Thematic Brief: US Cybersecurity Efforts

Takeaways

Cybersecurity—ensuring malicious actors cannot harm us online—is a top national security issue for the United States. Director of National Intelligence Dan Coats highlighted the current cyber threats that the United States is facing, stating the "warning lights are blinking red."[1] A wide range of actors, including nation-states, terrorist and criminal groups, and lone actors, have launched cyberattacks and committed cybercrime over the Internet, causing devastating impacts to US national and economic security.

Unfortunately, the Trump Administration's cybersecurity efforts lack cohesiveness and effectiveness, starting with President Trump's refusal to acknowledge Russia's interference in America's 2016 presidential election, which utilized cyber tools to spread disinformation and hack into election infrastructure and Democratic Party accounts. While Congress has pushed for more legislation in recent years, these efforts do not reflect a comprehensive strategy to impose consequences on malicious actors.

To strengthen the US government's efforts to combat malicious cyber activity, Congress must now take action to:

1. **Improve** the US government's capabilities to identify, stop, and punish human cyber attackers in order to close the growing cyber enforcement gap: the number of cyberattacks launched per year in the United States versus the number of arrests of malicious cyber actors;
2. **Invest** in securing America's election infrastructure and combating foreign disinformation efforts; and
3. **Re-establish** the United States as a global leader in setting policy around how different actors should behave in cyberspace and boost international cooperation and capacity around these issues.

Cybersecurity is a top national security issue for the United States, with cyber threats posed by a wide range of actors causing devastating national and economic security consequences.

Malicious cyber activity, including cybercrime, has caused devastating impacts to US national and economic security. This activity continues to grow and evolve. According to recent polling Americans view malicious cyber activity as their top security concern, ahead of the economy, nuclear threats, and the Islamic State of Iraq and Syria (ISIS).[2]

The cyber threat affects all sectors of the economy in the United States and globally. A single cyber incident can disrupt thousands of systems worldwide and cost millions of dollars. For example, the NotPetya cyberattack, the most damaging in history, caused over $10 billion in damage.[3] The White House Council of Economic Advisors estimated in 2016 that malicious cyber activity costs the US economy between $57 billion and $109 billion per year.[4] Other estimates put the number as high as $3 trillion for the global economy annually.[5] Because of the borderless nature of cyberspace, a single cyber incident can impact victims in many different countries and can be committed by a perpetrator who is not in any of these locations.

Beyond financial harm, cyberattacks are a serious threat to US national security. Malicious cyber actors have attacked health care systems and critical infrastructure in the United States, such as Industrial Control Systems (ICS), the electric grid, and dams. A successful attack executed on these systems can threaten life and property, and cause large-scale destruction. Hostile nations have used cyberattacks to halt the operations of, and steal sensitive information from, critical US national security institutions and personnel.[6] For example, in 2014 and 2015, the Office of Personnel Management suffered a massive data breach exposing the sensitive information of up to 22 million people, including personal information in their security clearance forms.[7] Terrorists and illicit criminal networks have continued to use the Internet as a key operational tool, presenting a threat to US national security.

Perhaps most alarmingly, Russia's interference in the 2016 presidential election—in which they used malicious cyber tools to spread disinformation and hack into election infrastructure and Democratic Party accounts in favor of then-candidate Donald Trump—demonstrates the grave danger cyber threats can pose to US national security and confidence in American democracy.[8]

Of particular concern, there is a burgeoning cybercrime wave in the United States. Cybercrime are crimes that use or target computer networks no matter the perpetrator, and can include such things as data theft, fraud, distributed denial-of-service (DDoS) attacks, worms, ransomware, and viruses.[9] The Federal Bureau of Investigation (FBI) received more than 300,000 reports of cybercrime via its Internet Crime Complaint Center (IC3) last year.[10] Since the FBI estimates that only 15% of victims report incidences of cybercrime, that number is probably a vast undercount.[11] Cybercrime is a major concern to the US government because malicious cyber actors have been able to commit criminal activity, such as stealing assets from America's largest financial institutions, over the Internet. Cybercriminals also benefit from the high demand for malicious cyber tools from nation-states like Russia, Iran, and North Korea, who use these tools to perpetrate attacks on US institutions and people.[12]

The Trump Administration's cybersecurity efforts lack cohesiveness and effectiveness. Congress has done little to strengthen the US government's response to cyber threats.

