A HOOVER INSTITUTION ESSAY

2018 and Beyond

THE US GOVERNMENT SHOULD DEVELOP A CREDIBLE RESPONSE TO RUSSIAN ELECTION INTERFERENCE—AND SO SHOULD THE PRIVATE SECTOR

JOHN CARLIN AND DAVID NEWMAN

Aegis Series No. 1815

After brazenly interfering in the 2016 US election, Russia now "perceive[s] . . . its past efforts as successful and views the 2018 U.S. midterm elections as a potential target for Russian midterm operations."[1] That was the warning delivered by Director of National Intelligence Dan Coats on behalf of the US Intelligence Community to the Senate Select Committee on Intelligence (SSCI) as part of the worldwide threat briefing that took place February 13, 2018.

Speaking alongside CIA Director Mike Pompeo and FBI Director Christopher Wray, among other senior intelligence officials, Coats stressed to Congress the "need to inform the American public that this is real, that this is going to be happening, and the resilience needed for us to stand up and say we're not going to allow some Russian to tell us how to vote, how we ought to run our country."[2] Later that same week, the Department of Justice (DOJ) further pulled back the curtain on the extent of the threat when it released a thirty-seven-page grand jury indictment that charged thirteen Russian nationals and three companies and described in detail a large-scale, coordinated Russian effort to interfere in the 2016 election and sow division in the US electorate.[3] In a second indictment, released in July 2018, the DOJ charged twelve Russian military intelligence officers with leading extensive hacking efforts to steal troves of presidential campaign communications and state boards of elections voter data and the strategic release of stolen documents to affect the election.[4]

While 2018 has seen significant details emerge, including reports that the Office of Special Counsel is examining data acquired by Cambridge Analytica regarding social media usage, core elements of the narrative and the national security community's high level of confidence in the bottom line have been emphasized to the American public for over a year.[5] Indeed, what Coats conveyed in February 2018 about Russia's future aims—and what the indictments from the Special Counsel illuminated about Russia's past actions—closely tracked the position of the US Intelligence Community at a similar congressional hearing more than a year earlier.[6]

The bottom line assessment that Russia interfered in the past and will continue this type of activity in the future has long been broadly held in Congress by members of both political parties.[7] They are informed by the fact that national security experts of all persuasions have expressed concern that the aftermath of the 2016 election will only embolden Russia and other US adversaries to try again in the future.[8] Indeed, while the context and many of the witnesses were different, the warning from Coats essentially repeated one conveyed at a hearing two months into the new administration when then FBI director James Comey and National Security Agency (NSA) Director Mike Rogers testified before Congress in March 2017 and sounded the alarm about interference in the 2018 election in unusually stark terms.[9]

If the leading intelligence officials had warned more than a year and a half ago of a likely foreign attack on any other aspect of American society, it is hard to imagine anything less than an all-out bipartisan effort in Congress and in the White House to secure the nation. In July 2018, Coats warned that US digital infrastructure "is literally under attack" and that "the warning lights are blinking red."[10] And yet, over the past year, the dire predictions on this topic from experts are not generating national action—and few concrete proposals appear to have any significant traction among policy makers.

The inaction is increasingly part of the problem, as Russia and the Putin regime are able to exploit the fact that the country's political attention has been fixated on—and deeply polarized by—the investigation into what happened in the 2016 election. The Russia inquiry has occupied the field and diverted attention away from planning for the future. Without question, there are difficult policy choices to make, including defining the red lines these activities cross, building a credible public case for what happened, and identifying a proportionate and effective US deterrent. Many of these challenges are exacerbated by the virtual realm in which the hostile activities took place. This makes it more difficult for the activities to be "seen" by the public than in the case of a kinetic attack and complicates the task of rallying the public behind a decisive response. (Some of these challenges are discussed at greater length below.)

This paper contends, however, that the inaction partially stems from *political* and *bureaucratic* obstacles to preparing a US response to any future interference—including obstacles to overcoming public apathy, the concern that any measures taken might favor one political party, and federalism questions that arise whenever the federal government considers proposals affecting state election conduct. The summer's imbroglio over President Trump's summit with Russian President Vladimir Putin in

Helsinki—at which Trump drew immediate criticism for his statement that "I don't see any reason why it would be" Russia that hacked the 2016 election only to quickly assert that he had meant the exact opposite—is but the most vivid example of how the public debate related to all things Russia reflects not just drastically different policy assessments and prescriptions but also vastly different depictions of the facts.[11] Additionally, efforts to prevent election interference in the future raise important questions about the role of social media companies and other private actors in protecting their platforms against exploitation by foreign adversaries—as well as the limits of the federal government's ability to act.

Addressing future interference now and not in the run-up to the 2020 US elections is critical to mounting a more effective response to any future interference.

This paper proposes doing so through three principal means:

Demand Action: Public officials, media organizations, and our broader civic institutions should make a sufficiently compelling case to spur government officials to act and the public to demand such action.

Create a Dead Man's Switch: Policy makers should put in place a "dead man's switch" approach that would insulate (to as large an extent as feasible) the intelligence community's unbiased assessment of whether there is foreign interference and create a presumptive set of US responses when such activities are detected.

Enable the Private Sector: The private sector and policy makers should work together to develop a broader preparedness framework premised on a recognition that certain forms of foreign interference need to be mitigated and addressed through a coordinated response.

Conditions Necessary for a Credible Deterrent

To be effective, a credible deterrent against future interference in American elections requires several preconditions.

We Need a Common Set of Facts

Despite more than a year of testimony and assessments from senior officials (including over the past year from Coats, Pompeo, Wray, and others), large swaths of the American public remain unconvinced that Russian meddling is a grave threat.[12]

Given the strength of the intelligence community's and other experts' assessments, Americans can unite against this foreign threat. But they must have access to the facts.

In the area of cyberthreats, this may require reconsidering the balance between what information is classified and what is shared to allow greater public visibility into the kinds of threats that national security professionals observe and confront every day. A House Committee on Oversight and Government Reform hearing in late 2016 examined the costs of overclassification on transparency and security.[13] It found that an estimated 50 to 90 percent of classified materials are not properly labeled.[14] There are many contexts in which information must be classified to protect sources and methods. Unnecessary classification, however, deprives the public of valuable information and prevents information sharing between federal agencies and with state and local law enforcement.[15]

This is a particular challenge in the area of cyberthreats. Even well-resourced and sophisticated corporations with security-cleared personnel often struggle with how to receive and take action based on government-shared threat information. That is in part because of the delays and limitations of what is shared—and in part because even if a company has some cleared personnel, it is still often difficult to take effective action without active involvement by a broader workforce that lacks clearances.

