CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

RUSSIAN ELECTION INTERFERENCE

Europe's Counter to Fake News and Cyber Attacks

Erik Brattberg and Tim Maurer

MAY 2018

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

RUSSIAN ELECTION INTERFERENCE

Europe’s Counter to Fake News and Cyber Attacks

Erik Brattberg and Tim Maurer

© 2018 Carnegie Endowment for International Peace. All rights reserved.

Carnegie does not take institutional positions on public policy issues; the views represented herein are the authors' own and do not necessarily reflect the views of Carnegie, its staff, or its trustees.

No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Carnegie Endowment. Please direct inquiries to:

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue, NW
Washington, DC 20036
P: +1 202 483 7600
F: +1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost
at CarnegieEndowment.org/pubs.

CP 333

Contents

About the Authors

Erik Brattberg is the director of the Europe Program and a fellow at the Carnegie Endowment for International Peace. He is an expert on European politics and security and transatlantic relations.

Tim Maurer, co-director of the Cyber Policy Initiative, is a fellow at the Carnegie Endowment for International Peace. Since 2010, his work has centered on cybersecurity, human rights in the digital age, and internet governance. His current focus is on cybersecurity and financial stability.

***

The authors thank Thomas Carothers and George Perkovich for their close review of the draft paper and incisive feedback and suggestions. Gratitude also goes to Etienne Soula and Viola Meyerweissflog who provided valuable research assistance and to several other individuals who contributed helpful input throughout the research and writing processes.

Carnegie's Europe Program and Cyber Policy Initiative thank the Hewlett Foundation for its support, which helped make this project possible.

Summary

Russia's aggressive campaign targeting the 2016 U.S. election revealed not only the extent to which information and communications technologies are being used to undermine democratic processes but also the weaknesses of protection measures. The U.S. government was effectively caught off guard, once again highlighting that such interference presents a rising global threat. Comprehensive strategies and tools are clearly needed as part of a long-term, holistic approach to building resilience, but to be effective, they should be informed by the regular sharing of best practices and lessons learned between countries.

In reaction to Russia's disruptive campaigns in Europe and the United States, European governments took steps before and during their 2017 elections to better protect against disinformation campaigns and cyber attacks. Unsurprisingly, an examination of their efforts shows the importance of identifying risks at the local, regional, and national levels and actively engaging political parties and traditional and social media outlets. These lessons and others could provide the basis for a common, analytical framework to assess the different dimensions of risk and guide countries' preparatory actions.

Lessons From European Efforts

- Consider electoral systems as part of critical infrastructure, institutionalize preparations to protect election processes, and broaden activities to the subnational levels.
- Focus on resilience measures, for example, by conducting regular vulnerability analyses and developing contingency plans. Legal measures should be explored through an inclusive process.
- Issue public statements to deter threat actors and educate voters about disinformation campaigns.
- Train and educate political parties and campaigns to better protect against potential interference.

- Conduct government-media dialogue, encourage media to take voluntary protective measures, and engage social media companies in mitigating potential threats.
- Support international cooperation, particularly the sharing of lessons learned and best practices.

Preparing for the 2018 U.S. Midterm Elections

- Issue a clear warning that interference in the 2018 elections by Russia or any other actor will result in severe consequences.
- Coordinate government efforts to protect against cyber attacks and disinformation.
- Provide more training and support to state and local election officials.
- Regularly assess election infrastructure.
- Encourage states to reevaluate the use of electronic voting machines.
- Encourage political parties and their candidates, staff, and volunteers to follow basic cybersecurity practices.
- Encourage donors to require that political parties and campaigns implement basic cyber hygiene for their candidates, staff, and volunteers.
- Urge political parties and campaigns to explicitly state that they will not use or support social media bots.
- Increase society's resilience by clearly communicating the risks of foreign interference in U.S. democracy.
- Promote independent citizen fact-checking and investigative journalistic initiatives.
- Improve media literacy among the public.

Introduction

In 2016, Moscow brought a threat that has long plagued many Central and Eastern European capitals to the heart of Washington, DC. Russia hacked the U.S. Democratic National Committee's system and subsequently released the confidential material to the public in a clear attempt to influence the outcome of the 2016 U.S. presidential election.[1] The cyber attack was paired with a disinformation campaign whose scope and reach is still being assessed more than a year later. The administration of then president Barack Obama was certainly concerned about potential hacking—especially given the malware attack during Ukraine's 2014 presidential election—but all evidence to date suggests that the Russian government achieved significant success without actually hacking election infrastructure. The U.S. government was essentially caught off guard.

After witnessing the events in the United States, a number of European leaders scrambled to protect their countries against similar interference in their 2017 elections. Some of their actions appear to have been successful, but given the urgency, they were likely hindered by ad hoc coordination and knowledge sharing. Systematically studying these efforts and others could proactively help to inform the development of long-term strategies and tools to improve countries' resilience to future attacks. More importantly, such analysis could pave the way for sharing lessons learned and best practices across countries—an urgent effort considering that, in 2018 alone, elections will take place in Georgia, Latvia, Sweden, Brazil, and Mexico, among others. And in 2019, elections to the European Parliament will occur. Looking ahead to the November 2018 U.S. midterm elections and the next presidential election in 2020, U.S. officials are particularly worried about further meddling. According to U.S. Director for National Intelligence Daniel Coats, "there should be no doubt that Russia perceives its past efforts as successful and views the 2018 U.S. midterm elections as a potential target."[2] So as the United States and other countries ponder how to better prepare for interference,[3] what can be drawn from Europe's recent experiences?

Systematically studying these [Europe's] efforts and others could proactively help to inform the development of long-term strategies and tools to improve countries' resilience to future attacks.

An examination of the protection measures that Germany, France, the Netherlands, and the United Kingdom enacted in 2017 and prior offers a good starting point for assessing the dimensions of risk and the effectiveness of preparations for, and responses to, election interference. These countries are geopolitically important within Europe as well as with regard to Russia. Their specific experiences are also useful to compare. The hacking of French President Emmanuel Macron's campaign during the presidential election arguably stands out as the Kremlin's most brazen action. The elections in Germany, on the other hand, are remarkable because no significant attempts at interference were reported. The events of the past year and a half merit a closer look to determine what actually happened and why. Sweden, which will hold elections in September 2018, is also worth including, as it offers potential insights into how a country can prepare well ahead of time to protect its elections.

When studying Russian interference and country preparations and responses, it is important to differentiate between "fake news" and hacking operations. This ensures that the full range of vulnerable targets are accounted for—including the databases of political parties and campaigns, social media platforms and conventional news organizations, the personal accounts of candidates and their families, voter registration systems, voting machines and software, and transmission channels for voting results. Thus far, based on open-source information, government tools to protect such targets have largely included operational and policy changes, such as the banning of electronic vote counting; technical changes to election infrastructure; legal measures, such as new laws; and awareness-raising campaigns.

However, eliciting best practices—and, more importantly, a long-term, holistic approach to interference—cannot come from merely studying these targets and tools in isolation. And doing so would not be conducive to ongoing, systematic knowledge sharing. Thus, it could be helpful to combine their general dimensions within an analytical framework—to inform both future strategies and more in-depth research. Drawing on the experiences of Central and Eastern European countries in recent years and the United States during the 2016 election, a framework begins to take shape. It conceptualizes the different risk dimensions of disinformation campaigns and hacking operations, places them in the context of an election cycle, and lists the types of preparatory actions governments can take at all levels. Stakeholders in the United States and other countries could further develop this framework, perhaps as part of an internationally coordinated effort. Meanwhile, lessons learned and best practices garnered from case studies could inform stronger legal, technical, operational, policy, civil society, and educational measures against likely interference perpetrated by Russia and other actors.

Five European Experiences With Russian Election Interference

Netherlands: General Elections, March 2017

Following warnings from Dutch intelligence, officials in the Netherlands took the issue of potential Russian interference in its elections seriously. But because of either their active preparations or an apparent lack of Russian effort at interference, the elections were carried out successfully and without any noteworthy interference.

Preparatory Actions

Reports of Russian activities during the U.S. election placed The Hague on high alert. It was already concerned about potential interference due to two major incidents: the alleged hacking of the Dutch Safety Board's computers in October 2015 by a group of Russian hackers known as Pawn Storm (also known as APT28 and Fancy Bear) and the alleged meddling leading up to the April 2016 Dutch referendum on a European Union (EU)–Ukraine trade deal by either Netherlands-based, pro-Russian sympathizers or activists.[4] The timing of the former incident made the objective clear: it occurred both before and after the board published its report investigating the downing of flight MH17 in eastern Ukraine. Despite the apparent failure, Moscow's activities had a significant impact. Local pro-Russian voices in the Netherlands actively tried to counter the hacking accusations.[5]

Interference leading up to the referendum was perhaps more blatant. The Kremlin was vehemently against the EU-Ukraine trade deal. A consortium of local pro-Russian, anti-Ukraine expats—led by a left-wing Dutch parliamentarian, Harry van Bommel—vocally opposed the deal and referred to Ukraine's pro-Western government as a "bloodthirsty kleptocracy."[6] The opposition used in-person meetings, television, and social media to echo their views. In addition, pro-Russian agents passed themselves off as Ukrainians to infiltrate town hall meetings and Dutch groups akin to U.S. political action committees, such as the conservative Forum for Democracy, which became a major political party in 2016.[7] During the referendum, the party repeated the Kremlin's talking points and shared Moscow's propaganda videos.[8]

Of course, Russian interference was not the only factor that influenced the referendum; the referendum also reflected the Dutch population's growing antipathy toward the EU.[9] The Hague has been particularly concerned about the more amorphous threat of local populists who, knowingly or unknowingly, champion Russia's agenda in their attempts to disrupt the political status quo.

The fact that the General Intelligence and Security Service (AIVD) began surveilling the Russian hacking group Cozy Bear in mid-2014 and alerted U.S. officials to its activities in 2016 reveals just how seriously the Netherlands was taking the threat of interference.[10] Notably, the agency was able to corroborate the U.S. Democratic National Committee hack because it was monitoring Russian activities in the aftermath of the Dutch Safety Board hack and interference in the EU-Ukraine referendum.

In its 2016 annual report, the AIVD highlighted an increase in Russian influence operations targeting the country's economic, political, scientific, and defense sectors.[11] The report specifically cites cyber attacks, attempted recruitments of human intelligence, espionage, false flag operations, and the manipulation of public opinion.[12] It states that "the dissemination of disinformation and propaganda plays an important role in clandestine political influence." It also attributes an attack against 100 government email accounts to Russian activity. Dutch intelligence officers openly assert that Russians have persistently tried to "penetrate the computers of government agencies and businesses."[13]

The Dutch government took several measures to protect against potential Russian interference ahead of its March 2017 elections. Electronic voting was banned in the Netherlands in 2007 to ensure the public's trust in the democratic process, but the government felt that additional steps were necessary after receiving reports of software-related vulnerabilities. Fearing that Russia would attempt to hack into vote counting technology, it decided to ban the electronic counting of ballots and election officials' use of USB flash drives and email.[14] The Dutch interior minister was particularly concerned about the technology's outdated software but also wanted to enhance public confidence so that "not a shadow of doubt should hang over the results."[15] Further contributing to the government's decision were rumors that Russia was looking to hack other elections after the 2016 U.S. election.[16] During a visit in Washington, DC, in January 2017, then Dutch foreign affairs minister Bert Koenders met with U.S. officials to discuss any specific information pertaining to potential Russian cyber attacks against the Netherlands. While it is unclear whether any such information was exchanged, the trip is evidence of the seriousness the Dutch government ascribed to the issue of Russian meddling.

Fearing that Russia would attempt to hack into vote counting technology, it [the Netherlands] decided to ban the electronic counting of ballots and election officials' use of USB flash drives and email.

In addition to the bans, the government made efforts to raise public awareness of Moscow's persistent efforts to infiltrate domestic and international governments, disrupt the political process, and influence policymaking by acquiring clandestine information through cyber espionage and human-acquired intelligence. These efforts also aimed to sensitize the Dutch public to disinformation and alternative facts by highlighting and discrediting troll-manufactured videos and by sharing forensic evidence that linked social media feeds by activists to Russian media outlets.[17]

Social media companies also took action ahead of the March 2017 elections. Facebook announced that it would introduce a fact-checking function to newspaper articles in the Netherlands.[18] However, in the Netherlands, mainstream media outlets continue to have a much stronger foothold than tabloids, overtly partisan news outlets, and social media companies. Consequently, there was already a significant baseline against which disinformation and alternative facts could be benchmarked.

Still, the Netherlands' preparations had some shortcomings. Efforts to train politicians and government officials—carried out by The Hague Security Delta and other groups—generated little interest. In addition, according to information technology (IT) experts, Dutch political parties did not take sufficient steps to protect their websites prior to the elections.[19]

Notable Interference

According to the AIVD, Russia was not able to "substantially influence" the 2017 election process; its interference was mostly contained to spreading false information in the public debate.[20] The Netherlands was therefore spared another high-profile incident.

One reason for the limited interference might be the increased attention given to the issue by Dutch officials in recent years and the commensurate efforts to enhance preparedness—such as removing electronic counting of ballots—which denied Russia any opportunity to meddle. Moscow may also have been wary of further inflaming public opinion in a country where nearly 200 Dutch nationals were killed by Russian-backed rebels in the MH17 incident in Ukraine. Another reason could be that Russia values its relationship with the Netherlands, which is a major trading partner, and did not want to sow tension with Dutch leaders, especially after the MH17 incident.

Post-Election Responses

To further ensure the availability of reliable information during elections and referenda, Kajsa Ollongren, minister of the interior and kingdom relations, launched a dialogue with representatives of social media and technology companies to discuss the dissemination of fake news. As a result, Facebook partnered with Leiden University and a Dutch news website called Nieuwscheckers to fact-check news shared on social media. The website employs Google's fact-checking feature,[21] Google Project Shield, which, incidentally, helped protect a popular Dutch voting-information website, Kieskompas, from a distributed denial of service (DDoS) attack during the days leading up to the March 2017 election.[22]

The government has also taken steps to strengthen Europe's collective efforts. It is considering more Dutch support for the East StratCom Task Force, part of the European External Action Service, and is advocating more dialogue between the EU and North Atlantic Treaty Organization (NATO) on countering disinformation.

