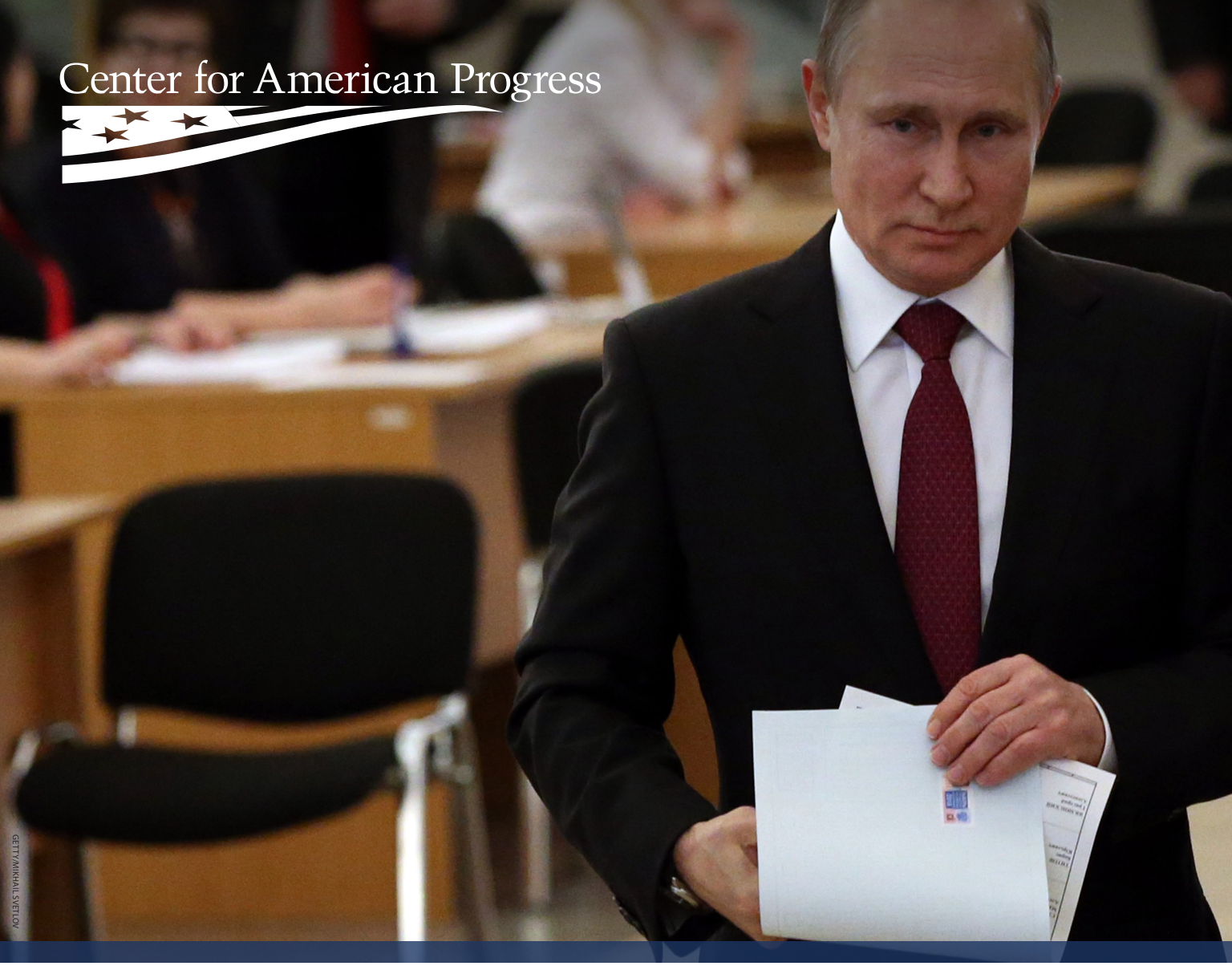
Center for American Progress



GETTY/MIKHAIL SVETLOV

Democratic Resilience

A Comparative Review of Russian Interference in Democratic Elections and Lessons Learned for Securing Future Elections

By James Lamond and Talia Dessel September 2019

Center for American Progress

Democratic Resilience

A Comparative Review of Russian Interference in Democratic Elections and Lessons Learned for Securing Future Elections

By James Lamond and Talia Dessel September 2019

Contents

Introduction and summary

The upcoming U.S. presidential election will be the first since Russia's extensive and systematic attack on the 2016 cycle. Unfortunately, the interference campaign did not end on November 8, 2016. Multiple law enforcement filings, intelligence warnings, private sector alarms, and watchdog group reports prove that Russia's attacks continued throughout the 2018 midterm elections—and continue to this day.

Every indicator suggests that Russia will continue to be actively engaged in disrupting U.S. democratic processes throughout the 2020 election cycle. Compared with midterms, presidential elections are more tempting because the potential return on investment is much greater. Foreign policy tends to play a larger role in debates, as presidents have a much larger executive say in foreign policy decisions than domestic policy. And in 2020, President Donald Trump, a politician for whom the Russian government has a preference and on whose behalf the Kremlin is willing to intervene, will mostly likely be on the ticket again.

To further complicate the matter, the threat of foreign interference goes beyond Russia. Countries such as China, as well as Iran and other Gulf states, are advancing their foreign interference capabilities.[1] And the lack of any substantive response to Russia's interference in 2016 has sent the signal to these countries—in particular, to China—that there are no consequences for interfering with American elections.[2] In fact, in an interview with ABC News, President Trump said he would accept information from a foreign state, creating a perverse incentive for foreign intelligence services to engage in such activity.[3]

Russian attempts to sow discord in the United States are ongoing, as Russian President Vladimir Putin continuously seeks to weaken and undermine Western democracies. Some lines of effort, such as disinformation, are perpetually active, even between election cycles. In fact, Project Lahkta, which was the code name given to the Russian disinformation campaign targeting the 2016 election, began in 2014 and ran through the 2018 midterm elections, and there is no reason to believe that it has ceased.[4] Others, such as a WikiLeaks-style hack and release campaign, can be specifically deployed during crucial campaign moments, but these can be

months, even years, in the planning.[5] Furthermore, Russia is consistently shifting and updating its interference tactics, making it even harder to protect future elections. Prior to the 2016 election, for example, candidates had little understanding of how troll farms could be used to influence voters, which made it difficult to defend against this new type of interference.

An election year presents a tempting target, then, a situation in which Russia can ramp up its ongoing interference attacks and launch brand-new ones for maximum impact. Therefore, it is matter of when and how—not if—Russia intervenes in the 2020 election. As Dan Coats, the former director of national intelligence, said, "The warning lights are blinking red."[6] Unfortunately, the Trump administration appears either unable or unwilling to put up a meaningful defense against foreign interference. The White House has refused even to recognize Russia's ongoing interference efforts and has prevented other government offices from raising the issue. In fact, the White House has reportedly told former Secretary of Homeland Security Kirstjen Nielsen not to raise election security with other Cabinet members.[7] The administration also dramatically downsized two offices at the U.S. Department of Homeland Security that were established to combat this issue—one on election security and the other on foreign interference.[8]

While the Trump administration itself appears unlikely to fight foreign interference, there are multiple stakeholders who have agency and can either contribute to, or curb, the impact of a foreign influence operation. These include voters; the press; political parties and candidates; and law enforcement and career government officials.

America is also not the only target for Russian influence operations; democracies in Europe and around the world are combating Russian election interference. Some of these countries have dealt with this interference better than others, and there are important lessons to be derived from these experiences. With these factors in mind, this report outlines Russian election influence operations and evaluates the responses from stakeholders. It determines the lessons the United States can learn from these democracies, including what works and what does not when confronting Russian interference.

There is no single formula for protecting democratic processes, nor is there a way to provide 100 percent guaranteed protection. However, based on this report's review of how other democracies have confronted Russian interference, it is clear that any successful strategy must be multifaceted and include a combination of a forceful government response, an alert and educated public, a trusted media, paper ballots, and efforts to monitor and combat illicit financial flows.

Russian strategy

In understanding Russia's approach to election interference, and therefore what methods the country is likely to employ or amplify during the 2020 election and beyond, it is helpful to take a step back and understand how such interference fits into Russia's broader geopolitical strategy. It should be noted that this report uses "Russia" as an umbrella term to describe efforts that are connected—often loosely—to the Kremlin. This may encompass military or intelligence services acting on direct orders, or oligarchs and friends of President Putin simply trying win his favor, though usually with explicit or implicit direction from the Kremlin.

Following Russia's 2016 interference campaign, analysts and journalists have spent a great deal of time dissecting Russian strategy, arguing that Putin has developed a new way of war.[9] Terms such as "hybrid war" and the "Gerasimov Doctrine" have become commonplace.[10] But in reality, Russia's interference campaign is a renewal of Soviet-era intelligence operations, dating back to the earliest days of the Soviet Union.[11] George Kennan, the American diplomat and architect of America's Cold War containment strategy, referred to this approach as "political war."[12] In a classified 1948 memo to the National Security Council, Kennan described what the Soviets were doing:

> *Political warfare is the logical application of Clausewitz's doctrine in time of peace. In broadest definition, political warfare is the employment of all the means at a nation's command, short of war, to achieve its national objectives. Such operations are both overt and covert. They range from such overt actions as political alliances, economic measures (as ERP—the Marshall Plan), and 'white' propaganda to such covert operations as clandestine support of 'friendly' foreign elements, 'black' psychological warfare and even encouragement of underground resistance in hostile states.*[13]

The Soviets themselves had a different term: active measures. This effort was considered the heart and soul of Soviet intelligence and run by a special branch of the

KGB's foreign intelligence directorate, Service A.[14] KGB Major General Oleg Kalugin described active measures, saying it is:

> *not intelligence collection, but subversion: active measures to weaken the west, to drive wedges in the western community alliances of all sorts, particularly Nato, to sow discord among allies, to weaken the United States in the eyes of the people of Europe, Asia, Africa, Latin America, and thus to prepare ground in case the war really occurs.*[15]

While influence operations are not new, and information warfare is as old as warfare itself, there has recently been an important development that has allowed these operations to be much more potent: advancements in information technology. The proliferation of social media has created a new venue to disseminate disinformation, fake news, and propaganda. Modern reliance on digital communications has created a new vulnerability for candidates and challenges to campaigns' operational security, as campaigns maintain a trove of information that state-supported hackers can steal and use how they see fit, including releasing to the public or to rival campaigns.

Information—both legitimate and fabricated—spread quickly in the digital age compared with successful efforts in the past, such as Operation Infektion, a Russian effort to undermine America's credibility in nonaligned countries. This 1990s conspiracy theory claimed that the U.S. military created HIV as a biological weapon. But it took three years for this planted scheme to make its way from a KGB-founded newspaper in India to outlets across developing nations.[16] It was one of the most successful disinformation campaigns in history—in spite of the years it took to spread—thanks to the KGB helping it along the way. Russia promoted it through overt propaganda outlets, had assets write pseudo-academic papers and present them at conferences, and employed allied intelligence agencies.[17] Compare this with the @TEN_GOP Twitter handle, a Russian troll farm account posing as the Tennessee Republican Party.[18] In a matter of a few weeks, the handle was retweeted by prominent figures close to President Trump, including Roger Stone, Eric Trump, Donald Trump Jr., and Kellyanne Conway, with more than a million followers among them.[19] This account peddled in racist and Islamophobic material, but it also advanced more specific policy decisions that played to the advantage of Russian intelligence, including advocating for firing former FBI Director James Comey and against prosecuting WikiLeaks founder Julian Assange.[20]

Putin's strategy is also not confined to American targets. Across Europe, Putin has been providing support in one way or another to movements and parties whose political platforms align with the Kremlin's objectives. There is evidence of Russian support for the Brexit vote in the United Kingdom; Marine Le Pen and the National Rally, formerly the National Front, in France; Alternative for Germany (AfD) in Germany; and the 5-Star Movement in Italy, just to name a few.[21] This type of support falls under Kennan's framework discussed above, as it uses a wide range of methods, either overt or covert, to achieve Russia's objectives. Whether Putin is supporting specifically anti-democratic parties or just parties whose victory would have a destabilizing effect, this support has a cumulative effect that amounts to a political assault. Each of these political assaults has helped to further three overarching goals:

1. To sow political and social discord in the target countries
2. To undermine and challenge the Western democratic system, especially in the eyes of transitioning democracies
3. To shift policies in target countries to undermine the trans-Atlantic alliance and the European project

To achieve these goals, Russia has deployed a multifaceted strategy, which has included a social media campaign, fueled by automated bots and online operatives or trolls, that drives disinformation and promotes divisive voices. This tactic was on display during the Catalonia independence referendum, where Russian bots and trolls were actively supporting the pro-secessionist movement.[22]

Another common method is funneling money to candidates aligned with the Kremlin's goals, often through elaborate schemes. This was exposed most recently in Italy, where a Russian-linked energy giant allegedly hatched a plan to funnel money to Deputy Prime Minister Matteo Salvini's Lega party ahead of the European Parliament election this past spring.[23] Another common method is the hack and release tactic of stealing information from individuals, either the candidates or those close to them, and publicly releasing the information in a way that benefits the candidate of choice. This was on display with different levels of success in both the 2016 American presidential election and the 2017 French presidential election.[24]

Most often, however, Russia deploys a combination of these tools, depending on the unique nature of the particular country's political culture and fault lines. While the political dynamics in each country are unique, each country's response to Russian election interference has yielded helpful lessons for other democracies. This report

contains a review of recent elections where evidence of Russian interference has been a factor, an analysis of how different stakeholders responded, and what lessons can be learned moving forward.