A second, related step to laying the factual predicate involves maintaining public trust in the intelligence community and in our law enforcement professionals. Even in a world in which classification standards are reformed, the credibility of assessments by the intelligence community will be paramount to marshaling public support for a swift response to election interference. As Mieke Eoyang, Ben Freeman, and Benjamin Wittes pointed out in the fall of 2017, notwithstanding a long period of polarizing incidents and press coverage, "public confidence in the intelligence community as a national security actor [remains] relatively high in general—significantly higher than confidence in any other institution about which [they] poll, save the military."[16] Those figures generally remained stable into 2018.[17] There are some indications, however, that the FBI in the aftermath of a series of high-profile controversies may be experiencing a decline in public trust. A poll conducted in late January 2018 reported that only 51 percent of the public had at least a "fair amount" of trust in the FBI, a 12-point reduction from 2015.[18] While the activities of law enforcement and the intelligence community should never be beyond criticism and political debate, it is essential for those on all sides to understand the extent to which broadside, unfounded attacks

on the dedicated public servants who work in these areas can have serious national security ramifications. Maintaining a high degree of public trust is critically important to the ability of the intelligence community to perform its mission in general, of course, and it is particularly important if the intelligence community is to play the role necessary to build support for a response to the type of attack perpetrated against the United States in 2016.

Finally, the intelligence community should consider working with leading private sector actors in exploring ways to reinforce one another's judgments and credibility in attributing cyberactivities to particular malicious actors. There are often sources-and-methods concerns and other challenges to the US government publicly attributing a cyber event to a particular actor and even greater concerns with giving the public *reasons* for that attribution. Even where such concerns can be overcome, the process for doing so is often cumbersome and does not declassify great detail about the underlying rationale. Thus, even in the rare instance in which official US attribution is publicly announced, such official attribution often comes long after the same information has been reported in the press and is much less persuasive than the classified assessment on which it is based.

In December 2017, for example, senior US government officials from the White House podium announced that after "careful investigation, the United States [was] publicly attributing the massive WannaCry cyberattack to North Korea."[19] Although the announcement represented a significant effort at transparency, commentators pointed out that the official statements were not accompanied by any public evidence of the attribution claim and that media outlets had reported North Korea's involvement months earlier, as had the British government.[20]

Such challenges suggest that, in assessing possible election interference, there may be value in having the intelligence community coordinate more closely with (or, at the very least, work in parallel to) outside vendors who could reinforce the intelligence community's conclusions with additional information gleaned from unclassified sources and who might have a greater ability to substantiate and defend their analysis publicly. In some instances, one would expect these outside firms to reach different conclusions or to articulate a different level of confidence than the US government about such matters (and, indeed, the fact that such firms regularly do so is core to their credibility). Nevertheless, there is value in having regular interactions between the private sector and government so that information can be shared and findings

reinforced where appropriate. The National Cyber-Forensics & Training Alliance, a nonprofit organization that facilitates information sharing across subject-matter experts from the public, private, and academic sectors, provides one example of how such a nongovernment group might operate.[21] There may also be value in creating an oversight body that could audit those assessments to enhance confidence in them and add accountability. Finally, as David Kris recently argued—and as one of us has argued in the past—the actions of law enforcement (the Special Counsel's Russia indictments being prime examples) can serve an important function in providing a powerful, public account in a form that is familiar and credible to the public.[22]

We Need a Common Red Line and Shared Understanding of What Is out of Bounds

The second part of making a sufficiently compelling case requires greater precision about exactly what the Russian government tried to do that crossed a red line. Lost amid the high-profile hacking of the Democratic National Committee and Clinton campaign chairman John Podesta's emails—as well as, perhaps, the targeting of Republican campaigns such as Marco Rubio's—is the fact that this hacking effort was just one of a series of efforts by the Russian government to interfere in the election and that these efforts were already in progress several years before the 2016 election.[23] Indeed, as is clear from the testimony and analysis of current and former US intelligence officials, Russian interference can come in many shapes and sizes. Russian-backed hackers attempted to penetrate US voting systems directly.[24] Russia used fake social media accounts and fake websites to help spread disinformation and to amplify anti-Clinton messages.[25] There is good reason to believe, moreover, that what we witnessed last year might just be the opening salvo of even more sophisticated attacks that could take on yet more variations.[26]

There is an urgent need for greater articulation and clarity from the United States about which forms of interference guarantee a strong US response and why. To begin with, as Mike Rogers, former chair of the House Permanent Select Committee on Intelligence, and Rick Ledgett, former deputy director of the National Security Agency, have proposed, the administration should issue a declaration along the lines of the following: "The United States views any foreign attempt to influence our election processes through covert or clandestine means as an attack on the fundamental underpinnings of our system of government. We will not tolerate such activity and reserve the right to respond to such activities."[27] As Rogers and Ledgett argue, it is important for the US government to "establish a clear line that delineates unacceptable behavior and puts others on notice that we will act as needed to defend ourselves."[28]

Their formulation would add clarity to the US position but would only be a start. While many of the Russian activities (e.g., attempted cyber intrusions into voting systems) represented clear violations of domestic law and potential violations of international law, the legal and policy frameworks applicable to "fake news" and other forms of state-sponsored propaganda are less well established.[29] Also, the First Amendment and the American role in information operations abroad make it difficult for the US government to be the conclusive arbiter of such lines.[30] A lack of clarity or consensus about what is truly "out of bounds" makes it more difficult to design a response that is proportionate to the violation and to justify that response to a domestic and international audience.

For that reason, it will be important to advance bipartisan work to catalog the types of hostile activities that would trigger a US response. For example, there appears to be broad support for the proposition that any effort on the part of a foreign actor to alter vote tabulations or voter registration rolls would fall into this category, as would instances in which a foreign adversary's malicious code was deliberately inserted into US voting-related equipment even if the purpose and impact of such code were not immediately clear. More challenging but equally important would be to address topics such as releases of nonpublic information about a candidate acquired through malicious cyberactivities and covert information campaigns intended to mislead American voters.

