S. HRG. 115–579

OPEN HEARING: POLICY RESPONSE TO THE RUSSIAN INTERFERENCE IN THE 2016 U.S. ELECTIONS

HEARING

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE

OF THE

UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

WEDNESDAY, JUNE 20, 2018

Printed for the use of the Select Committee on Intelligence

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
30–501 PDF WASHINGTON : 2019

SELECT COMMITTEE ON INTELLIGENCE

[Established by S. Res. 400, 94th Cong., 2d Sess.]

RICHARD BURR, North Carolina, *Chairman*
MARK R. WARNER, Virginia, *Vice Chairman*

JAMES E. RISCH, Idaho
MARCO RUBIO, Florida
SUSAN COLLINS, Maine
ROY BLUNT, Missouri
JAMES LANKFORD, Oklahoma
TOM COTTON, Arkansas
JOHN CORNYN, Texas

DIANNE FEINSTEIN, California
RON WYDEN, Oregon
MARTIN HEINRICH, New Mexico
ANGUS KING, Maine
JOE MANCHIN III, West Virginia
KAMALA HARRIS, California

MITCH MCCONNELL, Kentucky, *Ex Officio*
CHUCK SCHUMER, New York, *Ex Officio*
JAMES INHOFE, Oklahoma, *Ex Officio*
JACK REED, Rhode Island, *Ex Officio*

CHRIS JOYNER, *Staff Director*
MICHAEL CASEY, *Minority Staff Director*
KELSEY STROUD BAILEY, *Chief Clerk*

CONTENTS

JUNE 20, 2018

OPENING STATEMENTS

WITNESSES

OPEN HEARING: POLICY RESPONSE TO THE RUSSIAN INTERFERENCE IN THE 2016 U.S. ELECTIONS

WEDNESDAY, JUNE 20, 2018

U.S. SENATE,
SELECT COMMITTEE ON INTELLIGENCE,
Washington, DC.

The Committee met, pursuant to notice, at 11:05 a.m., in Room SH–216, Hart Senate Office Building, Hon. Richard Burr (Chairman of the Committee) presiding.

Present: Senators Burr, Warner, Risch, Rubio, Collins, Lankford, Feinstein, Wyden, Heinrich, King, Manchin, and Harris.

OPENING STATEMENT OF HON. RICHARD BURR, CHAIRMAN, A U.S. SENATOR FROM NORTH CAROLINA

Chairman BURR. I'd like to not only welcome our witnesses, I'd like to apologize to our witnesses for the hour delay. Unfortunately, neither the Vice Chairman nor I have any control on the floor schedule for votes. And we had a couple snuck in on us, and it may not be the last time today. But I'll do everything I can to navigate us through this open session, and then the closed session, as quickly as we possibly can.

I'd like to welcome Ambassador Victoria Nuland, former Assistant Secretary of State for European and Eurasian Affairs, and Michael Daniel, former special assistant to the President and cybersecurity coordinator at the White House. I thank both of you for making the time for us today.

Today's hearing is the next step in our efforts to fully investigate and explain how Russia interfered in the 2016 U.S. elections, how we reacted, and more importantly, what we've learned. Earlier this year, the committee moved quickly to discuss with the American people the threat to the voting system, and we welcomed legislation that sent urgent assistance to the states.

We thoroughly reviewed the Intelligence Community Assessment on Russia Interference produced in November of 2017, and all the sources that underpin it, and held a closed hearing with the agency directors responsible for that product. The committee is ready to finalize our assessment of the Obama Administration's response to the Russian interference. And today's hearing will be the first of a series of several capstone events. We have invited Ambassador Rice and her deputies to join us in a few weeks. We've also invited former leaders from the FBI and the Department of Justice to testify again in July.

Today, Ambassador Nuland and Mr. Daniel have joined us for this important hearing. You sat on different sides of the same policy debate. Mr. Daniel sat atop the government's cyber apparatus, seeing indicators of Russian hacking activity unfold both here in the U.S., as well as in countries like Germany and Ukraine. Meanwhile, Ambassador Nuland sat at the State Department watching Moscow aggressively pursue its interest in Ukraine, Syria, and elsewhere.

Russia's interests and methods were a carryover from the old Soviet Union that we knew, but with a new twist. The Kremlin began to use social media, hack and leak operations, and quasi-governmental agencies to discredit enemies and to weaken adversaries. Ambassador, you and your team at State were well-versed in the Russian toolkit. And you understand Putin's political will to use those tools. In effect, to use the metaphor, each of our witnesses will be touching a different part of the same elephant. Today, we'd like to know when the bigger picture emerged and how policymakers responded. Did they seek to deter Russia from undermining our democratic institutions? Did they take action? If not, what held them back?

