182f676.

14 Alex Griswold, "Trump Defends Putin's Murder of Journalists: 'Our country Does Plenty of Killing Also,'" *Mediaite,* December 18, 2015, https://www.mediaite.com/tv/donald-trump-defends-putins-murder-of-journalists-our-country-does-plenty-of-killing-also/.

15 Abby Philip, "O'Reilly Told Trump That Putin Is a Killer. Trump's Reply: 'You Think Our Country Is So Innocent?'" *The Washington Post,* February 4, 2017, https://www.washingtonpost.com/news/post-politics/wp/2017/02/04/oreilly-told-trump-that-putin-is-a-killer-trumps-reply-you-think-our-countrys-so-innocent/?utm_term=.5d54f7ad3b79.

16 "Presidential Candidate Donald Trump Primary Night Speech," *C-SPAN*, April 26, 2016, https://www.c-span.org/video/?408719-1/donald-trump-primary-night-speech&start=1889&transcriptQuery=putin.

17 Jeremy Diamond, "Timeline: Donald Trump's praise for Vladimir Putin," *CNN,* July 29, 2016, http://www.cnn.com/2016/07/28/politics/donald-trump-vladimir-putin-quotes/index.html and Andrew Kaczynski, "80 Times Trump Talked about Putin," *CNN,* March 2017, http://www.cnn.com/interactive/2017/03/politics/trump-putin-russia-timeline/.

18 "Donald Trump Campaign Rally in Hilton Head, South Carolina," *C-SPAN,* December 30, 2015, https://www.c-span.org/video/?402610-1/donald-trump-campaign-rally-hilton-head-south-carolina&transcriptQuery=putin&start=787.

19 "Donald Trump Campaign Rally in Vandalia, Ohio," *C-SPAN*, March 12, 2016, https://www.c-span.org/video/?406393-1/donald-trump-campaign-rally-vandalia-ohio&transcriptQuery=putin&start=1907.

20 Reena Flores, "Donald Trump gives Russia's Putin an 'A' in leadership," *CBS News,* September 30, 2015, https://www.cbsnews.com/news/donald-trump-gives-russias-putin-an-a-in-leadership/.

21 On the differences between President Trump and his administration regarding Russia policy, see Michael McFaul, "Sorry, but Trump is not 'tough on Russia'," *The Washington Post*, January 19, 2019, https://www.washingtonpost.com/opinions/2019/01/16/sorry-trump-is-not-tough-russia/?utm_term=.fb100c094e50.

22 "Background to 'Assessing Russian Activities and Intentions on Recent US Elections': The Analytic Process and Cyber Incident Attribution," *Office of the Director of National Intelligence*, January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

23 "Remarks by President Trump and President Putin of the Russian Federation in Joint Press Conference," *The White House,* issued on July 16, 2018, https://www.whitehouse.gov/briefings-statements/remarks-president-trump-president-putin-russian-federation-joint-press-conference/

24 Hillary Clinton, *What Happened* (Simon & Schuster, 2017), 327.

25 Special Counsel Robert S. Mueller, III., "Report On The Investigation Into Russian Interference In The 2016 Presidential Election: Volume I," *U.S. Department of Justice*, March 2019, 1 ("Mueller Report").

26 Ibid.

27 Ibid., 9.

28 The counterintelligence component of the Special Counsel investigation has not been published and is most likely ongoing.

29 Mueller Report, 4. The Special Counsel Office charged 12 GRU officers for crimes arising from the hacking of these computers, principally with conspiring to commit computer intrusions, in violation of 18 U.S.C. §§1030 and 371. See Volume I, Section V.B, infra; Indictment, United States v. Netyksho, No. I :18-cr-215 (D.D.C. July 13, 2018), Doc. 1 ("Netyksho Indictment").

30 Netyksho Indictment, r 1.

31 Separate from the Special Counsel Office's indictment of GRU officers, in October 2018 a grand jury sitting in the Western District of Pennsylvania returned an indictment charging certain members of Unit 26165 with hacking the U.S. Anti-Doping Agency, the World Anti-Doping Agency, and other international sport associations. United States v. Aleksei Sergeyevich Morenets, No.18-263 (W.D. Pa.).

32 Netyksho Indictment, paragraph 9.

33 Mueller Report, 37.

34 Ibid., 38.

35 Ibid.

36 Ibid., 41.

37 Dmitri Alperovitch, "Bears in the Midst: Intrusion into the Democratic National Committee," *CrowdStrike Blog*, June 14, 2016. CrowdStrike updated its post after the June 15, 2016 post by Guccifer 2.0 claiming responsibility for the intrusion.

38 Releases of documents on the Guccifer 2.0 blog occurred on June 15, 2016; June 20, 2016; June 21, 2016; July 6, 2016; July 14, 2016; August 12, 2016; August 15, 2016; August 21, 2016; August 31, 2016; September 15, 2016; September 23, 2016; October 4, 2016; and October 18, 2016.

39 Mueller Report, 43.

40 Ibid., 44.

41 James Ball, "Julian Assange could face arrest in Australia over unredacted cables," *The Guardian,* September 2, 2011, https://www.theguardian.com/media/2011/sep/02/julian-assange-arrest-australia-wikileaks.

42 Mueller Report, 48.

43 7/6/16 Twitter DMs, @WikiLeaks & @guccifer_2.

44 Mueller Report, 51.

45 Ibid., 53.

46 Ibid., 59.

47 At the time, the link took users to a WikiLeaks archive of stolen Clinton campaign documents.

48 10/12/16 Twitter DM, @WikiLeaks to @DonaldJTrumpJr.

49 @DonaldJTrumpJr 10/14/16 (6:34 a.m.) Tweet.

50 Mueller Report, 62. Flynn 4/25/18 302, at 5-6; Flynn 5/1/18 302, at 1-3; Flynn 5/1/18 302, at l-3.

51 "Donald Trump on Russian & Missing Hillary Clinton Emails," *C-SPAN*, Posted 7/27/16, available at https://www.youtube.com/watch?v=3kxG8uJUsWU (starting at 0:41).

52 Mueller Report, 36, 58.

53 Kathleen Hall Jamieson, *Cyber-War: How Russian Hackers and Trolls Helped Elect a President* (Oxford: Oxford University Press, 2019).

54 Mueller Report, 4.

55 Colin Stretch, *Social Media influence in the 2016 U.S. election, hearing before the senate select committee on intelligence,* 115th Congr. 13 (11/1/17).

56 Ibid.

57 Eli Rosenberg, "Twitter to Tell 677,000 Users they Were Had by the Russians. Some Signs Show the Problem Continues," *The Washington Post,* January 19, 2019; Twitter, "Update on Twitter's Review of the 2016 US Election," updated January 31, 2018. Twitter also reported identifying 50,258 automated accounts connected to the Russian government, which tweeted over a million times in the ten weeks before the election.

58 Gerrit De Vynck and Selina Wang, "Russian Bots Retweeted Trump's Twitter 470,000 Times," *Bloomberg,* updated January 29, 2018, https://www.bloomberg.com/news/articles/2018-01-26/twitter-says-russian-linked-bots-retweeted-trump-470-000-times.

59 Politico Staff, "The social media ads Russia wanted Americans to see," *Politico,* November 1, 2017, https://www.politico.com/story/2017/11/01/social-media-ads-russia-wanted-americans-to-see-244423.

60 Mueller Report, 24-25.

61 4/19/16 Facebook Advertisement ID 6045151094235.

62 Mueller Report, 26.

63 Instagram ID 2228012168 (Stand For Freedom) 11/3/15 Post ("Good evening buds! Well I am planning to organize a confederate rally[...] in Houston on the 14 of November and I want more people to attend.").