We Need to Break out of a Zero-sum Election Mindset

There is inherent political tension in officials of one party making judgments that could have serious implications for an upcoming election. For that very reason, the Department of Justice and the FBI (under both Republican and Democratic administrations) have instituted policies that counsel *against* taking certain investigative actions in politically sensitive matters in the immediate lead-up to an election.[31] Yet if foreign actors attempt to interfere in our election process, America must be able to defend against the threat. As more information about the response to Russian interference is publicly disclosed, it is clear that key decisions made by good people trying to do the right thing for the right reasons nevertheless have been the source of significant controversy. The accounts by Comey and other government officials indicate that, in the run-up to the election, their choices were influenced by the fear of appearing political—even as their actions inadvertently may have created just that impression. Former vice president Joe Biden recently spoke about the difficult discussions that took place inside the White House, acknowledging that a "constant

tight rope was being walked . . . as to what would we do."[32] This echoed comments President Obama made in December 2016 in which he emphasized that in the lead-up to the election, the administration was focused on "playing this thing straight—we weren't trying to advantage one side or the other," adding, "Imagine if we had done the opposite. It would have become one more political scrum."[33]

The Challenges Only Increase as 2020 Draws Closer

Working to address the problem of foreign election interference without partisanship is difficult. But it is also imperative given the assessment that Russia is emboldened and will try to meddle again. We currently do not have a nonpartisan entity or body that is positioned to convince the citizenry of the need for action and could effectively respond to Russian election interference—or interference by any other foreign adversary. Without change, the exact same situation could present itself in this year's congressional midterms or in the 2020 presidential election and our leaders will not be able to respond any more effectively than they did in 2016.

The Building Blocks of a US Detection and Response System

The US government must take additional steps to harden voting systems from foreign intrusion and to include cybersecurity in all aspects of election planning. That effort will require the provision of additional resources, dedicated planning, sustained federal-state and public-private cooperation, and active monitoring of new threats.

The Department of Homeland Security (DHS) took an important first step a year ago by designating the nation's voting and election infrastructure as "critical infrastructure," thus enabling the federal government to offer more in the way of cybersecurity and other assistance to state and local governments responsible for keeping track of voter rolls and administering elections.[34] Now, DHS must deliver on providing assistance to state and local governments that request it. As Francis X. Taylor, former undersecretary for intelligence and analysis at DHS, recently observed, while it is "true that DHS's initial offers for cyber assistance were not embraced by state and locals in past elections . . . since last year, there's been a backlog of requests pouring in."[35] By working collaboratively with the growing number of state and local governments who have sought such assistance, DHS will build trust and persuade more to follow suit.[36] As Rogers and Ledgett have proposed, there is also value in creating a federal interagency task force entirely removed from investigations into past elections with a mandate to protect our elections going forward.[37]

The US government also needs to do more to offer cybersecurity assistance to nongovernment actors who participate in the election system. That includes everyone from political parties and campaign officials to news organizations, social media companies, and debate moderators. This apolitical assistance should include providing briefings from intelligence experts and other career government officials on precautions that can be taken against actual intrusion as well as the overall threat landscape. This reduces the risk of a scenario in which, for example, news organizations on election night are provided with and report falsified vote tallies as part of an effort to undermine confidence in the election.

A recent series of reports from the Belfer Center for Science and International Affairs at the Harvard Kennedy School make concrete recommendations for campaigns and state and local election officials on how to defend against cyberattacks and information operations and represent a good example of the kind of work product that can be generated to inform key actors about protective steps they should take.[38] These include everything from technical recommendations to changes in the way officials and organizations communicate internally and conceptualize cyber risk.

As a positive move in this direction, in December 2017, DHS and the Election Assistance Commission convened with public and private sector stakeholders to launch an industry-led Sector Coordinating Council, which provides a platform for a wide array of industry representatives and government agencies to interact on sector-specific strategies, policies, and activities.[39] While only a first step, public-private convenings can play an important role in helping to facilitate the sharing of threat information and in improving coordination between the federal government and industry.

Following through on the above will require ongoing attention from the senior ranks of the administration, Capitol Hill, and our law enforcement and intelligence agencies, as well as from state and local election officials around the country.

Moreover, at the end of the day, policy makers must also accept that there is no wall high enough or moat wide enough to keep a dedicated adversary out of an Internet-connected system. Responding to such an invasion requires sure-footed governance. The US government must therefore create policies to ensure that decision makers are able to navigate the same difficult political waters when the next attack comes. In other words, our approach to resilience also includes an emphasis on governance reform.

Assign Key Tasks to the Nonpartisan Intelligence Community

Policy makers should map—in advance—a nonpartisan assessment process that relies on career intelligence professionals and analysts whose lives have been spent drawing conclusions about foreign motives. A body like the National Intelligence Council (NIC), the group of career analysts who help issue consensus national intelligence assessments, could be designated in advance to monitor whether a foreign actor is seeking to interfere with an election—be it through disinformation campaigns, hacking candidates or political parties, actual attacks on the election infrastructure, or some combination of these things. In addition, there may be value in standing up an additional body of nongovernment officials (who may be respected former officials or private sector experts) to corroborate or independently assess these judgments.

Insulate Intelligence Collection on Election Interference from Partisan Interference and Political Considerations

To the greatest extent feasible, the NIC's analysis and conclusions relating to election interference should be entirely removed from political appointees. This process should employ similar protections, safeguards, and norms as those in place regarding the process for collecting and disseminating other forms of government-collected information with immediate national and political ramifications, such as census and employment data. An additional way to insulate this process from partisan suspicion would be to create by statute a requirement for the director of national intelligence to provide a summary report to Congress by a certain date (say, June 1 in an election year) that states whether the NIC has detected any attempted foreign interference and, if so, what form that interference has taken. That report should also be released in a public, unclassified form to the extent possible so that private sector actors can better inform themselves about the threat landscape.

Mandating that such a report be delivered on a specified date (with further updates as warranted by new developments so that a foreign actor cannot just wait until June 2, and with the possibility of supplemental reports for special elections) would operate as an action-forcing function and reduce the risk of responses having the appearance of politically driven timing. It also reduces the risk that the policy debates would be driven by "leaks" of what the intelligence community is seeing that are not corroborated by official reports. A requirement that these reports be issued would also give the intelligence community time to seek voluntary cooperation from state

and local governments whose systems might be at risk. By keeping all requests for cooperation voluntary, the US government can avoid federalism concerns about overstepping constitutional boundaries. To ensure accountability, the report should reflect the dissenting voices of any intelligence community elements that disagree in the major assessments, as is customary in the case of the NIC.

If the NIC (or other comparable body that is selected) finds with a high degree of confidence that a foreign power—Russia or any other country or nonstate actor—is taking certain kinds of actions to influence the election or undermine confidence in it, then the general practice should be to make that finding known to the public as quickly as possible. Even if some limited information must be omitted in order to protect intelligence sources and methods, the American people deserve real-time information regarding the sanctity and security of the democratic process, at least in the subset of cases where there is a risk that the actions being taken could undermine the legitimacy and credibility of the election.

