Defending Digital Democracy: The Four Corners of Election Security

Prepared Statement
by
Honorable Eric Rosenbach
Co-Director of the Belfer Center for Science and International Affairs at the Harvard Kennedy School; former Chief of Staff to the Secretary of Defense and Assistant Secretary of Defense for Homeland Defense and Global Security

Before the

United States Senate Select Committee on Intelligence

Hearing on

Russian Interference in the 2016 US Elections

March 21, 2018

Chairman Burr, Vice Chairman Warner, and distinguished members, thank you for the invitation to testify. As one of the very few bipartisan efforts to address the cybersecurity challenges to our country right now, this Committee is crucial in charting the course forward. As a former professional staff member on the Senate Intelligence Committee, I have great respect for your bipartisan approach and genuinely thank you for your service.

Our response to Vladimir Putin's ongoing attempts to undermine the strength of American democracy will be a defining issue of our digital age. The most important lesson we should internalize from Russia's interference campaign in 2016 is the price of complacency: we ignore continued cyber attacks and insidious information operations at our own peril.

Putin's attacks are not limited to our election systems. Recent reports from the Department of Homeland Security make clear that Russian military intelligence operatives continue to conduct the preparatory steps needed for a major cyberattack against our energy grid.

Imagine if we found out during the Cold War that Soviet intelligence operatives had placed secret explosives that could take down the electric grid all around the United States. Would US leaders stand by and debate the nature of the threat, or would we act?

Unfortunately, our national response to Russian cyber and info attacks—both against the US and our allies—has been too weak. America and democracies around the world need action. This should not be a partisan issue: we must shift gears from examining the problem to taking

assertive steps to address it. Given the current environment in Washington, the Senate Intelligence Committee will need to play a leading role in driving action and solutions.

Russia's actions underscore the urgency to pursue a whole-of-nation strategy that involves the four key players in our election ecosystem: states, campaigns, tech companies and the federal government. A "four-cornered" effort involving these actors would focus on four primary goals:

1. Bolster our domestic cyber defenses and systemic resilience;
2. Develop and rehearse a coordinated, national incident response plan;
3. Develop precise and legal offensive cyber capabilities that will disrupt cyber and information attacks at their source; and
4. Adopt a clear, public deterrence posture, which definitively signals that we will not accept threats to, or attacks on, our democratic institutions and critical infrastructure.

The Problem

Our country's reliance on digital technologies, coupled with our open and transparent information ecosystem, has created significant vulnerabilities. We increasingly live in a digital "glass house" that must be much better protected. The glass house analogy illustrates three important points.

- As technology advances and we become more connected, we become more vulnerable. This is because cyber warfare is asymmetric: a small nation with an offensive cyber capability can have an outsized effect on a larger power. In fact, the greater the technology gap between us and an adversary, the greater our vulnerability. For example, the US is significantly more vulnerable to cyberattack than North Korea, a nation where most citizens do not even have an internet connection. North Korea, however, has advanced offensive cyber capabilities.

- Democracies' transparent, open societies also make them vulnerable to foreign information operations. In democracies, free speech is protected, and internet accessibility is high. In contrast, authoritarian societies often control the media, censor the internet and shield their nations from outside information through national firewalls, such as the Great Firewall of China. America's enemies have learned to weaponize free speech.

- The vulnerabilities caused by openness are exacerbated by the way in which modern communications technologies facilitate near-instantaneous information sharing, the proliferation of online networks and communities, and the creation of massive troves of information and data. These factors enable information operations at a scale, and level of personalization, previously unimaginable.

The Russian Government was a first-mover in fully understanding the vulnerabilities in a digital democracy. As early as 2014—and possibly before—President Putin authorized a widespread campaign with the strategic goal of undermining trust in democracy and inciting political and social discord.

The facts about Russia's action in 2016 are now widely understood. Russian intelligence operatives and their thinly-disguised proxies stole and leaked sensitive information from political campaigns and employed hundreds of operatives in "troll farms" to spread and amplify toxic content on social media, and to orchestrate divisive political rallies on American soil. They used bots to further spread their narratives, and drown out legitimate voices. They also tried to hack, or at least test, vulnerabilities in multiple states systems.