64 Mueller Report, 31-32.

65 Ibid., 19-20.

66 Ibid.,16.

67 "Internet Agency Indictment," *U.S. Department of Justice,* filed February 16, 2018. https://www.justice.gov/file/1035477/download,12(b); see also 5/26/16 Facebook Messages, ID 1479936895656747 (United Muslims of America).

68 "Internet Agency Indictment".

69 Mueller Report, 21.

70 Ibid., 5.

71 For example, on August 18, 2015, on behalf of the editor-in-chief of the internet newspaper Vzglyad, Georgi Asatryan emailed campaign press secretary Hope Hicks asking for a phone or in-person candidate interview. 8/18/15 Email, Asatryan to Hicks. One day earlier, the publication's founder (and former Russian parliamentarian) Konstantin Rykov had registered two Russian websites-Trump2016.ru and DonaldTrump2016.ru. No interview took place.

72 Mueller Report, 71. 11/3/15 Email, Sater to Cohen (12:14p.m.).

73 Mueller Report, 5.

74 Ibid., 5-6.

75 Ibid., 6.

76 DJTJR00446 (6/3/16 Email, Trump Jr. to Goldstone); @DonaldJTrumpJr 07/11/17 (11:00) Tweet; RG000061 (6/3/16 Email, Trump Jr. to Goldstone).

77 Natasha Bertrand, "Putin's Big Tell?" *The Atlantic,* July 18, 2018, https://www.theatlantic.com/politics/archive/2018/07/putins-big-tell/565460/.

78 Mueller Report, 110.

79 Approximately one year later, the June 9 meeting became public and immediately provocative with regards to its implications. In a July 9, 2017 text message to Emin Agalarov, Goldstone wrote, "I made sure I kept you and your father out of [t]his story," and "[i]f contacted I can do a dance and keep you out of it," adding, "FBI now investigating," and "I hope this favor was worth for your dad-it could blow up." See Mueller Report, 121.

80 Ibid., 6-7.

81 As noted in Volume I, Section III. D.l.b, supra, Gates pleaded guilty to two criminal charges in the District of Columbia, including making a false statement to the FBI, pursuant to a plea agreement. He has provided information and in-court testimony that the Office has deemed to be reliable. See also Transcript at 16, United States v. Paul J Manafort, Jr., l:17-cr-201 (D.D.C. Feb. 13, 2019), Doc. 514 ("Manafort 2/13/19 Transcript") (court's explanation of reasons to credit Oates's statements in one instance).

82 Mueller Report, 129.

83 Ibid., 140.

84 Ibid., 9.

85 "Written testimony of I&A Cyber Division Acting Director Dr. Samuel Liles, and NPPD Acting Deputy Under Secretary for Cybersecurity and Communications Jeanette Manfra for a Senate Select Committee on Russian Intelligence hearing titled 'Russian Interference in the 2016 U.S. Elections,'" *U.S. Department of Homeland Security,* June 21, 2017, https://www.dhs.gov/news/2017/06/21/written-testimony-ia-cyber-division-acting-director-dr-samuel-liles-and-nppd-acting.

86 Pam Fessler, "Mueller Report Raises New Questions about Russia's Hacking Targets in 2016," *NPR,* April 19, 2019, https://www.npr.org/2019/04/19/714890832/mueller-report-raises-new-questions-about-russias-hacking-targets-in-2016.

87 Pam Fessler, "Russian Cyberattack Targeted Elections Vendor Tied To Voting Day Disruptions," *NPR,* August 10, 2017, https://www.npr.org/2017/08/10/542634370/russian-cyberattack-targeted-elections-vendor-tied-to-voting-day-disruptions.

88 Mueller Report, 50.

89 Ibid.

90 Ibid., 51.

91 For an assessment, see chapters ten and eleven in Morris Fiorina, *Unstable Majorities: Polarization, Party Sorting & Political Stalemate* (Stanford: Hoover Institution Press, 2017).

92 For a careful treatment of this difficult social science question, see Kathleen Hall Jamieson, *Cyber-War: How Russian Hackers and Trolls Helped Elect a President* (Oxford: Oxford University Press, 2019).

93 Cooperative Congressional Election Study, as quoted in Danielle Kurtzleben, "Here's How Many Bernie Sanders Supporters Ultimately Voted for Trump," *NPR,* August 24, 2017, http://www.npr.org/2017/08/24/545812242/1-in-10-sanders-primary-voters-ended-up-supporting-trump-survey-finds?utm_source=twitter.com&utm_medium=social&utm_campaign=politics&utm_term=nprnews&utm_content=20170824.

94 Jamieson, *Cyber-War,* Appendix One.

95 "The IRA, Social Media and Political Polarization in the United States, 2012-2018," *Computational Propaganda Research Project,* https://comprop.oii.ox.ac.uk/research/ira-political-polarization/.

96 According to the National Urban League's 2019 State of Black America report. the use of race as a weapon to divide Americans and dissuade African-American populations from voting has been largely overlooked in the public discussion of Russian interference. See "State of Black America," *National Urban League,* 2019, http://soba.iamempowered.com/2019-report.

97 "The Tactics and Tropes of the Internet Research Agency," *New Knowledge,* December 17, 2018, https://www.newknowledge.com/disinforeport.

98 Mirren Gidda, "Third Party Votes Could Have Cost Hillary Clinton the Presidency," *Newsweek,* November 9, 2016, http://www.newsweek.com/susan-sarandon-third-party-candidates-jill-stein-gary-johnson-hillary-clinton-519032.

99 Bruce Schneier, "Defending Democracies Against Information Attacks," *Schneier on Security,* April 30, 2019, https://www.schneier.com/blog/archives/2019/04/defending_democ.html.

100 Todd Ruger, "FBI director wants to 'up our game' on election interference," *Roll Call,* May 7, 2019, https://www.rollcall.com/news/congress/fbi-director-wants-game-election-interference.

CHAPTER TWO

1 "Help America Vote Act," *U.S. Election Assistance Commission*, accessed April 16, 2019, https://www.eac.gov/about/help-america-vote-act/.

2 Special Counsel Robert S. Mueller, III., "Report On The Investigation Into Russian Interference In The 2016 Presidential Election: Volume I," *U.S. Department of Justice*, March 2019, 49-51 ("Mueller Report").

3 Ibid., 51.

4 Julian E. Barnes and Adam Goldman, "F.B.I. Warns of Russian Interference in 2020 Race and Boosts Counterintelligence Operations," *The New York Times,* April 26, 2019, https://www.nytimes.com/2019/04/26/us/politics/fbi-russian-election-interference.html.

5 National Research Council, "Letter Report on Electronic Voting," *The National Academies Press,* 2006, https://www.nap.edu/catalog/11704/letter-report-on-electronic-voting.

6 The 2016 election was arguably not a close election, as Donald Trump lost the popular vote by 2.8 million votes, a margin of 2% of the total number of votes cast. But victories in individual states determine the electoral vote count, and in three key states, Trump won the popular vote by about 107,000 people, or a margin of 0.09 percent of all votes cast in this election, leading to his victory in the Electoral College. By any measure, a winning margin of 0.09 percent is very close indeed. See Tim Meko, Denise Lu, and Lazaro Gamio, "How Trump won the presidency with razor-thin margins in swing states," *The Washington Post,* November 11, 2016, https://www.washingtonpost.com/graphics/politics/2016-election/swing-state-margins/.

7 National Research Council, "Cybersecurity Today and Tomorrow: Pay Now or Pay Later," (Washington, DC: National Academy Press, 2002).

8 More precisely, concealing the internal operation of a system does provide a layer of protection for a system. But because concealment does not actually fix vulnerabilities, these vulnerabilities can be thus exploited, and overall, such exploitation outweighs the advantages provided by obscurity.