The indictments filed by the Special Counsel against Russian individuals and entities in February and July 2018 represent examples of what kind of information could be shared with the American people and an additional vehicle through which a detailed public recitation of efforts by foreign governments to interfere in US elections could be provided. In recent years, as discussed in the David Kris proposal referenced above, DOJ has increasingly made use of indictments that lay out the public case against foreign nation-states engaged in malicious cyberactivities, revealing their sources and methods and making clear that their conduct is out of bounds.[40] But indictments cannot meet the aims of an annual intelligence product and should not be relied on as the sole vehicle for communicating interference to the public. It is critical that this function be carried out by a more permanent body.

Set Conditions for Action in the Wake of Intelligence Findings

The report itself is just a first step. Retaliation for certain kinds of hostile actions should also be authorized in advance by Congress.

The United States has begun to employ, in recent years, the many weapons in its arsenal for responding to cyberattacks from foreign nations—including public condemnations, international sanctions, the expulsion of foreign diplomats, and the filing of criminal charges. Congress should act now to build upon these options by providing clear authority to respond to certain specified forms of election interference,

including by providing clear authorization for actions such as sanctions or, in certain circumstances, for retaliatory cyberoperations or other covert measures. This type of clear authorization would avoid the possibility of protracted deliberations over whether a response is authorized under a patchwork of existing authorities—and would also reduce the likelihood that Congress would need to leap into the fray and pass legislation on the eve of a new election. Moreover, passing legislation now would help bolster deterrence and send a message that any action that is taken under such authorities reflects bipartisan judgments about the way that foreign interference should be handled.

Through mechanisms such as presumptively applicable new measures in the absence of a presidential waiver, such legislation could create strong pressure (and political cover) for the executive branch to act decisively in the wake of the next such incident. Among other things, Congress through legislation could create a presumption that the president *should* in fact employ certain retaliatory measures such as sector-specific sanctions, new authority to sanction individuals, expulsion of diplomats, and removal of certain forms of foreign assistance in the event of high-confidence assessment of election interference by an adversary. Prescribed measures could be based on presidential findings that generally track the assessments called for in the DNI report provided to Congress. For example, if the intelligence community concludes that a foreign actor tampered with (or attempted to tamper with) voter registration records, the legislation could call for sanctions to be imposed against that actor.

As a legal matter, the president would retain the ultimate authority not to follow through on these responses. That is both a necessary feature of our constitutional structure and an important practical check in the event of scenarios that no one contemplated. But the greater the presumption of action in a predefined set of circumstances—and the fewer the opportunities for partisan gridlock and interference—the easier it would be for an administration to take decisive action without appearing political. Such a system would also enhance the deterrent effect by making clear to our adversaries which actions would all but assure a swift US response.

Maximize the Deterrent Impact of the "Dead Man's Switch"

To maximize the deterrent impact of the "dead man's switch," we need agreement about what foreign conduct warrants a swift and decisive US government response. The types of actions that trigger such a response should include any efforts by a

foreign adversary to use cyber-enabled intrusions to infiltrate voter rolls or voting machines or to otherwise impede the ability of Americans to come to the polls on Election Day and vote for their preferred candidates. While Election Day interference is paramount, the types of activities presumptively warranting a response should also in some defined instances include the use of cyberespionage tools and information warfare to sow discord among the American public or harm a candidate, mindful of what was done in 2016 with the steady release of stolen private communications coupled with efforts to spread false information. A bipartisan commission should work now to spell out as exhaustively as possible the types of activities that fall within this category—as well as to define other potential categories of actions that warrant a response—so that the report from the intelligence community can speak to them directly without room for interpretation.

Common Ground with Recent Legislative Proposals

While any election-related legislation faces a steep challenge in the current political environment, two recent proposals in the Senate and newly approved spending show that the elements above command bipartisan support and deserve serious consideration. Those bills are the Defending Elections from Threats by Establishing Redlines Act (the "Deter Act"), introduced by senators Marco Rubio (R-FL) and Chris Van Hollen (D-MD) in January 2018, and the Secure Elections Act, introduced by a bipartisan group of six senators in December 2017.[41]

The Deter Act would require the director of national intelligence to make a determination whether a foreign government had engaged in "interference in the election" within thirty days of a US election taking place and to report that determination to Congress.[42] The bill identifies specific activities that constitute such interference, ranging from obtaining "unauthorized access" to campaign or election infrastructure to spreading "significant amounts of false information" to individuals in the United States via social media (or traditional media).

In the event that an election interference determination is made against the Russian Federation, the bill would require the president to impose immediate additional sanctions against the Russian economy. In addition to Russia, the bill singles out China, Iran, and North Korea as potential threats in the next election cycle and requires the president to submit a strategy to Congress to mitigate such threats. While the Deter Act might benefit from additional definitional work on the subject of foreign

election interference (and while there might be value in requiring such a report before an election rather than afterward), the proposal represents a promising first step toward regularizing an intelligence assessment that examines foreign interference after every election.

Likewise, the Secure Elections Act contains a number of provisions to improve the quality and pace of information sharing regarding election-related threats between the federal government and the states.[43] It also includes a "sense of Congress" that "an attack on our election systems by a foreign power is a hostile act and should be met with appropriate retaliatory actions, including immediate and severe sanctions."[44] In addition, the bill provides for other protections such as the creation of a "bug bounty" program specifically addressed to identifying election vulnerabilities.

Included in the 2018 Consolidated Appropriations Act passed into law in March is funding for modernizing and enhancing the cybersecurity of state election infrastructure.[45] The bill provides for the Election Assistance Commission to make payments to states investing in measures to improve the security and integrity of elections such as the use of marked paper ballots in voting systems that are later audited.[46] (While the use of paper in the voting process is again on the rise across the country, there are still too many places that lack this basic protection.[47])

Acknowledging Gaps in the US Government's Response That Can Only Be Filled by the Private Sector

For the above to be achievable, it is important to recognize the limits of what the US government can do and the critical role that the private sector plays in our electoral system. Election "interference" comes in all shapes and sizes and a broad spectrum of activities may qualify as foreign interference. On one end of the spectrum, a prescribed set of government responses is more appropriate and workable where a foreign adversary actually hacks into voter systems. But as discussed previously, we are increasingly seeing that there are many other ways for foreign adversaries to attempt to interfere in an election.[48]

For one thing, foreign adversaries may hack private actors—such as candidates, political organizations, or even news media outlets—who play important roles in our election system. The July 2018 indictment depicted such an attack against the

Democratic Congressional Campaign Committee and the Democratic National Committee.[49] Moreover, they may seek to exploit the very platforms Americans use to exercise the rights to freedom of speech and freedom of the press by creating online user profiles, groups, and "bots" to publish and spread false information.[50] These types of actions are pernicious but are less amenable to direct government responses. With respect to disinformation operations, in particular, there are important limits to what the government can do. While the NIC report outlined above could describe the existence of such state-sponsored activities, the US government is not well positioned to be the final arbiter of "fake news"—let alone to dictate whether such content should continue to be available online.[51] As a result, in the case of these types of activities, the US government should find additional ways to educate and inform the public and the private sector.