The issue of foreign political interference is immense and continually expansive. This report focuses specifically on election interference perpetrated by foreign actors—actions specifically meant to influence the results of elections taking place in democracies. Many of the countries discussed below, as well as others not included in this report, have been very successful in countering disinformation, ensuring access to multilingual news sources so that no ethnic group is dependent on any single source, and advancing civic education to curb foreign influence for generations to come, among other strategies. However, this report focuses on the more immediate and direct impact that foreign interference can have on elections. The goal is a better understanding of the threat environment ahead of the 2020 election as well as what responses and mitigation practices have worked best.

Case studies: Country-by-country review of foreign interference campaigns and responses

To gain better insight into how democracies in Europe have responded to Russian interference, this report analyzes some of the most high-profile examples that have taken place since the 2016 election. This list is not comprehensive and does not focus on cases from before the 2016 American election.

2017 French presidential election

Perhaps the most important case study of Russian interference abroad was France's 2017 presidential election. This was in many ways a major test for the trans-Atlantic democratic community following the 2016 American election. The May 7 runoff election between the top two candidates offered a stark choice. Emmanuel Macron's En Marche! presented a new and rejuvenated vision of a pro-EU, moderate platform. On the other hand, Marine Le Pen's National Front ran on an anti-NATO, anti-EU, anti-immigrant, and pro-Russian platform. Le Pen and her party also had deep ties to Russia. When the party was in financial trouble, it was an obscure Russian bank, the First Czech-Russian Bank, that came to its rescue with a 9.4 million-euro, or $12.2 million, loan.[25] Le Pen even flew to Moscow just a few weeks ahead of the election to meet with President Putin. After the meeting, Le Pen said, "A new world has emerged in these past years. It's the world of Vladimir Putin, it's the world of Donald Trump in the US. I share with these great nations a vision of cooperation, not of submission."[26]

This was clearly a tempting target for Russia. And it acted.

Russia launched a coordinated attempt to undermine Macron's candidacy. Much like Russian interference in the 2016 American presidential campaign, the political assault was multifaceted, consisting of a disinformation campaign that included rumors, fake news, and the planting of forged documents; a cyberintrusion of the campaign staff and advisers; and a leak of stolen data timed to influence the election, just ahead of a media blackout. Just as in the U.S. case, the disinformation and stolen material were spread through an advanced network of bots and an army of trolls. It is also worth

noting that real-life alt-right activists not using fake personas played a major role. For example, the first person to use the hashtag #MacronLeaks—eventually adopted as the moniker for the entire series of events—was not a Russian troll or bot, but the American alt-right activist Jack Posobiec.[27]

In the end, the political assault on France was not successful enough to sway voters. Macron won the runoff election against Le Pen with 66.1 percent of the vote.[28] This makes France an important case study for two reasons. First, it was perhaps the most expansive foreign interference campaign Russia launched since the 2016 American election. But perhaps more importantly, it did not work. There was clearly a preferred Russian candidate in Le Pen, and yet Macron won a resounding victory despite Russian interference efforts.

Several factors limited the impact of Russian interference.

Like many countries in the post-2016 threat environment, the French government took Russian interference very seriously. The country's National Cybersecurity Agency (ANSSI), which is responsible for protecting government and key industries from cyberattacks, provided cybersecurity awareness-raising seminars for political parties, which all parties except Le Pen's National Front accepted. Similarly, the National Commission for the Control of the Electoral Campaign for the Presidential Election (CNCCEP) was a special body set up in the months preceding the election to serve as a campaign watchdog. The ANSSI and the CNCCEP both frequently alerted the media, political parties, and the public to the risk of cyberattacks and disinformation during the presidential campaign. Then-President François Hollande even ordered a "mobilization of all the means necessary" to face down cyberattacks.[29]

In addition to alerting the public to the threat, the French government issued warnings to Russia at multiple levels of government and in both public and private settings. The French foreign minister pledged before Parliament that France would not tolerate Russian interference.[30] President Hollande also warned President Putin in private. The French government's response was distinctly nonpartisan. These warnings came from the outgoing administration, even though the attacks targeted a different candidate. This was not treated as a partisan issue but rather as one of national security.

To help combat disinformation, trusted well-established newspapers such as *Le Monde* created platforms to verify the reliability of a piece of information's sourcing. Google also partnered with more than 30 media outlets, including mainstream newspapers and television stations, to build the CrossCheck fact-checking platform.[31]

Additionally, the French government engaged in the fight against disinformation when and where appropriate. For example, Russian state-run media outlet Sputnik ran a story during the first round of the election saying that François Fillon, the former French prime minister and supporter of improving ties with Russia, was leading the race. The story, which cited a Moscow-based analytics firm, was counter to every mainstream French poll, which showed Fallon in third place. The timing of the story was also notable: It was published when Macron was rising in the polls. In response to this event, the French polling commission issued a strong warning against polls deemed illegitimate under French law, making clear that the Sputnik story was not reliable.[32]

France also benefits from some preexisting structural advantages to countering disinformation. According to a Center for Strategic and International Studies study, the French media environment consists mainly of mainstream and trusted media sources: The "tabloid-style outlets and 'alternative' websites that are common in the United States and United Kingdom" are just not as common or prominent in France's media culture.[33] This provides a certain level of inoculation from the conspiracy theories and fake news phenomenon.[34] In fact, 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.[35]

The Macron campaign, which was the primary target of the Russian influence effort, took action itself and benefited from several of the preexisting advantages. Throughout the campaign, En Marche!—the movement and later political party backing Macron—communicated openly and extensively about its being targeted by hackers and about the hacking itself once it took place. The group also publicized the hacking attempts against it, which, in turn, generated awareness among the population and the authorities. French election laws require a blackout period that prevents the media from quoting presidential candidates or their supporters within 44 hours of the vote, and the electoral commission issued warnings that anyone who published stolen material obtained in the hacking attack against Macron's campaign would be prosecuted. The blackout period and the prosecution threat appear to have been effective and were observed, and, as a result, most French voters did not see the material stolen from the Macron campaign.[36] In fact, when the #MacronLeaks documents were released, the campaign reacted quickly, issuing a press release just ahead of the mandated media blackout making clear that "the movement had been the victim of a massive and coordinated hacking operation."[37]

En Marche! also employed some creative tactics to mitigate the impact of a cyberattack. For example, assuming that it would be hacked, the campaign deliberately

planted forged documents and fake emails intermingled with real ones. Doing this, and telling the press what they had done, confused hackers and created a situation where the whole population questioned the authenticity of any leaked material, blunting the impact of any potentially damaging real information.[38]

2019 European Parliament election

This past May, the European Parliament held an election across the regional bloc, in what was quite possibly the most closely watched European Parliament election in history.[39] With voters out in record numbers, the election was pivotal for the future of Europe.[40] As the Center for American Progress' Max Bergmann explained, it showed that "Europe's political center of gravity is shifting from national capitals to Brussels and the European Union."[41] At the core of this newfound enthusiasm for the pan-European election was a debate about the European Union's future, with far-right, anti-EU nationalists pitted against the pro-European political groups. Given these fundamental dynamics at stake, fears of Russian interference were high. In the end, the much-feared far-right, Euro-skeptic wave turned out to make less of a splash than anticipated. The traditional center-right and center-left parties that have dominated European politics lost seats to smaller parties such as the European Greens and a variety of populist groups. Over all, populists and Euro-skeptic parties increased their percentage of seats from around 20 percent up to 25 percent.[42]

While a full-scale Russian interference attack was not detected during the election, the European Commission did detect significant disinformation campaigns aimed at the election, finding that Russian-linked actors used disinformation tactics to undermine the European Union's credibility and drive down voter turnout.[43] These campaigns used, among other approaches, bots and fake accounts to spread divisive messages.[44] The findings stopped short of attributing these efforts to the Kremlin, which denied any election interference, and did not assess the efficacy of these disinformation tactics.[45]

European leaders attributed the absence of a more serious Russian attack to their intense preparation. A joint statement issued in the month following the election stated, "Our actions, including the setting-up of election networks at [a] national and European level, helped in protecting our democracy from attempts at manipulation. We are confident that our efforts have contributed to limit[ing] the impact of disinformation operations, including from foreign actors, through closer coordination between the EU and Member States."[46]

The European Union's defensive actions ahead of the election focused on several areas of improvement.[47] It established its Rapid Alert System (RAS) in March 2019 to improve cooperation and coordination among member states around issues of disinformation.[48] The platform sought to link all EU member states, allowing them to "share information and spot trends."[49] Only one-third of the states contributed to the system prior to the election, however, and serious concerns have been raised about the standards in place for the alert system.[50] *The New York Times* reported that the RAS had questionable success, noting one particular instance where it appears an overabundance of caution and unclear reporting standards led analysts to make a decision to not send an alert about Twitter accounts spreading disinformation regarding Austrian politics.[51] European officials interviewed by *The New York Times* revealed concerns that internal politics had led to a slow and ineffective system. Another complicating factor is that due to free speech concerns, the system, understandably, does not address domestic disinformation; when domestic actors use Kremlin tactics to spread their messaging, this can further obscure foreign interference.[52] Analysts are under constraints when it comes to debunking information that originates from European media sources due to concerns over free speech, meaning that far-right propaganda originating from Europe is often permitted to go unchecked.[53]

Various tech and social media companies, including Facebook, Google, Twitter, and Mozilla, signed a code of practice in 2018 that contained suggestions for how these companies could assist in defending elections from foreign interference.[54] The code of practice suggestions include increasing transparency around political advertisements, closing fake accounts, and advocating for the "demonetization of purveyors of disinformation."[55] While these recommendations are certainly sound, the impact of signing the code is unclear, and one postelection review indicated that only Facebook increased the transparency of issue-based ads.[56]

The European Union also worked to broaden its ability to identify disinformation by establishing the European External Action Service East StratCom Task Force.[57] This task force sought to identify, research, and analyze Russian disinformation campaigns, producing the weekly Disinformation Review based on professional media monitoring and disinformation analysis.[58] It maintains a website, EU vs Disinfo, which hosts a "database [of] over 3,800 disinformation cases since September 2015"; publishes news and analysis about Russian-linked disinformation campaigns; and links to additional reports and articles on the subject.[59] The European Union also made a clear and strong effort to promote media literacy, even holding a European Media Literacy Week in March 2019.[60]

One other critical story about Russian interference efforts during the European Parliament election is the alleged financial connection between Russia and Italy's far-right Lega party headed by Matteo Salvini, which won 34 percent of the vote in the 2019 election.[61] In February, an investigative exposé by *L'Espresso* revealed plans for an elaborate arrangement to covertly channel tens of millions of dollars of Russian oil money to the Lega party for the European election.[62] Since then, Buzzfeed has reportedly obtained the recording of a meeting discussing the details of such a potential plan.[63] The meeting came one day after Salvini denounced sanctions on Russia and met with a top Russian deputy. It is unclear if the deal ever went through or helped affect the European election. Italian prosecutors are reportedly investigating the matter, and Salvini has denied any involvement in the deal as well as taking any foreign money.[64]

2018 Swedish general election

In September 2018, Sweden held a general election that ended with both the center-left and center-right parties losing seats and the populist anti-immigrant Sweden Democrats gaining power.[65] Moscow had much at stake in the outcome of the Swedish election from a geopolitical perspective: A member of the European Union, Sweden is not a member of NATO, although it does have a partnership with the alliance. Additionally, support for Sweden joining the alliance as a full member has been increasing in recent years amid an increasingly assertive Russia.[66] Therefore, interfering to shift power away from parties that supported joining NATO or strengthening Sweden's relationship with the West would have been beneficial to Russia.[67]