Conclusions

Russian interference surrounding the Dutch EU-Ukraine trade referendum, combined with the reports of Russian interference in the 2016 U.S. elections, led Dutch officials to boost their efforts to safeguard the March 2017 elections. They took significant steps to strengthen the resilience of their electoral processes and systems. That being said, Russian influence is still at work in the Netherlands, and Dutch officials need to expand their efforts to include training politicians and protecting political parties. The Forum for Democracy party now wants a referendum on remaining in the EU and is polling in second place in the Netherlands.[23] Moreover, Geert Wilders' Freedom Party, an anti-immigration and euroskeptic party, has historically been closely aligned with Russian interests in the European Parliament and is advocating the lifting of the EU's "anti-Russian sanctions."[24]

Dutch officials need to expand their efforts to include training politicians and protecting political parties.

France: Presidential Election, May–June 2017

Russia's attempts at election interference in 2017 were perhaps the most brazen in France. While French security officials made admirable efforts to protect against interference, what is more remarkable are the significant preparations made at the party level, in particular by En Marche, the prime target for suspected Russian interference during the campaign.

Preparatory Actions

First, it is worth nothing that France has a highly centralized political system and thus has less built-in resilience to interference than other more decentralized systems. The French president is elected directly by voters, but the election occurs in two rounds. In the first round, every candidate who manages to obtain the signature of 500 elected officials is allowed to run. Unless one single candidate receives a majority of votes, the two candidates who obtain the most votes at the end of the first round then face off in the second round.

In October 2016, after learning about Russia's hacking of the U.S. Democratic National Committee and the subsequent information leaks, the head of the French Prime Minister's General Secretariat for Defense and National Security, Louis Gautier, wrote a letter to the leaders of the main political parties warning them against the risk of "sophisticated and repeated attacks, obviously carried out by organized groups."[25] To learn about recent cyber attacks and garner some security advice, he also invited all major parties to attend a closed briefing with the National Cybersecurity Agency of France (ANSSI). The agency provided them with a thirty-six-page cyber security handbook, a fifty-two-page primer on DDoS attacks, and a USB flash drive with additional information. Tellingly, Marine Le Pen's right-wing National Front party was the only one absent from the briefing.

In addition, other high-level government officials publically and emphatically stated that they would not tolerate Moscow's attempts to disrupt the country's democratic process. In February 2017, then French foreign minister Jean-Marc Ayrault strongly implied that Russia was behind the cyber attacks plaguing Emmanuel Macron's presidential campaign and warned that Paris would not accept "any interference in its electoral process."[26]

ANSSI's preparatory activities focused mainly on protecting election infrastructure. Following a systems vulnerability assessment, and contrary to initial plans, the agency announced that electronic voting—banned in France since 2012, with an exception for French overseas voters—would not be permitted at all in the June 2017 legislative elections. In addition, the agency gave parties a list of approved independent experts who could inspect and test their cyber infrastructure on-site. Individual parties have their own structures in place, and both conservative Republicans and center-left Socialists have their own dedicated IT teams.[27] The IT team for Macron's En Marche party developed unorthodox methods to confuse detected attackers: the policy was to "flood [phishing email] with multiple passwords and log-ins, true ones, false ones, so the people behind them [the attacks] use up a lot of time trying to figure them out."[28]

Preparations against disinformation campaigns were more ad hoc; government agencies did not appear to make a centralized effort to guard against them. Macron's IT team developed a system to feed attackers with bogus information to preemptively degrade the value that might be derived from leaked campaign documents. Macron also enlisted an "anti-fake news commando" team of three lawyers to actively stem the barrage of disinformation aimed against him.[29]

Macron's IT team developed a system to feed attackers with bogus information to preemptively degrade the value that might be derived from leaked campaign documents.

Media outlets also took proactive measures to counter disinformation campaigns. In February 2017, *Le Monde*, a prominent French newspaper, published an index that referenced hundreds of websites and their level of reliability.[30] Google partnered with more than thirty media outlets, including main newspapers and television stations, to build the CrossCheck fact-checking platform.[31]

Notable Interference

Malicious cyber activity during the 2017 presidential election was concentrated almost exclusively on Macron's campaign. His team first reported that it had been hacked in October 2016 but declined to give details about the nature of the attacker.[32] Facebook confirms that Russian agents set up twelve fake accounts and posed as acquaintances of people close to Macron in attempt to glean intelligence.[33] In addition, spear-phishing emails under the guise of a fake Microsoft storage website attempted to glean passwords and login data from staff members. One and a half days before the runoff vote between Macron and Le Pen on May 7, 2017, 9 gigabytes of stolen files and 21,000 emails were uploaded to the platform Pastebin under the username EMLEAKS. In late July, WikiLeaks republished the emails in a searchable cache.[34] Using the hashtag "#MacronLeaks," the leaks then spread rapidly on social media, becoming a worldwide trending topic.

In January 2017, the security firm Trend Micro attributed many initial phishing attacks to Pawn Storm, also known as APT28 or Fancy Bear. U.S. intelligence agencies consider the group an instrument of Russia's Main Intelligence Directorate (GRU) and believe it is responsible for the Democratic National Committee hack.[35] Prior to the leaks, then U.S. National Security Agency director Mike Rogers informed French counterparts that the agency had detected possible Russian hacking of France's election infrastructure.[36] Yet, despite similarities between the Macron campaign attackers and Pawn Storm, ANSSI declined to name Russia directly because the attackers could have intentionally passed themselves off as somebody else.[37] Indeed, some analysts have remarked that the Cyrillic metadata and appearances of the name Roshka Georgiy Petrovich, a supposed employee contracted by Russian intelligence, are almost too numerous when contrasted with the sparsity of evidence found in other Russian attacks.[38] That being said, Russia's surprising brazenness was clearly evident in 2016, and some believed the goal was to maintain a climate of uncertainty over the vote.[39] Macron's campaign maintains that "hundreds if not thousands of attacks" against their systems—though presumably not all of them successful—originated from inside Russia or its vicinity.[40]

Researchers from the Oxford Internet Institute estimate that junk news (propaganda and hyperpartisan news and false reporting) accounted for a relatively small percentage of the election-related content shared on Twitter in March 2017, about two months before the first round of votes.[41] Many of the most influential rumors targeted Macron, although some also pertained to early candidates François Fillon, Jean-Luc Mélenchon, and Alain Juppé. Macron was the only one who was unequivocally critical of Vladimir Putin's Russia.[42] In contrast, Le Pen's National Front party received direct financial assistance from a Kremlin-affiliated bank,[43] Fillon was spoken of fondly by Putin and advocated for the lifting of sanctions,[44] and Mélenchon wanted France to exit NATO and voiced support for Russia's interventions in Syria and Ukraine.[45] While many of the rumors about Macron were no doubt homegrown among France's far right, others originated overseas.

Interestingly, some rumors and memes appeared to come from U.S. Twitter users.[46] Sputnik France and RT France were highly active on Twitter during the lead-up to the election, and an analysis of their coverage by the Atlantic Council's Digital Forensics Research Lab reveals a strong bias against Macron.[47] Reputatio Lab, a French social media monitoring firm, estimates that RT's French election coverage reached roughly 145,000 individuals.[48] Among the conspiracies and narratives spread by Russian media about Macron were assertions that he is an agent for U.S. financial interests and secretly gay.[49] A network of hyperactive automated accounts (bots) expressing pro-Russian, anti-EU views helped to promote these stories, although it is not known whether these accounts originated in Russia.

Le Pen benefited from the most overt support out of Moscow. In addition to the loan her party received from a Russian bank, she met with Putin in the Kremlin in a photo op designed to reinforce her presidential allure.[50] That being said, the Kremlin hedged its bets and other pro-Russian candidates also benefitted from the Russian propaganda apparatus.[51] For instance, a sham study published by a Moscow-based consultancy declared Fillon the leading candidate. The study was loudly touted as being based on a reliable Sputnik poll, leading the French polling commission to swiftly denounce the Russian outlet.[52]

Post-Election Responses

The fallout of the En Marche documents leak—the most spectacular and overt incident during the election process—was limited by several factors. First, the Macron team launched its own influence campaign to reveal that some of the leaked documents were fakes.[53] This immediately discredited organizations such as WikiLeaks, which had prominently advertised the leaked cache. The fact that the candidate's team highlighted some of the fakes in record time supports the idea that they had planted the fakes themselves.[54] Second, existing French legislation limited public sharing of the documents considerably. French election rules prevent the media from quoting presidential candidates or their supporters within twenty-four hours of the vote.[55] The electoral commission also warned the media and the public at large that they could be prosecuted for publishing documents obtained in the attack.[56] The rule and the warning were largely heeded, and the majority of the French population did not see the documents.[57]

French election rules prevent the media from quoting presidential candidates or their supporters within twenty-four hours of the vote.

Another striking feature of France's response to Russian interference was the public, explicit reaction of government officials during and after the election. Outgoing president François Hollande openly warned Russia to let up its attacks on the Macron campaign, and, as a newly minted president, Macron squarely pointed the finger at Moscow. During the campaign, Macron banned RT and Sputnik from attending events organized at En Marche's headquarters.[58] And after his victory, he strongly criticized the Russian outlets at a joint press conference with Putin in Versailles.[59] In response to an RT journalist who complained about the restrictions put on her network, Macron unabashedly replied, "Russia Today [RT] and Sputnik were agents of influence and propaganda that spread falsehoods about me and my campaign."

In January 2018, Macron announced that his administration is working on a law to counter "fake news."[60] Despite concerns about free speech, there is widespread support for such legislation. Specific provisions of the law are still unclear, but the French minister for culture recently said that online platforms would be subjected to "new obligations" and that "manifestly false" information would be removed more promptly, especially during election periods.[61] Macron has also suggested that websites would have to declare who is funding them and that the law would be accompanied by a "strong action on media education."

Conclusions

Several key characteristics of France's political and social environment provide some fortuitous, built-in resilience to interference—particularly French citizens' long-standing trust of traditional media and general distrust of online media. Unlike in many other Western European countries, social media penetration is relatively low in France. According to Eurostat, of the French who regularly use the internet, less than half use social networks.[62] Similarly, among EU countries, France ranks second to last in the consumption of online news, and its population consumes it with a healthy degree of skepticism. A 2017 study found that 75 percent of the French people surveyed trust information from traditional media, while only 32 percent trust information from online media and only 25 percent trust information from social networks.[63] And it appears that their trust in traditional media is not misplaced. For example, the government's twenty-four-hour blackout rule was successful in containing the spread of the so-called "MacronLeaks" largely because of the traditional media's disciplined restraint.

The high level of cooperation in France among the state, political parties, and the media may be a model for others to emulate.

There are also some active measures that other democracies could adopt to stave off Russian interference. In particular, the high level of cooperation in France among the state, political parties, and the media may be a model for others to emulate. The government's transparent political strategy could also be useful. Once French authorities detected the attacks on its electoral system, they immediately issued clear public declarations and warnings. The Macron campaign followed suit by loudly declaring that they were the target of an organized interference campaign. This raised the stakes for the attackers considerably and mitigated the impact. The technical success underpinning the MacronLeaks was overshadowed by the political cost to Russia, and the French media and public were immediately suspicious of Russian efforts and saw the leak as an illegitimate effort to sway the election.

Of course, while robust, France's efforts are unlikely to dissuade further attacks. Just a few months after Macron was swept into the Élysée Palace, RT opened a new French channel in Paris.[64] How much influence this outlet will have on French public opinion is open to debate,[65] but its budget of 24 million euros is already one-third of leading French news channel BFM TV's budget. This implies that Moscow is intent on continuing at least some of its activities in France.[66]

United Kingdom: Snap Election, June 2017

Preparations for the British snap election focused primarily on protecting against cyber attacks rather than disinformation campaigns. While few Russian efforts to interfere were observed, the short time span between when British Prime Minister Theresa May announced the election and when it was held could have been an important factor. Russia has previously been accused of seeking to interfere with the Brexit and Scottish independence referenda.

Preparatory Actions

Theresa May announced the so-called snap election in April 2017. Her ostensible aim was to increase her party's majority in parliament and strengthen her hand in the Brexit negotiations with the EU. With the 2016 U.S. elections still on many minds, British authorities were keen to safeguard the integrity of the electoral process and moderate any attempts at interference. Before the snap election, Foreign Minister Boris Johnson warned that it was a "realistic possibility" that Russia would interfere.[67] U.S. Director of National Intelligence Daniel Coats concluded that the same kind of Russian "influence campaigns" were at work in the United Kingdom.[68]

Because British officials believed that the short time frame between the announcement and the election would limit Moscow's capacity to develop an elaborate scheme, they prioritized protecting election infrastructure over preparing for hostile disinformation campaigns. Nevertheless, the UK government kept a close eye on RT and Sputnik.

Learning from the U.S. Democratic National Committee hack and subsequent document leak, the UK's National Cyber Security Center (NCSC), part of the Government Communications Headquarters, reached out to British political parties to secure their systems. Many feared that campaign staff would be targeted by spear-phishing attackers attempting to obtain sensitive information.[69] The NCSC organized technical seminars for campaign staff,[70] released guidance material,[71] and made its experts available to assist political parties with cyber-related problems.[72] The United Kingdom has never allowed electronic voting, making interference with the vote more cumbersome. Moreover, local authorities in each district are responsible for organizing the vote, further complicating the task of would-be attackers. The

The UK's National Cyber Security Center (NCSC) . . . organized technical seminars for campaign staff, released guidance material, and made its experts available to assist political parties with cyber-related problems.

United Kingdom also has a parliamentary system where a party, or coalition, needs to control more than half of the country's 650 constituencies—each represented by one member of parliament—to govern.