We as a committee have benefited from the insight of many from the Obama Administration. I'd like to thank them publicly today on behalf of the committee for coming voluntarily to talk to our staff and for their candid interviews and testimony. They consistently said that they were operating in the summer and fall of 2016 without a playbook. This was a new threat with an undefined set of rules. It seemed they struggled to balance competing priorities.

They wanted to warn the Russians to stop interfering, but avoid the appearance that the White House was putting a thumb on the political scale during an election year. They wanted to warn the public about Russia's efforts, but not carry Russia's water for them. They wanted the states to rapidly secure voting systems, but not alienate State election officials or undermine public confidence. We can look back with the benefit of time and distance and talk about what could have been done. As we do so, we must also look forward a few short months to 2018 elections and forward a few more short years to the 2020 elections. More broadly, we now realize that the goal of the Russian campaign was to fracture our society and cause general discord using all the tools that our technologically connected society offers. Our focus should be to prevent, to deter, and to harden both our elections and our society for the future.

Again, I want to thank both of you for being here, and I turn to the Vice Chairman for any comments he might have.

OPENING STATEMENT OF HON. MARK R. WARNER, VICE CHAIRMAN, A U.S. SENATOR FROM VIRGINIA

Vice Chairman WARNER. Thank you, Mr. Chairman, and again, welcome to our witnesses. We appreciate your recapping of how much good work this committee has done on a bipartisan basis and we look forward to continuing that work.

At the January 2017 assessment, the Intelligence Community assessment correctly judged the Russian efforts to influence the 2016 presidential elections, quote, "demonstrated a significant escalation

in directness, level of activity, and scope of effort compared to previous operations."

As we examine the policy questions faced by the Obama Administration and this Congress during the 2016 campaign, it's evident that, in many ways, we were caught flat-footed at the outset and our collective response was inadequate to meet Russia's escalation. At the end of the day, it's hard to see the Russian influence campaign as anything but a success for Vladimir Putin. Today is about learning from these past missteps, because we all know on a going-forward basis we have to do better.

Now, let me stipulate upfront, there are far too many Monday morning quarterbacks around these days. However, looking back, we should not have been surprised about how far Russia was willing to go. The red flashing signals were all over there. Allies in the Baltics and Eastern Europe had long experienced aggressive Russian cyberattacks and disinformation campaigns. Ukraine in many ways a testbed for many of these tactics we saw in our own elections. Ambassador Nuland herself was a firsthand witness to the weaponization of leaks in 2014 when her private conversations were intercepted and released.

Separately, I believe we profoundly missed the mark in tracking and responding to influence operations on our social media platforms. Russian-backed operatives were wreaking havoc in spreading disinformation across Facebook, Twitter, YouTube, and other platforms. We, both at the governmental level and at the company level, were unprepared to address those attacks. Even to this day, over a year-and-a-half later, I have significant concerns that we are still behind the eight ball in effectively combating these efforts.

Despite perhaps being too slow to see the threat initially, it's not true that the Obama Administration stood idly by and did nothing. Numerous steps were taken, both public and classified, to try to better understand and defend against the Russian activities and objectives.

Director Brennan issued a direct warning to his Russian counterpart. The Administration engaged the cyber hotline with Russia for the first time ever to warn the Kremlin against further action. DHS attempted a series of engagements with State election officials. President Obama himself took the warning directly to President Putin at the September G20 in China.

Finally, in what should have been a much more significant event, the Administration attempted a fairly unprecedented public statement attributing recent hacks and leaks to Russia. But, as we all know, that joint DNI–DHS statement was quickly overshadowed, as the media diverted much of its attention to the Access Hollywood video and the WikiLeaks release of Podesta emails. It remains unclear if the WikiLeaks release was actually timed to undermine the joint statement. It is perhaps impossible to know whether these steps the Administration took ultimately deterred additional and even more aggressive action by the Russians. However, with the benefit of hindsight, it is evident that we could have done more to push back in the heat of the campaign.

But the Administration was not solely responsible here. Two factors made an already difficult policy challenge much more problematic. First, as we all know and have heard in testimony, the White

House was concerned that engaging more publicly would be seen as trying to put its thumb on the scale of the election. No one did more to fan the flames of what he termed, quote, "a rigged election," than Candidate Trump. The Trump campaign and its allies cravenly painted any attempt to call out Russia for its attacks as a political effort to help Clinton and to steal an election. Those irresponsible statements further reinforced the dangers of speaking publicly by the Obama Administration.