Leading up to the election, the Swedish government was extremely vocal about the Russian interference threat, raising situational awareness and regularly updating the public about how the government planned to secure the election.[68] In early 2018, the director of the Swedish Security Service stated that "the biggest threat to our security in that perspective is Russia," and the top Swedish counterintelligence official said, "Russian espionage is still the biggest threat to Sweden."[69] Having closely monitored Russia's interference in the United States and in other European countries, Sweden took an ambitious, "whole-of-society" approach to preparing for possible foreign election interference, which included working with media outlets and the private sector.[70] The government also announced early in the year that it was establishing a new agency "responsible for psychological defense … to counter disinformation and foreign influence."[71]

In December 2018, after the election, the Swedish Security Service stated that although foreign influence operations were carried out, the election was not affected.[72] In addition to these influence attempts, "state-backed IT incidents were carried out" against various parties involved in the election, although the Swedish Security Service did not attribute these incidents to a particular foreign government.[73] The Swedish Security Service did note, "No extensive influence campaigns were carried out" and attributes this in part to the country's preventative work and to the attention that such interference campaigns have received.[74]

An analysis published by the Institute for Strategic Dialogue and the London School of Economics' Institute of Global Affairs noted that Russian state-sponsored media tried to "smear Sweden's reputation internationally," and in the lead-up to the election, propaganda tried to present Sweden as "a country in demise."[75] Russian state-run media outlets also amplified far-right Swedish groups. The report noted that "while efforts by Kremlin actors to influence the election directly were apparently limited," Russian state-run media worked to smear Sweden.[76] In the lead-up to the election, media outlets RT and Sputnik increased their Sweden-focused reporting.[77] In various languages, not including Swedish, RT also focused its broadcasting and online coverage far more on issues such as Swedish migration policy than it had before.[78] RT also released an English-language documentary titled "Testing Tolerance," where it discussed Swedish migration issues "with a heavily biased slant supporting the voices of anti-immigrant parties and activists."[79] The documentary aired in June 2018, but most of the online engagement came from the United States, with only 13 percent coming from Sweden.[80]

In March 2019, the Swedish Security Service issued a press release titled "Facing a wider range of threats in 2018."[81] The head of the service is quoted in the release as saying, "Russia in particular has improved its ability to actively and covertly influence other states."[82]

The government placed a heavy emphasis on educating citizens about the threat of election interference.[83] These efforts spanned the entire population, from primary schoolchildren to adults. The government launched efforts to teach "digital competence" in primary schools to instruct children on how to distinguish reliable sources from unreliable ones, and high school students were educated about Russian propaganda.[84] Sweden also distributed pamphlets to 4.7 million households earlier that year titled "If Crisis or War Comes."[85]

On the issue of fake news, the government worked closely with the media, holding trainings and helping them identify and respond to fake news.[86] The government also held "regular, voluntary dialogue" with the media to discuss disinformation.[87] The Swedish Civil Contingencies Agency (MSB) held quarterly information exchanges and offered training to media outlets "to increase their capacity to spot and respond to falsified information pertaining to the election." The MSB has begun combating fake news stories by making sure the correct information is available to the citizenry.[88] Swedish media outlets also took their own initiative, most prominently by developing a "joint fact-checking initiative to combat both domestic and foreign disinformation."[89]

The government also gave both government and party officials handbooks to educate them on how foreign actors may try to interfere in the election[90] and to identify influence operations.[91] It also gave politicians at all levels a handbook that included "tips and guidance about disinformation campaigns, password protection, and cyber etiquette."[92]

Additionally, the government worked closely with social media companies such as Facebook to combat fake news, with a "Facebook hotline" provided for officials to report fake pages.[93] Facebook reportedly also took initiative in pledging "to report suspicious behavior around the election to Swedish authorities."[94]

In August 2018, the month before the election, the Swedish Security Service issued a press release titled "Attempts to influence confidence in the election process."[95] The service stated it had "noted attempts to damage confidence in the election process" but said that these attempts had been expected and did not "put the election result at risk."[96] These activities reportedly included electoral fraud, fake social media accounts, disinformation, denial of service attacks, and hacking attempts. While the Swedish Security Service stated it could not see "any extensive influence operations suspected of being orchestrated by foreign powers," it did note that Russian foreign media was attempting to "polarize Swedish society by making the country look bad."[97]

The incredibly forceful and proactive approach from the government is perhaps the most important lesson from the Swedish experience. Unlike many other Western governments that were caught off guard by Russian interference, the Swedish government was prepared and vigilant, working through multiple channels to prevent Russia's interference campaign from being more effective.

2017 German national election

Germany held its federal election in September 2017, almost a full year after the U.S. presidential election. From the outset, the election was marked by concerns over the rise of the far-right AfD party, its ties to Russia, and fears that Germany would be the next Western democracy to see a right-wing, anti-Europe, illiberal, and pro-Russia party come to power, potentially through the support of the Kremlin.[98] In the end, Angela Merkel won a fourth term as German chancellor, although forming a new coalition with four parties that "span the political spectrum" proved to be a difficult and lengthy process.[99] The AfD was able to claim victory as well, becoming the third-largest party represented in the Bundestag—and a new force in German politics.[100]

Germany and Russia have deep historical ties that create a complicated and often tense relationship.[101] And because Chancellor Merkel had been the primary driving force in Europe behind sanctions against Russia, the German government was keenly aware that the election created a very tempting target for the Kremlin. German officials were also worried that 16 gigabytes of data stolen by Russian hackers in a 2015 hack of the German Bundestag could be released prior to the vote, although no such release occurred.[102] As such, Germany was on high alert for foreign interference.

The AfD has an ardent anti-EU, anti-immigrant platform and is committed to fostering better German-Russian relations, which closely aligns with the Kremlin's goals. It is perhaps unsurprising then that the party's rise was due in part to its connections to Russia and Russian emigrants inside Germany. The Alliance for Securing Democracy (ASD)—a trans-Atlantic initiative formed to combat foreign efforts to undermine democracies—revealed that Russian online influence operations were strongly supporting the AfD's messages on the ASD's German-language dashboard."[103] The Atlantic Council's Digital Forensic Research Lab also demonstrated how Russian-linked troll and bot networks repeatedly amplified the AfD's messages.[104] Russian state-funded media also eagerly boosted the party, providing it with a platform and an outsize voice, particularly among the Russian-speaking population. The AfD also benefited from strong support from the Russian emigrant community living in Germany; in fact, the party estimated that as much as one-third of its support came from Russian-speaking voters.[105]

Leading up to the election, the German government was extremely vocal about its concerns over the threat of Russian election interference. First and foremost, the government took serious measures to shore up its cybersecurity to defend against election interference. These steps included publishing a government cybersecurity strategy

in 2016, creating a Cyber Defense Center, and creating a Cyber and Information Space Command as a branch of the German armed forces. The Federal Office for Information Security also ran tests on computer systems to ensure they were ready for an attack.[106]

Chancellor Merkel took a particularly strong stance.[107] Months before the election, Merkel held a meeting with the German Federal Security Council. Because the council only meets when the country faces the most serious threats, simply holding the meeting sent a significant message about the gravity of the issue and the government's posture. The Federal Security Council also developed a "hack-back" strategy, which involved the planned use of offensive cyberattacks to fend off hackers.[108]

Officials also sent a clear message to the Kremlin. Chancellor Merkel, heads of the security agencies, and German President Frank-Walter Steinmeier had all issued warnings about potential Russian election interference.[109] The message from the German government was clear and unified: It would not tolerate Russian interference.

Situational awareness among voters was a key factor as well. German officials routinely warned the public about the ongoing threat, with the head of Germany's foreign intelligence services saying cyberattacks could "delegitimiz[e] the democratic process."[110] Merkel also repeatedly warned about fake news.[111]

This situational awareness and alerts extended to the media. As one German election official stated, the media had a "significant responsibility to be diligent in their reporting."[112] But Germany's relationship with the press is also an important contributing factor, as the German public generally trusts more "traditional news media sources."[113] The country has also developed new independent media organizations that call out disinformation. Importantly these groups enjoy a high degree of public trust and set up important fact-checking operations to prepare for the election.[114]

The German government also offered assistance to the political parties. The German Federal Office for Information Security offered to assist parties to shore up their defenses, and Germany's domestic security agency, the Federal Office for the Protection of the Constitution, shared information about risks with the parties.[115] In order to cover as much ground as possible, the German government divided the election defense duties.[116] Recognizing that both the electoral process and the campaigns themselves needed to be protected, the government worked on defending the election infrastructure while the political parties and media took responsibility for the attacks

on the campaigns.[117] This strategy acknowledged that defending an election against foreign interference should be a group effort: It requires the government, the media, and political parties to work in tandem.

Social media and internet companies also took measures to deter interference. Facebook offered trainings for parties on cybersecurity basics, and Google organized educational materials on how to protect elections.[118]

German political parties proactively created an atmosphere that curbed the impact of Russian interference. With the encouragement of the German government, all the political parties, with the notable exception of the Russia-aligned AfD, pledged not to use social media bots, and parties also pledged to not use leaked information.[119] Political parties also took steps to strengthen their defenses against hacks, training their leadership on cybersecurity basics.[120] At least one party also planned ahead for a worst-case scenario, readying a statement that could be immediately released in the event it was hacked.[121]

Germany also benefited from certain structural advantages. For example, the country's election infrastructure encompasses many of the more common best practices to prevent illicit interference. Unlike many American states that use electronic-only machines, Germany uses paper ballots that are hand counted.[122] Germany's multiparty system also adds a layer of defense.[123] In contrast to the American two-party system, a total of six parties have to form a coalition through negotiations, making a much more complex and difficult political dynamic for the Kremlin to manipulate.[124]

Russian support for the AfD has deepened societal rifts and promoted what were previously fringe political stances in German politics, achieving one of Putin's goals of destabilizing major Western countries. Aside from supporting disruptive organizations, other common Russian interference tactics, notably disinformation, had less of an impact in the 2017 election. This is in large part because German voters are less susceptible than voters in many other democracies.[125] This can partly be attributed to the German public's awareness and the country's own experience with disinformation. Germany has already dealt with several high-profile instances of fake news having real-world effects, and, as a result, there has been a degree of inoculation against its impact. However, the government, the media, and political parties all took a very strong posture against Russian interference, sending a clear message that Germany was on guard and that foreign interference will not be tolerated. After all, influence campaigns such as these tend to work only if no one is expecting them.[126]

Brexit, Trump, and Russia's strategic use of business relationships

In 2016, two major votes shook the world. The victors for each seemed to some to have come out of nowhere for surprise wins that few thought were possible. Both professed to be capturing populist outrage toward the ruling elite and sought to overturn the status quo. Both deployed new campaign techniques that claimed to revolutionize digital campaign technologies.

But as reporters and investigators have focused more on each of these votes, there appears be one even more important parallel: Both of the winning parties had suspect business ties to Russia.

These votes are, of course, the "yes" vote in the British referendum on Brexit, funded largely by Arron Banks, and the victory of Donald Trump in the 2016 U.S. presidential election.

Because this report only examines cases that occurred after the latter, both the Brexit referendum and the 2016 U.S. presidential election fall outside of the scope of this report. However, both votes were targeted by Russian interference campaigns and can provide helpful lessons for future elections. In particular, these cases highlight Russia's strategic use of business relationships to wield influence abroad.

Both Arron Banks' and Donald Trump's business dealings with Russia around the same time as their respective political campaigns highlight a consistent pattern that should raise red flags for those looking to prevent future influence efforts.

First, just months ahead of the vote, both men became involved in too-good-to-be-true business opportunities in Russia where they were in a position to make enormous profits. For Banks, it was a multibillion-pound deal to oversee the consolidation of six Russian gold-mining companies, creating one behemoth company. The deal was proposed by a Kremlin-linked oligarch.[127] For Trump, it was a long-sought-after deal to build the tallest building in Europe, the Trump Tower Moscow, which would have reportedly made the Trump Organization a staggeringly large profit—possibly "hundreds of millions of dollars."[128] Both men actively pursued these deals in parallel with their political campaigns.

Second, under both deals, state-owned banks were allegedly going to be used to finance the deals—meaning both men knew that the Russian government was involved. On January 12, 2016, Andrew Umbers, Banks' business associate, sent Siman Povarenkin, the Kremlin-linked oligarch behind the gold-mining project, a proposal. It noted that funding would be "provided in concert with Sberbank's bank debt support," and in the proposal was a request for a meeting with Sberbank,[129] a Russian government-owned and sanctioned investment bank.

For Trump, it was a different Russian state-owned bank: VTB. According to emails between longtime Trump business associate Felix Sater and Sater's childhood best friend and personal Trump attorney Michael Cohen, VTB President and Chairman Andrey Kostin was allegedly on board to fund Trump Tower Moscow.[130] VTB was also under sanctions at the time the deal was being negotiated, meaning that American citizens and companies were forbidden from doing business with it.[131] VTB has denied any involvement in the Trump Tower Moscow project, and it is unclear how far the talks went between the Trump team and VTB. However, it is clear that Trump's personal attorney was told that a sanctioned state-owned Russian bank was going to be involved in the project, and that he eagerly pursued the deal nevertheless.