9 "Fact Sheet: The U.S. Election Assistance Commission's Voting System Testing and Certification Program," *U.S. Election Assistance Commission*, last modified March 7, 2017, https://www.eac.gov/news/2017/03/07/fact-sheet-the-us-election-assistance-commissions-voting-system-testing-and-certification-program-voting-systems-certification-communications-fact-sheet.

10 See, for example, Mark Niesse, "How to hack elections on Georgia's electronic voting machines: Demonstration shows malware could change election results," *The Atlanta Journal-Constitution*, last modified April 18, 2018, https://www.ajc.com/news/state--regional-govt--politics/how-hack-elections-georgia-electronic-voting-machines/K4s5F935330BS6fGDm3CVI/.

11 "The Verifier – Polling Place Equipment – November 2018," *Verified Voting*, accessed April 16, 2019, https://www.verifiedvoting.org/verifier/#.

12 Jordan Wilkie, "America's new voting machines bring new fears of election tampering," *The Guardian*, April 22, 2019, https://www.theguardian.com/us-news/2019/apr/22/us-voting-machines-paper-ballots-2020-hacking?CMP=share_btn_tw.

13 Ibid.

14 Ibid.

15 Joseph Anthony, "The Importance of Updating the Help America Vote Act," *Scholars Strategy Network*, February 9, 2017, https://scholars.org/brief/importance-updating-help-america-vote-act.

16 National Academies, *Securing the Vote: Protecting American Democracy*, National Academies Press, 2018.

17 In a risk-limiting audit, a percentage of electronic vote counts would be audited using the VVPAT depending on the closeness of the reported outcome—for close races, a greater percentage of votes are audited, but with wide margins of victory, a smaller percentage would be called for.

18 "Protecting American Votes and Elections Act of 2018," *Ron Wyden: United States Senator for Oregon*, accessed April 16, 2019, https://www.wyden.senate.gov/imo/media/doc/PAVE%20Act%20of%202018%20UPDATED.pdf

19 Ibid.

20 For example, the Harvard Kennedy School of Government has published a Campaign Cybersecurity Playbook that suggests cybersecurity recommendations for political campaigns. See "The Cybersecurity Campaign Playbook: Defending Digital Democracy," *Harvard Kennedy School*, May 2018, https://www.belfercenter.org/sites/default/files/files/publication/CampaignPlaybook_0.pdf.

21 The recommendations in the Harvard Kennedy School of Government's Campaign Cybersecurity Playbook are also applicable to those who work on election administration.

22 As one illustration of such a partisan leaning, in 2003, the CEO of a vendor trying to sell voting machines in Ohio said that he was "committed to helping Ohio deliver its electoral votes to the president next year." See Julie Carr Smyth, "Voting Machine Controversy," *Cleveland Plain Dealer*, August 28, 2003, https://www.commondreams.org/headlines03/0828-08.htm.

23 "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as Critical Infrastructure Subsector," *U.S. Department of Homeland Security,* January 6, 2017, https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

CHAPTER THREE

1 "Internet Agency Indictment," *U.S. Department of Justice,* filed February 16, 2018, https://www.justice.gov/file/1035477/download.

2 Alex Stamos, "An Update on Information Operations on Facebook," *Facebook Newsroom,* September 6, 2017, https://newsroom.fb.com/news/2017/09/information-operations-update.

3 For decades, social scientists have been attempting to estimate the causal influence of campaign advertising on electoral outcomes, but with limited success. See Jörg L. Spenkuch and David Toniatti, "Political Advertising and Election Results," *The Quarterly Journal of Economics* 133, no. 4 (November 2018): 1981-2036, https://doi.org/10.1093/qje/qjy010; Avi Ben-Bassat, Momi Dahan, and Esteban F. Klor, "Does campaign spending affect electoral outcomes?" *Electoral Studies* 40 (December 2015): 102-114, https://doi.org/10.1016/j.electstud.2015.06.012.

4 4/19/16 Facebook Advertisement ID 6045151094235.

5 Senator Amy Klobuchar, "S.1989 – Honest Ads Act," *Congress.gov,* https://www.congress.gov/bill/115th-congress/senate-bill/1989.

6 "Governor Cuomo Signs the New York State Democracy Protection Act to Secure the Integrity of New York Elections," *New York State: Governor Andrew M. Cuomo,* April 18, 2018, https://www.governor.ny.gov/news/governor-cuomo-signs-new-york-state-democracy-protection-act-secure-integrity-new-york.

7 Natasha Singer, "Tech Giants Now Share Details on Political Ads. What Does That Mean For You?" *The New York Times,* September 2, 2018, https://www.nytimes.com/2018/09/02/technology/03adarchive.html.

8 "Facebook and Google: This is What an Effective Ad Archive API Looks Like," *Mozilla Blog,* March 27, 2019, https://blog.mozilla.org/blog/2019/03/27/facebook-and-google-this-is-what-an-effective-ad-archive-api-looks-like/.

CHAPTER FOUR

1 Natalka Pisnia, "Why Has RT Registered as a Foreign Agent with the US?" *BBC*, November 15, 2017, http://www.bbc.com/news/world-us-canada-41991683.

2 Edward Delman, "When is a TV Channel a Foreign Agent?" *The Atlantic*, April 22, 2015, https://www.theatlantic.com/international/archive/2015/04/rt-lobbyist-russia-putin-media/390621/.

3 Jim Rutenberg, "RT, Sputnik and Russia's New Theory of War," *The New York Times*, September 13, 2017, https://www.nytimes.com/2017/09/13/magazine/rt-sputnik-and-russias-new-theory-of-war.html?_r=0.

4 Ibid.

5 Julia Ioffe, "What is Russia Today?" *Columbia Journalism Review,* 2010, https://archives.cjr.org/feature/what_is_russia_today.php

6 David Cloud, Tracy Wilkinson, and Joseph Tanfani, "FBI Investigates Russian Government Media Organizations Accused of Spreading Propaganda in U.S." *The LA Times,* 2017, https://www.latimes.com/nation/la-na-russia-propaganda-20170913-story.html; James Vincent,"Russia Today news anchor Liz Wahl resigns live on air in response to "whitewashed" Ukraine coverage," *The Independent,* 2014, https://www.independent.co.uk/news/world/russia-today-anchor-resigns-lives-on-air-in-response-to-whitewashed-ukraine-coverage-9172818.html.

7 James Vincent,"Russia Today news anchor Liz Wahl resigns live on air in response to 'whitewashed' Ukraine coverage," *The Independent,* 2014, https://www.independent.co.uk/news/world/russia-today-anchor-resigns-lives-on-air-in-response-to-whitewashed-ukraine-coverage-9172818.html.

8 Ibid.

9 Ibid.

10 Statements from several interviews, as quoted in: Ben Nimmo, "Question That: RT's Military Mission," *Digital Forensic Research Lab*, 2018, https://medium.com/dfrlab/question-that-rts-military-mission-4c4bd9f72c88.

11 U.S. Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections," *ICA,* 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

12 Danielle Ryan, "RT America Was Not 'Pro-Trump'," *The Nation*, 2017, https://www.thenation.com/article/rt-america-was-not-pro-trump/; Ben Nimmo, "Understanding the Role of Russian Propaganda in the US Election," *New Atlanticist,* 2016, https://www.atlanticcouncil.org/blogs/new-atlanticist/understanding-the-role-of-russian-propaganda-in-the-us-election.

13 "Photo of Clinton having trouble with stairs fuels rumors of bad health," *RT,* August 8, 2016, retrieved at https://www.rt.com/usa/355047-clinton-stairs-health-problem/.

14 "#PayToPlay: Hillary Clinton faces corruption scandal after links between donors & State Department exposed," *RT,* August 10, 2016, retrieved at https://www.rt.com/usa/355447-clinton-emails-state-department-foundation/.