Notable Interference

In February 2017, the NCSC's head stated that the United Kingdom had experienced at least 188 cyber attacks—dozens of them serious—during the previous three months.[73] Many were attributed to alleged Russian and Chinese attackers. However, with everyone on high alert, no overt disinformation campaign or cyber operation was detected during the snap election. According to Thomas Rid, a professor of strategic studies at Johns Hopkins University's School of Advance International Studies, the purpose of Russian hacking prior to the election was not to benefit a particular candidate but rather to sow distrust in democracy since there was "no need for Russian meddling"; following the Brexit vote, the situation in the United Kingdom was "already chaotic enough."[74]

It remains uncertain to what extent Russian influence campaigns played a role in the Brexit referendum. A study by two researchers from the University of Edinburgh highlighted that some of the Twitter accounts associated with the Internet Research Agency, a notorious troll factory in St. Petersburg, had posted over 3,000 tweets about Brexit.[75] Another team found that 150,000 accounts with various ties to Russia had turned their attention to Brexit in the run-up to the referendum.[76] And while the Kremlin publicly claimed to remain neutral on the matter,[77] Brexit coverage by state-funded RT and Sputnik was consistently pro-leave, with the euroskeptic politician Nigel Farage frequently appearing on the former.[78] Jeremy Corbyn, prior to becoming the leader of the Labor Party, also appeared several times as a guest on RT and has repeatedly voiced anti-American and anti-NATO sentiments.

The Digital, Culture, Media and Sport Committee in the House of Commons launched an investigation in September 2017 into Russia's use of social media during the [Brexit] referendum campaign.

Post-Election Responses

With British political actors still eager to get to the bottom of possible Russian interference in the Brexit vote, the Digital, Culture, Media and Sport Committee in the House of Commons launched an investigation in September 2017 into Russia's use of social media during the referendum campaign. Independently, the communications agency 89up conducted a study and published its findings in February 2018. It concludes that RT and Sputnik anti-EU articles "won the Twitter war" by ending up on far more feeds than statements made by more classic pro-leave groups.[79] In contrast, a report from the Oxford Internet Institute's Computational Propaganda Research Project found that Russian Twitter activity contributed relatively little to the overall Brexit conversation, Russian news content was not widely shared among Twitter users, and only a tiny portion of the YouTube content was of clear Russian origin, adding further uncertainty.[80] Regardless of the Twitter war's actual effect, Theresa May has openly accused Putin's government of "[planting] fake stories" to "sow discord in the West" and has warned, "We know what you are doing. And you will not succeed."[81] The executive director of the Government Communication Service made building "social media capability to deal quickly with disinformation" the body's second priority.[82] And, in January 2018, the British government decided to create a National Security Communications Unit. The full scope of its activities is currently unknown, but it will be "tasked with combating disinformation by state actors and others" and will report directly to the Cabinet Office.[83]

Conclusions

Russia's limited interference in the snap election can partly be attributed to British preparatory actions. As previously mentioned, the election's relatively short time frame was a key obstacle to the planning and execution of an effective disinformation campaign. However, the absence of a clear pro-Russian candidate may also have played a role in Russia's apparent inaction. The Brexit referendum was likely of much greater interest to Moscow given the opportunities to take advantage of polarizations and to influence the outcome. Investigations surrounding Brexit are still underway, and new evidence of interference continues to surface. The House of Commons has requested additional information from Facebook regarding its role in the Brexit campaign, an issue that is likely going to be even more sensitive following the recent Cambridge Analytica scandal.

In the United Kingdom, Russian media outlets are generally well established and are used to fuel discontent and division among regions. For example, as recently as November 2017, former Scottish National Party leader Alex Salmond announced that he would be hosting a talk show on RT.[84] With the majority of Scotland voting in favor of EU membership (after having voted to remain in the United Kingdom in a 2014 referendum), Moscow may have seen an opening to fuel the division. It is perhaps no coincidence that both Sputnik and Pravda International set up shop in Edinburgh in 2016.[85] Meanwhile, Russian cyber activities in critical British sectors show no sign of abating, suggesting that meddling in British politics and elections is likely to continue. The NCSC states that "Russian hackers attacked British media, telecoms, and energy companies" during 2017.[86]

Germany: Federal Elections, September 2017

The German federal elections were significant mostly because of the apparent absence of Russian interference despite previous alleged disinformation campaigns and cyber attacks against German government targets. Besides the government's active preparations, high-level officials' clear warnings to Russia against interfering likely served as an added deterrent.

Preparatory Actions

Similar to the Netherlands and the United Kingdom, Germany's concern was only heightened by Moscow's activities during the 2016 U.S. elections; the government was already on alert due to the high-profile hacks of the German Bundestag, Chancellor Angela Merkel's Christian Democratic Union (CDU) party, the Ministry of Finance, and the Ministry of Foreign Affairs.[87] All signs pointed to the threat actor APT28, also known as Fancy Bear or Pawn Storm, as the culprit of the 2015 Bundestag hack—the same malicious actor responsible for hacking Macron's campaign in France and the Democratic National Committee in the United States. And as noted earlier, experts are highly confident that APT28 is an arm of the GRU located in northeastern Moscow. German intelligence services were convinced that Putin was behind the 2015 operation and, in January 2017, the U.S. intelligence community issued its joint assessment of Russian activities during the 2016 U.S. elections.

Germany has been no stranger to the political ramifications of fake news and leaked data. The 2016 "Lisa" story powerfully illustrated the real world consequences of fake news. After spending the night with her boyfriend and being reported as missing by her parents, Lisa, a thirteen-year-old Russian-German girl, claimed to have been kidnapped and raped by migrants in Berlin. Russian media outlets quickly spread the uncorroborated news, the Russian foreign minister accused the German government of a cover-up, and protests erupted in Germany until Lisa eventually admitted the truth.[88] In another example, a minister of Brandenburg state stepped down in 2010 after data from a stolen laptop was leaked to the press, casting him in a dubious light.[89]

In March 2017, Merkel convened Germany's Federal Security Council, a body that only meets when the country faces the most serious threats. The country's senior security officials discussed a single agenda item: how to protect against potential Russian interference in the September election.

Over the past few years, media outlets, primarily right-wing, have been systematically challenging Merkel's CDU party, especially by calling into question her controversial decision to allow refugees to enter Germany by the thousands in August 2015.[90] The Russian activity helped amplify messages by the Alternative for Germany (AfD) party, which is one of the country's most nationalist, anti-immigrant party and a fervent advocate for closer ties with Moscow.[91] While only in existence since 2013, the AfD is the third-strongest party in Germany already—just a few percentage points behind the Social Democratic Party (SPD). Notably, voters are increasingly turning away from the "people's parties" (CDU and SPD), and Germany's party landscape is becoming increasingly splintered.

Against this background, in March 2017, Merkel convened Germany's Federal Security Council, a body that only meets when the country faces the most serious threats. During the meeting, the country's senior security officials discussed a single agenda item: how to protect against potential Russian interference in the September election.[92] The steps considered ranged from making potential interference as difficult and costly as possible to instigating retaliatory options if interference should occur. Discussions also centered on the need for a clear legal framework to support the government's defense against cyber attacks, including potentially neutralizing servers used to carry out the attacks.[93]

Dieter Sarreither, responsible for Germany's entire electoral area as the federal returning officer at the time, echoed the overall concern in Germany that a faulty election outcome "could undermine confidence in democracy in Germany."[i] Sarreither was concerned that even a small disruption of the process could cast doubt on the integrity of the process overall and fuel conspiracy theories.[94]

According to Sarreither, German authorities approached the task of defense by differentiating between two potential types of attack: attacks targeting the electoral process and attacks targeting election campaigns directly or indirectly. His office was responsible for the former, whereas responsibility for the latter was distributed among multiple actors—political parties, politicians, and media organizations.[95] At the same time, the federal returning officer "does not have the authority to issue instructions to the other electoral bodies," including at the state and local levels; these bodies are basically "self-governing bodies," complicating the task of his office.[96] Moreover, Sarreither clarified that his office is not "the referee of the election campaign" and that it is the "responsibility of all actors to ensure the security of their own systems," with media also having a "significant responsibility to be diligent in their reporting."

As early as spring 2017, the German government sent clear signals to Moscow that it should not dare to attempt what it did in the United States, France, and elsewhere.

As early as spring 2017, the German government sent clear signals to Moscow that it should not dare to attempt what it did in the United States, France, and elsewhere. According to a media report, "a Chancellery emissary delivered a stern warning during a visit to Moscow."[97] In May 2017, Merkel herself issued a warning to Putin, stating that "she assumes 'German parties will be able to decide their election campaign among themselves.'"[98] That same month, heads of the German domestic and foreign intelligence agencies and the German Federal Police all spoke of the growing dangers from cyberspace at a conference in Potsdam. On June 16, Germany's president, Frank-Walter Steinmeier—nominally the highest-ranking country official and head of state—took the warnings a step further, stating in an interview that "Were Moscow to interfere in the election of the Bundestag, then the share of commonalities will necessarily decrease

[i] The federal returning officer is the chairperson of the Federal Election Committee, which essentially acts as an independent fourth pillar of Germany's democracy during the time of an election. Although it must comply with relevant legal provisions, it is not beholden to other state agencies.

further. That would be damaging for both sides."[99] All their collective remarks essentially sent a message to Putin that, in the words of Hans-Georg Maaßen, head of the German domestic intelligence service (BfV), "Possibly there is no interest [in the Kremlin] to further strain its relations to Germany."[100]

In the months leading up to the September election, several actors took steps to minimize the potential impact of hostile influence campaigns. Political parties reportedly entered into a "gentlemen's agreement" not to use leaked information for political purposes.[101] They also pledged not to use social media bots.[102] Facebook offered to train political parties on two-factor authentication and other basic cyber hygiene, and Google expanded its Knowledge Panel to include specific information on publishers.[103] Together with Jigsaw, Google also started to develop a Protect Your Election package for organizations participating in election processes in Germany and elsewhere.[104] In addition, Germany's BfV reached out to political parties to share information on potential risks and threats, and the Office of the Federal Returning Officer established a verified Twitter account in early 2017 to allow swift clarifications of potential fake news that could disrupt the electoral process.[105] Similarly, at least one party prepared a draft press statement to buy time in case of a last-minute, MacronLeaks-style hack. Finally, media organizations set up teams of fact checkers to help verify the authenticity of material.[106]

Political parties reportedly entered into a "gentlemen's agreement" not to use leaked information for political purposes. They also pledged not to use social media bots.

Measures were also taken to safeguard against the hacking of political party computer systems. The Federal Office for Information Security (BSI) offered its services to the main political parties but, for fairness reasons, could not change the services according to each party's computer programs; thus, some parties could not take advantage of its offer.[107] At least one party sought assistance from private cybersecurity firms but found their services to be too costly. Instead, the party developed in-house training material for its leadership—described as a "30 minute crash course in 'what is spear phishing.'"[108] Yet even bigger parties with more resources struggled to enhance protections, highlighting that the challenge is both technical and organizational. For example, in 2010, an IT professional from one party proposed encrypting email communications, but it did not begin until 2017.

With regard to election infrastructure, Germany has an advantage: it relies on paper ballots, which election volunteers at about 70,000 voting stations count by hand. The results are then written down. In 2009, Germany's Constitutional Court issued a ruling that effectively banned the use of electronic voting machines countrywide, declaring them to be in conflict with the principle of reliability and transparency of the election process.[109] Media reports at the time mentioned the potential for manipulation, highlighting that all of the voting machines used in Germany were produced by the Dutch company Nedap and therefore offered a single point of entry for hackers to more easily manipulate them.[110] The Constitutional Court set the standards for the permissible use of electronic voting machines so high that their use remains unrealistic in the foreseeable future.

Although Germany relies on paper ballots, computers do play a role in collecting, aggregating, and submitting election results from the local to the state level and subsequently to the Office of the Federal Returning Officer.[111] That is why Sarreither's focus was on the integrity and authenticity of election data and the submission of election results. In spite of public assurances about the security of existing systems, only a few weeks before the September election, members of the Chaos Computer Club—Germany's hub for hackers and security researchers—identified a critical vulnerability in the PC-Wahl software. While each local entity can choose what software it wants for the election, PC-Wahl is used in at least half of Germany's sixteen states.[112] The security researchers were able to manipulate the software in spite of several protection mechanisms.[113] The BSI promptly informed Sarreither of the potential vulnerabilities in late July, before they were publicly reported by the media.[114]

The security researchers' findings essentially affirmed the government's internal confidential warning that "cyber attacks could aim to manipulate election results during transmission, inject false election results, or technically suppress the transmission of preliminary election results."[115] In response to their findings, and the media attention, German authorities asked the company producing the software to issue a security update, issued guidance that election results submitted to the statistical agencies of each federal state should be checked against those in the local municipalities, and required that any potential discrepancies be flagged via phone.[116] The Office of the Federal Returning Officer stated that with these changes, "A manipulation of the election outcome is therefore excluded."[117]

Only a few weeks before the September election, members of the Chaos Computer Club—Germany's hub for hackers and security researchers—identified a critical vulnerability in the PC-Wahl software.

Notable Interference

The German case study stands out because no significant Russian interference in the September election has been reported—despite several incidents of Russian activity in years prior, including the Bundestag hack, misinformation campaigns, and the registration of two websites (btleaks.info and btleaks.org) that mirror the "DC Leaks" website from the Democratic National Committee hack. While German officials monitored btleaks.org, no leaks occurred.[118] Similarly, as of a week before the September 2017 election, Facebook had not found ad purchases similar to those during the 2016 U.S. election.[119]

This raises the question: "Why no Russian meddling?" as the *New York Times* put it.[120] Some observers have argued that it is the less partisan nature of German politics, continuing trust in mainstream media sources, reliance on paper ballots, and Germany's multiparty and proportional system that explain this outcome. Others have suggested that the Kremlin reconsidered its approach because it had lost the element of surprise (although that did not keep APT28 from targeting Macron's campaign) or because it chose subtler techniques, such as focusing on Russian-speaking Germans. Or perhaps Moscow ultimately considered the risk too large—believing that its interference would negatively impact Germans' views on Russia and weaken its relationship with Germany in the long run.[121] When the United States imposed sanctions against Russia in the summer of 2017 because of the Kremlin's 2016 interference, it increased the likelihood of European governments taking similar measures, raising the cost for Putin.[122]

Perhaps Moscow ultimately considered the risk too large—believing that its interference would negatively impact Germans' views on Russia and weaken its relationship with Germany in the long run.