Most of the digital tools Russia did use were cheap, and did not require technical sophistication. Russia also relied more on information operations than it did on cyberattacks. But the hybrid nature of cyber and information operations was effective and provides a model for attacks in the future. Without a major shift in US policy, this problem is not going away. Instead, we should expect Russia, and other actors emboldened by Russia's success, to conduct increasingly potent cyber and information attacks against our elections and other core systems that underpin our democracy.

Defending Digital Democracy Project

The Defending Digital Democracy Project, a bipartisan initiative I co-lead at Harvard's Belfer Center along with Robby Mook and Matt Rhoades, is developing real-world, practical solutions to defend against cyber and information attacks. The team has breadth and depth of talent—including cybersecurity experts from government and the private sector, technologists and political operatives. Ahead of the 2018 midterms, we have released practical election security guides, including for political campaign staff, state and local election officials, and for election cyber incident communications teams.

Through our work, we have come to believe that election security can only be achieved by a whole-of-nation effort. Specifically, it will require a four-corned effort by:

1. State governments, whose election officials are now front-line defenders of our democratic systems, and must adopt cybersecurity best practices, and lead on incident response to cyber and information operations.
2. Political campaigns, who must internalize their responsibility to adopt good cyber hygiene and bolster their own cyber defenses.
3. Social media companies, who must accept that our adversaries will continue to manipulate their platforms unless they dramatically change their organizational culture and operational paradigm.
4. The federal government, which must better *support* state and campaign efforts, *oversee* social media and *lead* on creating a credible national defensive posture equal to the cyber and information threats our elections face.

State Governments

States run and control elections in the United States. That puts local election officials on the front lines of the effort to defend against nation-state attacks on our democracy. They accept this

mission admirably: the Defending Digital Democracy team has been consistently impressed by the professionalism, and dedication of state and local election officials. And I would like to acknowledge my fellow panel member Secretary Condos for the work he has done up in Vermont and will continue with his service as the future President of the National Association of Secretaries of State.

Our team conducted field research at 34 state and local election offices, observed the November 2017 elections in three states, conducted a nationwide survey on cybersecurity with 37 states and territories, and engaged state and local election officials in three national "tabletop exercise" simulations.

This research revealed the complex and decentralized nature of the US election system. Every state has to protect and monitor an election ecosystem that is an interconnected "system of systems." This ecosystem includes core election systems—like registration databases, voting machines, and counting and reporting systems. But it also includes non-core systems, like state and county administrative and office databases, email systems, public-facing websites, and third party vendor systems.

On top of this, the fact that election decision-making is delegated to multiple counties, and in some cases municipalities, results in several hundred, if not thousands, of different election processes across the country. Conventional wisdom leads many officials to claim that this makes our democracy more secure; however, my time serving as the "Cyber Czar" for the Department of Defense convinced me that security through complexity is a myth. In fact, complexity is a force multiplier for our adversaries. It creates a huge attack surface that is difficult to patch, monitor, and defend. To succeed in destroying Americans' trust in democracy, Russia doesn't need to successfully attack the entire voting infrastructure. A cybersecurity incident in just a handful of counties could undermine public confidence in the national electoral process.

State election officials clearly understand that they are at risk and, in many cases, under attack. Many state election officials worked to improve their cyber defenses well before the Russian attacks in 2016, but nearly all of them have significantly upped their game over the past six months. That said, the states need more help: they simply are not equipped to face the pointy-end of the spear of cyber attacks from advanced nation-states.

The primary goal of the Defending Digital Democracy team is to provide as much assistance as possible to the states and campaigns. Last month, we released an Elections Cybersecurity Playbook, which sets out measures we believe are essential: using audits to maintain trust in the system; isolating sensitive systems; and requiring paper vote records.

One important, underemphasized issue is the ability of state and federal governments to respond publicly to cyber and information operations. Understandably, many election officials' initial instinct is to not talk to the press, or otherwise communicate. However, in elections, perception is reality. An adversary does not need to engage in actual cyber operations to manipulate the outcome of an election. They can erode trust in the process by using information operations to make the public believe that the election was manipulated or fraudulent. One of the few real

antidotes to aggressive information operations is effective public communications about the true state of affairs. We developed an additional public communications incident response playbook for the states with this in mind.

Next week, the Defending Digital Democracy team will host over 160 state and local election officials from 38 states to run them through a series of crisis simulations and training exercises to train and empower them to improve their cyber defenses and incident response capabilities.