In addition, any fair scrutiny of policy decisions during the campaign needs to also address congressional inaction. Congress, all of us, need to look ourselves in the mirror and see whether we could have done better, in particular the lack of a bipartisan congressional warning to Russia. And the weeks of delay it took to even get a letter out to State election officials now looks like a failure to put our democracy ahead of politics.

Again, I appreciate the witnesses' willingness to come forward and relive 2016. But as the Chairman mentioned, 2018 is already upon us, and this time there's no excuses for missing the threat. We've heard unanimously from the Intelligence Community that Russia continues to try and undermine our democracy. They are attacking us and our allies on a regular basis even today. If we allow this to happen again, if we don't do all we can in a united front to protect our democracy, then shame on all of us. I hope to hear from our witnesses today some thoughts on where we go from here. The threat, as we all know, is real. The time to act is urgent.

And, again, thank you, Mr. Chairman. I am eager to hear from our witnesses.

Chairman BURR. I thank the Vice Chairman. And before I turn to the ambassador for opening remarks from both her and Mr. Daniel, let me say that we don't have a full complement today, not because they're not interested, but because we're in competition with a Rules Committee hearing on elections, the first one, a meeting at the White House, and numerous other things. So, I apologize to you.

I also say this to members. If, in fact, our delayed start causes a conflict in your schedules, if anybody would just let me know, I'll try to expedite recognition of you if that helps alleviate anybody's problems with schedules.

With that, Ambassador Nuland, the floor is yours.

STATEMENT OF AMBASSADOR VICTORIA NULAND, FORMER ASSISTANT SECRETARY OF STATE FOR EUROPEAN AND EURASIAN AFFAIRS

Ambassador NULAND. Thank you, Chairman Burr. Thank you, Vice Chairman Warner, and members of this committee. I appreciate the opportunity to appear before you today to discuss the policy response to Russian malign influence in U.S. politics.

As a citizen, as a 32-year veteran of the U.S. diplomatic service, and as a regular target of Russian active measures, I want to commend the leadership of this committee and all its members for your thoroughness and your integrity in pursuing your investigation into Russia's involvement in the 2016 elections. I especially commend the bipartisan spirit with which you've done your work, which sets a powerful example in this country.

When I testified before you in classified session last summer, I put forward a number of recommendations regarding how the U.S. government could organize itself and work with the private sector to expose, deter, and defeat this threat to our national security and our democracy. Rather than going backwards into history, I'm going to focus my remarks on what we can do. Since then, many of the ideas that I put forward a year ago have been advocated publicly by others, including the Atlantic Council, the Alliance for Securing Democracy at the German Marshall Fund, the Belfer Center at Harvard, and in the minority report of the Senate Foreign Relations Committee.

Russia, meanwhile, has not stopped its efforts to divide our society and use our open system against us to spread false narratives. There's every reason to believe the Kremlin will again target our elections this fall and in 2020. Our major technology companies whose platforms they exploit have all taken some countermeasures but not enough. Other countries and malign actors are now adopting and improving on Russia's methodology. China, for example, now runs disinformation campaigns and influence operations in Taiwan, Australia, and other neighboring countries, and is working to acquire information technology assets and data sets across Asia, Europe, and the United States.

While the Trump Administration has taken some important sanction steps to punish Russia for past actions, strengthen Cyber Command, and harden our electoral infrastructure, it has not launched the kind of presidentially led, whole-of-government effort that's needed to protect our democracy and security from malign state actors who are intent on weaponizing information and the internet. We must urgently put the policies, the funding, and the systems in place to speed our ability to identify malicious activity, call it out, and take countermeasures; to sharpen our deterrence toolbox so our adversaries know that they will face crippling consequences; to improve regulatory and legal standards to close the space that bad actors exploit; and to lead a global campaign with allies and partners to expose and defeat this threat together.

Today, I put forward five steps to protect our democracy, improve deterrence, and blunt this new weapon in the hands of any of our adversaries.

First, on the President's direction and with congressional support, the Trump Administration could immediately establish a multiagency fusion center modeled on the National Counterterrorism Center, but smaller in size, to pull together all of the information and resources of our government, classified and open source, to identify, expose, and respond to state-sponsored efforts to undermine American democracy through disinformation, cyberattack, and abuse of the internet. All the relevant intelligence and national security agencies should be represented, as should the Treasury Department, the Justice Department, and other agencies who have knowledge about how dirty money and criminality often fuel these activities, and with the tools to help with deterrence.