Despite the growth and evolution of cyber threats, the Trump Administration's approach has lacked coherence. The Administration's strategy to combat this threat has not matched with the president's words and deeds.

The US Intelligence Community (IC) has unanimously concluded that Russia launched malicious cyber operations to influence the outcome of the 2016 presidential election.[13] Yet President

Trump continues to deny their involvement, undermining the position of the IC and hindering our ability to work with international partners to combat this threat.[14] The president has also resisted imposing sanctions on Russia for its meddling in the 2016 election, despite pressure from Congress. The "Countering America's Adversaries Through Sanctions Act" (PL 115-44) set a deadline to impose sanctions on Russia for their involvement in the 2016 election. The Administration missed the deadline by several weeks, but eventually bowed to the pressure and agreed to impose the sanctions.[15]

Further, while the Trump Administration has taken important steps to expand the US government's cyber efforts—including by indicting a number of malicious cyber actors and creating new cyber threat information-sharing mechanisms for the private sector—the Administration's recently released *National Cyber Strategy* lacks a comprehensive approach to addressing this threat and does not meet the benchmarks for an effective strategic approach that allows for proper oversight.[16] While the *National Cyber Strategy* is an important first step, it centers heavily on cyber defense (i.e., trying to protect Americans from attacks) with only a few short sections committed to pursuing the attackers themselves. It proposes no advances in how the government will assess its progress in combating cyber threats and has few innovative, new solutions to address the number of tremendous challenges that exist in doing so.

The Trump Administration is actively undoing the progress made in recent years to establish such leadership. In particular, the Administration has eliminated two key positions on cybersecurity. First, it eliminated the White House Cyber Coordinator position within the National Security Council (NSC), leaving coordination to two senior director-level NSC officials.[17] Second, it downgraded the State Department's Coordinator for Cyber Issues.[18] The Office of the Coordinator for Cyber Issues at the State Department was established by the Obama Administration as the first senior-level position and office at the State Department working to advance America's diplomatic efforts on cyber issues and build the capacity of our nation's diplomats to deal with these threats.

Congress must hold the Trump Administration accountable for its lack of clarity and consistency in its cyber approach, and push for an aggressive and comprehensive cybersecurity strategy for the United States. However, the 115th Congress fell short in these efforts. A Third Way analysis of over 200 pieces of cybersecurity-oriented legislation introduced in the last congressional session shows that more than 87% of the proposed bills focus on defensive measures like information sharing, breach notifications, and investing in better infrastructure. The Senate was too often an impediment to new legislation; 42 bills did not receive a vote in the Senate after passing the House.

Defensive-oriented efforts are critical and deserve much larger support. But they must be balanced with a focus on policies that also help the United States stop, identify, and punish malicious cyber actors and reduce the current level of impunity. Further, the few bills that were introduced in the 115th Congress that are designed to impose consequences on aggressors or boost international cooperation to this end—such as the "Cyber Deterrence and Response Act" (H. R. 5576) and the "Cyber Diplomacy Act" (H.R. 3776)—failed to make progress and deserve reconsideration in the 116th Congress.

Congress must now take action to strengthen the US government's efforts to combat malicious cyber activity.

To strengthen the US government's efforts to combat malicious cyber activity and create coherence and effectiveness in the government's approach, Congress must now take action to:

1. Improve the US government's capabilities to identify, stop, and punish human cyber attackers in order to close the cyber enforcement gap.