The private sector and civil society have a critical role to play in taking reasonable measures to protect themselves and the public against cyber intrusions. These efforts can include social media companies and private sector researchers informing the public in real time about attempts by foreign adversaries to exploit social media services and platforms, as well as providing information to the public about ways to detect those activities and distinguish state-sponsored content from authentic news and opinion.[52] Facebook recently provided one example of effective action by successfully disrupting a coordinated disinformation campaign and sharing with its users examples of detected inauthentic content.[53] Social media companies should also consider ways in which they could pool resources to better address these threats. In addition, and to reinforce these efforts, Congress should adopt proposed reforms to strengthen the Foreign Agents Registration Act (FARA).[54]

In some respects, the private sector effort on this front could model itself on what has been done in recent years with respect to terrorist content online.[55] Just as an increasing number of private sector companies work collaboratively with one another and the government to develop ways to reduce the risk that their platforms are being exploited by ISIS and other terrorist groups(including where terrorists post content that the US government itself would have difficulty proscribing under the First Amendment), so too could these companies work together to come up with innovative and responsible ways to rebuff foreign governments' efforts at antidemocratic campaigns.[56] Rather than orchestrate this international response, the US government should prepare strategies to inform the private sector about ways in which foreign

adversaries make use of their systems so that these companies can have an informed basis to formulate their own responses and develop new technical solutions.

In addition, and as with the terrorist threat, it will be important for private sector companies to focus not only on what features of their platforms have been exploited in the past but on how they might be used in the future. The focus on the role of "fake news" and bot accounts in the 2016 election is important and appropriate. But the next time around, the threat could instead center on an insider at one of the technology companies, on the use of a cyber intrusion to give rise to a real-world, physical event, or any number of other destabilizing scenarios. In other words, better coordination between the technology industry and government can help to illuminate not only past threats but also potential future lines of attack.

Conclusion

America needs a system that credibly protects our elections and responds to foreign threat actors in real time. One component of that system should be an effort to reduce the role of partisan politics in response planning by creating a mechanism akin to a "dead man's switch" that triggers automatically when something goes awry.

Such a mechanism should include a requirement that the US Intelligence Community determine and report an assessment of election interference as of a specified date within a US election along with a presumption that this assessment and the analysis supporting it be made public (consistent with the need to protect classified sources and methods). In addition, because the credibility of this assessment will be paramount, consideration should be given to enlisting nongovernment experts to make their own determination in parallel to bolster the attribution claim as well as an oversight body charged with reviewing the assessment and the process that produced it. Public availability of technical analysis followed by official attribution successfully generated a coordinated international response to the "NotPetya" cyberattacks.[57] Elements of this approach already command at least some bipartisan support in Congress.

To be sure, no structure on its own will be sufficient to deter all actors or to anticipate and address every permutation of events. But if created carefully and with an eye toward reducing potential partisan divisions, such a "dead man's switch" increases the credibility of US threats to respond to a future attack and may dissuade others from following Russia's example in upcoming elections. At the same time, the exercise of creating such a mechanism requires acknowledging that certain types of interference

are less amenable to a US government response and instead must be redressed through the private sector. For those types of activities, the private sector should work collaboratively now to develop solutions so that we avoid making features of our democratic system into flaws that bad actors can exploit.

NOTES

1 Miles Parks, "Russian Threat to Elections to Persist through 2018, Spy Bosses Warn Congress," NPR, February 13, 2018, accessed September 24, 2018, https://www.npr.org/2018/02/13/584672450/intelligence-leaders-testify-about-global-threats-in-senate-hearing.

2 Ibid.

3 US Department of Justice, Indictment, *US v. Internet Research Agency LLC et al.*, D.D.C., February 16, 2018, accessed September 24, 2018, https://www.justice.gov/file/1035477/download.

4 US Department of Justice, Indictment, *U.S. v. Netyksho et al.,* D.D.C., July 13, 2018, accessed September 24, 2018, https://www.justice.gov/file/1080281/download.

5 Brett Samuels, "Mueller Examining Ties between Trump Campaign, Cambridge Analytica: Report," *The Hill*, March 21, 2018, accessed September 24, 2018, http://thehill.com/blogs/blog-briefing-room/379593-mueller-looking-at-ties-between-trump-campaign-and-cambridge; Rebecca Ballhaus, "Mueller Sought Emails of Trump Campaign Data Firm," *Wall Street Journal*, December 15, 2017, accessed September 24, 2018, https://www.wsj.com/articles/mueller-sought-emails-of-trump-campaign-data-firm-1513296899?mod=e2tw.

6 "Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent U.S. Elections," January 6, 2017, accessed September 24, 2018, https://www.dni.gov/files/documents/ICA_2017_01.pdf*;* Brian Naylor, "Intelligence Chiefs 'Stand More Resolutely' Behind Finding of Russia Election Hacking," NPR, January 5, 2017, accessed September 24, 2018, https://www.npr.org/2017/01/05/508355408/intelligence-chiefs-stand-more-resolutely-behind-finding-of-russia-election-hack.

7 Matt Flegenheimer, "New Bipartisan Sanctions Would Punish Russia for Election Meddling," *New York Times*, June 13, 2017, accessed February 6, 2017, https://www.nytimes.com/2017/06/13/us/politics/senate-sanctions-russia.html; Scott Neuman, "In a Rare Show of Bipartisanship, Senate Sends Russia Sanctions to Trump," NPR, July 27, 2017, accessed September 24, 2018, https://www.npr.org/2017/07/27/539864048/russia-sanctions-headed-to-trumps-desk-will-he-sign.

8 E.g., Asha Rangappa, "How Facebook Changed the Spy Game," *Politico*, September 8, 2017, accessed September 24, 2018, http://www.politico.com/magazine/story/2017/09/08/how-facebook-changed-the-spy-game-215587; Tom Donilon, "Russia Will Be Back. Here's How to Hack-proof the Next Election," July 14, 2017, accessed September 24, 2018, https://www.washingtonpost.com/opinions/russia-will-be-back-heres-how-to-hack-proof-the-next-election/2017/07/14/f085e870-67d5-11e7-a1d7-9a32c91c6f40_story.html?utm_term=.9f84ba452f2b.