As this committee knows, much of our problem in responding strongly and quickly enough in 2016 stemmed from insufficient integration of information and policy options among government

agencies, which led to delays in attribution, slow response times, and debates about the right overt and covert tools to apply.

Second, the White House could establish and host a standing U.S. public-private commission to combat internet abuse and disinformation, inviting participation by all the major U.S. technology companies with vulnerabilities and equities, the academic community, and the private forensic experts in this space. The commission would be charged with developing technical, regulatory, and legal recommendations to protect the integrity of the internet user experience and blunt the ability of malign state actors to suborn democracy through the internet. Done right, this commission could provide a protected space for private sector stakeholders to share information and experience with each other and with the government, and to collaborate on responses and build campaigns of common action.

Third, and flowing from the second recommendation, the U.S. government has to better advise, advocate for, and protect U.S. companies when they do take bold and commercially costly action to stand up to state sponsors of malign influence at home and abroad. In weighing when and how to act, our companies often face the threat of retaliation against their staffs and their platforms, stiff fines, or even the closure of their operations in countries that practice the dark arts of cyber and internet abuse. Our companies need a place at State, at Commerce, in this new commission to seek advice, pre-coordination, and rapid support from the U.S. government when they take decisions to resist foreign government pressure, when they close malign accounts, and when they expose anti-democratic tactics.

Fourth, the President could appoint an international coordinator to launch and lead a campaign to multilateralize our efforts in this space with America's closest allies and partners in line with the President's national security strategy, which highlights the dangers to the U.S. and our allies from this threat.

Fifth and finally, the Administration could put forward, and the Congress could support, a significant budget increase to strengthen U.S. capabilities in this area. The funding should be targeted to appropriate U.S. agencies to strengthen their forensic capability, shorten attribution timelines, improve the government's ability to expose and debunk truly fake news in real time, broaden public outreach to and education of the American people about these threats, and strengthen our stable of national experts in the field.

In the coming year, the Center for a New American Security, which I lead, plans to join the community of think tanks working on these issues. We will put special emphasis on pulling together the best minds in industry, academia, and government to craft full-spectrum deterrence strategies against malign state actors in the cyber realm. This work can't replace the responsibility of Federal and State government, but hope it will help inform wise choices.

Again, thank you for inviting me to appear before you today.

[The prepared statement of Ambassador Nuland follows:]

Statement for the Record
Senate Select Committee on Intelligence

Victoria Nuland
CEO, Center for a New American Security
June 20, 2018

Chairman Burr, Ranking Member Warner, members of the committee: Thank you for the opportunity to appear before you today to discuss the policy response to Russian malign influence in U.S. politics. As a citizen, as 32-year veteran of the U.S. diplomatic service, and as a regular target of Russia's "active measures," I want to commend the leadership of this committee and all its members for your thoroughness and integrity in pursuing your investigation into Russia's involvement in the 2016 elections. I especially commend the bipartisan spirit with which you have done your work, which sets a powerful example for the country.

I testified before this committee in classified session last summer, and shared my experience as Assistant Secretary of State for European and Eurasian Affairs between 2013 and early 2017 in tracking Russian government disinformation and participating in the formation of U.S. government policy responses. I won't repeat most of that in this open session, except to say that I urged stronger counter-measures earlier in 2016 to raise the costs on Russia for its action and thereby try to deter greater harm. For a variety of reasons, President Obama chose to wait until after the 2016 presidential election to launch a full interagency investigation into Russian actions and to respond. That investigation and response were time limited by President Obama's remaining tenure in office. Most of us involved in the process – both the career staff and the political appointees -- hoped and expected that the Trump Administration would deepen and accelerate the work.

When I testified last summer, I put forward a number of recommendations regarding how the U.S. government could organize itself and work with the private sector, to expose, deter and defeat this threat to our national security and our democracy. The good news is that many of these ideas have been advocated publicly by others in the intervening year, including the Atlantic Council, the Alliance for Securing Democracy at the German Marshall Fund, Harvard's Belfer Center, and your fellow Senators in last winter's minority report of the Foreign Relations Committee. The bad news is that Russia has not stopped its efforts to divide our society and use our open system against us to spread false narratives. There is every reason to believe the Kremlin will again target our elections this fall and in 2020. Our major technology companies, whose platforms they exploit, have all taken some counter-measures but not enough. And worse, other countries and malign actors are now adapting and improving on Russia's methodology, notably including China which now runs disinformation campaigns and influence operations in Taiwan, Australia and other neighboring countries and is working to acquire information technology assets and data sets across Asia, Europe and the United States.