The United States is facing a rising and often unseen cybercrime wave. Yet Third Way's research has found that cybercriminals operate with near impunity compared to their real-world counterparts. Right now, the United States is as far from a comprehensive strategy aimed at identifying, stopping, and punishing malicious cyber actors as the nation was from a strategic approach to countering terrorism in the weeks and months before 9/11. Congress must work to address this by putting in place the foundations for such a strategy.

Third Way has launched a new *Cyber Enforcement Initiative* to help Congress do just that.[19] Our research estimates that for every 1,000 cyber incidents, only three ever see an arrest—what we call the **cyber enforcement gap.** That is an enforcement rate of 0.3%.[20] By comparison, the clearance rate for property crimes was approximately 18% and for violent crimes 46%, according to the FBI's Uniform Crime Report (UCR) for 2016.[21]

The United States requires a rebalance in its cybersecurity policies: from a heavy focus on building better cyber defenses against intrusion to also waging a more robust effort to go after human attackers. Achieving this would require a more balanced approach that places much more emphasis on law enforcement and diplomacy, while preventing the overreliance on the military that currently exists. Rather than responding to cyber threats that come into the United States with military operations, the US government should and can use its Title XVIII authorities to bring law enforcement to bear against the attacker at any time. Unfortunately, the current prioritization undervalues and underinvests in that response. We can only stop the cybercrime wave and close the cyber enforcement gap by transforming law enforcement, enabled by diplomacy, to go after the human beings perpetrating or ordering attacks.

Third Way has established 10 policy areas that require urgent attention from Congress in order to reduce the cyber enforcement gap:

To Catch a Hacker: Summary of Recommendations

Domestic Enforcement Reform	International Cooperation and Coordination Reform	Structural and Process Reform
1. A Larger Role for Law Enforcement	5. An Ambassador-level Cyber Quarterback	8. Better Success Metrics
2. A Cyber Enforcement Cadre	6. Stronger Tools in the Diplomacy Arsenal	9. Organizational Changes and Interagency Cooperation
3. Better Attribution Efforts	7. Better International Capacity for Enforcement	10. Centralized Strategic Planning
4. A Carrot and Stick Approach to Fugitives		

THIRD WAY

As a first step, Congress must work to establish a baseline to understand the scope of the cyber enforcement problem. This will lay the foundation for a comprehensive strategy aimed at closing the cyber enforcement gap. There must be a comprehensive assessment of current government efforts across all agencies with a role in cyber enforcement to determine what is working, what might need to be amplified, and what might need to change. Establishing a baseline would include requiring a government-wide assessment of the current levels of US law enforcement actions, as well as an analysis of the amount and effectiveness of support provided to other countries by the US State Department to build their capacity around cyber investigations. Without baseline statistics, it is difficult to measure government efforts, develop budget estimates for current levels of effort, or make an informed case for budget increases necessary to support increased enforcement levels. Congress can address this by mandating these baseline assessments and pushing for cyber enforcement agencies to establish better metrics to measure the extent of the problem.

2. Invest in securing America's election infrastructure and combating foreign disinformation efforts.

As America's adversaries have utilized malicious cyber tools and information warfare to attack the United States, undermine its institutions, and sow discord, Congress needs to forcefully push back and invest in securing America's election infrastructure and combating disinformation efforts at all costs.

In 2016, the IC concluded that Russia attempted to not only influence the outcome of the US presidential election, but also inject public distrust in our democratic institutions and electoral systems. Russia took a series of actions aimed at boosting the candidacy of Donald Trump, who was seen as more likely to serve Russia's interests. The indictments from the investigation led by Special Counsel Robert Mueller demonstrate how Russian agents hacked the Clinton campaign, the Democratic Congressional Campaign Committee, and the Democratic National Committee in multiple operations.[22] The emails stolen from these hacks were then published on the website WikiLeaks in an effort to publicly undermine the candidacy of Hillary Clinton.[23]

While the leaked emails received plenty of press coverage, Russian operatives also targeted election infrastructure. They breached the voter databases and websites of seven states in the run up to the 2016 election.[24] There is no evidence these databases were manipulated, but the Russians clearly showed they have the capability to do so. Congress must take action to protect US election infrastructure from future interference and disruption.

