Securing America's Digital Democracy: Preparing for 2020

Prepared Statement by Honorable Eric Rosenbach Co-Director of the Belfer Center for Science and International Affairs at 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 House Committee on Appropriations
Subcommittee on Financial Services and General Government

Hearing on Election Security and the Integrity of Election Systems

February 27, 2019

Introduction

Thank you Chairman Quigley and Ranking Member Graves for the invitation to speak to your committee today. It is an honor to be here today to speak to you about our nation's election security and the integrity of our election systems. The House Committee on Appropriations' Subcommittee on Financial Services and General Government has jurisdiction over many of the independent federal agencies that are critical to election security in the U.S., including the Election Assistance Commission (EAC) and the Federal Election Commission (FEC). Your subcommittee can play a leading role in helping ensure our democracy is secure and resilient in the face of a myriad of threats.

In early February, the U.S. Intelligence Community confirmed that, "there is no evidence to date that any identified activities of a foreign government or foreign agent had a material impact on the integrity or security of election infrastructure or political and campaign infrastructure used in the 2018 midterm elections for the United States Congress."[1] This is certainly a testament to the increased preparedness of state and local election officials; however, we simply should not assume our adversaries have moved away from targeting U.S. elections.

The U.S. Intelligence Community Worldwide Threat Assessment Report, presented to Congress by DNI Dan Coats on January 29th, highlighted the persistent threat of foreign interference in 2020.[2] The Assessment assures us, and I agree, that our adversaries are already planning how they will disrupt the 2020 elections. As we saw in 2016, our adversaries will use cyber and information operations to undermine the core tenets of our democracy and we must do our part to make our elections resilient to these threats. They seek to exploit divisions in our society and

[1] https://www.justice.gov/opa/pr/acting-attorney-general-and-secretary-homeland-security-submit-joint-report-impact-foreign
[2] https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

erode our faith in the most important American values: a vibrant, free-market economy and our democracy, the hallmark of which is free and fair elections.

The Assessment also highlights the growing capabilities of key threat actors to interfere in U.S. elections. China is consistently improving its cyber capabilities and influence operations in the U.S. Iran has demonstrated its ability to manipulate social media and online content, and may do so around the election to impact voters. Russia clearly has the will and the means to disrupt U.S. elections, as it demonstrated in 2016. We should expect to see more hack and leak operations, as well as information operations aimed at poisoning genuine political dialogue and sewing doubt in the validity of the electoral process and results. The Justice Department's indictment in February 2018 of individuals associated with Russia's "troll factory," the Internet Research Agency, shows the sophisticated information operations employed by Russia. The IRA targeted U.S. citizens across the political spectrum, targeting members of both parties. On top of these existing means of election interference, new means of influencing elections are also emerging. Deep fakes -- fake but convincingly realistic videos of public figures created with artificial intelligence -- are already presenting a problem and will likely play a large part in the next election.

Disruptions to American elections are a whole-of-nation threat that requires a whole of government response. In the face of these threats, Congress needs to take the lead on securing our democracy. We will never be able to eliminate the cyber and information risks posed by our adversaries to elections, but we can manage this risk effectively by prioritizing actions to secure our elections now.

I will address the following actions that Congress should prioritize to secure our elections before 2020:

1. Bolster domestic defenses and resilience;
2. Develop precise and legal offensive cyber capabilities;
3. Adopt a clear, public deterrence posture.

Bolster domestic defenses and resilience

To help bolster national defense and resilience against election manipulation, Congress should take a few key steps. First, Congress should authorize and appropriate regular, ongoing federal funding focused on improving the security of our elections. The $380 million approved by Congress last year was an extremely important step forward; however, the states need a dependable source of funding to support the cybersecurity and upkeep of electronic voting systems. This funding should be flexible, but tied to concrete progress in adopting the NIST Cybersecurity Framework.

Furthermore, Congress should pass a comprehensive national privacy law that protects Americans' personal data and information from abuse by both leading tech firms and nation-state intelligence services in Russia and China. The privacy law passed by California last year provides a good foundation for national legislation, though Congress should work thoughtfully to ensure that new legislation provides the foundation for American firms to lead the world in innovation throughout the Information Age.

Congress should also immediately pass regulation to ensure that online platforms such as Facebook, Twitter, and YouTube are not used as tools of foreign information operations. These firms have taken initial steps towards identifying and removing content pushed by foreign intelligence services to manipulate and divide Americans. That said, Facebook's disregard for American's privacy represents a significant national security vulnerability to our democracy.

Additionally, Congress and the federal government should use the various levers at their disposal to improve cyber risk management. Congress should incentivize private companies to make cyber risk management a priority. For example, DHS and FBI can help the market for cyber risk management solutions by increasing the collection and dissemination of anonymized cyber incident data. The creation of the EI-ISAC (Election Infrastructure ISAC) in February 2018 has already improved election security. The EI-ISAC is hosted by the Center for Internet Security and supported by DHS. It provides free resources for states and counties to share key information about cyber and information threats to elections.[3] The EAC supports the EI-ISAC and Congress should continue to encourage this information sharing among states and localities. Private sector companies can also play an increased role in EI-ISAC by sharing threat intelligence on elections.