While the Trump Administration has taken some important sanctions steps to punish Russia for past actions and to harden our electoral infrastructure, it has not launched the kind of Presidentially-led, whole-of-government effort that is needed to protect our democracy and

security from malign state actors who are intent on weaponizing information and the internet. Every member of the President's national security cabinet and his own National Security Strategy identify the problem as one of the most dangerous for our country today. All the President's senior advisors stress that this is not about relitigating the past, it is about protecting the American people's free, democratic choice in the future.

Policy Recommendations

Going forward, I offer the following five steps, which could be taken immediately to protect our democracy and blunt this new weapon in the hands of our adversaries:

First, on the President's direction and with Congressional support, the Trump Administration could immediately establish a **multi-agency Fusion Center**, modeled on the National Counter Terrorism Center but smaller in size, to pull together all the information and resources of our government to identify, expose and respond to state-sponsored efforts to undermine American democracy through disinformation, cyberattack, and abuse of the internet. All the relevant intelligence and national security agencies should be represented, as should the Treasury Department, the Justice Department and other agencies with knowledge about how dirty money and criminality often fuel these activities, and with tools to help with deterrence.

As this Committee knows, much of our problem in responding strongly and quickly enough in 2016 stemmed from insufficient integration of information among government agencies, which led to delays in attribution, slow response times, and debates about the right overt and covert tools to use.

Second, the White House could establish and host a **standing U.S. public-private commission** to combat internet abuse and disinformation, inviting participation by all the major U.S. technology companies with vulnerabilities and equities, the academic community, and private sector forensic experts in the space. The commission would be charged with developing technical, regulatory and legal recommendations to protect the integrity of the internet user experience and to blunt the ability of malign state actors to suborn democracy through the internet. Its executive branch members could also be members of the Fusion Center, and key members of Congress and committee staffs could be regular participants to inform future legislation and regulatory efforts.

To date, U.S. government outreach to the major companies has been conducted largely one-to-one, and primarily among cyber security experts, without appropriate crosswalk to the policy and strategy communities in either government or the private sector. Done right, the Commission could provide a protected space for private sector stakeholders to share information and experience with each other and the government, to collaborate on responses and build campaigns of common action.

Third, and flowing from the second recommendation, the **U.S. government must better advise, advocate for and protect U.S. companies** when they do take bold and commercially costly action to stand up to state sponsors of malign influence at home and abroad. Whether at the State Department, the Department of Commerce or as a function of the public-private

commission that I've recommended, our companies need a place to seek advice, pre-coordination and rapid support from USG when they take decisions to resist to foreign government pressure, close malign accounts, and expose anti-democratic tactics. In weighing when and how to act, our companies often face the threat of retaliation against staff and platforms, stiff fines, and/or closure of their operations in countries that practice the dark arts of cyber and internet abuse. The mitigation and deterrence steps they need to take also cut into their bottom line. Just as we do in the field of export control, the government must make it a national security priority to work with, advocate for and defend our companies when they want to do the right thing. At the same time, the executive branch and Congress should publicly call to account those companies that choose profit over U.S. national security.

Fourth, the President could appoint an **International Coordinator** to launch and lead a campaign to multilaterize all our efforts in this space with America's closest Allies and partners. This individual would be responsible for pulling together all the current disparate efforts across government to share information, best practices, and technological and policy solutions bilaterally with Allies, and with the UN, NATO and the EU, into a coherent whole, with targeted outcomes that the President and his Cabinet could advocate consistently in all their international engagements. A visible U.S. international leadership role in this field would also fall squarely into line with the President's National Security Strategy, which highlights the dangers to the U.S., our Allies and friends.

Fifth and finally, the Administration could put forward and the Congress could support a **significant budget increase** to strengthen US capabilities in this area. This could include funding to stand up the fusion cell, the public-private commission, and the international coordinator's office. The additional funding could also be targeted to the appropriate USG agencies to strengthen their forensic capabilities, shorten attribution timelines, improve the government's ability to expose and debunk truly fake news in real time, broaden public outreach to and education of the American people about these threats, and strength our stable of national experts in the field.

In the coming year, the Center for a New American Security, which I lead, plans to join the community of think tanks working on these issues. We will put special emphasis on pulling together the best minds in industry, academia and government to craft full-spectrum deterrence strategies against malign state actors in the cyber realm. This work cannot replace the responsibility of federal and state government but we hope it will help inform wise choices going forward.