Third—and perhaps most revealing—both men repeatedly denied that they had any business relationship with Russia. Banks has said, in no uncertain terms, that he had no business with Russia. When asked if he had invested in Russia, Banks replied, "No. Flat. Zero. Nothing. In fact, I wouldn't do. Because I know it is a complicated place to do business."[132] This echoes quite clearly Trump's repeated claims—23 times by *The New York Times'* count—that he has "no deals" with Russia, no business there, and "nothing to do with Russia."[133]

Finally, both men donated large sums of money to their own respective campaigns without it being clear from where that money came. According to the study by the British parliamentary investigation, Arron Banks is believed to have donated 8.4 million pounds to the leave campaign, which would make it the largest political donation in British political history.[134] However, Damian Collins, the chair of British Parliament's Digital, Culture, Media and Sport Committee, notes that it is unclear from where Banks obtained that amount of money, adding, "He failed to satisfy us that his own donations had, in fact, come from sources within the UK."[135] Meanwhile, Trump used millions of dollars of his own money on his own campaign—$66 million, according to his disclosure forms.[136] At the time, this raised major questions from financial analysts who doubted such a famously debt-laden, illiquid businessman could find that much cash on hand.[137]

The similarities go on. During both campaigns, the Russian ambassador was an important interlocutor. In Banks' case, the gold deal offer came through the Russian ambassador in London; in Trump's case, senior campaign advisers including Jeff Sessions, Jared Kushner, and Michael Flynn, communicated with the Russian ambassador to the United States during the campaign and transition periods.[138] And in both campaigns, Cambridge Analytica played an important role. Banks reportedly wanted to work with Cambridge Analytica on fundraising issues, and Cambridge Analytica sent a team to work with the Trump campaign's digital director on data analysis during the campaign.[139]

But the question remains: Why were both of these men suddenly presented with such lucrative business deals, financed by the Russian government, right before their respective national votes?

2017 Dutch general election

In March 2017, the Netherlands held a general election. Many in the international community saw this election as a test for Europe; once again, a far-right candidate surged in a liberal, democratic country.[140] In the end, however, the center-right Prime Minister Mark Rutte prevailed, providing a degree of reassurance to the rest of Europe that the far-right wave cutting across the West was not inevitable.[141] Other European leaders expressed relief at the election results. Merkel stated it was a "good day for democracy" and Macron, who was at that point a candidate, stated that the election showed, "A breakthrough for the extreme right is not a foregone conclusion."[142]

The Dutch are no strangers to Russian interference. In 2014, Russian-backed separatists were responsible for downing Malaysia Airlines Flight MH17 over Ukraine, killing 298 people total and 196 Dutch citizens.[143] Russia immediately launched a massive disinformation campaign denying any involvement in the crash, using both social media and more traditional Kremlin-controlled media outlets, blaming Ukraine and circulating conspiracy theories about the crash.[144]

In 2016, the Dutch public rejected a referendum on an EU-Ukraine trade agreement, in which Russian involvement is widely suspected.[145] Dutch intelligence agencies also had a front-row seat to Russian influence operations during the 2016 U.S. election. The Dutch General Intelligence and Security Service (AIVD) had infiltrated the hacking group APT29, more commonly known as Cozy Bear, as far back as 2014.[146] The group has been linked to Russian intelligence and was one of the Russian hacking units behind the Democratic National Committee (DNC) hack in June 2016. The AIVD monitored Cozy Bear as it hacked the DNC prior to the U.S. presidential election, reportedly alerting U.S. authorities of the hack and passing along the information.[147]

The 2017 Dutch general election appears to have been conducted without major incident or interference. This success can likely be attributed to some combination of active defensive preparations by the Dutch and a lack of resolve on the part of Russia to actively intervene.

The AIVD assessed that Russia attempted to influence the Dutch election primarily through the use of disinformation and hacking but was ultimately unsuccessful in these attempts.[148] The AIVD concluded that the Russian effort mostly consisted of spreading false information, although in the months leading up to the election, Russia also reportedly "tried hacking email accounts of Dutch government employees."[149]

However, similar to what occurred in other European countries following the 2016 American election, the Dutch government took seriously the threat from foreign interference and launched a proactive and robust response, raising awareness among political parties and organizations.[150]

Many of the government's actions were taken with the specific goal of ensuring the public had full trust and confidence in the election so that the results of the vote would not be called into question.[151] The Dutch government also produces annual reports describing Russian efforts.[152] This measure mimics steps taken by the Baltic nations, which also publish annual reports detailing activities by Russian intelligence services and the governments' responses.[153] These reports help the public understand the imminent threat and serve as a way for the government to openly recognize Russian interference attempts, either election-related or otherwise.

In addition to publicly acknowledging the threat, the Dutch government worked with voters directly to prepare them for potential fake news campaigns. To this end, the government led efforts 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."[154]

Similar to Germany, the Dutch also had certain structural advantages to protect from cyberintrusions into their election infrastructure. Perhaps most importantly, the Netherlands employs an entirely technology-free approach to elections to ensure the election infrastructure cannot be hacked or tampered with. The government banned electronic voting and electronic ballot counting in 2007 and implemented additional protocols to prevent Russian hacking, including prohibiting election officials from using USB flash drives and email.[155] The electronic ban goes beyond just using paper ballots; the entire process is paper based.[156] Voters mark their paper ballots, which are then reviewed manually by volunteers. Election officials then hand-carry the tallies from one office to another, until the total tallies finally make their way by hand to the Hague. This was a deliberate move by the Dutch government to recognize the threat to election infrastructure and employ the closest thing to a foolproof method as possible. When announcing the decision to hand-count the votes, the Dutch interior minister stated that "no shadow of doubt can be allowed to hang over the result."[157]

Another important factor is that, as in Germany, mainstream Dutch media outlets have a high degree of public trust.[158] The main component of the Dutch media's response to the Russian interference threat seemed to be a fact-checking operation. Facebook also took the initiative, much like it did in Sweden, to introduce a fact-checking function

on its platform.[159] A Dutch media outlet and public university were given access to a Facebook dashboard highlighting articles that users marked as "fake news."[160] The outlets could then fact-check the article and mark it accordingly.

The Dutch government has also made a concerted effort to support Russian-language journalism that is not linked to the Russian government.[161] The Dutch minister of foreign affairs, when announcing a $1.4 million grant for such programs, stated that "misinformation from Moscow is a threat to media diversity in all countries in which Russian is spoken. However, counterpropaganda is ineffective and goes against democratic principles. We wish to support the work of independent media initiatives without dictating what they should write or broadcast."[162]

While the Dutch government and media's robust and proactive response certainly played an important role in limiting the impact of Russia's interference, there is also reason to believe that Russia decided not to intervene. Russia and the Netherlands are significant trading partners, and the Kremlin may have made the calculation that it did not want to risk damaging that relationship by being caught intervening in domestic affairs.[163] Russia may have been trying to avoid any more conflict with the Netherlands after the downing of Flight MH17 over Ukraine. The Netherlands held Russia formally and directly responsible for the crash.[164] Russian actors may have also lacked the foreign-language skills necessary to mount more intricate online disinformation campaigns; while the Internet Research Agency's "translator project" operated in English during the 2016 election, not much is known about the Russian troll farm's language capabilities in smaller language groups such as Dutch.[165] The full extent to which Russia chose to interfere will likely remain unclear, but the robust efforts by the Dutch government clearly played a role. If the Kremlin thought it could intervene without resistance or consequences, it almost certainly would have. However, Dutch officials made it very clear that there would be strong resistance and that an interference campaign could lead to severe consequences.

2017 Catalan independence referendum

Russian interference in the 2017 Catalan independence referendum is well documented, but this case study is markedly different from the other examples cited in this report, as it dealt with the question of secession and independence and was ultimately ruled illegal by the Spanish courts.[166] Nevertheless, instances of Russian interference in a vote for which the government refused to recognize the results are still dangerous. This interference campaign gave Russia another chance to practice and improve its election interference tactics. During the referendum, a significant amount of Russian bot activity was detected, and observers raised questions about illicit Russian money in Catalonia.[167] Bots and Russian money were both issues during the 2016 U.S. election, and those looking to secure the 2020 election should be aware of how Russia has been using and adapting these techniques over the past three years. In addition, Russian interference in the Catalan referendum is a clear example of how Russia supports secessionist movements in order to achieve its goal of destabilizing Western countries. The United States is not immune to this type of support, as Russia has already shown an interest in the Texas and California secessionist movements.[168]

In October 2017, the Catalonia region of Spain held a referendum on the question of whether or not the region should secede from Spain.[169] Although a strong police presence from national forces tried to prevent people from voting, the vote took place with 90 percent of voters voting in favor of leaving—although voter turnout was only at 42 percent.[170]

Russia has long supported secessionist movements in the West and throughout the world, holding a Dialogue of Nations conference in Moscow and funding an Anti-Globalization Movement.[171] The logic is very simple: support and amplify destabilizing movements whose messages undermine the legitimacy and credibility of democratic governments and whose claims tear at the social cohesion of NATO countries. It is no surprise, then, that the independence referendum was a ripe target for Russia to intervene. Russian support for the Catalan independence movement primarily took the form of an influence operation. Russian state-run news outlets published articles alleging corruption in the Spanish government and promoted "an overarching anti-EU narrative" before the election, and Russian bots also amplified posts that supported the independence movement.[172] The interference campaign also included attempted email cyberattacks against individuals who opposed the independence movement.[173]

Catalonia's ties to Russia, particularly the more unsavory elements of Russia, long predate the referendum. According to a report by the U.S. Senate Committee on Foreign Relations, "Russia-based criminal organizations have reportedly been active in Catalonia for years, building their influence in politics and business and working to exploit rivalries between regional and national law enforcement entities."[174] Furthermore, according to one American intelligence source, Russian money was allegedly funneled to the Catalan nationalist party Convergence and Union.[175] The U.S. Department of the Treasury even reportedly worked with Spanish security services on an investigation that "targeted money laundering by Russian crime syndicates through Catalonian banks, shell companies, and real estate investments," according to a Senate Foreign Relations Committee investigation.[176]

Unlike the other case studies in this report, maintaining the integrity of the referendum was not among the Spanish government's priorities—quite the opposite, in fact. The Spanish government in Madrid declared the referendum unconstitutional and Spanish courts ruled the vote as illegal.[177] On the day of the vote, Spanish police seized ballots and closed polling stations and "launched a concerted effort to prevent people from casting their ballots."[178] Rioters clashed with police, and hundreds of people were injured.[179]

Nevertheless, despite their public disapproval of the referendum, the Spanish government has responded negatively to the election interference allegations. Both the Spanish government and NATO are reportedly investigating the use of Russian trolls during the Catalonia referendum.[180] In November 2017, the Spanish prime minister publicly accused Russian bots of spreading fake news during the referendum.[181] Spanish government officials from the defense and foreign ministries also stated that they "had evidence that state and private-sector Russian groups, as well as groups in Venezuela, used Twitter, Facebook, and other Internet sites to massively publicize the separatist cause."[182]

Lessons learned and recommendations for 2020

Foreign election interference is not a new phenomenon, but the new tactics used by authoritarian countries—most notably Russia and China—require new approaches. Powered by new developments in information technology, guided by geopolitical ambitions, and encouraged by a growing feeling of resentment and distrust in institutions, the rewards, and thus the incentive structures, for foreign interference have shifted. Therefore, malign political interference from authoritarian states will likely be an ongoing factor for the foreseeable future. All stakeholders in the democratic process have a responsibility to help defend that process and prevent themselves from becoming tools for foreign adversaries.

Every country's political process, history, and culture are unique, and there is no single model or formula for how to prevent and respond to foreign interference. However, there are many commonalities and lessons to be learned from each other. Based on the review of the above case studies, the authors have developed the following recommendations to be considered ahead of the 2020 U.S. election.

Lesson 1: A forceful government response is the most important deterrent and mitigating factor

While combating threats such as disinformation and election interference are absolutely a whole-of-society endeavor, the government is perhaps the single most important actor in preventing and mitigating foreign interference attacks. This was apparent in Germany, the Netherlands, and Sweden, where the governments both made clear to Russia that they would not tolerate interference in their elections and also appropriately put the public on high alert.

Unfortunately, the leadership of the American government has made it clear that fighting Russian interference is not a priority. In fact, when discussing whether he would accept such assistance if it came in the form of information in a recent interview with ABC News, President Trump said, "I think I'd take it."[183] From a deterrence perspec-

tive, this an extremely troubling position, as it creates an incentive for foreign powers to procure and provide such information. Foreign interference works most effectively when there is a willing participant on the receiving end.[184] This sends a particularly concerning message to any foreign power looking to interfere in future elections.