15 Pepe Escobar, "Hillary, Queen of War: The Road Map Ahead," *Sputnik International,* August 4, 2016, https://sputniknews.com/columnists/201608041043937453-hillary-clinton-war-queen/.

16 See, e.g., RT America, "Watching the Hawks: The Nation Endorses Bernie Sanders," *YouTube*, January 18, 2016, https://www.youtube.com/watch?v=hZL-ztfeVIA.

17 Philip Howard, Bharath Ganesh, Dimitria Liotsiou, John Kelly, and Camille Francois, "The IRA, Social Media and Political Polarization in the United States, 2012-2018," *Computational Propaganda Project,* 2018, https://comprop.oii.ox.ac.uk/research/ira-political-polarization/.

18 Daisuke Wakabayashi and Nicholas Confessore, "Russia's Favored Outlet is an Online News Giant. YouTube Helped," *The New York Times,* 2017, https://www.nytimes.com/2017/10/23/technology/youtube-russia-rt.html;"RT Leads Among TV News Channels on YouTube with 5 Billion Views," *RT News,* 2017, https://www.rt.com/about-us/press-releases/rt-youtube-5bn-views/.

19 RT America, "Secret World of US Election: Julian Assange Talks to John Pilger," *YouTube*, November 5, 2016, https://www.youtube.com/watch?v=_sbT3_9dJY4.

20 Jack Nicas, "Russian State News Site Thrives on YouTube, Facebook," *The Wall Street Journal*, 2017, https://www.wsj.com/articles/russia-state-news-outlet-rt-thrives-on-youtube-facebook-1508808937.

21 Robert M. Faris, Hal Roberts, Bruce Etling, Nikki Bourassa, Ethan Zuckerman, and Yochai Benkler, "Partisanship, Propaganda and Disinformation: Online Media and the 2016 U.S. Presidential Election," *Berkman-Klein Center For Internet & Society Research Paper,* 2017.

22 Megan Metzger and Steven Wilson, "The Other Russian Strategy: RT and the U.S. Midterms," Unpublished Working Paper, 2018.

23 Andrew Osborn and Christian Lowe, "Russian names nine U.S.-backed news outlets likely to be labeled 'foreign agents,' *Reuters,* November 16, 2017, https://www.reuters.com/article/us-russia-usa-media-restrictions-idUSKBN1DG25N.

24 Jeanne Whalen and David Crawford, "How WikiLeaks Keeps its Funding Secret," *The Wall Street Journal*, updated August 23, 2010, https://www.wsj.com/articles/SB10001424052748704554104575436231926853198.

25 Pisnia.

26 Motion to Dismiss or Affirm, Bluman v. FEC, No. 11-275, slip op. at 2 (2011).

27 Ibid.

28 Ibid., 3 (quoting Act of July 4, 1966, Pub. L. No. 89-386, § 8(a) (originally codified at 18 U.S.C. 613 (1970)).

29 See ibid., § 611(c). The definition includes other actions less applicable to this paper.

30 Ibid., § 611(d).

31 Ibid., § 612(a).

32 Ibid., § 612(a)(1)-(10).

33 Ibid., § 614(b).

34 Ibid., § 615.

35 See Cynthia Brown, "The Foreign Agents Registration Act (FARA): A Legal Overview," *Congressional Research Service*, December 4, 2017.

36 See Pub. L. 104-65 § 9(1)(A) (1995).

37 Meese v. Keene, 481 U.S. 465 (1987).

38 Ibid. China Daily is a Chinese "state-run English-language newspaper" that is "widely available". See Bethany Allen-Ebrahimian and Elias Groll, "China's Flagship TV Network Hasn't Registered as a Foreign Agent," *Foreign Policy*, December 19, 2017, http://foreignpolicy.com/2017/12/19/why-isnt-chinas-flagship-tv-network-registered-as-a-foreign-agent-fara-russia-cctv-america-beijing/.

39 Bill Chappell, "TV Company Linked To Russia's RT America Registers As Foreign Agent In U.S.," *Reuters*, November 14, 2017, https://www.npr.org/sections/thetwo-way/2017/11/14/564045159/rt-america-firm-registers-as-foreign-agent-in-u-s-russia-looks-to-retaliate.

40 "Production Company Registers Under the Foreign Agent Registration Act as Agent for the Russian Government Entity Responsible for Broadcasting RT," *U.S. Department of Justice,* November 13, 2017, https://www.justice.gov/opa/pr/production-company-registers-under-foreign-agent-registration-act-agent-russian-government.

41 Hadas Gold, "Russia's RT American registers with DOJ as a foreign agent," *CNN Money,* November 13, 2017, https://money.cnn.com/2017/11/13/media/russia-rt-fara/index.html.

42 Twitter Public Policy, "Announcement: RT and Sputnik Advertising," *Twitter Public Policy Blog,* 2017, https://blog.twitter.com/en_us/topics/company/2017/Announcement-RT-and-Sputnik-Advertising.html. In retaliation, RT published documents showing Twitter's offer to sell *RT* up to a 15% "share of voice" (SOV) in their election-based advertising prior to the 2016 elections, although it seems that *RT* did not accept the proposal. See Alex Kantrowitz, "Twitter Offered Russian Television Network RT 15% of Its Total Share of US Election Advertising," *Buzzfeed News*, 2017, https://www.buzzfeednews.com/article/alexkantrowitz/twitter-offered-rt-15-of-its-total-share-of-us-elections.

43 Elizabeth Dwoskin, "Twitter bans Russian government-owned news sites RT and Sputnik from buying ads," *The Washington Post,* 2017, https://www.washingtonpost.com/news/the-switch/wp/2017/10/26/twitter-bans-russian-government-news-sites-rt-and-sputnik-from-buying-ads/?noredirect=on&utm_term=.0ce937f95972.

44 Wakabayashi and Confessore.

45 Alexandra Ma, "Russia's RT attacks Facebook for suspending 4 viral news channels that broadcast Kremlin talking points to millennials," *Business Insider,* 2019, https://www.businessinsider.com/rt-attacks-facebook-for-suspending-in-the-now-soapbox-other-pages-2019-2.

46 Alina Polyakova, "The Kremlin's Latest Crackdown on Independent Media: Russia's New Foreign Agent Law in Context," *Foreign Affairs*, December 5, 2017, https://www.foreignaffairs.com/articles/russia-fsu/2017-12-05/kremlins-latest-crackdown-independent-media.

CHAPTER FIVE

1 Alex Stamos, "An Update on Information Operations on Facebook," *Facebook Newsroom,* September 6, 2017, https://newsroom.fb.com/news/2017/09/information-operations-update.

2 Nathaniel Gleicher, "Removing Coordinated Inauthentic Behavior and Spam From India and Pakistan," *Facebook Newsroom,* April 1, 2019, https://newsroom.fb.com/news/2019/04/cib-and-spam-from-india-pakistan/; Nathaniel Gleicher, "Removing More Coordinated Authentic Behavior From Russia," *Facebook Newsroom,* May 6, 2019, https://newsroom.fb.com/news/2019/05/more-cib-from-russia/.

3 Alexandra Ma, "Russia's RT attacks Facebook for suspending 4 viral news channels that broadcast Kremlin talking points to millennials," *Business Insider,* 2019, https://www.businessinsider.com/rt-attacks-facebook-for-suspending-in-the-now-soapbox-other-pages-2019-2.

4 Cameron F. Kerry, "A federal privacy law could do better than California's," *Los Angeles Times,* April 25, 2019, https://www.latimes.com/opinion/op-ed/la-oe-kerry-ccpa-data-privacy-laws-20190425-story.html.

5 Kathleen Hall Jamieson, *CYBERWAR: How Russian Hackers and Trolls Helped Elect a President What We Don't, Can't, and Do Know* (Oxford University Press, 2018).

