February 13, 2018

Testimony before the Cyber Subcommittee of the Senate Armed Service Committee (SASC) – Countering Russian Influence in the United States Elections Process

Robert J. Butler
Senior Vice President, Critical Infrastructure Protection Operations, AECOM
Adjunct Senior Fellow, Center for a New American Security

Mr. Chairman, Ranking Member Nelson, and distinguished members of the Cyber Subcommittee, thank you for inviting me to speak on the topic of countering Russian influence in the United States elections infrastructure. I would like to begin by noting that my opinions are mine and do not reflect the views of any organization.

For more than 37 years, my work life has been about Information Technology (IT) and its application across Defense and other sectors. Along the way, I was afforded the opportunity to help guide the evolution of information warfare; information and cyberspace strategy and operations within the Department of Defense (DOD); and the United States Government (USG) as a planner and commander. My work in DOD included the stand-up of information operations (IO) organizations, development of IO campaign plans, and serving as the DOD lead in the first USG negotiation with the Russians on cyber arms control in 1998. I was also privileged to serve as the Director of Intelligence at US Transportation Command (TRANSCOM) during Operations Enduring and Iraqi Freedom. I culminated my military career by commanding the intelligence operations organization that is now commonly referred to as NSA-Texas.

After retirement from the United States Air Force (USAF), I served as the senior civilian executive for DOD's premiere joint information operations command before joining a US-based global IT services firm as its Director of its Military Intelligence Programs. Returning to government service in 2009, I served as the first Deputy Assistant Secretary of Defense (DASD) for Space and Cyber Policy. During my time as a DASD, I witnessed and was alarmed at the expansion of the cyber threat around the globe - specifically, China's rampant on-line theft of US intellectual property and Russia's continued disruptive cyber-attacks in the Ukraine and other parts of the world.

Since leaving government service in 2011, I have spent most of my time in the private sector. As a corporate Chief Security Officer and now as an AECOM[1] security executive, I

[1] AECOM is an American multinational engineering firm that provides design, consulting, construction, and management services to a wide range of clients. AECOM has approximately 87,500 employees, and is number 156 on

had the opportunity to build and implement enterprise security programs to countering foreign threats. Additionally, I have served and continue to serve as a consultant to various Defense Science Board (DSB) task forces including the recent cyber deterrence task force. It is from this experience base, I address you today. I've organized my remarks around three topics: 1) my assessment of the Russian threat, specifically to our electoral process; 2) my recommendations for what the federal – including DoD – and state governments, along with US industry should do to further counter Russian or any other foreign government influence; and 3) my suggestions for how this committee could help in this national security work. While my testimony focuses on enhancing the resilience of the US electoral process, I have also made some suggestions regarding the resilience of critical infrastructures more generally as the threats and responses overlap.

The Russian Threat and our Election Process.

Our ability to counter Russian influence operations is a function of what we know about the Russian threat and our ability to address that threat through hardening, resilience, and other countermeasures. The National Security Strategy (NSS) and the National Defense Strategy (NDS) identify Russia as "attempting to erode American security and prosperity" including "using information tools in an attempt to undermine the legitimacy of democracies."[2] As reported by our intelligence agencies, the Russian Federation has been engaged in a campaign aimed at interference with our 2016 presidential election process. Russian intelligence obtained and maintained access to elements of multiple US state or local electoral boards. Russia's influence campaign has been multi-faceted and has included Russian government cyber and media activities along with the use of third party intermediaries and social media "trolls."[3] Importantly, we have no indication that this Russian influence campaign against democratic elections has stopped. In fact, Russian Government interference in European national elections leads us to a very different judgment, namely that this type of Russian aggression is growing.[4] NATO assessments about Russia's capabilities and intent confirm this assessment.[5] CIA Director Pompeo has stated that Russia can be expected to meddle in the 2018 elections.[6]

A key focus of the Russian influence actions has been against the election infrastructure in our states. The threat to state electoral systems is dependent on the state election

---

the 2016 Fortune 500 list. (2018, January 01). About AECOM. Retrieved February 06, 2018, from http://www.aecom.com/about-aecom/

[2] Trump, D. (2017, December). National Security Strategy. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf pp. 2, 14.