Recommendation: Send a clear, bipartisan message

Leaders at every level of government should make clear in public remarks that interference in U.S. elections will not be tolerated. While President Trump has already made his position clear, there are other important voices through the executive and legislative branches that can and should send a clear and credible message to Russia that there will be consequences for interfering in America's elections. This should be done through a series of public statements from the director of national intelligence, the FBI director, secretary of state, National Security Agency director, and secretary of homeland security. Congressional leaders also have a responsibility to present a unified, bipartisan front against foreign interference in the election. Ahead of the 2020 election, leadership from both the U.S. House of Representatives and U.S. Senate, along with relevant committee chairs and ranking members, should issue statements making clear that interference will not be tolerated and that there are a wide range of legislative tools that Congress itself can deploy to respond internationally. If there are incidents during the election, it is important for leaders to respond in unison, sending the public message that partisan politics is a domestic competition, not an international one. If Russia does not have a willing partner and believes that its assistance will be roundly rejected, and that it will suffer consequences for its actions, its incentive to interfere will decrease.

Recommendation: Enact robust sanctions legislation

While presenting a bipartisan unified front is incredibly important, America's response to foreign interference needs to go beyond rhetorical warnings. Rhetorical warnings must be credible to be effective, yet to date, America's rhetoric has not been backed up by meaningful action. Russia has yet to pay a meaningful price for its interference in democratic processes, including in the 2016 U.S. election. In 2017, Congress passed the Countering America's Adversaries Through Sanctions Act nearly unanimously; this legislation authorized tough sanctions in response to Russia's interference.[185] However, these sanctions have been undermined consistently by the Trump administration, most recently through a deal between the Treasury Department and Oleg Deripaska that freed Deripaska from hundreds of millions of dollars of debt while also allowing him and his allies to keep majority ownership of his most important companies.[186] The Kremlin will continue to attack American democracy as long as it feels it can get away with it. Failing to properly take action to respond effectively to the events in 2016 will undermine any future attempts to seriously deter malignant activities around the 2020 election.

Therefore, as part of a measure to deter further interference in the 2020 election, Congress should immediately move forward with sanctions legislation against Russia for its interference in U.S. and European elections. Targets of the sanctions should include the Russian banks that support efforts to interfere in foreign elections, Russia's cybersector, and individuals in Putin's orbit who support and facilitate such illicit behavior. Additionally, with bipartisan support, Congress should develop a series of corresponding escalatory measures that could be applied if Russia is found to interfere in upcoming elections. These measures should include punitive sanctions applied to Russia's sovereign debt, offensive cyberoperations, cutting off Aeroflot flights, and even cutting off diplomatic relations if necessary. While extreme, understanding that there will be real and specific penalties for illicit behavior is a necessary deterrent.

Lesson 2: Situational awareness among voters is a very powerful defense

In today's threat environment, where voters are targets of foreign influence operations, members of the public are simultaneously the most important and the most vulnerable stakeholders in the election process. One of the reasons that Russian interference had a harmful impact in the 2016 U.S. election, but has been less definitive in elections since, is the simple fact that the voters around the word are more aware of Russia's activities. Public awareness about foreign influence campaigns is perhaps the single most important defense against such interference and an essential tool toward building a resilient democracy.

Recommendation: Develop and vigorously promote a public awareness campaign

This points to the incredible importance of long-term civic and media education for the public, which many countries have underway. In terms of shorter-term solutions that can be implemented prior to the 2020 election, however, Congress should mandate and fund a public awareness campaign about foreign election interference, potentially modeled after the If You See Something, Say Something campaign that successfully raised attention around domestic terrorism threats.[187] The slogan, originally created for New York's Metropolitan Transit Authority, has since been adopted by the Department of Homeland Security and cities around the country. In 2018, the FBI, in partnership with the Department of Homeland Security and director of national intelligence, launched a program called Protected Voices, with similar goal.[188] However, the program has not received the level of attention needed to successfully create public awareness. In fact, its

efforts in 2018 went largely unnoticed by campaigns and consultants—the program's target audience.[189] The campaign should be a whole-of-government strategic communications push, spearheaded by the Department of Homeland Security.

Lesson 3: An interference operation does not need to alter the outcome of an election to have a harmful impact

Another important lesson is that the preferred candidate or party does not need to win the actual election in order for the foreign actor to consider it a victory. When considering Russia's goals of sowing discord, undermining the image and reputations of democratic governments, and building support for more pro-Russian policies, there are many circumstances in which the Russian-preferred candidate does not win the election outright, but Russia's goals are still advanced. For example, the German election in 2017 were largely seen as absent of Russian interference in the election. However, the rise of the AfD as a political force in Germany, including becoming a powerful voice in the Bundestag following the 2017 election, is due in part to Russian support for the party.

American politics are certainly not immune from this phenomenon. It is almost certain that Vladimir Putin did not believe that his support would actually help Donald Trump win the presidency, but supporting Trump inherently worked to sow discord in the United States and heightened social divisions, and these effects would have continued even if Trump had lost. The indictment of Russian spy Maria Butina also highlighted the part of the Kremlin's multifaceted strategy aimed at trying to influence U.S. policy by changing the stance of the Republican Party—one of two major American political parties—thereby influencing almost half of the country's views toward Russia.[190] It did this by trying to infiltrate one of the Republican Party's most important interest groups, the National Rifle Association. The goal was not to win elections, but rather to influence policy and positions toward Russia—first from within the organization and, by extension, in the Republican Party.

Recommendation: Demand full transparency

Ultimately, this lesson speaks to the need for long-term civic education on subjects such as media literacy and fundamental issues of democratic norms and traditions. However, those recommendations are outside the scope of this report, which focuses on measures that can be taken ahead of the 2020 election. With this in mind, the strongest tool immediately available is transparency. Congressional leaders should hold hearings on Russia's support for fringe movements around the world. When appro-

priate, law enforcement and prosecutors should also make indictments and related documents public to help expose these influence campaigns to all U.S. citizens. This includes releasing the full, unredacted Mueller report as well as the underlying documents from the special counsel's investigation.

Recommendation: Strengthen disclosure requirements

Congress should institute stringent, low-threshold requirements to disclose to the public when foreign interference is detected. Additionally, there should be mandatory, in-depth briefings for lawmakers and any affected campaigns or individuals on any such attacks.

Lesson 4: Paper ballots help provide confidence in the integrity of the system

Another lesson is the importance of paper ballots in maintaining the integrity of the election infrastructure. This measure covers two important functions. While there are no known documented instances of Russian hackers changing vote tallies in a democratic process, Russia has made attempts to hack into key election infrastructure.[191] Having paper ballots creates a paper trail that can then be tallied to ensure that the votes were properly counted. Perhaps just as important is that a paper trail provides a significant degree of confidence among the public in the integrity of the voting system. Both German and Dutch anti-interference efforts support this, as having a paper trail amid heightened concerns about Russian hacking created a degree of confidence in the system that prevented challenges to the legitimacy of the vote. With Russia's goal of undermining faith in the democratic process, even the simple act of fostering doubt or an unease about the vote advances Russia's geopolitical goals.

Recommendation: Require paper ballots and comprehensive audits

The United States should set a nationwide standard requiring every state to have a paper ballot system. Because paper trails are only effective when paired with comprehensive postelection audits, mandatory, comprehensive audits should also be required. Current legislative proposals that have passed in the House of Representatives, including H.R. 1 and the SAFE Act, would require such measures for federal elections. Unfortunately, the Senate has prevented these bills from moving forward. Considering recent concerns raised by national security officials about foreign interference in the 2020 election, Congress should immediately move forward with election security legislation that mandates both paper ballots and comprehensive audits.

Lesson 5: A trusted and reliable media is critical to cutting through foreign manipulation

Another important lesson learned from surveying how other democracies have responded to Russian interference is the critical role that a reliable and trusted media plays in informing the public. Although the modern media environment is increasingly defined by social media and decentralized news sources, the public's faith in news sources turned out to be critical in France, Germany, and the Netherlands. This is especially true in France, where the mainstream media, which enjoys widespread trust among the French public, showed restraint and upheld the 44-hour media blackout rule, successfully containing the spread of the #MacronLeaks.

This lesson is critical in the United States, where an independent press has been a cornerstone of the democracy since its inception. Unfortunately, the media—like any other actor—can be manipulated by foreign actors. As *New York Times* reporters Eric Lipton, David E. Sanger, and Scott Shane wrote in their December 2016 post-mortem on the Russian attack on the U.S. presidential election, "Every major publication, including The Times, published multiple stories citing the D.N.C. and Podesta emails posted by WikiLeaks, becoming a de facto instrument of Russian intelligence."[192]

Recommendation: Refuse to incentivize interference efforts

As the United States enters into a new presidential campaign season, the press will need to stay vigilant to resist falling for traps set up by malicious actors. Media outlets should refuse to quote stolen material that clearly has been released as part of an influence operation by a foreign power, as this creates a reward or incentive for Russia to hack and release stolen information. Additionally, Russia and other foreign actors are constantly innovating and improving their tactics and methods used to interference in elections.[193] Reporters will need to be on guard for these new techniques to avoid being manipulated.

Lesson 6: Financial flows are often an important component of Russian influence

In reviewing multiple cases across Europe, it is clear that Russia often finds ways to provide financial support to candidates and parties of their preferred candidates. The form that this financial support takes can vary widely from instance to instance. Depending on the country, its campaign finance laws, and how willing of a partner there is on the receiving end, the financial support can take very different forms.

Some of these forms are hidden and illicit, others more overt, and some just mysterious. The most well-covered cases discussed above are the loan to Marine Le Pen from an obscure Kremlin-linked bank that later disappeared, as well as the complex arrangement to allegedly funnel oil money to Matteo Salvini's Lega party ahead of the European Parliament election this past spring.

The American political system is not immune from this type of foreign interference. There are still outstanding questions about several suspicious financial transactions linked to Russia around the time of the 2016 election that have yet to be explained, including an almost $20 million transfer from Aras Agalarov, the Russian oligarch whose representative arranged the June 9 Trump Tower meeting, to an American bank account just days after the meeting.[194]

Recommendation: Strictly regulate foreign money in U.S. elections

The challenge of furtive foreign money in American politics is a critical issue and has been covered in more detail in other Center for American Progress reports, including "Cracking the Shell: Trump and the Corrupting Potential of Furtive Russian Money" and "Following the Money: Trump and Russia-Linked Transactions From the Campaign to the Presidential Inauguration." These reports provide detailed policy recommendations that focus on curbing the abuse of shell companies, addressing gaps in campaign finance disclosure regulations, and overall requiring greater corporate transparency.[195] However, financial support is one of the key—and often underexamined—aspects of foreign interference in democratic systems politics. It is not only money from Russia that is a concern. Foreign investment from around the world into American corporations is extensive. In a post-*Citizens United* world, these partially foreign-owned U.S. corporations can then engage in political spending, including through dark money channels where no disclosure is required. The United States needs a comprehensive approach to prevent foreign entities from exploiting the political system—and particularly to prevent foreign-influenced U.S. companies from spending in U.S. elections. This approach should include foreign ownership thresholds that would prevent inappropriate election spending; beneficial ownership provisions to curb the abuse of shell companies; combating money laundering through executive and legislative means, especially in the real estate market; and addressing existing gaps in campaign finance disclosure regulations.

Lesson 7: There is no foolproof way to protect elections

Perhaps the single most important lesson to be learned from European efforts to combat Russian interference is that it is impossible to fully protect elections from foreign actors. The French example provides an interesting case study pertaining to this lesson. Many of the stakeholders involved did the right thing: The government took the cyberthreat seriously and publicly warned Russia ahead of the election. Macron's campaign also engaged in sophisticated cybersecurity and information-security practices. Despite these countermeasures, hacks did occur; their impact was softened significantly by Macron's proactive approach, but there are only so many so many protections against mis- and disinformation. Perpetrators are also learning and adapting, discovering new techniques to mask their activities, which means that even the most forward-thinking campaigns may find themselves behind the curve when it comes to best defenses against foreign interference campaigns.[196]

Recommendation: Develop a plan for fighting interference

This speaks to the need for political campaigns to have detailed and comprehensive plans in place. Either during the primary period or during the general election, campaigns will likely deal with some form of a foreign interference. The contours of such a plan should include a joining pact not to use stolen materials, which will serve to disincentivize interference attempts; willingness to call out suspected interference when a campaign or group sees it; being aware that a foreign actor is looking to inflame tensions, even within the parties; and being on guard against attempts to infiltrate or entrap campaigns through false flag operations. As bad actors evolve, campaigns need to be equally willing to update and change their tactics to avoid falling prey to interference efforts.[197]

Conclusion

Russia is always attempting to subvert Western democracies. As elections present an especially easy target, ongoing as well as ramped-up Russian interference in the 2020 race is all but certain. It has been a factor in one way or another in almost every democratic process since 2016, and when examining these recent interference efforts, it becomes clear that democracies around the world can learn a great deal from each other. America's democratic allies can learn from the American experience; there has not been the equivalent of the Mueller investigation in any other country. The special counsel investigation in the United States is the only comprehensive legal investigation of its kind that looked at the entirety of the political attack and held many of those involved accountable.