Despite a renewed focus on election security before the 2018 midterms, US election infrastructure and mechanisms remain woefully inadequate. Russia's hacking into state election databases shows the vulnerability of election security systems to manipulation. Further, most information security experts agree that paper backups for ballots are crucial for election integrity and the ability to perform accurate and trustworthy audits; yet five states in the United States do not use paper backups.[25] The technology used to vote in some states is also often outdated and unreliable.[26] Congress has only allocated $380 million to help states strengthen and modernize their election security systems after the 2016 election. After the voting irregularities of 2000, Congress had allocated an amount 10 times greater.[27]

Unfortunately, congressional Republicans have stymied efforts to provide more funds for election security and give states the critical resources they need to protect future elections.[28] House Democrats have now introduced the "For the People Act" (H.R.1), which contains substantial funding for election security and makes paper backups compulsory for all federal elections.[29] The bill is an important first step to ensuring safe, secure, and reliable American elections and instilling public confidence in US democratic institutions.

Additionally, Congress must work to combat foreign disinformation campaigns aimed at sowing division among the American public and injecting doubts in voters' minds about their democratic systems. Russia's efforts to interfere in the 2016 US presidential election included exploiting social and traditional media platforms, including widely utilized platforms such as Facebook and Google, to promote propaganda and spread false or misleading information through the use of fraudulent accounts and advertisements.[30] The IC has concluded that Russia's disinformation campaigns were aimed at supporting the candidacy of Donald Trump.[31] However, Russian operatives often did so by talking less about the election itself. Instead, they focused on issues that have prominence in current US political debates, such as gun rights and support for veterans, with the goal of dividing the American public against each other and promoting Donald Trump's positions on these issues.[32]

Countering foreign election interference efforts will require dedicated action from policymakers, working in coordination with private sector companies whose platforms are used to spread disinformation. Members of Congress must educate the public about Russian disinformation efforts and condemn President Trump's attempts to ignore or downplay them. Congress must also work to assess whether the US government has all of the tools it can possibly use to combat foreign meddling in America's elections. The Department of Defense has expanded its cyber operations targeting Russian hackers and agents with "digital alerts," letting them know that the US government can see what they are doing. Congress must evaluate whether these efforts are having enough impact in deterring Russia and other foreign actors from using malicious cyber tools to interfere in US elections.[33]

Action is also required from technology companies to shore up their defenses against foreign influence operations and protect against the spread of disinformation. These companies have a responsibility to protect their users from these efforts and to crack down on malicious cyber actors that use their platforms to meddle in democratic elections and divide societies. Bills

such as the "Honest Ads Act" (S. 1989), demanding more transparency for election-related advertising on online platforms, are a step in the right direction.[34] That act is now a part of H.R. 1, along with a number of other election security and voting measures that should be made into law.[35] Congress needs to ensure that social media companies are stringent in enforcing policies that prevent the spread of disinformation and use of fraudulent accounts on their platforms.

3. Reestablish the United States as a global leader in setting policies on behavior in cyberspace and boost international cooperation and capacity on this issue.

The global nature of the cyber threat requires dedicated and deliberate leadership and coordination at the highest echelons of the US government. Given the scope of countries that are impacted by cyber threats, little progress can be made in America's cybersecurity efforts if our cyber diplomatic and development efforts are not expanded and ties to partner nations around the globe are not strengthened. To catch international cybercriminals, America needs a coordinated international effort and cooperation on cyber investigations.