6 Special Counsel Robert S. Mueller, III., "Report On The Investigation Into Russian Interference In The 2016 Presidential Election: Volume I," *U.S. Department of Justice*, March 2019, 42.

7 Tony Biasotti, "Reports shouldn't profile mass shooters, say experts," *Columbia Journalism Review,* August 31, 2018, https://www.cjr.org/united_states_project/jacksonville-shooting-contagion.php; Cindi Deutschman-Ruiz, "Reporting on Suicide," *Poynter,* November 11, 2003, https://www.poynter.org/archive/2003/reporting-on-suicide/.

8 Dipayan Ghosh and Ben Scott, "The Technologies Behind Precision Propaganda on the Internet," 2018.

9 "Standards, Guidelines & Best Practices," *Internet Advertising Bureau*, https://www.iab.com/guidelines/.

10 Bethany Shiner, "Self-Regulation Is Not Enough: The Law on Micro-Targeted Online Political Campaigns and Big Data Needs Reform," *Democratic Audit*, February 4, 2019, http://www.democraticaudit.com/2019/02/04/self-regulation-is-not-enough-the-law-on-micro-targeted-online-political-campaigns-and-big-data-needs-reform/.

11 Hamsini Sridharan, "Principles and Policies to Counter Deceptive Digital Politics," *Maplight,* February 12, 2019, https://maplight.org/story/principles-and-policies-to-counter-deceptive-digital-politics/; Dipayan Ghosh and Ben Scott, "Digital Deceit II: Executive Summary," *New America,* https://www.newamerica.org/public-interest-technology/reports/digital-deceit-ii/executive-summary/.

12 Howard et al.

13 *CrowdTangle,* 2019, https://www.crowdtangle.com/.

14 Kai-Cheng Yang, Onur Varol, Clayton A. Davis, Emilio Ferrara, Alessandro Flammini, and Filippo Mencz, "Arming the public with artificial intelligence to counter social bots," *Human Behavior and Emerging Technologies* 1 (2019): 48– 61, https://doi.org/10.1002/hbe2.115; Denis Stukal, Sergey Sanovich, Richard Bonneau, and Joshua A. Tucker, "Detecting Bots on Russian Political Twitter," *Big Data* 5, no. 4 (2017): 310-324, http://dx.doi.org/10.1089/big.2017.0038.

15 Jamie Fly, Laura Rosenberger, and David Salvo, "Policy Blueprint for Countering Authoritarian Interference in Democracies," *The Alliance for Securing Democracy/German Marshall Fund*, http://www.gmfus.org/publications/asd-policy-blueprint-countering-authoritarian-interference-democracies.

16 Timothy Garton Ash, Robert Gorwa, and Danaë Metaxa, "GLASNOST! Nine ways Facebook can make itself a better forum for free speech and democracy," *Reuters Institute,* https://reutersinstitute.politics.ox.ac.uk/our-research/glasnost-nine-ways-facebook-can-make-itself-better-forum-free-speech-and-democracy.

17 "Disinformation and 'fake news': Final Report," *House of Commons, Digital, Culture, Media and Sport Committee*, https://www.parliament.uk/business/committees/committees-a-z/commons-select/digital-culture-media-and-sport-committee/news/fake-news-report-published-17-19/; Sridharan.

18 ISAO Standards Organization, 2019, https://www.isao.org.

19 Renee DiResta, Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Jonathan Albright, and Ben Johnson, "The Tactics & Tropes of the Internet Research Agency," *New Knowledge*, 2018, https://www.newknowledge.com/articles/the-disinformation-report/.

20 See Electricity Information Sharing and Analysis Center, https://www.eisac.com/, and Financial Services Information Sharing and Analysis Center, https://www.fsisac.com/.

21 Denis Stukal, Sergey Sanovich, Richard Bonneau, and Joshua A. Tucker, "The Use of Twitter Bots in Russian Political Communication," *PONARS Eurasia Policy Memo No. 564*, 2019, http://www.ponarseurasia.org/memo/use-twitter-bots-russian-political-communication.

22 Sam Stein, Jackie Kucinich, and Scott Bixby, "Trump Won't Rule Out Using Stolen Data in 2020 Campaign," *The Daily Beast,* February 21, 2019, https://www.thedailybeast.com/every-2020-candidate-but-trump-promises-no-stolen-data.

23 Sam Wineburg and Sarah McGrew, "Lateral Reading: Reading Less and Learning More When Evaluating Digital Information," *Stanford History Education Group Working Paper No. 2017-A1*, October 2017, http://dx.doi.org/10.2139/ssrn.3048994.

24 Gordon Pennycook and David Rand, "Who falls for fake news? The roles of bullshit receptivity, overclaiming, familiarity, and analytic thinking," *Journal of Personality* (2019): 1–16, https://doi.org/10.1111/jopy.12476.

25 Sergei M. Guriev and Daniel Treisman, "Informational Autocrats," July 2018, http://dx.doi.org/10.2139/ssrn.3208523.

26 To put it differently, Western democracies need to update *The Open Society and Its Enemies* for the age of digital globalization.

27 Henry John Farrell and Bruce Schneier, "Common-Knowledge Attacks on Democracy," *Berkman Klein Center Research Publication No. 2018-7,* October 2018, http://dx.doi.org/10.2139/ssrn.3273111.

28 See the following for an example of a comprehensive course at the college student level: https://webliteracy.pressbooks.com/.

29 European Commission, "A Multi-Dimensional Approach to Disinformation," *Report of the Independent High-Level Group on Fake News and Online Disinformation,* 2018, https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation, 27.

30 Andrew Guess, Jonathan Nagler, and Joshua Tucker, "Less than you think: Prevalence and predictors of fake news dissemination on Facebook," *Science Advances* 5, no. 1, 2019, https://advances.sciencemag.org/content/5/1/eaau4586.

CHAPTER SIX

1 Matt A. Vega, "The First Amendment Lost in Translation: Preventing Foreign Influence in U.S. Elections After Citizens United v. FEC," 44 Loy. L.A. L. Rev. 951, 2011, https://digitalcommons.lmu.edu/llr/vol44/iss3/3.

2 The conviction of Russian national Marina Butina for her activities to cultivate contacts with the American National Rifle Association is a most recent example. She was convicted in April 2019 for failing to register as a foreign agent under FARA.

3 Karen Yourish and Larry Buchanan, "Mueller Report Shows Depth of Connections Between Trump Campaign and Russians," *The New York Times,* April 19, 2019, https://www.nytimes.com/interactive/2019/01/26/us/politics/trump-contacts-russians-wikileaks.html.

4 Rosalind S. Helderman, Tom Hamburger, Kevin Uhrmacher, and John Muyskens, "The making of the Steele dossier," *The Washington Post,* February 6, 2018, https://www.washingtonpost.com/graphics/2018/politics/steele-timeline/?noredirect=on&utm_term=.c6e72506b3d9.

5 Rosalind S. Helderman and Spencer S. Hsu, "American political consultant admits foreign money was funneled to Trump inaugural," *The Washington Post,* September 1, 2018, https://www.washingtonpost.com/local/public-safety/washington-consultant-for-ukraine-party-set-to-plead-guilty-to-violating-lobbyist-disclosure-law/2018/08/31/172cf2c8-ad23-11e8-a8d7-0f63ab8b1370_story.html?noredirect=on&utm_term=.65ba62128243.

6 Jonathan Swan and Harper Neidig, "Trump campaign solicits illegal foreign donations despite warnings," *The Hill,* July 16, 2016, https://thehill.com/homenews/campaign/288031-trump-campaign-solicits-illegal-foreign-donations-despite-warnings.