The work we've done at the Harvard Kennedy School is really just a small part of the assistance that the states need—and deserve—to defend themselves. The states need additional support in the following areas:

- **Funding for election security.** Many states adopted digital voting systems after the 2000 presidential elections, but have not received the funding needed to keep these systems upgraded and secure. The most frequent concern noted by election officials in our nationwide security survey was insufficient resources to secure elections, especially in smaller counties. Funding could be tied to states following best practice cybersecurity recommendations, and could also be given in the form of grants for incident response planning, and "red team" exercises.
- **Access to information.** The Department of Homeland Security is working hard to increase intelligence sharing to the states through the multi-state Information Sharing and Analysis Center, and to grant security clearances to some officials. However, we need a paradigm shift in this area. Unlike nearly every other national security threat, federal agencies are the support, not the lead, on election security. Collecting intelligence therefore has limited utility if it is not shared with the state officials on the frontline. One option: strengthen the role that state-run fusion centers play in election-related threat information sharing. Threat intelligence from private sector cybersecurity and tech firms will also be key to any information sharing arrangement.
- **Cybersecurity expertise.** All sectors of the American economy are starving for additional personnel with cybersecurity expertise and states are no different. Working with the private sector, the country needs to find ways to surge more cybersecurity expertise to the states in the run-up to the 2018 midterms and the 2020 presidential vote. One option: the Defending Digital Democracy team is working to develop a Democracy Defense Service of deployable experts who could help states in need. Built on the model of the Defense Digital Service, this could provide states with help when they need it...without creating unnecessary bureaucratic organizations.
- **Vendor security.** In many states, vendors design and maintain hardware and software that affect voter registration, vote capture and tallying, electronic pollbooks, election night reporting, and public communication. In our nationwide security survey, 97% of states and territories used a vendor in some capacity. Some vendors service multiple states—meaning an attack on one vendor could affect many jurisdictions. One option: states should demand explicit security stipulations in requests for proposals and all acquisition and maintenance contracts. Congress should bolster this by requiring vendors to provide notification of any system breach immediately after they become aware of it.

Campaigns

Political campaigns are the soft underbelly of the American election process. Unfortunately, even after the cyberattacks on 2012 and 2016 presidential campaigns, many campaign workers do not yet fully appreciate the important role they have in improving the integrity of our elections.

Russia did not need sophisticated cyber-weapons to hack into the Democratic campaign in 2016. It used spear phishing—which requires persistence, more than technical capability. This points up the urgent need for campaigns to adopt basic standards of cyber hygiene. The Defending Digital Democracy team has developed a "Top Five Checklist," as part of a broader Campaign Cybersecurity Playbook, specifically designed for resource-constrained campaign workers. At a minimum, campaigns need to move data to the cloud, and require two-factor authentication on all important accounts. We are pleased to see that Kentucky and West Virginia's Secretaries of State have officially issued the Playbook to candidates in their states.

Campaigns can significantly improve their cyber defenses by following cybersecurity best practices, but they can't fight our adversaries' national intelligence services on their own. The most urgent need for campaigns is much better access to threat information and intelligence. Unlike the states, currently no Information Sharing and Analysis Center or information sharing arrangement exists to facilitate the flow of threat information from the government and private sector to campaigns. This type of assistance is complicated by current campaign finance law. Robby Mook and Matt Rhoades are leading the Defending Digital Democracy effort in this area, where we've developed several blueprints for campaign information sharing architectures that could work within the existing realities of law and politics.

Social media

Imagine how Americans in the 20th century would have reacted to news that our manufacturing titans were building weapons, on American soil, for US adversaries, or that broadcast television networks were providing a megaphone to Soviet spies. Social media companies have revolutionized communication and commerce in the 21st century, and they are an essential aspect of American economic power in the Information Age. But social media companies have also created tools and systems which can be used to subvert democracy.

Government oversight has not kept pace with these changes. But, more significantly, neither have the leadership and organizational culture essential to organizations that wield so much power and influence in a digital democracy. Their very business models are enabled by the democratic protections afforded by the American system of government, including the First and Fourth Amendments. Simply put: Facebook and Twitter are no longer scrappy start-ups that can move fast, break things, and beg forgiveness later. They are some of the world's most powerful, and capitalized corporations and they should act that way.