Again, thank you for inviting me to appear before you today.

Chairman BURR. Thank you, Ambassador. Mr. Daniel, the floor is yours.

STATEMENT OF J. MICHAEL DANIEL, FORMER WHITE HOUSE CYBERSECURITY COORDINATOR AND SPECIAL ASSISTANT TO PRESIDENT BARACK OBAMA

Mr. DANIEL. Thank you, Mr. Chairman. Thank you, Mr. Vice Chairman and other distinguished committee members, for the opportunity to come and testify this morning on the issue of Russian interference in the 2016 election cycle.

Although ostensibly retrospective, understanding what happened in 2016 is really critical to better protecting ourselves in future elections and in future activities that we do. And given that this committee has extensively reported on this topic and those findings I very strongly support, I'm going to keep my opening remarks at a very high level this morning.

I think going into the late spring of 2016, we fully expected Russian cyber-based espionage activities against our major political campaigns. It had happened in previous election cycles, and we assumed that it would happen again in 2016. But by late June/early July, as stolen information began to show up in public and as states began reporting suspicious activity against some of their electoral infrastructure, we began to realize that the Russians were doing something more than just collecting intelligence.

They were carrying out operations aimed at the very least at influencing our election and potentially even disrupting it. But the true scope, scale, and breadth of this activity remained unclear and actually developed over time, and in fact this committee has contributed a lot to our understanding of what was actually going on. But within the U.S. government, we really developed two lines of effort in order to respond to this activity. One was very public and outward-facing, and it was designed to improve the security of our electoral infrastructure across the board. The second was more behind the scenes, and it was designed to respond to the actions that the Russians were carrying out, to impose costs on them and to deter future escalation or future actions.

So, the first line of effort, better protecting our electoral infrastructure, was really focused on the State and local electoral systems. But the first step was actually deciding what it was that we were trying to protect. And given that most of us at the Federal level didn't have a lot of experience with how elections actually worked as a mechanical thing at the State and local level, we all got a crash course in how elections actually operate down at the State and local level.

And we very quickly realized as part of that process that the voting machines, while vulnerable, were not the most likely vector for any Russian activity, nor was changing the outcome of the election the most likely goal. Achieving that goal was simply not feasible, as you've actually noted in some of your reports. Instead, undermining confidence in the electoral process and disrupting it were the more likely goals. So, we then began to look for the points where the Russians could most easily accomplish that goal, and that turned out to be the points at which the electoral infrastruc-

ture touched the public internet: voter registration databases, voter tabulation reporting, and media reporting on election night.

And since State and local governments run the election process in the U.S., by necessity our efforts then became focused on providing assistance to the states. The Department of Homeland Security spearheaded those efforts for the Administration backed up by the Department of Justice and the FBI. Over time, we also then began to shift our focus to preparing for Election Day and being able to respond quickly to any disruption that might have occurred. Fortunately, by the time we got around to Election Day, none of what we feared actually materialized. So, from that perspective, that turned out to be a good thing.

On the second line of activity, pushing back on the Russians and imposing costs, this line of effort was focused on developing options for the decision-makers. The goal was to respond to ongoing activity and to defer further escalation or future activity. We used the normal NSC-led interagency process to develop a suite of options to respond to this activity. One of the key bodies that worked on that was the cyber response group that I chaired within the White House, which had representatives from all of the relevant agencies that could have a role in developing and implementing response options.

The specific actions and options we developed were, and to my knowledge remain, classified, other than those that became public by necessity once they were implemented. However, I can say that the options that we developed spanned the full gamut of U.S. power, including diplomatic, intelligence, law enforcement, economic, and cyber activities. Within these broad categories, we created a range of potential actions, from low risk/low impact, to high risk/higher impact options, as we would for any national security issue. My responsibility in that process was ensuring that the NSC principles, up to and including the President, had a full range of options to consider, along with the pros and cons of each of those.

Due to the significant concerns around escalation, the overall geopolitical situation that we were in, the tensions within the U.S. election, the presidential race that was happening as both of you have noted, the desire not to do the Russians' work for them by undermining confidence in the electoral process, senior decision-makers proceeded carefully and judiciously, and eventually we settled—eventually they settled—on a set of options and actions that have been widely reported in the press.

Now, not all of the options that we laid out were taken, but that's not a surprise to anyone who's worked in the policy process. That's how it works. Decision-makers never take all of the possible actions that you develop.