CHAPTER SEVEN

1 Samuel C. Woolley and Philip N. Howard, "Computational Propaganda Worldwide: Executive Summary," *Oxford Internet Institute, Computational Propaganda Research Project,* http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf; Adrian Shahbaz, "Freedom on the Net 2018: The Rise of Digital Authoritarianism," *Freedom House*, https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism; David Wemer, "Has Progress Been Made in Containing Disinformation?" *Atlantic Council* April 28, 2019, https://www.atlanticcouncil.org/blogs/new-atlanticist/has-progress-been-made-in-containing-disinformation; and Matt Apuzzo and Adam Atarioano, "Hackers Sow Discord as Vote Looms in Europe," *New York Times*, 1.

2 "Cyber Norms Index," *Carnegie Endowment for International Peace,* https://carnegieendowment.org/publications/interactive/cybernorms.

3 Article 21: "The will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures." See "Universal Declaration of Human Rights," *United Nations,* https://www.un.org/en/universal-declaration-human-rights/index.html.

4 Article 1 assures self-determination to all peoples. Article 25 states in part: "Every citizen shall have the right and the opportunity, without any of the distinctions mentioned in Article 2 and without unreasonable restrictions:(a) To take part in the conduct of public affairs, directly or through freely chosen representatives; (b) To vote and to be elected at genuine periodic elections which shall be by universal and equal suffrage and shall be held by secret ballot, guaranteeing the free expression of the will of the electors." "Universal Declaration of Human Rights," *United Nations,* https://www.un.org/en/universal-declaration-human-rights/index.html.

5 Michael N. Schmitt, ed., *The Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013).

6 Michael N. Schmitt, ed., *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017).

7 "Aims and Priorities," *Freedom Online Coalition,* https://freedomonlinecoalition.com/about-us/about/.

8 A/HRC/RES/20/8: The promotion, protection and enjoyment of human rights on the Internet.

9 For example, these include the Global Commission on the Stability of Cyber Space and the Transatlantic Commission on Election Integrity.

10 Daniel Twining and Kenneth Wollak, "Russia's Nefarious Meddling is Nothing Like Democracy Assistance," *The Washington Post*, April 10, 2018, https://www.washingtonpost.com/opinions/russias-nefarious-meddling-is-nothing-like-democracy-assistance/2018/04/10/b8942f20-3ce2-11e8-a7d1-e4efec6389f0_story.html?utm_term=.4381b8f7a0e2.

11 Jack Goldsmith, "Uncomfortable Questions in the Wake of Russia Indictment 2.0 and Trump's Press Conference with Putin," *Lawfare,* July 16, 2018, https://www.lawfareblog.com/uncomfortable-questions-wake-russia-indictment-20-and-trumps-press-conference-putin.

12 Joshua Geltzer and Jake Sullivan, "How to Prevent the Next Election Disaster," *Politico*, January 22, 2019, https://www.politico.com/magazine/story/2019/01/22/prevent-election-disaster-224032.

13 "Warsaw Declaration: Toward a Community of Democracies," *Community of Democracies*, June 27, 2000, https://community-democracies.org/app/uploads/2017/02/2000-Warsaw-Declaration-ENG.pdf.

14 "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," *United Nations General Assembly,* July 22, 2015, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

15 "The Pledge for Election Integrity," *Alliance for Democracies: Transatlantic Commission on Election Integrity,* 2019, https://electionpledge.eu.

16 See "Universal Declaration of Human Rights".

17 "Norm Package Singapore," *Global Commission on the Stability of Cyberspace,* November 2018, https://cyberstability.org/wp-content/uploads/2018/11/GCSC-Singapore-Norm-Package-3MB.pdf.

18 Toomas Hendrik Ilves, "A Digital Defense Alliance," *Berlin Policy Journal,* January 10, 2018, https://berlinpolicyjournal.com/a-digital-defense-alliance.

CHAPTER EIGHT

1 See, for example, "Ukraine and Russia Sanctions," *U.S. Department of State*, https://www.state.gov/e/eb/tfs/spi/ukrainerussia/; "Ukraine-/Russia-related Sanctions," *U.S. Department of the Treasury,* https://www.treasury.gov/resource-center/sanctions/Programs/pages/ukraine.aspx. See also Executive Orders 13660, 13685, 13694, 13757, int. al. For sanctions legislation see Countering America's Adversaries Through Sanctions Act (CAATSA), PL 115-44; Ukraine Freedom Support Act of 2014 (UFSA); Support for the Sovereignty, Integrity, Democracy, and Economic Stability of Ukraine Act of 2014 (SSIDES); International Emergency Economic Powers Act (IEEPA), 50 U.S.C. §§ 1701-1706; National Emergencies Act (NEA), 50 U.S.C. §§ 1601-1651. For the most recent (as of publication) update to the list of "Specifically Designated Nationals" related to Russia sanctions by the U.S. Office of Foreign Assets Control (OFAC), see "Specifically Designated Nationals List Update," *U.S. Department of the Treasury, Office of Foreign Assets Control,* March 15, 2019, https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20190315.aspx.

2 In a press conference on April 19, 2019, Secretary of State Mike Pompeo responded to questions about the Special Counsel report saying, "We will make very clear to them [the Russians] that this is unacceptable behavior… We will take tough actions which raise the cost for Russian malign activities. And we will continue to do that" as quoted in "Mueller probe over, but little chance for US-Russia reconciliation," *Agence France-Presse (AFP) wire service*, April 19, 2019, https://www.france24.com/en/20190419-mueller-probe-over-but-litte-chance-us-russia-reconciliation. For a detailed listing of how Trump has described Putin and Russian meddling in the five years up to the July 2018 Helsinki Summit, see Erica R. Hendry, "The many different ways Trump has described Putin and Russian election interference," *PBS NewsHour*, July 16, 2018, https://www.pbs.org/newshour/politics/the-many-different-ways-trump-has-described-putin-and-russian-election-interference.

3 Specifically, referring to reports that U.S. Cyber Command "basically took the [St. Petersburg-based Russian Internet Research Agency] offline" during the day of the 2018 midterms. See Ellen Nakashima, "U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms," *The Washington Post*, February 27, 2019, https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.

4 With respect to deterring nation state malicious cyber actions more generally, see Christopher Painter, "Deterrence in cyberspace: Spare the costs, spoil the bad state actor: Deterrence in cyberspace requires consequences," *Australia Strategic Policy Institute, International Cyber Policy Centre Policy Paper*, 2018, https://www.aspi.org.au/report/deterrence-cyberspace.

5 The authors recognize the multiple forms of deterrence contained in the security literature, including deterrence by denial, entanglement, and norms, in addition to deterrence by cost-imposition (often called punishment.) We emphasize here only the last form of deterrence. What constitutes in effect these other aspects of deterrence are addressed in other chapters of this paper, especially those on election infrastructure security and international norms.

6 Eric Schmitt, David E. Sanger, and Maggie Haberman, "In Push for 2020 Election Security, Top Official Was Warned: Don't Tell Trump," *The New York Times*, April 24, 2019, https://www.nytimes.com/2019/04/24/us/politics/russia-2020-election-trump.html.

7 See Bernard Brodie, *Strategy in the Missile Age* (Princeton University Press, 1959); Thomas Schelling, *The Strategy of Conflict* (Harvard University Press, 1960); and Herman Kahn, *On Thermonuclear War* (Princeton University Press, 1960), among additional literature.

8 More recent work since the end of the Cold War, drawing on findings from cognitive psychology such as Tversky and Kahneman's work on prospect theory, has shown how cognitive biases inhibit rational decision-making. For example, loss-aversion (or defense of perceived status-quo) has been found more likely to lead to conflict than otherwise rationally-equivalent gain-seeking. See Robert Jervis, "Political Implications of Loss Aversion," *Political Psychology* 13, no. 2, June 1992, 187-204, https://www.researchgate.net/publication/271785014_Political_Implications_of_Loss_Aversion.