The outcome could also be reasonably attributed to high-level government deterrence signals, especially the warning that any interference by Moscow would significantly damage the German-Russian relationship. Following this logic, perhaps Moscow, in spite of having laid the groundwork, decided not to move forward and instead to send the message that it valued the German-Russian relationship. In line with this reasoning, it is worth noting that Steinmeier traveled to Moscow a month after the elections, marking the first time a German president had visited Russia in seven years.[123]

Post-Election Responses

On October 1, 2017, the government passed the German Act to Improve the Enforcement of the Law in Social Networks—known as the Network Enforcement Law.[124] Although the bill was first proposed in April 2017 to primarily reduce hate speech crimes online, the law is now also seen as a mechanism to combat fake news. It compels social networks such as Facebook and Twitter to remove flagged "illegal content" within twenty-four hours or up to a week in special circumstances. If companies fail to establish the processes required to systematically remove the content, they face a fine of up to 50 million euros. The flagging of inappropriate content by users began on January 1, 2018, after a test period.[125]

Despite the good intentions of the law, some groups were quick to criticize it. The United Nations special rapporteur on freedom of opinion and expression, David Kaye, as well as representatives of human rights groups, argued that it limited free speech and introduced incentives for companies to overcomply.[126] It is true that the government and internet companies have dozens of staff dedicated to the law's implementation—illustrating the law's heavy compliance requirements—but the total numbers represent very small proportions of the overall staff sizes and revenues of multinational companies.

Conclusions

Due to the underlying principle of proportional representation and the absence of a winner-takes-all rule, the German electoral system is structurally less vulnerable to interference, especially efforts that aim to propel a specific candidate or party to power. For example, Germany's chancellor is not chosen directly by voters but rather by the party that wins the majority. The chancellor must then be able to successfully form a coalition government with other parties. Meanwhile, parties must garner at least 5 percent of the overall vote to enter parliament. In addition, Germany's political environment is also significantly less polarized than in some other countries. Finally, regarding the election's integrity overall, Sarreither considers the "analogue election process with pen and paper still to be the best solution."[127]

Nevertheless, Germany faces a few key challenges. First, the fact that no significant Russian interference was detected in September 2017 is both a blessing and a curse. Momentum to better protect the election process seems to be waning as political party members and senior officials shift their focus to other priorities.[128] However, several technical and organizational vulnerabilities require continued high-level attention. For example, the Bundestag hack was partly carried out through servers the BSI had on its blacklist for the executive government, but sharing the blacklist with the legislative branch was beyond the scope of its mandate at the time. Further, it appears that certain security measures instituted in 2017 are being circumvented because they are inconvenient to use, and multifactor authentication, data encryption, and other technical fixes have yet to be implemented uniformly across party and parliamentary offices.[129] Applying the fixes will be important, even though they raise both technical and legal issues that are difficult to resolve, including potentially those related to campaign financing. Making other steps that had been of a temporary nature permanent, such as the BSI being able to offer its services to political parties for free, is also important. Finally, because some efforts, including those under the Network Enforcement Law, will not reveal their overall impact for months or years, they should be monitored for necessary adjustments.

On October 1, 2017, the government passed the German Act to Improve the Enforcement of the Law in Social Networks. It compels social networks such as Facebook and Twitter to remove flagged "illegal content" within twenty-four hours or up to a week in special circumstances.

Sweden: General Elections, September 2018

Having been a target of Russian cyber attacks in the past, Sweden is another European country deeply concerned about Russian election interference. Swedish government officials began taking active defensive measures more than a year ago. While it is too soon to evaluate these efforts, they have likely raised the country's preparedness and may serve as a deterrent against Russia.

Preparatory Actions

Like other European countries, Sweden has been on high alert since Russia's interference in the 2016 U.S. election. However, in this case, the Swedish government has the advantage of time and has been actively preparing for foreign interference in its September 2018 general election. And its efforts appear to be warranted. In December 2016, the head of the Swedish Military Intelligence and Security Service explicitly stated that Russia was responsible for the majority of cyber attacks against Sweden.[130] In March 2017, Prime Minister Stefan Löfven said the country was already ". . . seeing clear attempts at influencing . . . for example . . . [its] security politics."[131] And, in January 2018, Löfven publicly called Russian attempts to meddle in the upcoming Swedish election "completely unacceptable" and has pledged to expose any further attempts "without mercy."[132]

Under the Swedish unicameral parliamentary system, voters elect members through proportional representation, and the members, in turn, elect the prime minister. Parties must garner at least 4 percent of the vote to enter parliament (eight parties are currently represented), and the government rules through party coalitions. The Swedish Police Authority, the Security Service (SÄPO), and the Election Authority are the primary bodies responsible for protecting the integrity of elections. While there is one national election authority, there are twenty-one regional and 290 local election authorities who are mainly independent but adhere to national election laws. Sweden's fairly decentralized election system thus makes it less vulnerable to potential election meddling.

In June 2017, the [Swedish] government presented a specific "societal information and cyber security" strategy that promotes a whole-of-society approach.

Ahead of the upcoming elections, Sweden is allocating additional resources toward strengthening information and cyber security efforts across the government. The Swedish Armed Forces and the Swedish National Defense Radio Establishment are working together to strengthen the country's cyber defense capability. The Swedish Government Offices is striving to increase its own ability to identify major cyber incidents and disinformation campaigns and its understanding of how influence operations are carried out.

The high importance that Sweden attributes to guarding against disinformation is reflected in the government's January 2017 national security strategy document.[133] The document emphasizes the protection of democracy, freedom of opinion, and elections based on the threat from foreign interference. To complement this overall strategy, in June 2017, the government presented a specific "societal information and cyber security" strategy that promotes a whole-of-society approach. It focuses on the roles of national, regional, and local government actors as well as nonpublic, private companies and individuals.[134] And, in January 2018, the establishment of a new government agency responsible for psychological defense—separate from the Civil Contingencies

Agency (MSB)—was announced. While still in its infancy, the new agency's key objective will be to counter disinformation and foreign influence.

A core focus of Sweden's efforts to protect the upcoming election process is countering foreign influence operations. The government has assigned the MSB—an agency normally responsible for managing domestic crises—to be the lead agency and coordinator of national efforts to counter disinformation and influence operations (it received its first government mandate to address the threat from Russian disinformation in 2015). In February 2017, the agency began to actively prepare for the upcoming September election. As part of its efforts, the agency—with SÄPO, the Swedish Police Authority, and the Election Authority—has carried out a threat and vulnerability analysis. The analysis covers Russia's attempts to influence the U.S. and other European elections, the methods used in these cases, and the particular vulnerabilities in Sweden. The final report is classified but has been shared with relevant government agencies, including local election authorities, to help guide their efforts to safeguard the elections.

The government has been holding regular, voluntary dialogue with traditional and social media representatives to discuss possible measures against disinformation and cyber security.

Informed by the above-mentioned analysis, the MSB has provided specific guidance and information to relevant entities, such as the Elections Authority and electoral districts.[135] In total, approximately 7,000 civil servants at the national, regional, and local levels have received general training on influence operations and the risks associated with them.[136] The main focus has been to increase their capacity to identify vulnerabilities and counter any threats to the election process. As part of the MSB's efforts, a "Facebook hotline" has been established to provide government officials a forum to quickly report forged Facebook pages—such as a fake page for the Election Authority. The hotline is not to be used to report nongovernmental websites that are spreading false information. However, Facebook has pledged to report suspicious behavior pertaining to the election to Swedish authorities.[137] The MSB has also, with SÄPO and the Election Authority, established a high-level national forum to help coordinate defensive efforts and strengthen Sweden's ability to mitigate any incidents that occur.

The Swedish government has also been directly engaging the media to further ensure the public's access to reliable and fact-checked information. The government has been holding regular, voluntary dialogue with traditional and social media representatives to discuss possible measures against disinformation and cyber security. This dialogue complements the formal exchange of information that occurs quarterly through the MSB-chaired Media Preparedness Council.[138] In addition, the MSB and Election Authority are jointly offering training to all major Swedish media houses to increase their capacity to spot and respond to falsified information pertaining to the election. The Swedish Media Council—a government agency whose primary task is to empower minors as conscious media users—has launched a nationwide education program to teach high school students about Russian propaganda. Individual Swedish media outlets have also launched their own efforts. For example, four leading news outlets have begun a joint fact-checking initiative to combat both domestic and foreign disinformation.

Educating politicians and political parties is another government priority. SÄPO is working to raise political parties' awareness of potential foreign influence operations during the 2018 election campaign and to increase their preparedness and resilience—going as far as giving party officials a handbook.[139] The agency devotes specific attention to this issue in its 2017 annual report.[140] It has educated all parties in parliament on how external actors hack into computer systems to access data, how they disseminate false information, and what steps the parties can take to protect themselves. SÄPO has also distributed a handbook to 50,000 politicians at the national, local, and municipal levels that includes tips and guidance about disinformation campaigns, password protection, and cyber etiquette. To promote a common national understanding of the risks of election interference, the prime minister has also invited leaders of the other parties to a SÄPO briefing.

It [SÄPO] has educated all parties in parliament on how external actors hack into computer systems to access data, how they disseminate false information, and what steps the parties can take to protect themselves.

Notable Interference Prior to the September 2018 Election

As in many other European countries, the issue of Russian interference has become increasingly salient in Sweden, especially since the start of the Ukraine crisis in early 2014 (although sophisticated and coordinated cyber attacks against Swedish government targets were observed before that).[141] In recent years, Swedish authorities have noted an uptick in hacking operations and dissemination campaigns aimed at polarizing Swedish society, undermining stability, and spreading falsehoods.[142] According to the supreme commander of the Swedish Armed Forces, Russian cyber attacks against the country occur daily.[143]

One prominent example took place in March 2016, when at least seven major Swedish newspapers were subject to prolonged DDoS attacks. Allegedly conducted by Russia, the cyber operation was particularly noteworthy since an anonymous threat had appeared on Twitter days before the attacks, warning the Swedish government against spreading false propaganda.[144] The warning came after the government announced its plans to adopt a new defense strategy in response to Russian aggression. Sweden was also deepening its military partnership with the United States and NATO at the time. After conducting preliminary investigations, the cyber crime unit of Sweden's national police reported that the attacks had originated in Russia. The Swedish minister of interior labeled the incident an "attack against free speech." Incidents such as these are likely intended to intimidate Russia's opponents.[145]

Sweden is also a frequent victim of Russia's psychological warfare activities. U.S. Senator Ben Cardin's report to the Senate Foreign Relations Committee refers to the Nordic countries as "a favorite target of the Kremlin's propaganda machine."[146] Recent examples include Russia's attempts to spread fake news about Sweden's defense policy and the government's handling of the migration crisis. In May 2017, the Swedish government warned the public about Russian disinformation campaigns during the Aurora 17 joint military exercise with the United States and other NATO countries, which was to occur in Sweden in September. Observed Russian efforts included spreading a false picture of the exercise's purpose and portraying it as provocative and aggressive in nature to foment fear and distrust among the Swedish public. Previously, false stories about a host nation support agreement with NATO were circulated, suggesting that Sweden would have to accept the installation of nuclear weapons and permanent NATO bases on Swedish soil. Other incidents have involved the creation of fake social media accounts of prominent politicians. For example, false Twitter accounts of Minister of Defense Peter Hultqvist have appeared at least three times.

The migration crisis has also presented Russia with an equally attractive opportunity to spread propaganda. Through Swedish and international media outlets, Russia has allegedly depicted Sweden as a country in chaos, aiming to fuel societal tensions and delegitimize Sweden's reputation internationally. Russian media platforms, such as RT and Sputnik, have regularly promoted such a depiction, which has been further amplified by far-right and alt-right outlets in Europe and the United States. After launching an outlet in Sweden in April 2015, Sputnik propagated stories suggesting that the Swedish government is struggling to cope with the inflow of migrants. However, on March 11, 2016, Sputnik reportedly closed its Swedish operation—possibly because of the authors' poor Swedish and the high number of exaggerated or incorrect stories published.

Conclusions

The Swedish government has placed protecting the democratic system at the heart of its national security objectives. It is taking the threat of foreign interference in its election very seriously and is actively implementing measures to protect itself (preparations begun in earnest at least a year and a half ago). Russia's efforts to meddle in other countries' elections clearly served as an impetus for Swedish authorities to step up their initiative. They have already taken significant steps to raise awareness of the risks of interference among politicians, media outlets, and the broader Swedish society.

While it is too early to assess the efficacy of Sweden's efforts, some unique strengths should be expected to play a role. Among these are a well-educated population with high levels of civic literacy and public trust, the use of paper ballots and manual counting, and the employment of one agency to coordinate national responses to protect the election from disinformation. Particularly noteworthy is Sweden's whole-of-society approach, which engages media outlets and the education and private sectors. Finally, the willingness of Swedish officials at all levels of government to openly discuss the threat of interference has contributed to raising public awareness and the potential political cost to hostile attackers.