A congressional authorization to elevate the Office of the Coordinator for Cyber Issues at the State Department is a good first step, but it is not enough. The office must also be provided with a clear mandate that includes a focus on closing the enforcement gap, strengthening its efforts to identify the perpetrators of cyberattacks, and implementing diplomatic training programs. It must also be provided by Congress with the necessary resources and personnel to be able to implement those initiatives. This is critical to drive forward a rebalance in America's cybersecurity approach to one that puts the State Department front and center as a key entity for progress.

Additionally, Congress must provide adequate resources to global cyber capacity-building efforts. Currently, the United States provides capacity-building assistance to countries on cybersecurity and cybercrime through US diplomatic, development, and international judicial programs. It is clear that the current levels of funding and manning for capacity-building efforts are not adequate to meet the challenge. To strengthen the capability of partner nations, the US government must assess and expand its support of global cyber enforcement capacity building. It must help foreign authorities understand and address cyber threats as it also works to strengthen its own cybersecurity efforts.

Conclusion

The United States is facing a burgeoning cybercrime wave, and we do not have a cohesive strategy to combat it. Malicious cyber activity costs the United States between $57 billion and $109 billion each year, and may cost trillions of dollars globally. It poses a serious national security threat—we have already seen attacks not only against private technology companies, but also the electrical grid, election systems, health care systems, and government agencies. Still, only three in 1,000 cyber incidents result in an enforcement action. We must do more to identify, stop, and punish malicious cyber actors.

While the Administration has made a number of indictments through the Department of Justice, their approach to this threat remains incoherent and inadequate, starting with the president's refusal to acknowledge Russia's attempt to influence the 2016 presidential elections.

The Administration has eliminated critical positions from the White House and the State Department, undoing the progress made in previous administrations. Congressional Republicans, along with the White House, have impeded substantial investment to secure our elections.

Congress has an opportunity to assert its authority and act in our national security interest by taking these three steps: 1. improve the US government's capability to identify, stop, and punish malicious cyber actors; 2. invest in election security and combatting foreign influence operations; and 3. reestablish the US as a global leader in cyberspace.

ENDNOTES

1 Barnes, Julian E. "'Warning Lights Are Blinking Red,' Top Intelligence Officer Says of Russian Attacks." *The New York Times*, 13 July 2018, www.nytimes.com/2018/07/13/us/politics/dan-coats-intelligence-russia-cyber-warning.html. Accessed 3 Dec. 2018.

2 Poushter, Jacob, et al. "Climate Change Still Seen as Top Global Threat, but Cyberattacks Rising Concern." Pew Research Center, 11 Feb. 2019, www.pewglobal.org/2019/02/10/climate-change-still-seen-as-the-top-global-threat-but-cyberattacks-a-rising-concern/#changing-threats-in-a-changing-world. Accessed 15 Feb. 2019.

3 Greenberg, Andy. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *Wired*, 7 Dec. 2018, www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/. Accessed 4 Jan. 2019.

4 United States, White House, The Council of Economic Advisers. *The Cost of Malicious Cyber Activity to the U.S. Economy.* February 2018, pp. 1. https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf. Accessed 4 Jan. 2019.

5 Sterling, Bruce. "Global Cybercrime. Costs a Trillion Dollars. Maybe 3." *Wired*, 19 July 2017, www.wired.com/beyond-the-beyond/2017/07/global-cybercrime-costs-trillion-dollars-maybe-3/. Accessed 4 Jan. 2019.

6 United States, Department of Homeland Security. "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors." 15 March 2018. https://www.us-cert.gov/ncas/alerts/TA18-074A. Accessed Oct. 3 2018.

7 Nakashima, Ellen. "Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say." *The Washington Post*, 9 July 2015, www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/. Accessed 22 Oct. 2018.

8 Mazzetti, Mark, and Katie Benner. "12 Russian Agents Indicted in Mueller Investigation." *The New York Times*, 13 July 2018, www.nytimes.com/2018/07/13/us/politics/mueller-indictment-russian-intelligence-hacking.html. Accessed 9 Oct. 2018.