9 "Full Transcript: FBI Director James Comey Testifies on Russian Interference in 2016 Election," *Washington Post*, March 20, 2017, accessed September 24, 2018, https://www.washingtonpost.com/news/post-politics/wp/2017/03/20/full-transcript-fbi-director-james-comey-testifies-on-russian-interference-in-2016-election/?utm_term=.b688678a55ba.

10 "Transcript: Dan Coats Warns the Lights Are 'Blinking Red' on Russian Cyberattacks," NPR, July 18, 2018, accessed September 24, 2018, https://www.npr.org/2018/07/18/630164914/transcript-dan-coats-warns-of-continuing-russian-cyberattacks.

11 Matthew Rosenberg, "U.S. Intelligence Community Reacts with Fury to Trump's Rebuke," *New York Times*, July 16, 2018, accessed September 24, 2018, https://www.nytimes.com/2018/07/16/us/politics/us-intel-community-reacts-with-fury-to-trumps-rebuke.htm; Julie Hirschfeld Davis, "Trump, at Putin's Side, Questions U.S. Intelligence on 2016 Election," *New York Times*, July 16, 2018, accessed September 24, 2018, https://www.nytimes.com/2018/07/16/world/europe/trump-putin-election-intelligence.html; Matt Flegenheimer, "Would It or Wouldn't It Be Russia: Trump Goes Double Negative," *New York Times*, July 17. 2018, accessed September 24, 2018, https://www.nytimes.com/2018/07/17/us/politics/trump-putin-russia.html.

12 An NBC News/Survey Monkey poll released in February 2018 found that 41 percent of respondents did not view it as likely that Russia will attempt to influence the 2018 midterm elections. See "Poll: Most Americans Think Russia Will Interfere Again in 2018 Elections," NBC News, February 8, 2018, accessed September 24, 2018, https://www.nbcnews.com/politics/politics-news/poll-most-americans-think-russia-will-interfere-again-2018-elections-n845076. These findings were consistent with a *Washington Post*/ABC News poll released in July 2017 that found that 40 percent of respondents either thought Russia did not try to influence the presidential election or had no opinion on the matter. *Washington Post*/ABC News Poll, July 19, 2017, accessed September 24, 2018, https://www.washingtonpost.com/page/2010-2019/WashingtonPost/2017/07/16/National-Politics/Polling/question_18943.xml?uuid=YUEe3mnbEeeUq1sfD_RZ3w#. An Atlantic and Public Religion Research Institute poll released in July 2018 found that 45 percent of Americans viewed outside influence from foreign governments as a major problem in US elections. See "One Country, Two Radically Different Narratives," *Atlantic*, July 17, 2018, accessed September 24, 2018, https://www.theatlantic.com/politics/archive/2018/07/poll-prri-republican-democratic-voter/565328. An NBC/WSJ poll released in July found that 65 percent of voters believe the Russian government interfered in the 2016 election: Mark Murray, "NBC/WSJ poll: Public Gives Trump Thumbs-down on Russia, Thumbs-up on Economy," NBC News, July 22, 2018, accessed September 24, 2018, https://www.nbcnews.com/politics/first-read/nbc-wsj-poll-public-gives-trump-thumbs-down-russia-thumbs-n893266.

13 "Examining the Costs of Overclassification on Transparency and Security," Full House Committee on Oversight and Government Reform, December 7, 2016, accessed September 24, 2018, https://oversight.house.gov/hearing/examining-costs-overclassification-transparency-security.

14 Ibid.

15 See, e.g., *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, accessed September 24, 2018, https://www.9-11commission.gov/report/911Report.pdf.

16 Mieke Eoyang, Ben Freeman, and Benjamin Wittes, "The Public is Not that Fussed about the Surveillance State: Confidence in the Intelligence Community and its Authorities," *Lawfare* (blog), November 8, 2017, accessed September 24, 2018, https://www.lawfareblog.com/public-not-fussed-about-surveillance-state-confidence-intelligence-community-and-its-authorities.

17 Mieke Eoyang, Ben Freeman, and Benjamin Wittes, "Confidence in Government on National Security Matters: January 2018," *Lawfare* (blog), February 9, 2018, accessed September 24, 2018, https://www.lawfareblog.com/confidence-government-national-security-matters-january-2018.

18 Ariel Edwards-Levy, "Republican Confidence in the FBI Has Dropped Since 2015," *Huffington Post*, February 5, 2018, accessed September 24, 2018, https://www.huffingtonpost.com/entry/republican-confidence-in-the-fbi-has-dropped-since-2015_us_5a721bbbe4b09a544b5616a7.

19 "Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea," The White House, December 19, 2017, accessed September 24, 2018, https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917. The press briefing followed publication of an op-ed in the *Wall Street Journal* penned by Thomas P. Bossert, then the assistant to the president for homeland security and counterterrorism. See Thomas P. Bossert, "It's Official:

North Korea Is Behind WannaCry," *Wall Street Journal*, December 18, 2017, accessed September 24, 2018, https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537.

20 See, e.g., Jack Goldsmith, "The Strange WannaCry Attribution," *Lawfare* (blog), December 21, 2017, accessed September 24, 2018, https://www.lawfareblog.com/strange-wannacry-attribution: "Probably what I am missing is that the public attribution sends an important signal to the North Koreans about the extent to which we have penetrated their cyber operations and are watching their current cyber activities. But that message could have been delivered privately, and it does not explain why the United States delayed public attribution at least six months after its internal attribution, and two months after the U.K. had done so publicly."

21 National Cyber-Forensics & Training Alliance, "One Team, One Goal—Companies, Government, and Academia Working Together to Neutralize Cyber Crime," accessed September 24, 2018, https://www.ncfta.net.

22 John P. Carlin, "Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats," *Harvard National Security Journal* 7 (2016): 391, 420–21, explaining that the filing of public charges "also serve[s] important expressive functions." David Kris, "Law Enforcement as a Counterintelligence Tool," *Lawfare* (blog), March 6, 2018, explaining "[i]ndictments are only charges, not proof—but when they are credible they send a strong message, even if that is not their primary purpose," accessed September 24, 2018, https://www.lawfareblog.com/law-enforcement-counterintelligence-tool.

23 Greg Miller and Adam Entous, "Declassified Report Says Putin 'Ordered' Effort to Undermine Faith in U.S. Election and Help Trump," *Washington Post*, January 6, 2017, accessed September 24, 2018, https://www.washingtonpost.com/world/national-security/intelligence-chiefs-expected-in-new-york-to-brief-trump-on-russian-hacking/2017/01/06/5f591416-d41a-11e6-9cb0-54ab630851e8_story.html?utm_term=.4fbcb9d6d018.