Outside organizations and civil society also have an important role to play in bolstering our defenses against cyber and information operations against U.S. elections. I co-lead the Belfer Center and started a project in the wake of the 2016 election to provide resources and training for state and local election officials across the country. The Defending Digital Democracy Project (D3P) is a bipartisan initiative, co-led by myself, Robby Mook, Hillary Clinton's former campaign manager, and Matt Rhoades, Mitt Romney's former campaign manager. Our team has provided concrete support to campaigns and state and local election officials by way of playbooks and intense simulation exercises. We have a team of over 30 students, cyber security experts, political operatives, and election leaders who work to create free resources for campaigns and election officials, including the Cyber Security Campaign Playbook, the State and Local Cybersecurity Playbook, and the Election Cyber Crisis Communication Guide and Template.

As part of our field research, we have worked with election officials from every one of your states. We ran three crisis simulation exercises for over 350 state and local election officials from

[3] https://www.cisecurity.org/ei-isac/ei-isac-membership-faq/

over 40 states. Following our national level simulation in March 2018, 15 states have conducted their own crisis simulations, which is a valuable part of increasing preparedness and resiliency. Ten states specifically used their Help America Vote Act (HAVA) funds, approved by Congress and administered by the EAC, to run simulations based on our project's work. Other NGOs are doing incredibly valuable work in this space and we can all continue to bolster election preparedness and resiliency ahead of 2020.

Finally, the role of the federal government in defending elections is crucial. I applaud Congress and Secretary Nielsen for creating the Cybersecurity and Infrastructure Security Agency (CISA), which elevated the mission of the former National Protection and Programs Directorate (NPPD) within DHS and established CISA.[4] Chris Krebs, Jeanette Manfra, and Senior Advisor Matt Masterson have clearly prioritized securing elections, and I urge Congress to continue to support their efforts. The EAC also continues to be a great resource to the states, and I am pleased to see it at quorum now that Ben Hovland and Donald Palmer were sworn-in earlier this month.[5]

Develop precise and legal offensive cyber capabilities

The second priority in securing elections is to develop precise and legal offensive cyber operations that change the current dynamic of America simply sitting back and absorbing the blows of adversarial actions. Good defenses are important, but defense will not alone mitigate the threat of foreign attacks. To complement defensive measures, the U.S. government, led by the Department of Defense, needs to bolster its capabilities to disrupt and degrade cyber and information operations at their sources.

NSA Director and Commander of USCYBERCOM, General Paul Nakasone, has stated that CYBERCOM is conducting offensive cyber operations against Russia and other adversaries to deter Russian operatives from interfering in U.S. elections.[6] While the actions are not threatening the operatives directly, CYBERCOM's actions will raise the cost of interference for our adversaries. This is a good start and I hope we will continue to see CYBERCOM acting against foreign actors who target our elections as we get closer to 2020.

In addition to CYBERCOM's current efforts, the Intelligence Community should also strengthen its indicators and warnings of cyber and information operations against elections. Most election officials do not have security clearances, but information sharing up and down between election officials and intelligence agencies is an area with room for improvement in 2020.

---

[4] https://www.dhs.gov/cisa/about-cisa

[5] https://thehill.com/policy/cybersecurity/423672-senate-confirms-commissioners-to-election-agency-giving-it-full-powers

[6] https://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=.563d55d9d25f

DoD should also bolster Cyber Command's capability to address information operations. Looking beyond U.S. elections, CYBERCOM should take a stronger role in stemming attacks from their source, particularly relating to information operations.

Adopt a clear, public deterrence posture

Our response to Russian interference in 2016 was not strong enough; that has resulted in a perception by our adversaries that they can attack American democracy without incurring any pain or costs. We need a strong national response that interfering in our elections in any manner is unacceptable. Imagine if we found out during the Cold War that Soviet operatives gained access to polling places and vote counting machines and attempted to change the outcome of the election? Would President Reagan have stood by and debated the threat, or would he have acted? We have to raise the cost of attacks and decrease the benefits that our adversaries seek.

Public attribution is the most important component of raising those costs. The increased willingness of the Intelligence Community, DHS, and FBI publically to attribute attacks through indictments is a crucial and positive first step. In conjunction with swift and strong sanctions, and targeted offensive cyber operations, this will send a clear message to foreign adversaries that interference in our elections will never be tolerated. Without these types of actions, we can expect these nations' attacks against our democracy to continue.

We need to support our allies and partners too, many of whom face the same threats. Ukraine's presidential elections are at the end of March, and the European Parliament elections are coming up in May 2019. "Las Vegas Rules" don't apply to elections -- we cannot allow Russia to use its neighbors and our partners as a testing ground for cyber and information operations against elections like they have done in the past. If we do not respond, we will see increased attacks against --and decreased public confidence in-- western elections.

Conclusion

Defending our nation and our elections from adversaries is ultimately a government responsibility, so I am glad that you are holding this hearing to encourage further discussion around election security ahead of 2020.

No defense will ever be perfect. We need a robust private sector to maintain our position as the world's technological leader. We need a federal government that is engaged in helping state and local election officials, who are on the frontlines of defending our democracy. Elections are at the core of our democracy, and at the end of the day, require a whole-of-nation effort to be prepared for any adversaries who try to target the 2020 elections.

Thank you for your time, and I look forward to your questions.