9 "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World," *The White House*, May 2011, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. See also Christopher Painter, "International Cybersecurity Strategy: Deterring Foreign Threats and Building Global Cyber Norms," *U.S. Department of State,* May 25 2016, https://2009-2017.state.gov/s/cyberissues/releasesandremarks/257719.htm.

10 "Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats," *U.S. Department of State,* May 31, 2018, https://www.state.gov/s/cyberissues/eo13800/282011.htm.

11 Nakashima.

12 Renee DiResta, Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Jonathan Albright, and Ben Johnson, "The Tactics & Tropes of the Internet Research Agency," *New Knowledge*, 2018, https://www.newknowledge.com/articles/the-disinformation-report/.

13 The new Commander's vision of U.S. Cyber Command involves persistent engagement and defending forward. Under this direction, the new authorities have reportedly permitted U.S. Cyber Command to engage in certain offensive cyber operations under certain circumstances without direct White House approval. Nevertheless, advocates of these and similarly related changes have not yet publicly acknowledged that they entail additional cyber risk, compared to a strategy based on cyber restraint.

14 When the President undercuts the messaging, such as the current President casting doubt on whether Russia interfered with U.S. elections, that alone undercuts even the best efforts and actions of others in the government. Of course, no one can force a president to take a particular factual stand, and it may be that we will need to wait for a future president to robustly condemn Russia's actions, but tools such as mandatory sanctions help alleviate that issue.

15 "Defending Elections against Trolls from Enemy Regimes (DETER)" (S.2785), https://www.congress.gov/115/bills/s2785/BILLS-115s2785is.pdf.

16 "Recommendations to the President on Deterring Adversaries and Better Protecting the American People From Cyber Threats," *U.S. Department of State,* May 31, 2018.

17 Pursuant to its new deterrence initiative, the U.S. Department of State and the interagency are currently developing a list of potential consequences that provide a menu of options for responding to malicious state cyber conduct. In addition, the State Department is bringing in a range of U.S. allies and partners to discuss the program and considering ways to communicate warnings of potential consequences to adversaries in advance of an attack. Though admittedly difficult, this work should be completed as soon as possible.

18 To illustrate, sanctions for activities related to the situation in Ukraine (but unrelated to election interference) were undertaken by the Obama Administration in 2014. At that time, the following individuals were designated by the U.S. Treasury because each is controlled by, has acted for or on behalf of, or has provided material or other support to, a senior Russian government official: Gennady Timchenko (a founder of Gunvor, an independent commodity trading company involved in the oil and energy markets), Arkady Rotenberg and Boris Rotenberg (executors of contracts for the Sochi Olympic Games and Gazprom), and Yuri Kovalchuk (largest single shareholder of Bank Rossiya and personal banker for senior officials of the Russian Federation). Bank Rossiya (the personal bank for senior officials of the Russian Federation) was designated for the same reasons. Assets of designated entities within U.S. jurisdictions are frozen, and transactions by U.S. persons or within the United States involving designated individuals and entities are generally prohibited. See "Treasury Sanctions Russian Officials, Members of the Russian Leadership's Inner Circle, And An Entity For Involvement In The Situation In Ukraine," *U.S. Department of the Treasury,* March 20, 2014, https://www.treasury.gov/press-center/press-releases/Pages/jl23331.aspx.

19 The EU Cyber Diplomacy Toolbox that authorizes economic sanctions at the EU level for malicious cyber actions is a good example. See, for example, Erica Moret and Patryk Pawlak, "The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?" *European Union Institute for Security Studies*, July 2017, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2024%20Cyber%20sanctions.pdf.

20 For the outline of a comprehensive strategy for dealing with Russia today, see Michael McFaul, "Russia as It Is: A Grand Strategy for Confronting Putin," *Foreign Affairs* 97, no. 4, (July-August 2018), 82-91.

ABOUT THE AUTHORS

Allison Berke is Executive Director of the Stanford Cyber Initiative at the Freeman Spogli Institute for International Studies (FSI) at Stanford University, where she manages research, education, and outreach activities related to the secure integration of cyber technologies into society.

Larry Diamond is Principal Investigator of the Global Digital Policy Incubator (GDPi) at FSI's Cyber Policy Center; Senior Fellow at FSI; Senior Fellow at the Hoover Institution; and Professor, by courtesy, of Political Science and Sociology at Stanford University. He is founding co-editor of the Journal of Democracy and serves as Senior Consultant at the International Forum for Democratic Studies of the National Endowment for Democracy.

Eileen Donahoe is Executive Director of GDPi, former U.S. Ambassador to the United Nations Human Rights Council in Geneva, and former Director of Global Affairs at Human Rights Watch. Eileen is a member of the Board of Directors of the National Endowment for Democracy; the World Economic Forum Council on Digital Economy and Society; the University of Essex Advisory Board on Human Rights, Big Data and Technology; the Dartmouth College Board of Trustees, and the Council on Foreign Relations. She is a Distinguished Fellow at the Center for International Governance Innovation.

Andrew Grotto is Director of the Cyber Policy Center's Program on Geopolitics, Technology, and Governance; a William J. Perry International Security Fellow at CISAC at FSI; and a Research Fellow at the Hoover Institution. Prior to Stanford, Grotto was the Senior Director for Cybersecurity Policy at the White House in both the Obama and Trump administrations, where he served as a principal architect of President Obama's Cybersecurity National Action Plan and President Trump's cybersecurity executive order, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure".

Toomas Ilves is a GPDi Fellow, Distinguished Visiting Fellow at the Hoover Institution, and Berggruen Fellow at the Center for Advanced Studies in the Behavioral Sciences at Stanford University. He was elected President of the Republic of Estonia in 2006 and re-elected for a second term in 2011, during which he was appointed to serve in several high positions in the field of ICT in the European Union. He served as chairman of the EU Task Force on eHealth from 2011 to 2012 and chairman of the European Cloud Partnership Steering Board from 2012 to 2014. From 2014 to 2015, he was the co-chair of the advisory panel of the World Bank's World Development Report 2016 "Digital Dividends" and chair of the World Economic Forum's Global Agenda Council on Cyber Security beginning in June 2014.

Bronte Kass is the Program Manager for FSI Director Michael McFaul at Stanford University.

Zachary Krowitz is a Research Assistant for Professor Nate Persily and student at Stanford Law School.

Herbert Lin is a Senior Research Scholar at CISAC; Hank J. Holland Fellow in Cyber Policy and Security at the Hoover Institution; and former Chief Scientist of the Computer Science and Telecommunications Board, National Research Council of the National Academies. He is also an Adjunct Senior Research Scholar and Senior Fellow in Cybersecurity at the Saltzman Institute for War and Peace Studies in the School for International and Public Affairs at Columbia University, a member of the Science and Security Board of the Bulletin of Atomic Scientists, and a member of the Aspen Institute Cybersecurity Group.

Michael McFaul is the Director of FSI; the Ken Olivier and Angela Nomellini Professor of International Studies, Department of Political Science; and Peter and Helen Bing Senior Fellow at the Hoover Institution, all at Stanford University. He also works as an analyst for NBC News and writes a monthly column for The Washington Post. He served five years in the Obama administration, first as Special Assistant to the President and Senior Director for Russian and Eurasian Affairs at the National Security Council at the White House from 2009-12), and then as U.S. Ambassador to the Russian Federation from 2012-14. He has authored several books, including most recently The New York Times bestseller From Cold War to Hot Peace: An American Ambassador in Putin's Russia (2018).

Megan Metzger is a Research Scholar at FSI and Associate Director for Research at GDPi at Stanford University.