That said, Sweden also faces some notable shortcomings. Although MSB is mandated to support national coordination and assist other agencies with strengthening cyber preparedness and countering hostile influence, the government has not specifically ordered it to lead coordination efforts related to the September 2018 election. In addition, following the end of the Cold War, Sweden gradually scrapped its instruments aimed at implementing a "total defense" approach to information and psychological warfare. As a result, it is having to swiftly reinvent policies and responses to keep pace with the growing demands in the field. The government still lacks several key, supportive legal conditions. For example, it is currently not illegal to spread fake news in Sweden, meaning anyone (including foreign entities) can in principle purchase ads and finance and operate media outlets in Sweden. Currently, the Swedish government's main tool for countering disinformation—exposing such activities—is reactive rather than preventative in nature. Another legal shortcoming is the limits imposed on the government to map who is spreading opinions in Sweden. Ultimately, the upcoming election will indicate whether Sweden needs to bolster its legal framework and, more broadly, will serve as a crucial test of the government's current approach and preparedness.

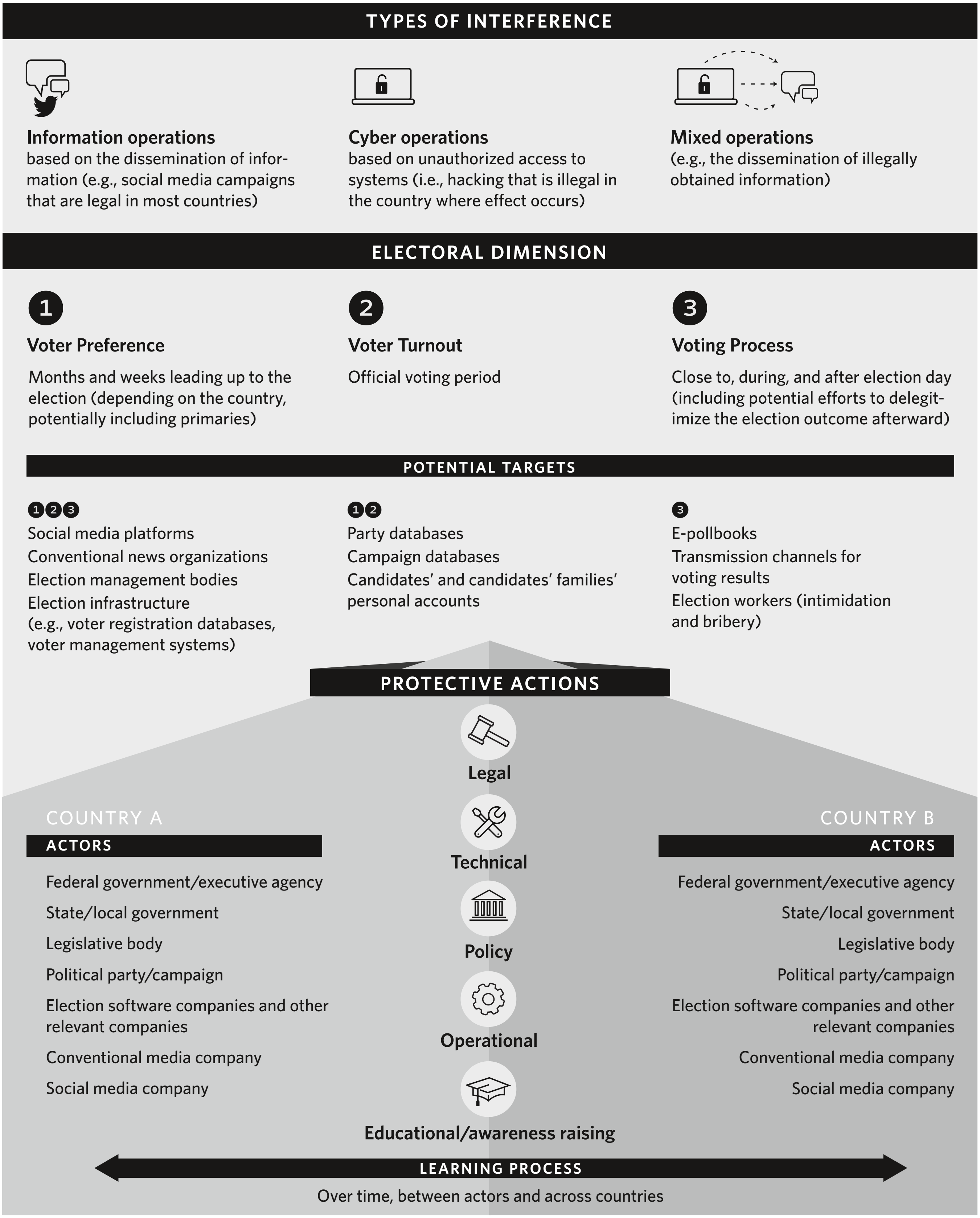
Among these [Sweden's strengths] are a well-educated population with high levels of civic literacy and public trust, the use of paper ballots and manual counting, and the employment of one agency to coordinate national responses to protect the election from disinformation.

Building an Analytical Framework and Roadmap

The central takeaways from these five case studies and others could usefully inform an analytical framework to help collect and organize lessons learned and best practices. In addition, as more data become publicly available, such a framework could guide in-depth comparative studies aimed at collating countries' preparatory actions and defensive responses. It could also serve as a tool for academics and governments to share and compare information.

Overall, there is growing consensus that the overarching strategic objective of Russian election interference is to undermine confidence in democratic institutions and processes generally. To achieve this goal, Russia has exploited information and communications technology to target different dimensions of an electoral process. Based on these activities, an analytical framework begins to emerge (see figure 1). It groups the dimensions into three categories: (1) attempts to influence voters' preferences for a candidate or party, (2) attempts

Figure 1. Analytical Framework for Election Interference



TYPES OF INTERFERENCE

Information operations based on the dissemination of information (e.g., social media campaigns that are legal in most countries)

Cyber operations based on unauthorized access to systems (i.e., hacking that is illegal in the country where effect occurs)

Mixed operations (e.g., the dissemination of illegally obtained information)

ELECTORAL DIMENSION

1 **Voter Preference**

Months and weeks leading up to the election (depending on the country, potentially including primaries)

2 **Voter Turnout**

Official voting period

3 **Voting Process**

Close to, during, and after election day (including potential efforts to delegitimize the election outcome afterward)

POTENTIAL TARGETS

1 2 3
Social media platforms
Conventional news organizations
Election management bodies
Election infrastructure (e.g., voter registration databases, voter management systems)

1 2
Party databases
Campaign databases
Candidates' and candidates' families' personal accounts

3
E-pollbooks
Transmission channels for voting results
Election workers (intimidation and bribery)

PROTECTIVE ACTIONS

Legal

Technical

Policy

Operational

Educational/awareness raising

COUNTRY A

ACTORS

Federal government/executive agency
State/local government
Legislative body
Political party/campaign
Election software companies and other relevant companies
Conventional media company
Social media company

COUNTRY B

ACTORS

Federal government/executive agency
State/local government
Legislative body
Political party/campaign
Election software companies and other relevant companies
Conventional media company
Social media company

LEARNING PROCESS

Over time, between actors and across countries to manipulate the voting process itself, and (3) attempts to affect voter turnout (these are sometimes overlooked and usually aim to delegitimize the election outcome and the democratic process). Each is tied to a different time horizon, with the first occurring over a period of months and the latter two typically occurring in a single day or over a few days. Information and cyber operations under these three categories can focus on a variety of targets, including social media platforms and conventional news organizations; the databases of political parties, campaigns, and voter registration organizations; the personal accounts of candidates or their families; and voting machines, software developers, or the transmission channels of voting results.

The central takeaways from these five case studies and others could usefully inform an analytical framework to help collect and organize lessons learned and best practices.

Government actions to protect against these information and cyber operations and others include new legal measures, awareness-raising campaigns, technical changes to election infrastructure, and operational and policy changes, such as the banning of electronic vote counting. Constitutional and legal requirements in all countries limit the federal or central government's ability to implement these actions unilaterally. A comprehensive analysis of a country's response to election interference therefore requires studying the actions of all relevant actors. Those incorporated into this framework include federal, state, and local government authorities; legislative bodies; political parties and campaigns; election software and other relevant companies; and conventional media and social media organizations. To populate and expand the framework, further research and additional case studies should be conducted.

Recommendations

While research and case studies on Russian election interference are ongoing, available data point to numerous steps governments can take now to improve their preparedness. Quick action remains essential since elections will continue to be vulnerable to manipulation. Russia's decision to meddle in elections and democratic processes on both sides of the Atlantic, using cyber and disinformation tactics in particular, reflects a consistent trend that blends premeditation with opportunism. At the same time, the risk is not limited to Russian interference and must therefore be addressed regardless of the origin—be it foreign or domestic. While there is heightened awareness around the issue in both the United States and European states in the aftermath of the 2016 U.S. elections, efforts to safeguard elections and protect democratic systems are still in their infancy in many countries.

It is imperative that countries launch a concerted international effort to share best practices and lessons learned: time is of the essence. Understandably, with some ad hoc exceptions, most efforts to date have been inward-focused; governments have had to quickly adjust to the new threat landscape ahead of scheduled elections. It is now urgent and crucial to begin sharing a wealth of information and knowledge before the next wave of upcoming elections. And it is a resilience-building effort that should include both advanced and struggling democracies, regardless of whether their political systems are robust or currently under stress.

Below are key governmental takeaways derived from open-source information and the European country case studies presented above. The applicability of the lessons learned herein far exceed the transatlantic relationship and can be a reference for greater international cooperation.

- **Consider election systems as part of critical infrastructure:** To ensure that sufficient attention and resources are dedicated to guarding against potential interference using information and communications technology, governments should prioritize the protection of election systems and processes, treating them as critical infrastructure. Placing this protection high on the national agenda could help send a clear message to the potential attacker that any meddling would not go unnoted and would trigger a serious response.

- **Institutionalize preparations to protect election processes:** Preparations for protecting against election interference require close coordination across various relevant government agencies overseeing intelligence, law enforcement, foreign policy, internal security, and election administration at all levels. Assigning a lead entity to establish an interagency process and whole-of-government approach has proved useful in some countries, but the entity needs a clear mandate and adequate resources to be successful. It should institutionalize the monitoring of potential threats by, for example, establishing and tasking teams within the country's intelligence community to regularly analyze potential signs for planned election interference by foreign powers or domestic adversaries.

Assigning a lead entity to establish an interagency process and whole-of-government approach has proved useful in some countries, but the entity needs a clear mandate and adequate resources to be successful.

- **Focus on resilience measures:** All preparatory actions must aim to strengthen cyber defense capabilities and make any potential interference as costly and cumbersome as possible. This may include switching to nonelectronic systems for casting and counting ballots, as well as keeping secured backups. As the Dutch and French cases show, this switch could be done as a precautionary measure to fully protect the integrity of the voting system and reduce any doubt among the public that the election is free and fair.

- **Conduct regular vulnerability analyses:** Stress tests are important to help identify unknown risks. For example, the German case study illustrates the importance of tasking technical experts and security researchers with penetration testing of electronic systems. Special attention should be given to supply-chain integrity challenges, specifically potential hidden choke points such as software or hardware suppliers.
- **Issue public statements:** Public warnings against potential election interference or statements about actual incidents that have occurred can support two important objectives: deterrence and the sensitization of the public to such activities. In several cases where political leaders explicitly identified Russia as a potential perpetrator and threatened retaliation, actual interference was less than expected.
- **Aid political parties and campaigns:** Government officials should actively engage with political parties and campaigns to improve their cybersecurity practices and basic cyber hygiene. Gaining the strong support of all party leaderships is essential, and educating them on the overall threat to democratic processes will ensure that they feel an overall responsibility for protecting them. This will also help normalize the role that security teams and their resources should play in support of these endeavors. Potentially useful models can be found in several European countries. In France, the government provided parties with a list of vetted, independent cyber experts. In the United Kingdom and Germany, the governments made their cyber experts available to parties should they require additional assistance in addressing a technical problem.

The recent detection of highly targeted, local-level interference in some countries highlights the importance of increasing awareness among state and local officials, election authorities, and volunteers involved in campaigns.

- **Broaden activities to subnational levels:** Governments must also expand their activities from the national or federal level to the regional and local levels. The recent detection of highly targeted, local-level interference in some countries highlights the importance of increasing awareness among state and local officials, election authorities, and volunteers involved in campaigns. Addressing this gap requires tailored and concerted efforts.
- **Develop contingency plans:** Governments and political parties and campaigns should prepare contingency plans in case interference does occur. For example, to buy time and avoid panicking, parties can prepare a press statement in advance of a cyber breach. Individual political parties and organizations with strong in-house IT teams may also want to study the counter-information efforts of En Marche in France. By anticipating cyber operations and taking steps to undermine the reliability of potentially stolen information, Macron's party was able to undermine the attackers' ability to utilize the stolen information.[147]

- **Educate voters about disinformation campaigns:** Educating individual voters is paramount to increasing societal resilience. In Sweden, for example, the government launched a nationwide program aimed at teaching high school students about Russian propaganda. It is also vital that government and intelligence officials publicly release relevant information about cyber operations targeting democratic institutions. And whenever possible, the information should include forensic evidence to enhance public awareness and inform future preparedness.
- **Establish government-media dialogue:** Active engagement between government officials and media providers helps to protect against deliberately planted misinformation. For example, countries might want to establish a permanent media council similar to the one in Sweden, which regularly convenes government and media representatives. Government and social media companies might also want to study and emulate recent coordination on fact-checking operations. Several European governments have actively cooperated with Facebook and other social media companies to combat disinformation. Particularly noteworthy is Sweden's creation of a dedicated Facebook hotline for election officials to quickly report fake government Facebook pages—although its effectiveness is still too early to judge.
- **Encourage the media to take voluntary steps:** Media organizations must reinforce existing journalistic quality standards and practices to protect against disinformation campaigns. For example, they might consider adopting fact-checking initiatives similar to CrossCheck in France or Correctiv in Germany. Governments, instead of imposing laws to regulate reporting—like France has done—could encourage media companies to voluntarily implement reporting restrictions. This would first require efforts to ensure that journalists are fully aware of the effects of propaganda and disinformation.

Countries might want to establish a permanent media council similar to the one in Sweden, which regularly convenes government and media representatives.