In looking forward to the future, which is, I think, the key aspect of what this committee is working on, now that the Russians have proven that it can be done, we should expect not only the Russians but others to follow their lead. We should expect other nation-states and, frankly, other non-nation-state actors to also attempt to do similar activities. And so, in response, I think that we need to do several actions.

One is that we need to continue to invest in improving the cybersecurity of our electoral infrastructure in its entirety across the

board. We need to figure out how to enable the Federal Government to better support State and local governments, because I think maintaining that State and local control of elections is incredibly important. It's very central to our system of federalism and democracy, and we need to sustain that. But it's also not realistic to expect State and local governments on their own to go up against nation-state actors. So, we need to figure out how to enable the Federal Government to assist those entities to better protect themselves while enabling them to still maintain control of the electoral process.

We should also, as Ambassador Nuland highlighted, invest in our resilience to information operations, which is related to but separate from these cybersecurity issues. Internationally, we should continue to promote the idea that it is unacceptable to surreptitiously interfere in another nation's electoral process. The U.S. should continue to work with other allied governments to identify, expose, and respond to Russian activity in this area and embed it with our actions to deal with other Russian activity. And we also need to maintain a whole-of-government campaign to counter Russian cyber activity across the board.

So those are my thoughts on where we need to head in the future in order to continue dealing with this issue that I think will be with us for all of our future election cycles, and it's something we're going to need to learn how to deal with and be able to counter as a Nation going forward.

Thank you very much.

[The prepared statement of Mr. Daniel follows:]

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.

Chairman BURR. Michael, thank you very much for that testimony and to you, Ambassador.

The Chair would like to announce for members: I understand that two votes are scheduled for about 12:30, so it's my intention to finish this open session no later than 12:45. We will immediately then, after completing the second vote, come back for a closed session, and that will give our witnesses time to do a choke and run on some lunch.

I'll recognize members by seniority for up to five minutes. And the Chair would recognize himself.

Michael, let me just say, looking back, what seemed like the right thing at the time, which was for the Secretary of the Department of Homeland Security to declare that the election system was critical infrastructure, in hindsight was the worst thing we could have said to State officials because they took it as the Federal Government taking over the election process. So, we've tried to point some of these things out and need to be sensitive in the future.

Ambassador, we've been told that all potential responses to Russia's acts were on the table, most of them debated. And at the end of the day, prior to the election, not the period in between the election and swearing-in, really, the only big thing that was done, the President contacted Putin personally and raised this issue. One, is that an accurate depiction that we have been given by people that we've interviewed? And, two, what should have we done that would have changed where we are today?

Ambassador NULAND. Thanks, Chairman. In this open session, let me say I assume you're talking about what was done with regard to the adversary, with regard to Russia, rather than the things that Mr. Daniels has talked about with states, et cetera.

Chairman BURR. Yes, Ma'am.

Ambassador NULAND. So, it's accurate to say that, in September, the President made a stern and personal warning to President Putin, that there were follow-up conversations in other government channels with appropriate counterparts including use of some preexisting channels that we had with the Russians. But we did not take deterrent measures in this electoral period.

There was a lot of work going on, I would say, from June onward as to what kinds of deterrent measures we could take either in the electoral period or afterwards. A lot of that work informed what was done later in December. But for a variety of reasons—some of them you highlighted yourself, some of them Mr. Daniels mentioned, there are others that are more classified—the President chose to launch the full investigation and response after the election.

I think, you know, it's fair to say that all of us in the process assumed that what was done in December-January of 2016–2017 would be a starting point for what the incoming Administration would then build on. So, I think there's still plenty of work to be done.

Chairman BURR. We would agree with you. Why do you think it is Russia thought they could get away with treating the United States just like the other countries that they meddled in, that they really considered to be part of the Soviet Union?

Ambassador NULAND. You know, I think they saw and increasingly understood the vulnerabilities in our democratic system, that these same technologies and ways of communicating that are so powerful in terms of the way we connect with each other, also offered opportunities to turbocharge techniques that they'd been applying even since the Soviet period to try to cause dissent in U.S. politics, to try to pit us against each other, and they got better and better at it. I think, as a general matter, this Kremlin is highly opportunistic. It will do—whether it's in their own country, whether it's in Ukraine, whether it's in Europe, whether it's on other continents, whether it's in the United States—they'll throw out lots of chaff, lots of opportunities to probe, and when they feel a weak spot, they'll push further and probe a little bit further.

There's a great quote attributed to Lenin: "Thrust in the bayonet. When you hit bone, stop. If you hit mush, push." And I think they hit a lot of mush.

Chairman BURR. Michael, how exposed do you think that the social media platforms make us in the future? And do you have any confidence in the belief that they can self-police bad actors?

