Senate Select Committee on Intelligence

"Responding to Russian Interference in the 2016 U.S. Presidential Election"

Written Testimony of:

Michael Daniel

Former Special Assistant to the President and Cybersecurity Coordinator for President Barrack Obama

June 20, 2018, 9:30 a.m.

Hart Senate Office Building – Room 216

U.S. Response to Russian Interference in the 2016 U.S. Presidential Elections

Chairman Burr, Vice-chairman Warner, other Members of the Committee:

Thank you for this opportunity to testify this morning on the issue of the U.S. response to Russian interference in the 2016 Presidential elections. I appreciate the ongoing work the committee is doing to investigate Russian interference in the elections, to apprise the American people of what occurred, and to ensure that we are taking these matters seriously as a Nation and responding appropriately.

During President Obama's administration, I served from June 2012 to January 2017 as the Special Assistant to the President and Cybersecurity Coordinator on the National Security Council staff. In that capacity, among other things, I oversaw the development of cybersecurity-related policy, coordinated our responses to significant cyber threats and incidents, and facilitated the development of inter-agency plans to disrupt our adversaries' cyber activities.

Although the topic of this hearing may appear to some to be purely retrospective, understanding the U.S. response to what happened during the elections in 2016, and what we did about it, is critical to better protecting future elections and the Nation more generally.

Background

This Committee is currently conducting an extensive investigation into the events in 2016 and the U.S. response to those events. Therefore, I will limit my remarks in this regard and merely highlight a few important points from my perspective. My remarks are limited with respect to certain aspects of the U.S. government response, and do not address the response of the various States, the campaigns, or the private sector more generally to the events.

Going into late spring of 2016, as the Presidential election got into full swing, we fully expected Russian cyber-based espionage activities against the major political campaigns – it had happened in previous election cycles and our operating assumption was that the Russians would target the campaigns for intelligence collection. However, by late June / early July 2016, as information from the Democratic National Committee began to be released, and as a few States began to report intrusions into certain parts of their electoral infrastructure, we realized that the Russians were doing something more than merely collecting intelligence. They were carrying out operations aimed at least at influencing the election and potentially even disrupting it.

This prompted us to take action, including with respect to the following two lines of effort:

- Improve the cybersecurity of the electoral infrastructure; and
- Impose costs on the Russians for their current actions and deter escalation or future actions.

I will now turn to each of these lines of effort in more detail.

Improving the Cybersecurity of the Electoral Infrastructure

The goal for this line of effort was to make it more difficult for the Russians to disrupt or interfere with the actual voting process, while maintaining Americans' confidence in the electoral system. Although many cybersecurity experts have focused on cybersecurity issues surrounding electronic voting machines, we quickly determined that the voting machines, while vulnerable, were not the most vulnerable part of the infrastructure. We also quickly determined that Russia's goal was probably not to use cyber means

to surreptitiously change the outcome of the election by changing votes. In order to achieve that goal, the Russians would have had to have selected the precincts that were going to be close several months in advance, gained undetected access to the voting machines, installed malware that flipped just enough votes to change the outcome but not so many as to be detected, and then remain undetected through any post-election auditing. We did not believe carrying out such an operation was feasible.

Instead, we realized that a far more practical goal would be to use cyber means to undermine confidence in the election; once the potential scenarios included more than vote flipping, the potential for malicious activity expanded considerably. Widening the aperture to include the entire electoral process from beginning to end revealed segments that would be much more vulnerable to remote cyber operations. That turned out to be the points at which the electoral infrastructure touches the public internet: voter registration databases; vote tabulation reporting; and media reporting on election day.

Once we had concluded what were more likely targets and vectors for Russian activity, the Administration used the regular, NSC-led interagency process to develop and implement activities to address the threat. Since States and local governments run the election process in the U.S., by necessity our efforts became focused on providing assistance to States and localities. The Department of Homeland Security spearheaded those efforts for the Administration. These actions focused on determining what assistance we could provide States and local governments in the near term and alerting States and local governments to the potential threat.

By October, we began to shift our focus to preparing for election day and being able to respond quickly to any disruption that could occur. Again, we worked the regular interagency process to develop an election day response plan, focused on being able to rapidly identify a significant incident, having the assets ready to support a State or local government in responding to that incident, and having a communications plan ready if such an event occurred. Fortunately, we did not detect or discover any significant malicious cyber activity on election day.

Imposing Costs on the Russians for Their Current Actions and Deter Escalation or Future Actions

Although our defensive activities played out in a more public fashion, our second line of effort focused on responding to the Russian activity, imposing costs on them, and deterring further escalation or future activity.

This line of effort played out from the end of July 2016 until the Administration left office in January 2017. From my perspective, the core of this effort involved using the normal, NSC-led interagency process to develop a suite of options to respond to the Russian activity. Along with other complementary efforts coordinated by other directorates in the NSC, a key body that worked on this effort was the restricted Cyber Response Group, which had representatives from all the Federal agencies that could have a role in developing and implementing response options.

The specific options we developed were and remain to my knowledge classified, other than those that by necessity became public. However, broadly speaking, the options included diplomatic, intelligence, law enforcement, economic, and cyber activities. Within these broad categories, the NSC solicited input from the agencies to identify a range of actions, from low-risk, lower-impact to high-risk, higher impact, that decision-makers could consider. My responsibility in this process was to ensure that decision-makers, up to and including the President, had a full range of options to consider, along with the pros and cons of

each. Not all of the options we laid out were taken, but that outcome is a normal, expected part of the policy development process.

Due to significant concerns about the potential for escalation between Russia and the U.S., the overall geopolitical situation, and the desire not to do the Russian's work for them by undermining Americans' confidence in the electoral process, senior decision-makers proceeded carefully and judiciously. Eventually, senior decision-makers opted to proceed with several actions that were widely reported in the media.

Lessons for the Future

I commend the Committee's March 2018 recommendations to improve election infrastructure. As I mentioned at the beginning, the point of reviewing the activities from 2016 from my perspective is to help us learn how to better protect the Nation in the future and to respond to such events should they occur in an appropriate and meaningful manner. Now that the Russians have proven that cyber means can be used to engage in election interference in the United States, we should expect that they will continue to engage in such activities and that other actors will follow their lead, including non-nation state actors. Therefore, I recommend that:

- We continue to invest in improving the cybersecurity of our electoral infrastructure in its entirety, including, but not limited to, voter registration databases, pollbooks, voting machines, vote tabulation, and vote reporting. Since it is an important principle of Federalism that State and local governments maintain their traditional control over the electoral process, the Federal government should increase its support to the States and local governments in the effort to secure the critical electoral infrastructure. Support must take several forms: financial, technical, training, improved information sharing, and other activities. DHS has laid a good foundation in this regard and it must enhance its work along with the rest of the Federal government. The integrity of such systems is essential to the confidence of the electorate in the electoral process. Our system of governance depends on our success; we should approach the cybersecurity of our electoral infrastructure with the same seriousness that we treat the security of the electrical grid, the telecommunications network, or other critical infrastructure sectors.

- We should increase our resilience to information operations through a variety of means. We should support programs that are analyzing such operations and developing measures to properly manage and deter them.

- Internationally, we should continue to promote the principle that it is not acceptable to surreptitiously interfere in another nation's electoral process through cyber means.

- The U.S. should work with other allied governments to identify, expose, and respond to Russian and other activity in this area.