[3] Director of National Intelligence. (2016, January). Background to "Assessing Russian Activities and Intentions in Recent US Elections". https://www.dni.gov/files/documents/ICA_2017_01.pdf

[4] Greenberg, A. (2017, June 02). NSA Director Confirms That Russia Really Did Hack the French Election. Retrieved February 06, 2018, from https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/

[5] Giles, K. (2016, November). Handbook of Russian Information Warfare. https://krypt3ia.files.wordpress.com/2016/12/fm_9.pdf

[6] Cohen, Z. (2018, January 31). CIA director Pompeo met top Russian spies. Retrieved February 06, 2018, from https://www.cnn.com/2018/01/30/politics/cia-director-pompeo-russia-spies/index.html

infrastructure architecture. Some states have highly automated infrastructure while others continue to employ paper ballot systems. In the latter case, digital interactions still exist with web interfaces for voter registration and election day voter verification along with the use of digital ballot counting machines which scan paper ballot and store results.

Based on my conversations with government representatives from geographically dispersed states, the integrity and quality of election infrastructure has improved since 2016. States have reviewed the exposure and configuration of their end-to-end voting system, and known areas of technical and procedural weaknesses have been remediated.[7] Nonetheless, the ***threat to electoral processes remains high***. For one, it is difficult to identify and nullify disinformation campaigns that are portrayed as news coverage.

Recommendations to Counter Russian Influence in our Election Process.

America has been and will continue to be involved in a campaign of continuous engagement and pressure from the Kremlin to weaken US and allied critical infrastructure and democratic processes. To counter, we need a "whole of America" campaign approach aimed directly at preventing Russian or any other foreign government interference. This campaign must be led by a National Security Council (NSC)-sanctioned task force (not too dissimilar to the National Counter-Terrorism Center) with membership from empowered government agencies and industry representatives. One line of operation in this campaign is countering Russian interference to influence our electoral process.

This standing national task force needs to have two synchronized components – one focused on continuous strengthening of the states' election infrastructure as well as "hardening" American citizens to Russian media and other cyber-enabled influence operations. Importantly, these activities should include a partnership with industry to regularly red team state election infrastructure; share relevant intel with state election and cybersecurity officials; bar Russian or other foreign online election material (just as we bar foreign election contributions;) continuously identify fake and harmful messages; and quickly disseminate the truth about USG actions. As a starting point, this USG-industry partnership could build off the actions already underway to counter on-line terrorist propaganda.[8]

The second component of this task force should be focused to directly impose cost on the Russian Federation, including activities ranging from cyber-enabled social media operations and botnet disruptions to sanctions and other enforcement actions.

---

[7] Department of Homeland Security. (2018, January). National Cyber Incident Coordination Center. https://www.dhs.gov/national-cybersecurity-and-communications-integration-center

[8] Robertson, A. (2017, June 26). Facebook, Microsoft, Twitter, and YouTube launch anti-terrorism partnership. Retrieved February 06, 2018, from https://www.theverge.com/2017/6/26/15875102/facebook-microsoft-twitter-youtube-global-internet-forum-counter-terrorism

Importantly, these cost imposition measures, when and where possible, need to be multilateral in nature, involving other allied nations and coordinated with appropriate private sector organizations.[9] The formation of an International Cyber Stability Board (ICSB) of allied nations and industry partners could support rapid coordination and enforcement of actions across Internet infrastructure. The NSC staff should lead in the development of the ICSB.

The two components should be supported by an integrated fusion center that enables continuous situational awareness and engagement through human capital intelligence, intelligence at large, law enforcement, and active defense actions. Although centrally planned, execution of action must be decentralized to support persistent and agile engagement against Russian "trolls," bots, and other surrogates of the Russian Government.