- **Engage social media companies to be actively involved in mitigating potential threats:** Engaging social media companies deserves highlighting and specific attention. For most countries, the local population is using social media platforms provided by companies located abroad. Yet social media companies can help mitigate potential threats by identifying disinformation campaigns, sharing information, and taking steps to identify and take down fraudulent accounts. They can also label content known to be inaccurate and provide the correct information alongside to better inform the reader.
- **Explore potential legal measures through an inclusive process:** It is vital that traditional media outlets, social media companies, and civil

society groups be extensively consulted during the process of drafting new legislation. Various governments are considering taking legal measures to help protect against potential election interference. These include removing illegal content from social media; delineating consequences for those who create, disseminate, or amplify misinformation; or requiring transparency regarding political advertisements. Ensuring the broad-based buy-in of relevant societal actors will be crucial to successful implementation.

- **Actively support international cooperation:** Regular exchanges with officials from other countries, especially in the lead-up to important elections, remain ad hoc. There is no institutionalized mechanism for the sharing of lessons learned and best practices. Existing vehicles—including the European External Action Service/East StratCom, the NATO StratCom Communications Center of Excellence (COE), or the Finnish COE on Countering Hybrid Threats—could become the focal point for such an effort. However, given the potential global scope of the threat, any initiatives must go beyond transatlantic cooperation. Foreign ministries and diplomats can make a vital contribution and be the conveners for other government agencies and nongovernmental actors, including media organizations, political parties, and social media companies.

Preparing for the 2018 U.S. Midterm Elections

Some of the aforementioned takeaways are particularly relevant for the United States as it prepares for its 2018 midterm elections and 2020 presidential election. In considering these lessons, the following specific steps could be useful in bolstering proactive and defensive measures.

- **Issue a clear warning that interference in the 2018 elections by Russia or any other actor will result in severe consequences.** Ideally, the U.S. president, senior administration officials, and leading politicians should all send a clear warning signal to Moscow to more effectively deter potential interference and generally set a clear norm against such interference.
- **Coordinate efforts to protect against cyber attacks and disinformation across the government.** The recent creation of a Cyber-Digital Task Force—comprising representatives from the Justice Department, including the Federal Bureau of Investigation and the Office of the Director of National Intelligence—is a useful first step to improve coordination efforts.[148] Given the toxically partisan political environment, an important, complementary step could be establishing a supportive Congressional bipartisan effort.
- **Provide more training and support to state and local election officials.** In addition to the trainings offered by the Department of Homeland Security (DHS), the federal government should offer additional assistance

and resources to state and local election officials.[149] Requests for such assistance could help to map the districts that require particular attention both for those who requested assistance, and, importantly, those that did not.

- **Conduct regular risk assessments of election infrastructure.** Leading up to the midterm elections, the U.S. Elections Assistance Commission, the DHS, or an independent third party should regularly test election systems for vulnerabilities. The recent establishment of the Elections Infrastructure Information Sharing and Analysis Center is an important step in this direction.[150]

- **Encourage states to reevaluate the use of electronic voting machines.** Educating state officials on the details and pros and cons of electronic voting machines will help them determine whether they should return to paper ballots. Given the likely cost involved, federal financing could be offered to facilitate the transition. At the very least, electoral districts should keep paper records as backups to allow for a recount in case the electronic voting system is tampered with.

- **Encourage political parties and their candidates, staff, and volunteers to follow basic cybersecurity practices.** These practices include the use of multifactor authentication for email accounts, encryption tools, and verified social media accounts.

- **Encourage donors to require that political parties and campaigns implement basic cyber hygiene standards for their candidates, staff, and volunteers.** Absent other mechanisms to ensure widespread implementation and adherence to basic security practices such as two-factor authentication, donors are a promising avenue to nudge the behavior of those involved.

- **Urge political parties and campaigns to explicitly state that they will not use or support social media bots.** Social media platforms have become important tools for political parties and campaigns to get their media out. It is also important for citizens to be able to express their views on social media, including through pseudonyms or anonymously. At the same time, there is a difference between humans and machines producing content and a line can be drawn when it comes to the use of social media bots.

- **Increase society's resilience by clearly communicating the risks of foreign interference in U.S. democracy.** Senior officials should work to educate voters across the country on the risks associated with election interference. However, their communications should walk the fine line of raising awareness while avoiding alarmism that could further fuel mistrust in the democratic system.

- **Promote independent, citizen fact-checking and investigative journalistic initiatives.** Official government fact-checking channels would likely be less effective in the United States, where distrust in the federal government is significantly higher than in most Western European countries. However, there is a need for more independent, citizen fact-checking and investigative journalistic initiatives, such as FactCheck.org, the *Washington Post's* Fact Checker, PolitiFact.com, Snopes.com, the German Marshall Fund's Hamilton 68 dashboard, and the Atlantic Council's Digital Forensics Research Lab.
- **Improve media literacy among the public.** Given the widespread use of social media and nontraditional media outlets in the United States—as well as the low level of public trust in traditional news organizations—it is important to educate youth, parents, and teachers about disinformation campaigns and ways to counter them. In light of the particular challenges involving misinformation, U.S. regulators and educators should consider placing a greater emphasis on critical thinking and fact-checking in school and college curricula.

* *This paper has been corrected to delete the mention of Russia Today (RT) in connection with promoting assertions that Macron is "an agent for U.S. financial interests and secretly gay."*

Notes

1 Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections," National Intelligence Council, January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf, p.ii.

2 Matthew Rosenberg, Charlie Savage, and Michael Wines, "Russia Sees Midterm Elections as Chance to Sow Fresh Discord, Intelligence Chiefs Warn," *New York Times*, February 13, 2018, https://www.nytimes.com/2018/02/13/us/politics/russia-sees-midterm-elections-as-chance-to-sow-fresh-discord-intelligence-chiefs-warn.html.

3 Tim Maurer and Agustin Rossi, "Why Latin America Needs to Prepare Now for Election Meddling," *Lawfare*, February 8, 2018, https://www.lawfareblog.com/why-latin-america-needs-prepare-now-election-meddling.

4 Andrew Higgins, "Fake News, Fake Ukrainians: How a Group of Russians Tilted the Dutch Vote," *New York Times*, February 16, 2017, https://www.nytimes.com/2017/02/16/world/europe/russia-ukraine-fake-news-dutch-vote.html.

5 Ibid.

6 Ibid.

7 Ibid.

8 Huib Modderkolk and Tom Kreling "Deze man is volgens de NY Times een verlengstuk van het Kremlin. 'Fake news', zegt hij zelf" [According to the *New York Times*, this man is an agent of the Kremlin. To which he replies: "fake news"], *De Volkskrant*, February 25, 2017, https://www.volkskrant.nl/buitenland/deze-man-is-volgens-de-ny-times-een-verlengstuk-van-het-kremlin-fake-news-zegt-hij-zelf~a4467422/.

9 James McAuley, "Dutch Voters Reject Trade Deal Out of Anger Against E.U.," *Washington Post*, April 6, 2016, https://www.washingtonpost.com/world/europe/dutch-vote-on-eu-ukraine-trade-becomes-forum-for-wider-anger-against-brussels/2016/04/06/af8079bc-fb43-11e5-813a-90ab563f0dde_story.html?utm_term=.7801e3329092.

10 Rick Noack, "The Dutch Were a Secret U.S. Ally in War Against Russian Hackers, Local Media Reveal," *Washington Post*, January 26, 2018, https://www.washingtonpost.com/news/worldviews/wp/2018/01/26/dutch-media-reveal-country-to-be-secret-u-s-ally-in-war-against-russian-hackers/.

11 "AIVD Annual Report 2016," General Intelligence and Security Service, April 2017, https://english.aivd.nl/publications/annual-report/2017/04/04/annual-report-2016.

12 Ibid.

13 Higgins, "Fake News, Fake Ukrainians."

14 "Dutch to Hand-Count Ballots in March Vote Due to Hacking Fears," *Deutsche Welle*, February 1, 2017, http://www.dw.com/en/dutch-to-hand-count-ballots-in-march-vote-due-to-hacking-fears/a-37375137.

15 Thomas Escritt, "Dutch Will Hand Count All Election Ballots Due to Hacking Fears," Reuters, February 1, 2017, http://www.reuters.com/article/us-netherlands-election-cyber-idUSKBN15G55A.

16 Thessa Lageman, "Russian Hackers Use Dutch Polls as Practice," *Deutsche Welle*, March 10, 2017, http://www.dw.com/en/russian-hackers-use-dutch-polls-as-practice/a-37850898.

17 Peter Teffer, "Fake News or Hacking Absent in Dutch Election Campaign," EU Observer, March 15, 2017, https://euobserver.com/beyond-brussels/137240.

18 Justina Crabtree, "Here's Why the Dutch Election Is Resilient to Fake News," CNBC, March 14, 2017, https://www.cnbc.com/2017/03/14/heres-why-the-dutch-election-is-resilient-to-fake-news.html.

19 "Technologiebedrijven gaan helpen bij beveiliging van verkiezingen" [Technology companies to help with electoral security], NOS, January 1, 2017, https://nos.nl/artikel/2154017-technologiebedrijven-gaan-helpen-bij-beveiliging-van-verkiezingen.html.

20 "AIVD Annual Report 2016," General Intelligence and Security Service; and Cynthia Kroet, "Russia Spread Fake News During Dutch Election: Report," *Politico*, April 4, 2017, https://www.politico.eu/article/russia-spread-fake-news-during-dutch-election-report-putin/.

21 Janene Pieters, "Facebook to Also Tackle 'Fake News' in the Netherlands," NL Times, March 3, 2017, https://nltimes.nl/2017/03/03/facebook-also-tackle-fake-news-netherlands.

22 Eric Auchard and Toby Sterling "Google and Sister Company to Offer Cyber Security to Election Groups," Reuters, March 21, 2017, https://www.reuters.com/article/us-cyber-election/google-and-sister-company-to-offer-cyber-security-to-election-groups-idUSKBN16S166.

23 Jon Stone, "Forum for Democracy: New Dutch Eurosceptic Party That Wants EU Referendum Now Polling in Second Place," *Independent*, February 19, 2018, http://www.independent.co.uk/news/world/europe/forum-for-democracy-netherlands-eu-referendum-pvv-fvd-mark-rutte-a8217956.html.

24 Ken Gude, "Russia's 5th Column," Center for American Progress, March 15, 2017, https://www.americanprogress.org/issues/security/reports/2017/03/15/428074/russias-5th-column/; "Russia Index 1.1: European Parliament Votes," EUbloggen, January 3, 2015, https://eublogg.files.wordpress.com/2015/01/skc3a4rmavbild-2015-01-10-kl-18-29-47.png.

25 John Leicester, "After US Election Hacks, France Girds Against Cyberattacks," Associated Press, December 15, 2016, https://apnews.com/fff5d7194d1a4053bda70f7ffe6f8bd9/after-us-election-hacks-france-girds-against-cyberattacks.

26 "Soupçons de cyberattaques russes: Ayrault dénonce "une forme d'ingérence inacceptable" [Russian cyberattack suspicions: Ayrault slams "an unacceptable interference method"], France24, February 19, 2017, http://www.france24.com/fr/20170219-cyberattaques-russie-presidentielle-ayrault-denonce-ingerence-inacceptable.

27 Marie-Alix Véran, "Quand la cybermenace pèse sur les démocraties" [When the cyber threat weighs on the democracies], Insitut Montaigne, November 10, 2016, http://www.institutmontaigne.org/blog/2016/11/10/Quand-la-cybermenace-p%C3%A8se-sur-les-d%C3%A9mocraties.

28 Christopher Dickey, "Fighting Back Against Putin's Hackers," *Daily Beast*, April 25, 2017, https://www.thedailybeast.com/fighting-back-against-putins-hackers.

29 Francesco Bechis, "Ecco chi sono i tre (ben pagati) avvocati di Emmanuel Macron" [Here are the three (well-paid) lawyers of Emmanuel Macron], Formiche, August 1, 2017, http://formiche.net/2017/08/01/ecco-chi-sono-i-tre-strapagati-avvocati-di-emmanuel-macron/.

30 Adrien Sénécat, "Le Décodex, un premier pas vers la vérification de masse de l'information" [The Decodex: a first step toward the mass verification of information], *Le Monde*, February 2, 2017, http://www.lemonde.fr/les-decodeurs/article/2017/02/02/le-decodex-un-premier-pas-vers-la-verification-de-masse-de-l-information_5073130_4355770.html.

31 The CrossCheck website is still available at: https://crosscheck.firstdraftnews.org/france-en/.

32 Mehdi Chebil, "France Takes Steps to Prevent an Election Hack Attack," France24, January 16, 2018, http://www.france24.com/en/20170114-france-vulnerable-cyber-attacks-hacking-presidential-elections.

33 Joseph Menn, "Exclusive: Russia Used Facebook to Try to Spy on Macron Campaign – Sources," Reuters, July 27, 2017, https://www.reuters.com/article/us-cyber-france-facebook-spies-exclusive/exclusive-russia-used-facebook-to-try-to-spy-on-macron-campaign-sources-idUSKBN1AC0EI.

34 Eric Auchard and Bate Felix, "French Candidate Macron Claims Massive Hack as Emails Leaked," Reuters, May 5, 2017, https://www.reuters.com/article/us-france-election-macron-leaks/french-candidate-macron-claims-massive-hack-as-emails-leaked-idUSKBN1812AZ.

35 Feike Hacquebord, "Two Years of Pawn Storm: Examining an Increasingly Relevant Threat," Trend Micro, April 25, 2017, https://documents.trendmicro.com/assets/wp/wp-two-years-of-pawn-storm.pdf.

36 Martin Matishak, "NSA Chief: U.S. Warned France About Russian Hacks Before Macron Leak," *Politico*, May 9, 2017, https://www.politico.com/story/2017/05/09/us-warned-france-russia-hacking-238152.