Chris Painter is a William J. Perry Fellow at FSI, Commissioner on the Global Commission for the Stability of Cyberspace, former Coordinator for Cyber Issues for the Department of State, and former White House Senior Director for Cybersecurity Policy. He was named the Bartels World Affairs Fellow for 2017-18 by Cornell University and awarded the Order of the Rising Sun in 2018 by the Government of Japan for promoting Japan-U.S. Cyber collaboration.

Nate Persily is Co-Director of the Cyber Policy Center; Senior Fellow at FSI; James B. McClatchy Professor of Law at Stanford Law School; and Professor, by courtesy, of Communication and Political Science. He is co-author of the leading election law casebook, The Law of Democracy (2016). He has served as the Research Director of the Presidential Commission on Election Administration, as a court-appointed Special Master for the redistricting process in numerous states, and on the National Academy of Sciences Committee on The Future of Voting. In recognition of his current work examining the impact of changing technology on political communication, campaigns, and election administration, he has been honored as an Andrew Carnegie Fellow, a Fellow at the Center for Advanced Study in the Behavioral Sciences, and as a commissioner on the Kofi Annan Commission on Elections and Democracy in the Digital Age.

Sergey Sanovich is a Cyber Postdoctoral Fellow at CISAC at Stanford University. His report, commissioned by the Oxford Internet Institute, on the domestic origins of Russian government's disinformation campaigns abroad was published in an Oxford University Press volume on computational propaganda in November 2018.

Alex Stamos is Director of the Cyber Policy Center's Internet Observatory, an Adjunct Professor at FSI, and a visiting scholar at the Hoover Institution. Prior to joining Stanford, Alex served as the Chief Security Officer of Facebook, where he led the company's investigation into manipulation of the 2016 U.S. presidential election and helped pioneer several successful protections against these new classes of abuse. In April 2017, he co-authored "Information Operations and Facebook", a highly cited examination of the influence campaign against the U.S. election.

ABOUT THE STANFORD CYBER POLICY CENTER

The **Stanford Cyber Policy Center** at the Freeman Spogli Institute is Stanford University's premier center for the interdisciplinary study of issues at the nexus of technology, governance, and public policy. Through research, policy engagement, and teaching, the Stanford Cyber Policy Center seeks to bring cutting-edge insights and solutions to national governments, international institutions, and industry with its four principal programs. Professors Dan Boneh and Nate Persily are co-directors of the Center.

1. The **Global Digital Policy Incubator** (GDPi) is a multi-stakeholder collaboration hub for the development of norms and policies to protect human rights, civic space, and democratic processes in digital society. GDPi evaluates the human-rights impacts of digital technologies themselves, as well as the impacts of policy and regulatory responses to technology, with particular emphasis on risks to free expression, privacy, security, and democratic engagement. Larry Diamond and Eileen Donahoe are co-directors of this program.

2. The **Program on Geopolitics, Technology, and Governance** (GTG) is dedicated to world-class scholarly and policy-oriented research on the political, legal, and economic implications of digital innovation and global competition. Andrew Grotto is director of this program.

3. The **Stanford Internet Observatory** is a cross-disciplinary program of research, teaching, and policy engagement for the study of abuse in current information technologies, with a focus on social media. In addition, the Observatory was created to develop a novel curriculum on trust and safety that is a first in computer science, and to translate research discoveries into training and policy innovations for the public good. Alex Stamos is director of this program.

4. The **Program on Democracy and the Internet** (PDI) produces research, hosts events and convenings, and teaches current and future leaders about the challenges that new technologies pose to democracy in the digital age. PDI seeks to establish and survey this new field of digital democracy, setting forth what is known and what needs to be discovered, in order to evaluate and promote public, private, and civil society policy responses to address these trends and challenges. Francis Fukuyama, Nate Persily, and Rob Reich are co-directors of this program.

ABOUT THE FREEMAN SPOGLI INSTITUTE FOR INTERNATIONAL STUDIES

The Freeman Spogli Institute for International Studies (FSI) is Stanford University's premier research institute for the study of international affairs. Our Mission is threefold:

1. **Produce world-class, world-wide research** – With 50 appointed faculty, FSI is a hub for Stanford scholars who conduct research across multiple disciplines with an international impact. With a diverse group of seven research centers and 50 programs dedicated to deep investigation of critical global issues, our research topics include governance, security, health, energy, international development, and cyber policy.

2. **Teach and train tomorrow's leaders** – Each year, we educate dozens of graduate students and hundreds of undergraduates in both traditional and innovative ways. Our faculty teach over 65 classes a year and mentor students through guided research. FSI is also home to the Ford Dorsey Master's in International Policy, a two-year master's degree.

3. **Engage policymakers** – Our work provides context for decision-making in Washington, Geneva, Beijing and beyond. FSI's International Policy Lab ensures our research has real-world impact.

In addition to the new Cyber Policy Center, FSI has six research centers that serve as the focal points for the institute's activities:

- The **Center on Democracy, Development and the Rule of Law** (CDDRL) is dedicated to the study of the political and economic institutions that constitute modern liberal democracy. CDDRL's mission is to understand how countries can overcome poverty, instability and abusive rule to become well-governed states. CDDRL's work spans the globe and bridges the divide between academic research and policy analysis, forging partnerships not only with other research centers, but also with international development agencies, governments, and civil society organizations in numerous countries.

- The **Center on Food Security and the Environment** (FSE) is a joint effort of FSI and the Stanford Woods Institute for the Environment. With the goal of designing new approaches to solving global hunger and environmental degradation, FSE is building an evolving research portfolio with a team of experts in scientific, economic, and policy areas that are critical to global food security, such as adapting to climate change, managing aquaculture, raising smallholder farm productivity, and leveraging big data.

- The **Center for International Security and Cooperation** (CISAC) contributes to world peace by addressing critical security challenges, including cybersecurity, nuclear security, biotechnology, and counterterrorism. CISAC is dedicated to world-class teaching, research, and policy impact by training the next generation of scholars and policymakers through an undergraduate honors program, a fellowship program for military service members, and pre- and post-doctoral research opportunities.
- The **Europe Center** (TEC) promotes interdisciplinary research and teaching on Europe and its role in the world. By supporting scholarly and policy dialogue across nearly all of Stanford's schools, TEC serves as a hub for the study of Europe and global affairs.
- **Stanford Health Policy** (SHP) is devoted to improving healthcare and well-being through improved policy worldwide. SHP comprises research groups within FSI and the Stanford University School of Medicine, a worldwide leader in biomedical innovation, research, and precision medicine. The dual affiliation provides access to researchers who span engineering, medicine, and the social sciences—from pediatrics to geriatrics, politics and law, economics, population health, and decision science.
- The **Walter H. Shorenstein Asia-Pacific Research Center** (APARC) focuses on the interdisciplinary study of contemporary Asia, illuminating policy issues critical to both Asia and the United States. Established in 1983, Shorenstein APARC produces outstanding research, educates the next generation of scholars and policymakers, promotes constructive interaction in the pursuit of influencing U.S. policy toward the Asia-Pacific region, and contributes to Asian nations' understanding of issues key to regional cooperation and to their relations with the United States.

DESIGN: ALEXANDER ATKINS DESIGN, INC.

The **Stanford Cyber Policy Center** at the Freeman Spogli Institute for International Studies is Stanford University's premier center for the interdisciplinary study of issues at the nexus of technology, governance, and public policy. Program areas address topics including cybersecurity, election security, misinformation, digital democracy and human rights, artificial intelligence, and emerging technologies. Through research, policy engagement, and teaching, the Cyber Policy Center seeks to bring cutting-edge insights and solutions to national governments, international institutions, and industry.

Stanford | Cyber Policy Center
Freeman Spogli Institute

Encina Hall
616 Serra Mall C100
Stanford University
Stanford, CA 94305-6055
650.723.4581

fsi.stanford.edu/cyber **stanford-cyber@stanford.edu** **Stanford_Cyber**