Noting this, Facebook and Twitter must:

- **Transform their organizational culture.** Leading tech firms need to internalize the role they play in protecting democracy, and ensure that their business models do not damage the very democratic protections that have enabled their success. Transparency will be an essential component in rebuilding trust in these organizations.
- **Adjust their algorithms to reflect their role in democracy.** Because of their market dominance, Twitter and Facebook do not just house public discourse; they shape it. Currently, social media algorithms are optimized for user engagement, because clicks and views maximize revenue. As a result, Facebook, YouTube and Twitter often promote and prioritize controversial information—something that Russian trolls and bots exploited to great effect. However, it is possible—and necessary—to adjust these algorithms.
- **Increase human involvement in decisions.** Real humans must be involved in flagging problematic content and accounts. Autonomous agents are still easily fooled, and, despite growing excitement about the promises of artificial intelligence, for the foreseeable future there will remain no substitute for human language processing and cognition when it comes to addressing national security threats.

Congress should also ensure that social media is treated in the same way as other industries which create negative externalities for society. In particular, Congress should strongly consider legislation to:

- **Enhance transparency.** Users have a right to know when they are seeing paid political advertisements, and, in some cases, why they are being targeted by particular political or social campaigns. Congress should pass legislation that mandates the same disclosure for political ads on social media as for traditional media.
- **Strengthen data protection rules.** Data collected by social media companies is extraordinarily powerful, and social media firms have proved themselves unable to properly protect it. This was reinforced by allegations concerning the transfer of sensitive Facebook user data to Cambridge Analytica. We do not permit hospitals or financial institutions to monetize sensitive consumer data without consent, and we hold them accountable when sensitive information is leaked. The data collected by social media firms can be just as sensitive since we now know it will be used to created detailed psychological profiles of users. And its misuse has even broader implications for society, since those profiles can be harvested and "weaponized."

Government

Protecting democratic institutions from cyber and information attacks by nation-states is an inherently governmental role. Unfortunately, our national response to Russian cyber and info attacks—both against the US and our allies—has been too weak. The recent move by the Trump Administration to increase sanctions on Russian entities involved in cyber attacks against Ukraine and the US is a step in the right direction, but not nearly enough.

The US and international community must respond to cyber and information operations with actions that are sufficiently visible and serious to deter future attacks. Given the depth of the

"glass house" problem I outlined above, our weak response puts America in a very vulnerable position.

Thus, the US must urgently act to bolster its deterrence posture by both raising the costs of attacks and decreasing the benefits to hostile actors of engaging in this conduct. In addition to a host of non-cyber foreign policy options, the US should pursue the following initiatives:

- **Bolster Cyber Command's capability to address information operations.** The US military lacks the structure and capability necessary to defend the nation from future attacks. Special Operations Command has historically led Department of Defense efforts in information operations, but the lead must now shift to Cyber Command in order to strengthen the nexus of cyber and information operations capabilities necessary for the Information Age. That said, the DoD's recent efforts to combat ISIS through a joint SOCOM-CYBERCOM effort, known as Task Force Ares, represents an outstanding model for future operations.
- **Strengthen indications and warning of cyber and information operations attacks.** The Intelligence Community, and the National Security Agency in particular, need to bolster the "early warning" system for information operations which target US democratic institutions. This will require better collaboration with the private sector, which should shed its post-Snowden reluctance to cooperate with the government on pressing national security issues.
    - LTG Paul Nakasone is an outstanding leader who is absolutely the best person to lead CYBERCOM and NSA in an effort to accomplish both of these recommendations.
- **Continue to strengthen DHS information sharing and cybersecurity capacity.** Under the leadership of Secretary Nielsen and Under Secretary Krebs, DHS has prioritized and improved information sharing with the states. The Department's efforts to provide cybersecurity scans and risk assessments to the states have been productive and help to mitigate risk. Congress should strongly support these efforts and provide DHS with the resources it needs to bring them to full maturity, while DHS should broaden and strengthen efforts to support the cybersecurity of political campaigns.

Conclusion

This Committee has rightly observed that a whole-of-government response is required to address the problems of election security. I completely agree, but would go further: this must be a whole-of-nation effort, which involves each of the four key players in our election ecosystem. But, this four-cornered effort needs leadership, and the Senate Intelligence Committee is the team most likely to provide that cross-cutting, bipartisan leadership in the current environment.