9 United States, Department of Justice, Office of Legal Education, *Prosecuting Computer Crimes*, 1 Jan. 2015, pp. V. https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf. Accessed 3 Oct. 2018.

10 Federal Bureau of Investigation. *2016 Internet Crime Report*. 22 June 2017, pp. 17. https://pdf.ic3.gov/2016_IC3Report.pdf. Accessed 3 Oct. 2018.

11 "New National Commitment Required: The Changing Nature of Crime and Criminal Investigations." *Police Executive Research Forum*, Jan. 2018. https://www.policeforum.org/assets/ChangingNatureofCrime.pdf. Accessed Oct. 3, 2018.

12 Eddy, Max, "Inside the Dark Web." *PCMAG*, 4 Feb. 2015, www.pcmag.com/article2/0,2817,2476003,00.asp. Accessed 22 Oct. 2018.

13 Collins, Eliza. "Yes, 17 Intelligence Agencies Really Did Say Russia Was behind Hacking." *USA Today*, 16 Dec. 2016, www.usatoday.com/story/news/politics/onpolitics/2016/10/21/17-intelligence-agencies-russia-behind-hacking/92514592/. Accessed 13 Feb. 2019.

14 Fabian, Jordan. "Trump Refuses to Denounce Russian Involvement in Election at Joint Presser with Putin." *The Hill*, 16 July 2018, www.thehill.com/homenews/administration/397203-trump-denies-russian-involvement-in-election-at-joint-presser-with. Accessed 19 Dec. 2018.

15 Liptak, Kevin. "Trump Administration Finally Announces Russia Sanctions." *CNN*, 15 Mar. 2018, www.cnn.com/2018/03/15/politics/russia-sanctions-trump-yevgeniy-viktorovich-prigozhin/index.html. Accessed 13 Feb. 2019.

16 United States, White House, National Security Council. "President Trump Unveils America's First Cybersecurity Strategy in 15 Years." 20 Sept. 2018. https://www.whitehouse.gov/articles/president-trump-unveils-americas-first-cybersecurity-strategy-15-years/. Accessed Oct. 9, 2018.

17 Perloth, Nicole, and David Sanger. "White House Eliminates Cybersecurity Coordinator Role." *The New York Times*, 15 May 2018, https://www.nytimes.com/2018/05/15/technology/white-house-cybersecurity.html. Accessed 19 Oct. 2018.

18 Johnson, Derek B. "Senate Panel Votes to Revive State Cyber Office." *FCW*, fcw.com/articles/2018/06/26/cyber-state-senate-office.aspx. Accessed 19 Oct. 2018.

19 "Third Way Cyber Enforcement Initiative." Third Way, 29 Oct. 2018, www.thirdway.org/series/third-way-cyber-enforcement-initiative. Accessed 14 Feb. 2019.

20 Eoyang, Mieke, et al. "To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors." Third Way, 29 Oct. 2018, www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors. Accessed 3 Dec. 2018.

21 "Clearances." Federal Bureau of Investigation, 25 Aug. 2017, ucr.fbi.gov/crime-in-the-u.s/2016/crime-in-the-u.s.-2016/topic-pages/clearances. Accessed 3 Dec. 2018.

22 "U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations." The United States Department of Justice, 4 Oct. 2018, www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and. Accessed 19 Oct. 2018.

23 Nakashima, Ellen, and Shane Harris. "How the Russians Hacked the DNC and Passed Its Emails to WikiLeaks." *The Washington Post*, 13 July 2018, www.washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78_story.html. Accessed 14. Feb. 2019.

24 McFadden, Cynthia, et al. "U.S. Intel: Russia Compromised Seven States Prior to 2016 Election." *NBCNews*, 27 Feb. 2018, www.nbcnews.com/politics/elections/u-s-intel-russia-compromised-seven-states-prior-2016-election-n850296. Accessed 12 Dec. 2018.