But many European countries have been far more proactive when it comes to election security, and there is much that America can learn from its allies' experiences. Free and fair elections are a fundamental democratic principle. By studying the lessons outlined above, candidates, political parties, and members of the public can help ensure that the United States will be better prepared to defend its elections from hostile foreign actors.

About the authors

James Lamond is a senior policy adviser at the Center for American Progress.

Talia Dessel is a research analyst at the Center for American Progress.

Acknowledgements

The authors would like to thank all of the colleagues and experts who provided advice and feedback on the report, including Max Bergmann, Sam Berger, Danielle Root, Michael Sozan, and Katrina Mulligan. The authors would also like to thank Emily Young for her assistance with this report.

Endnotes

1 Carolyn Kenney, Max Bergmann, James Lamond, "Understanding and Combating Russian and Chinese Influence Operations" (Washington: Center for American Progress, 2019), available at https://www.americanprogress.org/issues/security/reports/2019/02/28/466669/understanding-combating-russian-chinese-influence-operations/; Jack Stubbs and Christopher Bing, "Exclusive: Iran-based political influence operation – bigger, persistent, global," Reuters, August 28, 2018, available at https://www.reuters.com/article/us-usa-iran-facebook-exclusive/exclusive-iran-based-political-influence-operation-bigger-persistent-global-idUSKCN1LD2R9; Rush Doshi and Robert D. Williams, "Is China interfering in American politics?", Brookings Institution, October 2, 2018, available at https://www.brookings.edu/blog/order-from-chaos/2018/10/02/is-china-interfering-in-american-politics/.

2 Ken Dilanian, "U.S. intel agencies: Russia and China plotting to interfere in 2020 election," NBC News, January 29, 2019, available at https://www.nbcnews.com/politics/national-security/u-s-intel-agencies-russia-china-plotting-interfere-2020-election-n963896; Martin Matishak, "Intelligence heads warn of more aggressive election meddling in 2020," *Politico*, January 29, 2019, available at https://www.politico.com/story/2019/01/29/dan-coats-2020-election-foreign-interference-1126077.

3 Lucien Bruggeman, "'I think I'd take it': In exclusive interview, Trump says he would listen if foreigners offered dirt on opponents," ABC News, January 13, 2019, available at https://abcnews.go.com/Politics/id-exclusive-interview-trump-listen-foreigners-offered-dirt/story?id=63669304.

4 Martin Matishak, "National security leaders warn of foreign meddling ahead of midterms," *Politico*, October 19, 2018, available at https://www.politico.com/story/2018/10/19/midterms-election-meddling-russia-china-865676.

5 Robert S. Mueller III, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election: Volume I of II" (Washington: U.S. Department of Justice, 2019), p. 76, available at https://www.justice.gov/storage/report.pdf.

6 Dan Coats, "Transcript: Dan Coats Warns The Lights Are 'Blinking Red' On Russian Cyberattacks," NPR, July 18, 2018, available at https://www.npr.org/2018/07/18/630164914/transcript-dan-coats-warns-of-continuing-russian-cyberattacks.

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

8 Erin Banco and Betsy Woodruff, "Trump's DHS Guts Task Forces Protecting Elections From Foreign Meddling," Daily Beast, February 13, 2019, available at https://www.thedailybeast.com/trumps-dhs-guts-task-forces-protecting-elections-from-foreign-meddling.

9 John Sipher, "Putin's One Weapon: The 'Intelligence State'," *The New York Times*, February 24, 2019, available at https://www.nytimes.com/2019/02/24/opinion/putin-russia-security-services.html.

10 Molly K. McKew, "The Gerasimov Doctrine," *Politico*, September/October 2017, available at https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538.

11 Mark Galeotti, "I'm Sorry for Creating the 'Gerasimov Doctrine'," *Foreign Policy*, March 5, 2018, available at https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/.

12 Ibid.

13 Wilson Center, "George F. Kennan, 'The Inauguration of Organized Political Warfare' [Redacted Version]" (Washington: 1984), available at https://digitalarchive.wilsoncenter.org/document/114320.

14 Calder Walton, "'Active Measures': a history of Russian interference in US elections," *Prospect Magazine*, December 23, 2016, available at http://www.prospectmagazine.co.uk/science-and-technology/active-measures-a-history-of-russian-interference-in-us-elections.

15 David Robert Grimes, "Russian fake news is not new: Soviet Aids propaganda cost countless lives," *The Guardian*, January 14, 2017, available at https://www.theguardian.com/science/blog/2017/jun/14/russian-fake-news-is-not-new-soviet-aids-propaganda-cost-countless-lives.

16 Clint Watts, *Messing with the Enemy: Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News* (New York: Harper-Collins Publishers, 2018).

17 Ibid.

18 Andrew Prokop, "23 tweets from @TEN_GOP, one Russian-run Twitter account mentioned in Mueller's new indictment," Vox, February 16, 2018, available at https://www.vox.com/policy-and-politics/2017/10/19/16504510/ten-gop-twitter-russia.

19 Philip Bump, "At least five people close to Trump engaged with Russian Twitter trolls from 2015 to 2017," *The Washington Post*, November 2, 2017, available at https://www.washingtonpost.com/news/politics/wp/2017/11/02/at-least-five-people-close-to-trump-engaged-with-russian-twitter-trolls-from-2015-to-2017/?utm_term=.25f1e0399bff.

20 Prokop, "23 tweets from @TEN_GOP, one Russian-run Twitter account mentioned in Mueller's new indictment."

21 Matthew Field and Mike Wright, "Russian trolls sent thousands of pro-Leave messages on day of Brexit referendum, Twitter data reveals," *The Telegraph*, October 17, 2018, available at https://www.telegraph.co.uk/technology/2018/10/17/russian-iranian-twitter-trolls-sent-10-million-tweets-fake-news/; Paul Sonne, "A Russian bank gave Marine Le Pen's party a loan. Then weird things began happening," *The Washington Post*, December 27, 2018, available at https://www.washingtonpost.com/world/national-security/a-russian-bank-gave-marine-le-pens-party-a-loan-then-weird-things-began-happening/2018/12/27/960c7906-d320-11e8-a275-81c671a50422_story.html?utm_term=.8f0199afa446.

22 Martin Arostegui, "Officials: Russia Seeking to Exploit Catalonia Secessionist Movement," Voice of America, November 24, 2017, available at https://www.voanews.com/europe/officials-russia-seeking-exploit-catalonia-secessionist-movement.

23 Giovanni Tizian and Stefano Vergine, "Quei 3 milioni russi per Matteo Salvini: l'inchiesta che fa tremare la Lega," *L'Espresso*, February 21, 2019, available at http://espresso.repubblica.it/plus/articoli/2019/02/21/news/tre-milioni-matteo-salvini-russia-1.331924.

24 Jean-Baptiste Jeangène Vilmer, "Successfully Countering Russian Electoral Interference: 15 Lessons Learned from the Macron Leaks" (Washington: Center for Strategic and International Studies, 2018), available at https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180621_Vilmer_Countering_russiam_electoral_influence.pdf.

25 Ibid.

26 Jon Henley, "Le Pen, Putin, Trump: a disturbing axis, or just a mutual admiration society?", *The Guardian*, April 29, 2017, available at https://www.theguardian.com/world/2017/apr/29/marine-le-pen-putin-trump-axis.

27 Jean-Baptiste Jeangène Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem" (Washington: Atlantic Council, 2019), available at https://www.atlanticcouncil.org/images/publications/The_Macron_Leaks_Operation-A_Post-Mortem.pdf.

28 Gregor Aisch and others, "How France Voted," *The New York Times*, May 7, 2017, available at https://www.nytimes.com/interactive/2017/05/07/world/europe/france-election-results-maps.html.

29 Laura Daniels, "How Russia hacked the French election," *Politico*, April 23, 2017, available at https://www.politico.eu/article/france-election-2017-russia-hacked-cyberattacks/.

30 Andrew Callus and Richard Balmforth, "France warns Russia against meddling in election," Reuters, February 15, 2017, available at https://www.reuters.com/article/us-france-election-cyber/france-warns-russia-against-meddling-in-election-idUSKBN15U22U.

31 Erik Brattberg and Tim Maurer, "Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks" (Washington: Carnegie Endowment for International Peace, 2018), available at https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435.

32 Richard Balmforth and Michel Rose, "French polling watchdog warns over Russian news agency's election report," Reuters, April 2, 2017, available at https://www.reuters.com/article/us-france-election-russia-idUSKBN1740JG.

33 Vilmer, "Successfully Countering Russian Electoral Interference."

34 Ibid.

35 Brattberg and Maurer, "Russian Election Interference."

36 Ibid.

37 La République En Marche!, "En Marche a été victime d'une action de piratage massive et coordonnée," Press release, May 5, 2017, available at https://en-marche.fr/articles/communiques/communique-presse-piratage.

38 Vilmer, "Successfully Countering Russian Electoral Interference."

39 Matt Apuzzo and Adam Satariano, "Russia Is Targeting Europe's Elections. So Are Far-Right Copycats," *The New York Times*, May 12, 2019, available at https://www.nytimes.com/2019/05/12/world/europe/russian-propaganda-influence-campaign-european-elections-far-right.html.

40 Steven Erlanger and Megan Specia, "European Parliament Elections: 5 Biggest Takeaways," *The New York Times*, May 27, 2019, available at https://www.nytimes.com/2019/05/27/world/europe/eu-election-takeaways.html?module=inline.

41 Max Bergmann, "Europe Is Back," *Foreign Policy*, July 17, 2019, available at https://foreignpolicy.com/2019/07/17/europe-is-back/.

42 Erlanger and Specia, "European Parliament Elections."

43 European Commission, "A Europe that protects: EU reports on progress in fighting disinformation ahead of European Council," Press release, June 14, 2019, available at http://europa.eu/rapid/press-release_IP-19-2914_en.htm; Adam Satariano, "Russia Sought to Use Social Media to Influence E.U. Vote, Report Finds," *The New York Times*, June 14, 2019, available at https://www.nytimes.com/2019/06/14/business/eu-elections-russia-misinformation.html.

44 European Commission, "A Europe that protects."

45 Satariano, "Russia Sought to Use Social Media to Influence E.U. Vote, Report Finds"; Apuzzo and Satariano, "Russia Is Targeting Europe's Elections. So Are Far-Right Copycats."

46 European Commission, "A Europe that protects."

47 Ibid.

48 Ibid.; European Commission and the European External Action Service, "Action Plan Against Disinformation: Report on progress" (Brussels: 2019), available at https://ec.europa.eu/commission/sites/beta-political/files/fact-sheet_disinfo_elex_140619_final.pdf.

49 Matt Apuzzo, "Europe Built a System to Fight Russian Meddling. It's Struggling," *The New York Times*, July 6, 2019, available at https://www.nytimes.com/2019/07/06/world/europe/europe-russian-disinformation-propaganda-elections.html.

50 Ibid.

51 Ibid.

52 Apuzzo and Satariano, "Russia Is Targeting Europe's Elections. So Are Far-Right Copycats."

53 Apuzzo, "Europe Built a System to Fight Russian Meddling. It's Struggling."

54 European Commission, "A Europe that protects."

55 Ibid.; European Commission, "Code of Practice on Disinformation," September 26, 2018, available at https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.

56 European Commission and the European External Action Service, "Action Plan Against Disinformation."

57 European Commission, "A Europe that protects"; EU vs Disinfo, "About," available at https://euvsdisinfo.eu/about/ (last accessed July 2019).

58 European External Action Service, "Questions and Answers about the East StratCom Task Force," May 12, 2018, available at https://eeas.europa.eu/headquarters/headquarters-homepage/2116/-questions-and-answers-about-the-east-.

59 EU vs Disinfo, "Home," available at https://euvsdisinfo.eu/ (last accessed July 2019); EU vs Disinfo, "About," available at https://euvsdisinfo.eu/about/ (last accessed August 2019).

60 European Commission, "A Europe that protects"; European Commission and the European External Action Service, "Action Plan Against Disinformation."