37 "The Latest: France Says No Trace of Russian Hacking Macron," Associated Press, June 1, 2017, https://www.apnews.com/fc570e4b400f4c7db3b0d739e9dc5d4d.

38 Stefan Soesanto, "The Macron Leak That Wasn't," European Council on Foreign Relations, May 9, 2017, http://www.ecfr.eu/article/commentary_the_macron_leak_that_wasnt_7285.

39 Emmanuel Paquette, "Cybercriminalité: et si la présidentielle était piratée?" [Cybercriminality: what if the presidential election was hacked?], *L'Express*, October 26, 2016, https://www.lexpress.fr/actualite/politique/elections/cybercriminalite-et-si-la-presidentielle-etait-piratee_1844365.html.

40 Michel Rose and Eric Auchard, "Macron Campaign Confirms Phishing Attempts, Says No Data Stolen," Reuters, April 26, 2017, https://www.reuters.com/article/us-france-election-macron/macron-campaign-confirms-phishing-attempts-says-no-data-stolen-idUSKBN17S127.

41 Philip N. Howard et al., "Junk News and Bots During the French Presidential Election: What Are French Voters Sharing Over Twitter?," Oxford Internet Institute, April 22, 2017, http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/04/What-Are-French-Voters-Sharing-Over-Twitter-v9.pdf.

42 Alan Crosby, "Putin May End Up the Winner in French Presidential Vote,'" Radio Free Europe/Radio Liberty, April 22, 2017, https://www.rferl.org/a/france-election-macron-le-pen-fillon-melenchon-putin-russia/28445679.html.

43 Gabriel Gatehouse, "Marine Le Pen: Who's Funding France's Far Right?," BBC News, April 3, 2017, http://www.bbc.com/news/world-europe-39478066.

44 Anne-Sylvaine Chassany and Max Seddon, "François Fillon Faces More Pressure Over Vladimir Putin Links," *Financial Times*, March 21, 2017, https://www.ft.com/content/98a34480-0e62-11e7-b030-768954394623.

45 Natalie Nougayrède, "Anti-German, Soft on Putin – Mélenchon Is No Saviour of the Left," *Guardian*, April 18, 2017, https://www.theguardian.com/commentisfree/2017/apr/18/jean-luc-melenchon-germany-putin-french-presidential-race.

46 DFRLab, ""Macron Antoinette": Alt-Right Targets France," Medium, April 29, 2017, https://medium.com/dfrlab/macron-antoinette-alt-right-targets-france-f5e5dcee5cfe.

47 DFRLab, "The French Election Through Kremlin Eyes," Medium, April 20, 2017, https://medium.com/dfrlab/the-french-election-through-kremlin-eyes5d85e0846c50.

48 Nicolas Vanderbiest, "Quelle est l'influence russe sur la campagne présidentielle française", Reputatio Lab, April 20, 2017, http://www.reputatiolab.com/2017/04/quelle-est-linfluence-russe-sur-la-campagne-presidentielle-francaise/.

49 "Ex-French Economy Minister Macron Could be 'US Agent' Lobbying Banks' Interests," *Sputnik*, February 4, 2017, https://sputniknews.com analysis/201702041050340451-macron-us-agent-dhuicq/.

50 Shaun Walker, "Putin Welcomes Le Pen to Moscow With a Nudge and a Wink," *Guardian*, March 24, 2017, https://www.theguardian.com/world/2017/mar/24/putin-welcomes-le-pen-to-moscow-with-a-nudge-and-a-wink.

51 Anton Shekhovtsov, "Moscow and the Far Right in France and Austria," *Eurozine*, February 6, 2017, http://www.eurozine.com/from-plan-a-to-plan-b-and-back/.

52 "'Fillon en tête' selon Sputnik, des prévisions qualifiées abusivement de sondage" ["Fillon ahead" according to Sputnik, predictions falsely characterized as polls], France24, April 4, 2017 http://www.france24.com/fr/20170403-france-politique-presidentielle-fillon-sputnik-tete-sondages-russie.

53 Maud Pierron "MacronLeaks: En Marche! piraté, dénonce une 'opération de déstabilisation'" [MacronLeaks: En Marche! hacked, slams a "destabilization operations"], *L'Express*, May 5, 2017, https://www.lexpress.fr/actualite/politique/elections/macronleaks-des-milliers-d-emails-de-l-equipe-de-campagne-de-macron-pirates_1905721.html.

54 Christopher Dickey, "Did Macron Outsmart Campaign Hackers?," *Daily Beast*, June 5, 2017, https://www.thedailybeast.com/did-macron-outsmart-campaign-hackers.

55 "French Media Rules Prohibit Election Coverage Over Weekend," France24, May 7, 2017, http://www.france24.com/en/20170506-france-media-rules-prohibit-election-coverage-over-weekend-presidential-poll.

56 Kim Willsher, "French Media Warned Not to Publish Emmanuel Macron Leaks," *Guardian*, May 6, 2017, https://www.theguardian.com/world/2017/may/06/french-warned-not-to-publish-emmanuel-macron-leaks.

57 Mark Scott "U.S. Far-Right Activists Promote Hacking Attack Against Macron," *New York Times*, May 6, 2017, https://www.nytimes.com/2017/05/06/world/europe/emmanuel-macron-hack-french-election-marine-le-pen.html.

58 Andrew Osborn and Richard Balmforth, "Macron Camp Bars Russian News Outlets, Angers Moscow," Reuters, April 27, 2017, https://www.reuters.com/article/us-france-election-macron-russia/macron-camp-bars-russian-news-outlets-angers-moscow-idUSKBN17T2GB.

59 Yasmeen Sehran, "Macron, Standing Alongside Putin, Says Russian Media Spread 'Falsehoods,'" *Atlantic*, May 30, 2017, https://www.theatlantic.com/news/archive/2017/05/macron-rt-supnik-are-agents-of-influence/528480/.

60 Scott Neuman, "France's Macron Says He Wants Law to Combat Fake News," NPR, January 4, 2018, https://www.npr.org/sections/thetwo-way/2018/01/04/575580790/frances-macron-says-he-wants-law-to-combat-fake-news.

61 "Loi contre les « fake news » : une procédure de référé judiciaire" [Anti-"fake news" law: an accelerated judicial procedure], *Le Monde*, February 4, 2018, http://www.lemonde.fr/economie/article/2018/02/04/loi-contre-les-fake-news-une-procedure-de-refere-judiciaire_5251569_3234.html.

62 "The Life of Women and Men in Europe," Eurostat, 2017, http://ec.europa.eu/eurostat/cache/infographs/womenmen/wide-menu.html?lang=en.

63 "3 Français sur 4 se méfient des informations diffusées via les réseaux sociaux" [3 out of 4 people in France are suspicious of information broadcast on social media], *La Tribune*, December 18, 2017, https://www.latribune.fr/technos-medias/3-francais-sur-4-se-mefient-des-informations-sur-les-reseaux-sociaux-762159.html.

64 "Russia's RT Launches New French Channel Despite 'Propaganda' Charges," Radio Free Europe/Radio Liberty, December 19, 2017, https://www.rferl.org/a/russia-today-rt-launches-new-french-language-channel-paris-despite-propaganda-charges-macron/28926043.html.

65 Marlene Laruelle, "Russian Soft Power in France: Assessing Moscow's Cultural and Business Para-diplomacy," Carnegie Council for Ethics in International Affairs, January 8, 2018, https://www.carnegiecouncil.org/publications/articles_papers_reports/russian-soft-power-in-france.

66 Donald N. Jensen, "RT France Television Debuts to Mixed Reviews," Center for European Policy Analysis, January 19, 2018, http://infowar.cepa.org/EN/RT-France-Television-debuts-to-mixed-reviews.

67 Gordon Rayner, "Exclusive: Brussels Could End Up Paying Britain a Brexit Divorce Bill, Says Boris Johnson," *Telegraph*, May 12, 2017 http://www.telegraph.co.uk/news/2017/05/12/exclusive-brussels-could-end-paying-britain-brexit-divorce-bill/.

68 "Coats: Russia Is Interfering in French, German and British Elections," *Washington Post*, May 23, 2017, https://www.washingtonpost.com/video/national/coats-russia-is-interfering-in-french-german-and-british-elections/2017/05/23/f6e9711c-3fbe-11e7-b29f-f40ffced2ddb_video.html?utm_term=.bac8e136f952.

69 Alex Hern, "Cyberattack on UK Political Party 'Only a Matter of Time,'" *Guardian*, May 30, 2017 https://www.theguardian.com/technology/2017/may/30/hacking-uk-political-party-matter-time-us-expert-phishing.

70 "Statement: NCSC Offer of Assistance to Political Parties," National Cyber Security Center, March 12, 2017, https://www.ncsc.gov.uk/news/statement-ncsc-offer-assistance-political-parties.

71 "Phishing: Guidance for Political Parties and Their Staff," National Cyber Security Center, May 15, 2017 https://www.ncsc.gov.uk/guidance/phishing-guidance-political-parties-and-their-staff.

72 "Statement: Guidance for Political Parties and Their Staff," National Cyber Security Center, May 15, 2017 https://www.ncsc.gov.uk/news/statement-guidance-political-parties-and-their-staff.

73 "UK Targeted by 'Dozens' of Serious Cyber Attacks Each Month," BBC News, February 12, 2017, http://www.bbc.com/news/uk-38951172.

74 Paul D. Shinkman, "British Say Election Was Free of Russian Meddling," *U.S. News & World Report*, June 16, 2017, https://www.usnews.com/news/world/articles/2017-06-16/british-say-election-was-free-of-russian-meddling.

75 Clare Llewellyn and Laura Cram, "We Find Brexit-Related Tweets From Twitter's List of Suspected Russian Troll Accounts," *Neuropolitics* (blog), University of Edinburgh, November 16, 2017, http://blogs.sps.ed.ac.uk/neuropolitics/.

76 Kate Holton, "Russian Twitter Accounts Promoted Brexit Ahead of EU Referendum: Times Newspaper," Reuters, November 15, 2017, https://ca.reuters.com/article/topNews/idCAKBN1DF0ZR-OCATP.

77 Guy Falconbridge, "Russia Scolds Britain for Saying the Kremlin Dreams of Brexit," Reuters, March 11, 2017, https://uk.reuters.com/article/uk-britain-eu-russia/russia-scolds-britain-for-saying-the-kremlin-dreams-of-brexit-idUKKCN0WD23H.

78 Ben Nimmo, "Putin's Media Are Pushing Britain for the Brexit," *Interpreter*, February 12, 2016, http://www.interpretermag.com/putins-media-are-pushing-britain-for-the-brexit/.

79 Mike Harris and Josh Feldberg, "89up Releases Report on Russian Influence in the EU Referendum," 89up, February 10, 2018, http://www.89up.org/russia-report.

80 Vidya Narayanan et al., "Russian Involvement and Junk News During Brexit," Computational Propaganda Research Project, December 19, 2017.

81 "Theresa May Accuses Vladimir Putin of Election Meddling," BBC News, November 14, 2017, http://www.bbc.com/news/uk-politics-41973043.

82 Alex Aiken, "Eight Challenges for the Government Communications Service in 2018," *PR Week*, January 17, 2018, https://www.prweek.com/article/1454621/eight-challenges-government-communication-service-2018.

83 "Britain to Set Up Unit to Tackle 'Fake News': May's Spokesman," Reuters, January 23, 2018, https://www.reuters.com/article/us-britain-politics-fakenews/britain-to-set-up-unit-to-tackle-fake-news-mays-spokesman-idUSKBN1FC2AL.

84 Holly Watt, "Ofcom Investigates Alex Salmond's TV Show on Kremlin-backed Channel," *Guardian*, December 18, 2017, https://www.theguardian.com/world/2017/dec/18/ofcom-investigates-alex-salmonds-tv-show-kremlin-backed-network.

85 "Russian News Agency Sputnik Sets Up Scottish Studio," BBC News, August 10, 2016 http://www.bbc.com/news/uk-scotland-scotland-politics-37036900; Roy Greenslade, "Pravda Comes to Scotland 'to Extend Russian Influence in UK,'" *Guardian*, October 12, 2016 https://www.theguardian.com/media/greenslade/2016/oct/12/pravda-comes-to-scotland-to-extend-russian-influence-in-the-uk.

86 Alex Hern, "Russian Hackers Targeted UK Media and Telecoms Firms, Confirms Spy Chief," *Guardian*, November 15, 2017, https://www.theguardian.com/technology/2017/nov/15/russian-hackers-targeted-uk-media-and-telecoms-firms-confirms-spy-chief.

87 Sumi Somaskanda, "The Cyber Threat to Germany's Elections Is Very Real," *Atlantic*, September 20, 2017, https://www.theatlantic.com/international/archive/2017/09/germany-merkel-putin-elections-cyber-hacking/540162/.

88 Maria Snegovaya, "Russian Propaganda in Germany: More Effective Than You Think," *National Interest*, October 17, 2017, https://www.berliner-zeitung.de/berlin/13-jaehrige-lisa-aus-marzahn-von-der-vergewaltigungsluege-zum-diplomatischen-gewitter-23544190.

89 "Brandenburger Innenminister Speer tritt zurück" [Brandenburg's Domestic Affairs Ministers steps down], *Spiegel*, September 23, 2017, http://www.spiegel.de/politik/deutschland/affaeren-brandenburger-innenminister-speer-tritt-zurueck-a-719177.html.

90 Abigail Fielding-Smith and Crofton Black, "The Rise of the German Alt-Right," EU Observer, September 20, 2017, https://euobserver.com/elections/139058.

91 Kim Hjelmgaard, "There Is Meddling in Germany's Election — Not by Russia, but by U.S. Right Wing," *USA Today*, September 20, 2017, https://www.usatoday.com/story/news/world/2017/09/20/meddling-germany-election-not-russia-but-u-s-right-wing/676142001/.

92 Michael Schwirtz, "German Election Mystery: Why No Russian Meddling?," *New York Times*, September 21, 2017, https://www.nytimes.com/2017/09/21/world/europe/german-election-russia.html.