25 Good, Chris. "5 States Will Vote without Paper Ballots; Experts Want That to Change." *ABC News*, 17 Sept. 2018, www.abcnews.go.com/Politics/states-vote-paper-ballots-experts-change/story?id=57835958. Accessed 13 Dec. 2018.

26 McFadden, Cynthia, and Kevin Monahan. "This Fall You May Be Voting with Obsolete Voting Machines and Ancient Software." *NBCNews*, 7 Sept. 2018, www.nbcnews.com/politics/elections/fall-you-may-be-voting-obsolete-voting-machines-ancient-software-n906651. Accessed 13 Dec. 2018.

27 Werner, Erica. "House GOP Refuses to Renew Election Security Funding as Democrats Fume over Russian Interference." *The Washington Post*, 19 July 2018, www.washingtonpost.com/business/economy/house-gop-refuses-to-renew-election-security-funding-as-democrats-fume-over-russian-meddling/2018/07/18/20761f88-8abb-11e8-8aea-86e88ae760d8_story.html. Accessed 14 Feb. 2019.

28 Demirjian, Karoun. "Senate Republicans Shoot down Extra Funds for Election Security." *The Washington Post*, 1 Aug. 2018, www.washingtonpost.com/powerpost/senate-republicans-shoot-down-extra-funds-for-election-security/2018/08/01/cac1750a-95a1-11e8-a679-b09212fb69c2_story.html. Accessed 13 Dec. 2018.

29 Shoorbajee, Zaid. "Here Are the Big Election Security Measures in the House Democrats' Massive New Bill." *Cyberscoop*, 7 Jan. 2019, www.cyberscoop.com/house-democrat-bill-election-security-measures-2019-hr-1/. Accessed 7 Jan. 2019.

30 Vitkovskaya, Julie, et al., "Who's been charged in Mueller-linked probes, and why." *The Washington Post*, 12 Dec. 2018, https://www.washingtonpost.com/graphics/2017/national/robert-mueller-special-counsel-indictments-timeline/?utm_term=.495ae1907778. Accessed 23 Jan. 2019.

31 Diamond, Jeremy. "Coats: Russian Interference in Politics Ongoing." *CNN*, 2 Aug. 2018, www.cnn.com/2018/08/02/politics/dan-coats-russia-interference-election-security/index.html. Accessed 14 Feb. 2019.

32 Howard, Philip et al. "The IRA, Social Media and Political Polarization in the United States, 2012-2018." Project on Computational Propaganda, Working Paper 2018. Oxford, UK. https://comprop.oii.ox.ac.uk/research/ira-political-polarization/. Accessed 19 Dec. 2018.

33 Nakashima, Ellen. "Pentagon Launches First Cyber Operation to Deter Russian Interference in Midterm Elections." *The Washington Post*, 23 Oct. 2018, www.washingtonpost.com/world/national-security/pentagon-launches-first-cyber-operation-to-deter-russian-interference-in-midterm-elections/2018/10/23/12ec6e7e-d6df-11e8-83a2-d1c3da28d6b6_story.html?utm_term=.d637d4bfe76b. Accessed 19 Dec. 2018.

34 United States, Congress, "Honest Ads Act." Congress.gov, https://www.congress.gov/bill/115th-congress/senate-bill/1989, 115th Congress. 2nd session, Senate Resolution 1989, introduced Jun. 6 2018.

35 Nilsen, Ella. "House Democrats Officially Unveil Their First Bill in the Majority: a Sweeping Anti-Corruption Proposal." *Vox*, 4 Jan. 2019, www.vox.com/policy-and-politics/2018/11/30/18118158/house-democrats-anti-corruption-bill-hr-1-pelosi. Accessed 14 Feb. 2019.