24 Alex Ward, "Russia Hacked Voting Systems in 39 states before the 2016 Presidential Election," *Vox*, June 13, 2017, accessed September 24, 2018, https://www.vox.com/world/2017/6/13/15791744/russia-election-39-states-hack-putin-trump-sessions.

25 Laura Sydell, "How Russian Propaganda Spreads on Social Media," NPR, October 29, 2017, accessed September 24, 2018, https://www.npr.org/sections/alltechconsidered/2017/10/29/560461835/how-russian-propaganda-spreads-on-social-media.

26 In mid-February 2018, both the US and British governments publicly identified Russia as being behind the NotPetya attack that badly damaged Ukraine's infrastructure and caused billions of dollars of damage around the world. See Andy Greenberg, "The White House Blames Russia for NotPetya, the 'Most Costly Cyberattack in History,'" *Wired*, February 15, 2018, accessed September 24, 2018, https://www.wired.com/story/white-house-russia-notpetya-attribution.

27 Mike Rogers and Rick Ledgett, "Four Steps to Fight Foreign Interference in U.S. Elections," *Washington Post*, February 14, 2018, accessed September 24, 2018, https://www.washingtonpost.com/opinions/four-steps-to-fight-foreign-interference-in-us-elections/2018/02/14/fb99b7a0-11c1-11e8-8ea1-c1d91fcec3fe_story.html?utm_term=.1b8e638f690d.

28 Ibid.

29 Jens David Ohlin, "Did Russian Cyber Interference in the 2016 Election Violate International Law?" *Texas Law Review* 95 (June 2017): 1579, accessed February 6, 2018, http://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=2632&context=facpub; Patrick Tucker, "Did Russia's Election Meddling Break International Law? Experts Can't Agree," *Defense One*, February 8, 2017, accessed September 24, 2018, http://www.defenseone.com/technology/2017/02/did-russias-election-meddling-break-international-law-experts-cant-agree/135255.

30 Ishaan Tharoor, "The Long History of the U.S. Interfering with Elections Elsewhere," *Washington Post*, October 13, 2016, accessed September 24, 2018, https://www.washingtonpost.com/news/worldviews/wp/2016/10/13/the-long-history-of-the-u-s-interfering-with-elections-elsewhere/?utm_term=.15937fc59f64; Dov Levin, "Database Tracks History of U.S. Meddling in Foreign Elections," interview by Ari Shapiro, NPR, December 22, 2016, accessed September 24, 2018, http://www.npr.org/2016/12/22/506625913/database-tracks-history-of-u-s-meddling-in-foreign-elections.

31 Attorney General Michael B. Mukasey, "Memo to All Employees Re: Election Year Sensitivities," March 5, 2008, accessed September 24, 2018, https://www.justice.gov/sites/default/files/ag/legacy/2009/02/10/ag-030508.pdf. Attorney General Eric Holder, "Memo to All Employees Re: Election Year Sensitivities," March 9, 2012, accessed September 24, 2018, https://www.justice.gov/sites/default/files/oip/legacy/2014/07/23/ag-memo-election-year-sensitivities.pdf.

32 Brett Samuels, "Biden on Russia: Easy to Say We Should've Said More," *The Hill*, January 23, 2018, accessed September 24, 2018, http://thehill.com/blogs/blog-briefing-room/370300-biden-handling-evidence-of-russian-election-interference-was-tricky.

33 Mark Landler and David E. Sanger, "Obama Says He Told Putin: 'Cut it Out' on Hacking," *New York Times*, December 16, 2016, accessed September 24, 2018, https://www.nytimes.com/2016/12/16/us/politics/obama-putin-hacking-news-conference.html.

34 US Department of Homeland Security, "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector," January 6, 2017, accessed September 24, 2018, https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

35 Francis X. Taylor, "Firewalling Democracy: Federal Inaction on a National Security Priority," *The Hill*, January 31, 2018, accessed September 24, 2018, http://thehill.com/opinion/national-security/371251-firewalling-democracy-federal-inaction-on-a-national-security.

36 As the 2018 elections drew nearer, a growing number of state election officials have recognized the importance of federal assistance in securing their elections and are urging Congress to support such efforts. See, e.g., Michelle Ye Hee Lee, "State Elections Officials Fret over Cybersecurity Threats," *Washington Post*, February 7, 2018, accessed September 24, 2018, https://www.washingtonpost.com/politics/state-elections-officials-fret-over-cybersecurity-threats/2018/02/17/1f850f46-1331-11e8-9065-e55346f6de81_story.html?utm_term=.b9c1da254e77, reporting that at a recent conference of secretaries of state, several state officials called for "more information from federal officials to ensure they are protected from cybersecurity threats in light of evidence that foreign operatives plan to try to interfere in the midterm elections."

37 Rogers and Ledgett, "Four Steps to Fight Foreign Interference": "Such a task force should combine U.S. policymaking and intelligence communities, including the Departments of Homeland Security, Justice, Commerce, Defense, State and Treasury, as well as relevant intelligence agencies."

38 See, e.g., Defending Digital Democracy Project, "The State and Local Election Cybersecurity Playbook," February 2018, accessed September 24, 2018, https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook.

39 Joe Uchill, "Homeland Security, Private Sector Launch Election Security Group," *The Hill*, December 15, 2017, accessed September 24, 2018, http://thehill.com/policy/cybersecurity/365081-homeland-security-private-sector-launch-election-security-group.

40 Carlin, "Detect, Disrupt, Deter."

41 Marco Rubio and Chris Van Hollen, "Our Elections Are in Danger. Congress Must Defend Them," *Washington Post*, January 16, 2018, accessed September 24, 2018, https://www.washingtonpost.com

/opinions/our-elections-are-in-danger-congress-must-defend-them/2018/01/15/c7b3aac8-fa28-11e7-ad8c-ecbb62019393_story.html?utm_term=.f87f899dfaea. Morgan Chalfant, "Bipartisan Group of Lawmakers Backs New Election Security Bill," *The Hill*, December 21, 2017, accessed September 24, 2018, http://thehill.com/policy/cybersecurity/365986-bipartisan-group-of-lawmakers-introduces-new-election-security-bill.

42 The text of the bill is available here: https://www.rubio.senate.gov/public/_cache/files/1467ea7c-ca91-45a6-be41-f5043d4bce88/BCFC8F63C1D8049CF5593DEB32703C2C.hen18060revised.pdf.

43 The text of the bill is available here: https://www.congress.gov/bill/115th-congress/senate-bill/2261/text.

44 Ibid.

45 The text of the bill is available here: https://www.congress.gov/bill/115th-congress/house-bill/1625/text.

46 Approved uses of funds can be found here: https://www.eac.gov/payments-and-grants/frequently-asked-questions-for-grants/#how-can-states-use-the-funds.