61 Silvia Sciorilli Borrelli and Jacopo Barigazzi, "Salvini wins big – but only in Italy," *Politico*, May 27, 2019, available at https://www.politico.eu/article/european-parliament-election-2019-matteo-salvinis-wins-big-but-only-in-italy/; Jack Guy and Helen Regan, "8 key takeaways from the European election 2019 results," CNN, May 27, 2019, available at https://www.cnn.com/2019/05/27/europe/european-elections-takeaways-intl/index.html.

62 Tizian and Vergine, "Quei 3 milioni russi per Matteo Salvini."

63 Alberto Nardelli, "Revealed: The Explosive Secret Recording That Shows How Russia Tried To Funnel Millions To The 'European Trump'," BuzzFeed News, July 10, 2019, available at https://www.buzzfeednews.com/article/albertonardelli/salvini-russia-oil-deal-secret-recording.

64 Lorenzo Tondo, "Italian prosecutors investigate League over alleged Russian oil deal claims," *The Guardian*, July 11, 2019, available at https://www.theguardian.com/world/2019/jul/11/matteo-salvinis-party-under-investigation-for-alleged-russian-oil-deal.

65 *Politico*, "Sweden's election: The essential guide," September 7, 2018, available at https://www.politico.eu/article/sweden-election-2018-the-essential-guide/; Sheri Berman, "Five takeaways about the Swedish election – and the far-right wave across Europe," *The Washington Post*, September 12, 2018, available at https://www.washingtonpost.com/news/monkey-cage/wp/2018/09/12/what-the-swedish-elections-tell-us-about-europes-democratic-upheavals/?utm_term=.6087e5ae043f.

66 Anna Wieslander, "What Makes an Ally? Sweden and Finland as NATO Partners," Atlantic Council, April 1, 2019, available at https://www.atlanticcouncil.org/blogs/new-atlanticist/what-makes-an-ally-sweden-and-finland-as-nato-partners; Michael Birnbaum, "Sweden is taking on Russian meddling ahead of fall elections. The White House might take note," *The Washington Post*, February 22, 2018, available at https://www.washingtonpost.com/world/europe/sweden-looks-at-russias-electoral-interference-in-the-us-and-takes-steps-not-to-be-another-victim/2018/02/21/9e58ee48-0768-11e8-aa61-f3391373867e_story.html?utm_term=.21b4b8161a10; Charlie Duxbury, "Under threat, Sweden rediscovers its Viking spirit," *Politico*, January 30, 2018, available at https://www.politico.eu/article/under-threat-sweden-rediscovers-its-viking-spirit-nato-russia/.

67 Duxbury, "Under threat, Sweden rediscovers its Viking spirit"; Anna Wieslander, "Will Sweden's Elections Lead to NATO Membership?", September 6, 2018, available at https://www.atlanticcouncil.org/blogs/new-atlanticist/will-sweden-s-elections-lead-to-nato-membership.

68 Erik Brattberg and Tim Maurer, "How Sweden Is Preparing For Russia to Hack its Election," Carnegie Endowment For International Peace, May 31, 2018, available at https://carnegieendowment.org/2018/05/31/how-sweden-is-preparing-for-russia-to-hack-its-election-pub-76484.

69 Gordon Corera, "Swedish security chief warning on fake news," BBC, January 4, 2018, available at https://www.bbc.com/news/world-europe-42285332; Johan Ahlander, "Sweden braced for possible Russian election meddling – security service," Reuters, February 22, 2018, available at https://af.reuters.com/article/worldNews/idAFKCN1G626K.

70 Brattberg and Maurer, "Russian Election Interference."

71 Ibid.

72 Swedish Security Service, "Successful preventive work prior to the elections," Press release, December 21, 2018, available at https://www.sakerhetspolisen.se/en/swedish-security-service/about-us/press-room/current-events/news/2018-12-21-successful-preventive-work-prior-to-the-elections.html.

73 Ibid.

74 Ibid.

75 Chloe Colliver and others, "Smearing Sweden: International Influence Campaigns in the 2018 Swdish Election" (London, UK: Institute for Strategic Dialogue and London School of Economics Institute of Global Affairs, 2018), available at http://www.lse.ac.uk/iga/assets/documents/arena/2018/Sweden-Report-October-2018.pdf?fbclid=IwAR07evP5NsgLCR6IBbO2coDJGejVRf5jv5CwbcW1TqU1nF_1HToNQ3n-SLY.

76 Ibid.

77 Ibid.

78 Ibid.

79 Ibid.

80 Ibid.

81 Swedish Security Service, "Facing a wider range of threats in 2018," Press release, March 14, 2019, available at https://www.sakerhetspolisen.se/en/swedish-security-service/about-us/press-room/current-events/news/2019-03-14-facing-a-wider-range-of-threats-in-2018.html.

82 Ibid.

83 U.S. Senate Committee on Foreign Relations, "Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security" (Washington: U.S. Congress, 2018). available at https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf.

84 Brattberg and Maurer, "Russian Election Interference."

85 BBC, "Sweden sends out leaflets on how to prepare for war," BBC, May 22, 2018, available at https://www.bbc.com/news/world-europe-44208921.

86 Brattberg and Maurer, "Russian Election Interference."

87 Ibid.

88 Ibid.; U.S. Senate Committee on Foreign Relations, "Putin's Asymmetric Assault on Democracy in Russia and Europe."

89 Brattberg and Maurer, "Russian Election Interference."

90 Ibid.

91 Brattberg and Maurer, "How Sweden Is Preparing For Russia to Hack its Election."

92 Erik Brattberg and Tim Maurer, "Russian Election Interference."

93 Ibid.

94 Brattberg and Maurer, "How Sweden Is Preparing For Russia to Hack its Election."

95 Swedish Security Service, "Attempts to influence confidence in the election process," Press release, August 31, 2018, available at https://www.sakerhetspolisen.se/en/swedish-security-service/about-us/press-room/current-events/news/2018-08-31-attempts-to-influence-confidence-in-the-election-process.html.

96 Ibid.

97 Ibid.

98 Matthew Karnitschnig and Janosch Delcker, "Germany's Merkel clings to power amid far right surge," *Politico*, September 24, 2017, available at https://www.politico.eu/article/merkels-party-wins-german-general-election-exit-poll/.

99 Seán Clarke, "German elections 2017: full results," *The Guardian*, September 25, 2017, available at https://www.theguardian.com/world/ng-interactive/2017/sep/24/german-elections-2017-latest-results-live-merkel-bundestag-afd; Melissa Eddy, "Angela Merkel's Tortuous Path Toward a German Coalition," *The New York Times*, November 8, 2017, available at https://www.nytimes.com/2017/11/08/world/europe/germany-election-merkel-coalition.html.

100 Kate Connolly, "German election: Merkel wins fourth term but far-right AfD surges to third," *The Guardian*, September 24, 2017, available at https://www.theguardian.com/world/2017/sep/24/angela-merkel-fourth-term-far-right-afd-third-german-election.

101 Melissa Eddy, "Merkel and Putin Sound Pragmatic Notes After Years of Tension," *The New York Times*, August 18, 2018, available at https://www.nytimes.com/2018/08/18/world/europe/merkel-putin-russia-germany.html.

102 Michael Schwirtz, "German Election Mystery: Why No Russian Meddling?", *The New York Times*, September 21, 2017, available at https://www.nytimes.com/2017/09/21/world/europe/german-election-russia.html; Jim Rutenberg, "Hacks and Leaks Pose New Challenges for Journalists. Next Up: Germany", *The New York Times*, July 30, 2017, available at https://www.nytimes.com/2017/07/30/business/media/as-election-nears-german-media-braces-for-devious-hacks.html.

103 David Salvo, "Russia's Interference in Germany Will Continue beyond the September 24 Elections," Alliance for Securing Democracy, September 20, 2017, available at https://securingdemocracy.gmfus.org/russias-interference-in-germany-will-continue-beyond-the-september-24-elections/.

104 DFRLab, "#ElectionWatch: Final Hours Fake News Hype in Germany," Medium, September 23, 2017, available at https://medium.com/dfrlab/electionwatch-final-hours-fake-news-hype-in-germany-cc9b8157cfb8.

105 Simon Shuster, "How Russian Voters Fueled the Rise of Germany's Far-Right," *Time*, September 25, 2017, available at https://time.com/4955503/germany-elections-2017-far-right-russia-angela-merkel/.

106 Schwirtz, "German Election Mystery"; Constanze Stelzenmüller, "Testimony: The impact of Russian interference on Germany's 2017 elections," Brookings Institution, June 28, 2017, available at https://www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections/.

107 Brattberg and Maurer, "Russian Election Interference."

108 Schwirtz, "German Election Mystery."

109 Stelzenmüller, "Testimony: The impact of Russian interference on Germany's 2017 elections."

110 Schwirtz, "German Election Mystery."

111 U.S. Senate Committee on Foreign Relations, "Putin's Asymmetric Assault on Democracy in Russia and Europe."

112 Brattberg and Maurer, "Russian Election Interference."

113 Schwirtz, "German Election Mystery."

114 Stelzenmüller, "Testimony: The impact of Russian interference on Germany's 2017 elections."

115 Brattberg and Maurer, "Russian Election Interference."

116 Ibid.

117 Ibid.

118 Ibid.

119 Ibid.; U.S. Senate Committee on Foreign Relations, "Putin's Asymmetric Assault on Democracy in Russia and Europe."

120 Brattberg and Maurer, "Russian Election Interference."

121 Ibid.

122 Ibid.

123 Joerg Forbrig, "Russian Hackers Can't Beat German Democracy," *Foreign Policy*, August 3, 2017, available at https://foreignpolicy.com/2017/08/03/russian-hackers-cant-beat-german-democracy-putin-merkel/.

124 Rick Noack, "How German politics became a beacon of stability compared with the United States," *The Washington Post*, September 22, 2017, available at https://www.washingtonpost.com/news/worldviews/wp/2017/09/22/how-german-politics-became-a-beacon-of-stability-compared-with-the-u-s/.

125 Brattberg and Maurer, "Russian Election Interference."

126 Schwirtz, "German Election Mystery."

127 Luke Harding, "Revealed: details of exclusive Russian deal offered to Arron Banks in Brexit run-up," *The Guardian*, August 9, 2018, available at https://www.theguardian.com/uk-news/2018/aug/09/revealed-detail-of-exclusive-russian-deal-offered-to-arron-banks-in-brexit-run-up.

128 *United States of America v. Michael Cohen*, 18 U.S. 1 (December 7, 2018), available at https://assets.documentcloud.org/documents/5453413/SCO-Cohen-Sentencing-Submission.pdf.

129 Channel 4 News, "The Banks Files: How Brexit 'bad boy' Arron Banks was eyeing a massive Russian gold deal," March 5, 2019, available at https://www.channel4.com/news/the-banks-files-how-brexit-bad-boy-arron-banks-was-eyeing-a-massive-russian-gold-deal.

130 Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election."

131 U.S. Department of the Treasury, "Announcement of Additional Treasury Sanctions on Russian Financial Institutions and on a Defense Technology Entity," Press release, July 29, 2014, available at https://www.treasury.gov/press-center/press-releases/pages/jl2590.aspx.

132 Luke Harding, "Investigators bound to scrutinise Arron Banks's Russian links," *The Guardian*, November 1, 2018, available at https://www.theguardian.com/uk-news/2018/nov/01/investigators-will-scrutinise-arron-banks-russian-links; Channel 4 News, "The Banks Files: How Brexit 'bad boy' Arron Banks was eyeing a massive Russian gold deal," March 5, 2019, available at https://www.channel4.com/news/the-banks-files-how-brexit-bad-boy-arron-banks-was-eyeing-a-massive-russian-gold-deal.

133 Linda Qiu, "Trump Denies Business Dealings With Russia. His Former Lawyer Contradicts Him," *The New York Times*, November 29, 2018, available at https://www.nytimes.com/2018/11/29/us/politics/fact-check-cohen-trump-.html.

134 British House of Commons Digital, Culture, Media and Sport Committee, "Chair comments on the decision to refer Arron Banks to the National Crime Agency," Press release, November 1, 2018, available at https://www.parliament.uk/business/committees/committees-a-z/commons-select/digital-culture-media-and-sport-committee/news/arron-banks-nca-quote-17-19/; British House of Commons Digital, Culture, Media and Sport Committee, "Disinformation and 'fake news': Interim Report" (London, UK: British House of Commons, 2018), available at https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf.

135 Harding, "Investigators bound to scrutinise Arron Banks's Russian links."

136 Ginger Gibson and Grant Smith, "Figures show Trump spent $66 million of his own cash on election campaign," Reuters, December 8, 2016, available at https://www.reuters.com/article/us-usa-election-trump/figures-show-trump-spent-66-million-of-his-own-cash-on-election-campaign-idUSKBN13Y0AE.