To enable this type of organization and ensure its success will require both cultural and legislative changes. The President needs to rally the US government and US industry. Infrastructure resilience and countermeasures need to be part of the President's "call to action" this year. Additionally, we need to leverage the best US organizational core competencies to include the following:

- Defense for campaign planning and exercise,
- US Intelligence Agencies and industry for rapid intelligence generation and fusion,
- Webscale companies for rapid identification of disinformation campaigns and response,
- Congress for potentially changing laws like the Computer Fraud and Abuse Act (CFAA) and enabling government and industry to work together to actively defend this nation.[10]

On the international front, it is critical to align our efforts with our allies and identify appropriate "red lines" for actions. For example, these would include attempts to hack or disrupt our electrical grid and voting machines. [11]

---

[9] Frank Kramer, Bob Butler, and Catherine Lotrionte. (2017, November 06). Raising the Drawbridge with an "International Cyber Stability Board". Retrieved February 06, 2018, from https://www.thecipherbrief.com/raising-drawbridge-international-cyber-stability-board

[10] McCain, U. S. (2017, October). Press Releases. Retrieved February 06, 2018, from https://www.mccain.senate.gov/public/index.cfm/2017/10/mccain-klobuchar-warner-introduce-legislation-to-protect-integrity-of-u-s-elections-provide-transparency-of-political-ads-on-digital-platforms . https://tomgraves.house.gov/uploadedfiles/discussion_draft_active_cyber_defense_certainty_act_2.0_rep._tom_graves_ga-14.pdf.; https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/CCHS-ActiveDefenseReportFINAL.pdf.and https://www.mccain.senate.gov/public/index.cfm/2017/10/mccain-klobuchar-warner-introduce-legislation-to-protect-integrity-of-u-s-elections-provide-transparency-of-political-ads-on-digital-platforms

[11] Miller, J. (2018, January). Navigating Dangerous Pathways. Retrieved February 06, 2018, from https://www.cnas.org/publications/reports/navigating-dangerous-pathways?utm_medium=email&utm_campaign=Project Pathways 3 Report Release&utm_content=Project Pathways 3 Report Release%2BCID_2bd61d40546a491ed2980e0568645014&utm_source=Campaign

Proposals for the Cyber Subcommittee and SASC.

To “jump start” the stand-up of an NSC-sponsored national task force, the SASC should coordinate with the Secretary of Defense in immediately establishing a joint interagency task force to begin and accelerate counter-Russian influence campaign planning. Key private sector elements from the Defense Industrial Base and webscale companies should be included as needed. Also, appropriate working arrangements with state and local officials through the Department of Homeland Security (DHS) and the National Guard Bureau (NGB) should be created. The SASC through its oversight jurisdiction should then monitor the progress of the task force.

To further support the stand-up of the new national task force for countering Russian or other foreign government influence, I recommend the SASC direct the NGB, in conjunction with US Cyber Command (CYBERCOM), to inventory and certify all cyber capable National Guard assets that could augment state resiliency and federal efforts. Working with other committees, the SASC should then develop a statute to grow ten NGB “cross-state mutual assistance” teams as certified active defense teams to work alongside Federal Emergency Management Agency (FEMA) regional leads, other government and industry partners at the state and federal level.

The SASC should direct the Defense Leadership Team to develop Defense-Defense Industrial Base Courses of Action (COA) to support the new national task force, and to provide in a closed session a summary of these COAs along with new resources and authority requests to the Committee. Related to this point, the SASC should work with the DoD and other Committees to update all statutes for enabling Defense counter-influence actions at home and abroad.

To deter further adversary action, we must harden our critical infrastructure. This includes the election infrastructure, but also all infrastructure which ensures national security, public safety and democratic processes. From a defense standpoint, this starts with the resilience of our nuclear strike capabilities, non-nuclear capabilities such as conventional strike, missile defense and offensive cyber. Specific recommendations are included in the 2017 DSB report on Cyber Deterrence.[12] The SASC should continue to act to operationalize these recommendations as part of developing the next National Defense Authorization Act.

Finally, the Committee should set up its own campaign of “table top” exercises that would help members to better understand different adversary scenarios which could involve

---

Monitor&utm_term=Navigating Dangerous Pathways A Pragmatic Approach to US-Russian Relations and Strategic Stability

[12] Defense Science Board. (2017, February). Task Force on Cyber Deterrence. https://www.acq.osd.mil/dsb/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf.

defense capabilities and highlight the need to the Committee for other Congressional actions in countering Russian influence.

Thank you again for the opportunity to share these thoughts. I stand ready to help the Committee as we seek to better protect and grow our nation.