47 Lawrence Norden and Ian Vandewalker, "Securing Elections from Foreign Interference," Brennan Center for Justice, accessed November 1, 2018, https://www.brennancenter.org/sites/default/files/publications/Securing_Elections_From_Foreign_Interference_1.pdf, emphasizing the importance of the federal government "help[ing] states and counties replace the old, paperless Direct Recording Electronic machines that are still used in 14 states, with more secure, accessible systems" and adding that "[p]aper records of votes have limited value against a cyberattack if they are never used to check that the software-generated total has not been hacked"; Elisabeth Weise, "Paper Ballots Are Back in Vogue Thanks to Russian Hacking Fears," *USA Today*, September 19, 2017, accessed September 24, 2018, https://www.usatoday.com/story/tech/news/2017/09/19/russia-hacking-election-fears-prompts-states-to-switch-to-paper-ballots/666020001, noting some states "are taking the unusual move of rewinding the technological dial, debating measures that would add paper ballots—similar to how many Americans voted before electronic voting started to become widespread in the 1980s."

48 See, e.g., Issie Lapowsky, "What We Know—And Don't Know—About Facebook, Trump, and Russia," September 26, 2017, accessed September 24, 2018, https://www.wired.com/story/what-we-know-and-dont-know-about-facebook-trump-and-russia.

49 See US Department of Justice, Indictment, *U.S. v. Netyksho et al.* D.D.C., July 13, 2018, accessed September 24, 2018, https://www.justice.gov/file/1080281/download.

50 Marisa Schultz, "Twitter Uncovered More than 200 Russia-linked Bots," *New York Post*, September 28, 2017, accessed September 24, 2018, http://nypost.com/2017/09/28/twitter-uncovered-more-than-200-russia-linked-bots; Nicholas Fandos and Kevin Roose, "Facebook Identifies an Active Political Influence Campaign Using Fake Accounts," *New York Times*, July 31, 2018, accessed September 24, 2018, https://www.nytimes.com/2018/07/31/us/politics/facebook-political-campaign-midterms.html.

51 These threats are only heightened by the growing availability and sophistication of tools that allow for the creation of "deep fake" video and audio footage that looks and sounds authentic. Robert Chesney and Danielle Citron, "Deep Fakes: A Looming Crisis for National Security, Democracy and Privacy?" *Lawfare* (blog), February 21, 2018, accessed September 24, 2018, https://www.lawfareblog.com/deep-fakes-looming-crisis-national-security-democracy-and-privacy.

52 Consider as one example the way private sector organizations quickly identified Russian bot activity attempting to push divisive content in the wake of the Parkland, Florida, school shooting in mid-February 2018. Sheera Frenkel and Daisuke Wakabayashi, "After Florida School Shooting, Russian 'Bot' Army Pounced," *New York Times*, February 19, 2018, accessed September 24, 2018, https://www.nytimes

.com/2018/02/19/technology/russian-bots-school-shooting.html, noting that Russian "automated Twitter accounts have been closely tracked by researchers. Last year, the Alliance for Securing Democracy, in conjunction with the German Marshall Fund, a public policy research group in Washington, created a website that tracks hundreds of Twitter accounts of human users and suspected bots that they have linked to a Russian influence campaign."

53 "Removing Bad Actors on Facebook," July 31, 2018, accessed September 24, 2018, https://newsroom .fb.com/news/2018/07/removing-bad-actors-on-facebook, discussing Facebook's continuing efforts to identify and take down accounts involved in coordinated inauthentic behavior.

54 The Repelling Encroachment by Foreigners into U.S. Elections Act (REFUSE Act) amends FARA to require foreign agents to file and label political propaganda and authorizes the attorney general to issue civil investigative demands. The text of the bill is available here: https://www.congress.gov/bill/115th-congress /house-bill/6249/text.

55 "Facebook, YouTube, Twitter and Microsoft Join to Fight against Terrorist Content," Reuters, June 26, 2017, accessed September 24, 2018, https://www.cnbc.com/2017/06/26/social-media-companies-join -to-fight-against-terrorist-content.html, "Social media giants Facebook, Google's YouTube, Twitter and Microsoft said . . . they were forming a global working group to combine their efforts to remove terrorist content from their platforms."

56 "Justice Department, Silicon Valley Discuss Online Extremism," Reuters, February 24, 2016, accessed September 24, 2018, https://www.reuters.com/article/us-cyber-justice/justice-department-silicon-valley -discuss-online-extremism-idUSKCN0VX2CL.

57 Dustin Volz and Sarah Young, "White House Blames Russia for 'Reckless' Notpetya Cyber Attack," Reuters, February 15, 2018, accessed September 24, 2018, https://www.reuters.com/article/us-britain -russia-cyber-usa/white-house-blames-russia-for-reckless-notpetya-cyber-attack-idUSKCN1FZ2UJ.

The preferred citation for this publication is: John Carlin and David Newman, "2018 and Beyond: The US Government Should Develop a Credible Response to Russian Election Interference—and So Should the Private Sector" Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 1815 (November 13, 2018), available at https://www.lawfareblog.com/2018-beyond-the-government-should-develop-credible-response.

About the Authors

JOHN P. CARLIN

John P. Carlin, who previously served as assistant attorney general for national security at the Department of Justice, chairs the Aspen Institute's Cybersecurity & Technology Program and is the author of *Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Cyber Threat* (PublicAffairs 2018).

DAVID A. NEWMAN

David A. Newman previously served as special assistant and associate counsel to the president, on the National Security Council staff, and as counsel to the assistant attorney general for national security at the Department of Justice.

Working Group on National Security, Technology, and Law

The Working Group on National Security, Technology, and Law brings together national and international specialists with broad interdisciplinary expertise to analyze how technology affects national security and national security law and how governments can use that technology to defend themselves, consistent with constitutional values and the rule of law.

The group focuses on a broad range of interests, from surveillance to counterterrorism to the dramatic impact that rapid technological change—digitalization, computerization, miniaturization, and automaticity—are having on national security and national security law. Topics include cybersecurity, the rise of drones and autonomous weapons systems, and the need for—and dangers of—state surveillance. The group's output will also be published on the Lawfare blog, which covers the merits of the underlying legal and policy debates of actions taken or contemplated to protect the nation and the nation's laws and legal institutions.

Jack Goldsmith and Benjamin Wittes are the cochairs of the National Security, Technology, and Law Working Group.

For more information about this Hoover Institution Working Group, visit us online at http://www.hoover.org/research-teams/national-security-technology-law-working-group.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
The Johnson Center
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200

HOOVER INSTITUTION