137 Jennifer Wang, "Donald Trump Doesn't Have The Cash To Self-Fund Unless He Sells Prized Properties," *Forbes*, June 22, 2016, available at https://www.forbes.com/sites/jenniferwang/2016/06/22/donald-trump-doesnt-have-the-cash-to-self-fund-unless-he-sells-prized-properties/#5e989b453079.

138 Luke Harding, "Revealed: details of exclusive Russian deal offered to Arron Banks in Brexit run-up"; The Moscow Project, "Trump's Russia Cover-Up by the Numbers – 272 Contacts With Russia-Linked Operatives," available at https://themoscowproject.org/explainers/trumps-russia-cover-up-by-the-numbers-70-contacts-with-russia-linked-operatives/ (last accessed August 2019).

139 Mark Townsend and Carole Cadwalladr, "Emails reveal Arron Banks' links to Steve Bannon in quest for campaign cash," *The Guardian*, November 17, 2018, available at https://www.theguardian.com/uk-news/2018/nov/17/arron-banks-emails-steve-bannon-brexit-campaign-funds; Issie Lapowsky, "What Did Cambridge Analytica Really Do For Trump's Campaign?", Wired, November 26, 2017, available at https://www.wired.com/story/what-did-cambridge-analytica-really-do-for-trumps-campaign/.

140 Chris Graham, "Who won the Dutch election and what does it mean for Geert Wilders and the far-Right in the Netherlands and Europe?", *The Telegraph*, March 16, 2017, available at https://www.telegraph.co.uk/news/2017/03/16/won-dutch-election-does-mean-geert-wilders-far-right-netherlands/.

141 Ibid.

142 BBC, "Dutch election: European relief as mainstream triumphs," March 16, 2017, available at https://www.bbc.com/news/world-europe-39297355.

143 Alan Cowell, "Russia 'Accountable' for Downed Airliner, Australia and Netherlands Say," *The New York Times*, May 25, 2018, available at https://www.nytimes.com/2018/05/25/world/europe/netherlands-australia-russia-mh17.html.

144 EU vs Disinfo, "Renewed Focus on MH17," June 20, 2019, available at https://euvsdisinfo.eu/renewed-focus-on-mh-17/.

145 Andrew Higgins, "Fake News, Fake Ukrainians: How a Group of Russians Tilted a Dutch Vote," *The New York Times*, February 16, 2017, available at https://www.nytimes.com/2017/02/16/world/europe/russia-ukraine-fake-news-dutch-vote.html; Laurens Cerulus, "Dutch go old school against Russian hacking," *Politico*, March 5, 2017, available at https://www.politico.eu/article/dutch-election-news-russian-hackers-netherlands/.

146 Huib Modderkolk, "Dutch agencies provide crucial intel about Russian's interference in US-elections," *de Volkskrant*, January 25, 2018, available at https://www.volkskrant.nl/wetenschap/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~b4f8111b/?referer=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/?utm_term%3D.949ccc4ade4a.

147 Rick Noack, "The Dutch were a secret U.S. ally in war against Russian hackers, local media reveal," *The Washington Post*, January 26, 2018, available at 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/?utm_term=.111baa13199e; Anthony Deutsch and Dustin Volz, "Dutch intelligence agency spied on Russian hacking group: media," Reuters, January 25, 2018, available at https://www.reuters.com/article/us-netherlands-russia-cybercrime/dutch-intelligence-agency-spied-on-russian-hacking-group-media-idUSKBN1FE34W.

148 Cynthia Kroet, "Russia spread fake news during Dutch election: report," *Politico*, April 4, 2017, available at https://www.politico.eu/article/russia-spread-fake-news-during-dutch-election-report-putin/.

149 Brattberg and Maurer, "Russian Election Interference"; Thessa Lageman, "Russian hackers use Dutch polls as practice," DW, March 10, 2017, available at https://www.dw.com/en/russian-hackers-use-dutch-polls-as-practice/a-37850898.

150 U.S. Senate Committee on Foreign Relations, "Putin's Asymmetric Assault on Democracy in Russia and Europe."

151 Brattberg and Maurer, "Russian Election Interference."

152 U.S. Senate Committee on Foreign Relations, "Putin's Asymmetric Assault on Democracy in Russia and Europe."

153 Ibid.

154 Brattberg and Maurer, "Russian Election Interference."

155 Ibid.

156 Cerulus, "Dutch go old school against Russian hacking."

157 DW, "Dutch to hand-count ballots in March vote due to hacking fears," February 1, 2017, available at https://www.dw.com/en/dutch-to-hand-count-ballots-in-march-vote-due-to-hacking-fears/a-37375137.

158 Brattberg and Maurer, "Russian Election Interference."

159 Ibid.

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

161 U.S. Senate Committee on Foreign Relations, "Putin's Asymmetric Assault on Democracy in Russia and Europe."

162 Ibid.

163 Embassy of the Russian Federation in the Netherlands, "Economic cooperation," available at https://netherlands.mid.ru/web/netherlands-en/economic-relations (last accessed July 2019).

164 Cowell, "Russia 'Accountable' for Downed Airliner, Australia and Netherlands Say."

165 *United States of America v. Internet Research Agency LLC*, 18 U.S.C.2, 371, 1349, 1028A (February 16, 2018), available at https://www.justice.gov/file/1035477/download.

166 Lauren Frayer, "Catalonia Votes For Independence; Spain Says It Won't Happen," NPR, November 10, 2014, available at https://www.npr.org/sections/parallels/2014/11/10/362952892/referendums-outcome-indicates-catalonias-desire-for-independence.

167 U.S. Senate Committee on Foreign Relations, "Putin's Asymmetric Assault on Democracy in Russia and Europe."

168 Casey Michel, "Inside the Russian effort to fuel American secessionists," ThinkProgress, February 26, 2018, available at https://thinkprogress.org/russia-texas-california-separatism-9809aca9f61d/.

169 Angela Dewan, Vasco Cotovio, and Hilary Clarke, "Catalonia independence referendum: What just happened?", CNN, October 2, 2017, available at https://www.cnn.com/2017/10/02/europe/catalonia-independence-referendum-explainer/index.html.

170 Ibid.

171 Neil MacFarquhar, "Russia, Jailer of Local Separatists, Welcomes Foreign Secessionists," *The New York Times*, September 25, 2016, available at https://www.nytimes.com/2016/09/26/world/europe/russia-kremlin-opposition-groups.html.

172 U.S. Senate Committee on Foreign Relations, "Putin's Asymmetric Assault on Democracy in Russia and Europe," Footnote 203.

173 Arostegui, "Officials: Russia Seeking to Exploit Catalonia Secessionist Movement."

174 U.S. Senate Committee on Foreign Relations, "Putin's Asymmetric Assault on Democracy in Russia and Europe."

175 Ibid.

176 Ibid.

177 Raphael Minder and Ellen Barry, "Catalonia's Independence Vote Descends Into Chaos and Clashes," *The New York Times*, October 1, 2017, available at https://www.nytimes.com/2017/10/01/world/europe/catalonia-independence-referendum.html; Amanda Erickson, "Catalonia's independence vote: What you need to know," *The Washington Post*, October 27, 2017, available at https://www.washingtonpost.com/news/worldviews/wp/2017/09/30/catalonia-independence-referendum-spain/?utm_term=.6769a318404e; Dewan, Cotovio, and Clarke, "Catalonia independence referendum."

178 Dewan, Cotovio, and Clarke, "Catalonia independence referendum."

179 Ibid.; Minder and Barry, "Catalonia's Independence Vote Descends Into Chaos and Clashes."

180 Arostegui, "Officials: Russia Seeking to Exploit Catalonia Secessionist Movement."

181 William Booth and Michael Birnbaum, "British and Spanish leaders say Russian trolls meddled in their elections," *The Washington Post*, November 14, 2017, available at https://www.washingtonpost.com/world/europe/britain-and-spanish-leaders-say-russian-trolls-meddled-in-their-elections/2017/11/14/51ffb64a-c950-11e7-b506-8a10ed11ecf5_story.html?utm_term=.e2872ce0db99.

182 Robin Emmott, "Spain sees Russian interference in Catalonia separatist vote," Reuters, November 13, 2017, available at https://www.reuters.com/article/us-spain-politics-catalonia-russia/spain-sees-russian-interference-in-catalonia-separatist-vote-idUSKBN1DD20Y.

183 Bruggeman, "'I think I'd take it.'"

184 Dov H. Levin, "When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results," *International Studies Quarterly* 60 (2) (2016): 189–202, available at https://academic.oup.com/isq/article/60/2/189/1750842.

185 Countering America's Adversaries Through Sanctions Act, H.R. 3364, 115th Cong., 1st sess. (July 24, 2017), available at https://www.congress.gov/bill/115th-congress/house-bill/3364/text.

186 Kenneth P. Vogel, "Deripaska and Allies Could Benefit From Sanctions Deal, Document Shows," *The New York Times*, January 21, 2019, available at https://www.nytimes.com/2019/01/21/us/politics/oleg-deripaska-russian-sanctions.html.

187 U.S. Department of Homeland Security, "If you see something, say something," available at https://www.dhs.gov/see-something-say-something (last accessed July 2019).

188 FBI, "The FBI Launches a Combating Foreign Influence Webpage," Press release, August 30, 2018, available at https://www.fbi.gov/news/pressrel/press-releases/the-fbi-launches-a-combating-foreign-influence-webpage.

189 Andy Kroll, "Why Did So Few Campaigns Sign Up for the FBI's Cybersecurity Briefing?", *Rolling Stone*, October 12, 2018, available at https://www.rollingstone.com/politics/politics-news/fbi-election-hacking-736907/.

190 U.S. Department of Justice, "Russian National Charged in Conspiracy to Act as an Agent of the Russian Federation Within the United States," Press release, July 16, 2018, available at https://www.justice.gov/opa/pr/russian-national-charged-conspiracy-act-agent-russian-federation-within-united-states.

191 U.S. Senate Select Committee on Intelligence, "Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 1: Russian Efforts Against Election Infrastructure with Additional Views" (Washington: U.S. Congress, 2019), available at https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.

192 Eric Lipton, David E. Sanger, and Scott Shane, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.," *The New York Times*, December 13, 2016, available at https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.

193 Atlantic Council DFRLab, "Operation 'Secondary Infektion': A Suspected Russian Intelligence Operation Targeting Europe and the United States" (Washington: 2019), available at https://docs.wixstatic.com/ugd/9d177c_3e548ca15bb64a85ab936d76c95897c7.pdf?index=true.

194 Anthony Cormier and Jason Leopold, "The Money Trail: The Trump Tower Meeting," Buzzfeed News, September 12, 2018, available at https://www.buzzfeednews.com/article/anthonycormier/trump-tower-meeting-suspicious-transactions-agalarov.

195 Diana Pilipenko, "Cracking the Shell: Trump and the Corrupting Potential of Furtive Russian Money" (Washington: Center for American Progress, 2018), available at https://www.americanprogress.org/issues/democracy/reports/2018/02/13/446576/cracking-the-shell/; Diana Pilipenko and Talia Dessel, "Following the Money: Trump and Russia-Linked Transactions From the Campaign to the Presidential Inauguration" (Washington: Center for American Progress, 2018), available at https://www.americanprogress.org/issues/democracy/reports/2018/12/17/464235/following-the-money/.

196 Pilipenko and Dessel,, "Following the Money."

197 Max Bergmann and James Lamond, "The Russians Are Coming in 2020. Dems Don't Have to Be Victims This Time," Daily Beast, February 26, 2019, available at https://www.thedailybeast.com/the-russians-are-coming-in-2020-dems-dont-have-to-be-victims-this-time?ref=author.

Our Mission

The Center for American Progress is an independent, nonpartisan policy institute that is dedicated to improving the lives of all Americans, through bold, progressive ideas, as well as strong leadership and concerted action. Our aim is not just to change the conversation, but to change the country.

Our Values

As progressives, we believe America should be a land of boundless opportunity, where people can climb the ladder of economic mobility. We believe we owe it to future generations to protect the planet and promote peace and shared global prosperity.

And we believe an effective government can earn the trust of the American people, champion the common good over narrow self-interest, and harness the strength of our diversity.

Our Approach

We develop new policy ideas, challenge the media to cover the issues that truly matter, and shape the national debate. With policy teams in major issue areas, American Progress can think creatively at the cross-section of traditional boundaries to develop ideas for policymakers that lead to real change. By employing an extensive communications and outreach effort that we adapt to a rapidly changing media landscape, we move our ideas aggressively in the national policy debate.

Center for American Progress

1333 H STREET, NW, 10TH FLOOR, WASHINGTON, DC 20005 • TEL: 202-682-1611 • FAX: 202-682-1867 • WWW.AMERICANPROGRESS.ORG