93 "Wie die Regierung gegen Hacker zurückhacken will" [How the government wants to hack back against hackers], Süddeutsche Zeitung, April 20, 2017 http://www.sueddeutsche.de/digital/it-sicherheit-wie-die-regierung-gegen-hacker-zurueck-hacken-will-1.3469456; "German Intel Chief Accuses Russia of Cyberattacks in Run Up to Election," *Haaretz*, May 4, 2017, https://www.haaretz.com/world-news/europe/german-intel-chief-accuses-russia-of-cyberattacks-in-run-up-to-election-1.5468398.

94 Maria Fiedler, "Wenn der Staat zum Hacker wird" [When the state becomes a hacker], *Der Tagesspiel*, June 20, 2017, https://www.tagesspiegel.de/politik/bundestag-entscheidet-zu-ueberwachung-wenn-der-staat-zum-hacker-wird/19958354.html.

95 Interview with Thorsten Severin, May 7, 2017.

96 "The Federal Returning Officer and His Responsibilities," Federal Returning Office, https://www.bundeswahlleiter.de/en/ueber-uns/aufgaben.html.

97 Patrick Beuth et al., "Merkel and the Fancy Bear," Zeit, May 12, 2017, http://www.zeit.de/digital/2017-05/cyberattack-bundestag-angela-merkel-fancy-bear-hacker-russia/seite-6.

98 Ibid.

99 Berthold Kohler and Eckart Lohse, "Interview mit der Frankfurter Allgemeinen Zeitung" [Interview with the FAZ], Der Bundespräsident, June 16, 2017, http://www.bundespraesident.de/SharedDocs/Reden/DE/Frank-Walter-Steinmeier/Interviews/2017/170616-Interview-FAZ.html.

100 Dirk Banse and Uwe Muller, "Verfassungsschutz warnt vor russischer Einflussnahme [Office for the Protection of the Constitution warns of Russian influence], *Welt*, August 27, 2018, https://www.welt.de/politik/deutschland/article168021550/Verfassungsschutz-warnt-vor-russischer-Einflussnahme.html.

101 Interview with Thorsten Severin, May 7, 2017.

102 "Justizminister Maas will, dass Parteien auf Social Bots verzichten" [Minister of Justice Mass wants parties not to use social bots], *Heise Online*, July 14, 2017, https://www.heise.de/newsticker/meldung/Justizminister-Maas-will-dass-Parteien-auf-Social-Bots-verzichten-3771556.html.

103 Barry Schwartz, "Google Adds New Knowledge Panel to Provide Information About News Publishers," Search Engine Land, November 7, 2017, https://searchengineland.com/google-adds-new-knowledge-graph-learn-news-publishers-286394.

104 Eric Auchard and Toby Sterling, "Google and Sister Company to Offer Cyber Security to Election Groups," Reuters, March 21, 2017, https://www.reuters.com/article/us-cyber-election/google-and-sister-company-to-offer-cyber-security-to-election-groups-idUSKBN16S166.

105 Interview with Andrew Loebbecke, August 8, 2017.

106 Interview with Thorsten Severin, May 7, 2017.

107 Ibid.

108 Author interview with local expert, December 2017.

109 "Verwendung von Wahlcomputern bei der Bundestagswahl 2005 verfassungswidrig" [Use of voting computers in the federal election 2005 deemed unconstitutional], Federal Constitutional Court, March 3, 2009, https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2009/bvg09-019.html.

110 Annette Meiritz, "Comeback für Papier und Bleistift" [Comeback for paper and pen], *Spiegel*, March 3, 2009, http://www.spiegel.de/netzwelt/tech/grundsatzurteil-zu-wahlcomputern-comeback-fuer-papier-und-bleistift-a-610960.html.

111 Fragen/Antworten von Dr. Marie v. Mallinckrodt (ARD-Hauptstadtstudio) zum Einsatz unsicherer Software zur Bundestagswahl [Questions/replies by Dr. Marie v. Mallinckrodt (ARD-Capital studio) regarding the use of unsecure software in federal elections].

112 Kohler and Lohse, "Interview mit der Frankfurter Allgemeinen Zeitung" [Interview with the FAZ].

113 For example, the sale of the software is not meant for private individuals but local municipalities to restrict public access to it. Yet, manuals for the software including passwords could be found online. Default passwords of the software were also available online and included easily identifiable ones like "test." The security researchers also found ways to abuse the vulnerable upload-server to enable a one-click download of malicious code. "Software zur Auswertung der Bundestagswahl unsicher und angreifbar" [Software used to tally votes in Federal elections unsafe and vulnerable], Chaos Computer Club, September 7, 2017, https://www.ccc.de/de/updates/2017/pc-wahl; and interview with Thorsten Severin, May 7, 2017.

114 Kohler and Lohse, "Interview mit der Frankfurter Allgemeinen Zeitung" [Interview with the *FAZ*].

115 Kai Biermann und Holger Stark, "Die Bundestagswahl kann manipuliert werden" [The federal elections can be manipulated], *Zeit Online*, September 7, 2017, http://www.zeit.de/digital/datenschutz/2017-09/bundestagswahl-wahlsoftware-hackerangriff-sicherheit-bsi-bundeswahlleiter.

116 Ibid.

117 "Verhinderung von Manipulation der Wahlergebnisse hat für Bundeswahlleiter höchste Priorität" [Preventing manipulation of election results a top priority for Federal Returning Office], Federal Returning Office, September 7, 2017, https://www.bundeswahlleiter.de/info/presse/mitteilungen/bundestagswahl-2017/17_17_manipulation.html.

118 Interview with Thorsten Severin, May 7, 2017.

119 Schwartz, "Google Adds New Knowledge Panel."

120 Interview with Thorsten Severin, May 7, 2017.

121 Schwartz, "Google Adds New Knowledge Panel."

122 Angela Dewan, "Russia Sanctions: What You Need to Know," CNN, August 2, 2017, https://www.cnn.com/2017/07/25/europe/russia-sanctions-explainer/index.html.

123 Claudia Kade, "Steinmeier Meets Putin: The Visit Ends With Speechlessness at the Highest State Level," *Welt*, October 25, 2017, https://www.welt.de/politik/deutschland/article170052667/Mit-dem-Besuch-endet-eine-Sprachlosigkeit-auf-hoechster-Staatsebene.html.

124 "Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG)" [Law to improve law enforcement in social media (Network Enforcement Act – NetDG)], October 1, 2017, https://www.buzer.de/s1.htm?g=NetzDG&f=1.

125 Eike Kuehl, "Was Sie über das NetzDG wissen müssen" [What you need to know about the NetDG], *Zeit*, January 4, 2018, http://www.zeit.de/digital/internet/2018-01/netzwerkdurchsetzungsgesetz-netzdg-maas-meinungsfreiheit-faq/komplettansicht.

126 Stefan Krempl, "Netzwerkdurchsetzungsgesetz: UN-Beauftragter sieht Anonymität gefährdet" [Network Enforcement Act: UN official sees anonymity at risk], *Heise Online*, June 9, 2017, https://www.heise.de/newsticker/meldung/Netzwerkdurchsetzungsgesetz-UN-Beauftragter-sieht-Anonymitaet-gefaehrdet-3739692.html.

127 Beuth et al., "Merkel and the Fancy Bear."

128 Expert interviews by author in Berlin in December 2017.

129 "Software zur Auswertung der Bundestagswahl unsicher und angreifbar" [Software used to tally votes in Federal elections unsafe and vulnerable].

130 Maria Holmin and Mats Knutson, "Must-chefen pekar ut Ryssland som it-hot" [Head of intelligence points to Russian cyber-threat], *SVT Nyheter*, December 11, 2016, https://www.svt.se/nyheter/inrikes/must-chefen-den-aktor-vi-framfor-allt-ser-ar-ryssland?cmpid=del:pd:ny:20161211:must-chefen-den-aktor-vi-framfor-allt-ser-ar-ryssland:nyh.

131 "Så ska vi skydda valrörelsen från andra staters påverkan" [How we will protect the elections from the influence of other states], *Dagens Nyheter*, March 19, 2017, https://www.dn.se/debatt/sa-ska-vi-skydda-valrorelsen-fran-andra-staters-paverkan/.

132 "Sveriges säkerhet i en ny värld" [Swedish security in a new world] (speech by Stefan Löfven, January 14, 2018), Regeringskansliet, http://www.regeringen.se/tal/2018/01/sveriges-sakerhet-i-en-ny-varld/.

133 "Nationell säkerhetsstrategi" [National security strategy], Government Offices of Sweden, January 2017, http://www.regeringen.se/48e36d/contentassets/a02552ad9de94efcb84154b0f6ed76f9/nationell-sakerhetsstrategi.pdf.

134 "Nationell strategi för samhällets informations- och cybersäkerhet" [National Strategy for Society Information and Cyber Security], Swedish Ministry of Justice, June 29, 2017, http://www.regeringen.se/rattsdokument/skrivelse/2017/06/skr.-201617213/.

135 Camilla Hedquist, “MSB:s arbete med valet 2018” [MSB’s work on the 2018 election], Swedish Civil Contingencies Agency, May 30, 2017, https://www.msb.se/sv/Insats--beredskap/Psykologiskt-forsvar/Valet-2018/.
136 “Hemlig rapport visar hoten mot svenska valet 2018” [Secret report shows the threat to the Swedish elections in 2018], *Dagens Nyheter*, December 17, 2017, https://www.dn.se/nyheter/hemlig-rapport-visar-hoten-mot-svenska-valet-2018/.
137 Pontus Mattsson, “MSB ska skydda valet” [MSB will protect the election], *SVT Nyheter*, December 18, 2017, https://www.svt.se/nyheter/inrikes/msb-ska-skydda-valet.
138 Christoffer Karsberg, “Medieberedskap” [Media Preparedness], Swedish Civil Contingencies Agency, March 15, 2017, https://www.msb.se/sv/Forebyggande/Medieberedskap/.
139 Linda Kante, “Säpo tränar partier i IT-säkerhet” [SÄPO trains parties in IT-security], *Aktuell Säkerhet*, July 3, 2017, https://www.aktuellsakerhet.se/sapo-tranar-partier-i-it-sakerhet/.
140 “Säkerhetspolisens årsbok 2017” [Security Service Annual Report 2017], February 2018, http://www.sakerhetspolisen.se/publikationer/rapporter-amnesvis/om-sakerhetspolisen/sakerhetspolisen-2017.html.
141 “Samordnad cyberattack mot svenska myndigheter” [Coordinated cyber-attack against Swedish authorities], Sverige Radio, September 3, 2012, http://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=5256231.
142 “MUST årsöversikt 2016 – Försvarsmakten” [Swedish Military Intelligence and Security Service Annual Review 2016 - Armed Forces], Swedish Armed Forces, August 15, 2016, http://www.forsvarsmakten.se/siteassets/3-organisation-forband/hogkvarteret/must/must-arsoversikt-2016.pdf.
143 Olle Lönnaeus, “ÖB: Ryska cyberattacker mot Sverige varje dag” [Supreme Commander: Russian cyber attacks against Sweden every day], *Sydsvenska*, February 10, 2016, https://www.sydsvenskan.se/2016-02-10/ob-ryska-cyberattacker-mot-sverige-varje-dag.
144 “Attack on Sweden’s Media,” Radware, March 22, 2016, https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/sweden-attack-threat-alert/.
145 Anders Ygeman (@Ygeman), “En djupt oroande attack mot media och det fria ordet,” Twitter, March 19, 2016, 6:20 pm, https://twitter.com/ygeman/status/711316372647706624.
146 “Putin’s Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. Security,” U.S. Senate Committee on Foreign Relations, January 10, 2018, https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf.
147 The Macron campaign’s decision to ban RT and Sputnik from accessing campaign events is also noteworthy but unlikely to be replicated elsewhere. The Macron campaign was an active target of Russian propaganda and cyber attacks whereas its main opponent was an openly pro-Russian candidate. Under these circumstances, Macron’s decision seems reasonable but is rather drastic in most other contexts.
148 Dustin Volz, “Sessions Forms U.S. Cyber Task Force After Election Warnings,” Reuters, February 20, 2018, https://www.reuters.com/article/us-usa-cyber-taskforce/sessions-forms-u-s-cyber-task-force-after-election-warnings-idUSKCN1G42RB.
149 For an overview of the type of cyber security assistance available to state and local officials, see: “DHS Cybersecurity Services Catalog for Election Infrastructure,” U.S. Department of Homeland Security, 2018, https://www.eac.gov/assets/1/6/DHS_Cybersecurity_Services_Catalog_for_Election_Infrastructure.pdf.
150 Zaid Shoorbajee, “Election Infrastructure ISAC Created to Share Threats Specific to Voting Systems,” CyberScoop, March 16, 2018, https://www.cyberscoop.com/election-infrastructure-isac-dhs-cis/.

Carnegie Endowment for International Peace

The **Carnegie Endowment for International Peace** is a unique global network of policy research centers in Russia, China, Europe, the Middle East, India, and the United States. Our mission, dating back more than a century, is to advance peace through analysis and development of fresh policy ideas and direct engagement and collaboration with decisionmakers in government, business, and civil society. Working together, our centers bring the inestimable benefit of multiple national viewpoints to bilateral, regional, and global issues.

The **Carnegie Europe Program** in Washington provides insight and analysis on political and security developments within Europe, transatlantic relations, and Europe's global role. Working in coordination with Carnegie Europe in Brussels, the program brings together U.S. and European policymakers and experts on the strategic issues facing Europe.

The **Carnegie Cyber Policy Initiative** focuses on addressing international cyber policy challenges, as cyberspace is increasingly central to international security and diplomacy. The initiative develops and promotes norms and policy recommendations for enhancing international stability and security in cyberspace.

BEIJING BEIRUT BRUSSELS MOSCOW NEW DELHI WASHINGTON

THE GLOBAL THINK TANK

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

CarnegieEndowment.org