Mr. DANIEL. So, I think that, as with all of that kind of technology, it's a double-edged sword, right? It provides a lot of opportunity to get messages out very rapidly that are clear and accurate, but it also provides a great opportunity for misinformation and disinformation. I think that, on their own, without assistance from not just the U.S. government but other allied governments, it's going to be very hard for the social media platforms to find all of the malicious actors. They're actually quite good at finding a fair amount of it, but I think that it's incumbent upon not just the U.S. government, but all Western governments—democratic governments—to figure out how to work with the social media platforms to better identify that kind of misinformation and malign information that's on those platforms.

Chairman BURR. We actually believe that there needs to be a new type of collaboration between us and those companies, and we're working on that.

Ambassador, I'm going to come back to you with a couple of quick things, and I'll get into specifics on it when we get to closed session.

At what point did you become aware of Mr. Steele's efforts?

Ambassador NULAND. Mr. Steele's efforts with regard to——

Chairman BURR. The dossier.

Ambassador NULAND. To the dossier?

Chairman BURR. Yes, Ma'am.

Ambassador NULAND. I was first shown excerpts from the dossier, I believe, in mid-July of 2016. It wasn't the complete thing, which I didn't see until it was published in the U.S. press.

Chairman BURR. Sure. I know you've talked extensively with our staff relative to Mr. Steele. Based upon our review of the visitor logs at the State Department, Mr. Steele visited the State Department briefing officials on the dossier in October of 2016. Did you have any role in that briefing?

Ambassador NULAND. I did not. I actively chose not to be part of that briefing.

Chairman BURR. But you were aware of the briefing?

Ambassador NULAND. I was not aware of it until afterwards.

Chairman BURR. Okay.

Vice Chairman.

Vice Chairman WARNER. Thank you, Mr. Chairman. I'm going to start with similar questions as the Chairman, but with a slightly different approach.

I don't think enough was done, but there were a series of actions taken. We had the President talking directly to Putin. We had Mr. Brennan talking to his counterpart. There was the first use of the cyber hotline. There was the October 7th ODNI–DHS warning.

Do you think any of those actions resulted—and this is a question for both of you—resulted in a diminution of the Russian activities? Did they slow down anything? Or do you think it was still full steam ahead? Or do you think if we had not done those that the Russians might have even been more nefarious?

Ambassador NULAND. I think it's certainly the case that it was very important to tell the Russians at every level, including the top level, that we were watching what they were doing. Whether they slowed the Russian's roll, whether they did less particularly after the President spoke directly to Putin in early September, I don't know.

If you look at the record of their activity, they were generally a little bit less active in September than they later were in October. And then they particularly were at the end of October, where they were quite active, when they thought that the election might turn out differently than they previously thought.

Vice Chairman WARNER. Mr. Daniel.

Mr. DANIEL. And I would generally agree with Ambassador Nuland's remarks on that. I would draw a distinction between when we saw a diminution of their cyberactivity aimed at the electoral infrastructure, and now looking back we see very much an increase in what they were doing on social media and the influence operations.

So, I think my conclusion would be that they shifted their focus away from pure cyber operations and more into the information operations area as a result of what we were communicating.

Vice Chairman WARNER. But clearly, even the President's warning, Brennan's warning, cyber hotline, DHS–ODNI public warning, really didn't seem to have that much effect in terms of diminution of their even more nefarious activities, I would argue, both with social media and selectively leaking of information that took place in October.

Ambassador NULAND. In my experience, the Russians and particularly this Kremlin watch what we do more than what we say. So active deterrence measures perhaps would have been more effective.

Vice Chairman WARNER. It appears to me—and again, for both of you—that we were caught relatively flat-footed in terms of how the Russians used social media. I would argue the companies were caught flat-footed, as well, and part of this is due to the fact that I think they exploited a seam between where foreign agents impersonating Americans, but generating content in Russia, delivering the content in America. That fell between the cracks.

In light of the fact that we'd seen activities in Eastern Europe, we've seen activities, again, Russians using social media, do you have an explanation, do you have any—this is the exact Monday morning quarterbacking that sometimes we'll do—of why we were caught so flat-footed vis-à-vis social media now?

Ambassador NULAND. I think there are a number of explanations, some of which we'll talk about in the follow-on session. But the Russians were, over time, perfecting their ability to target social media to specific political objectives in their own country, in Ukraine, and then across Europe well before 2016.

I think that some companies were aware of some abuse of their platforms in other countries, but because they weren't talking to each other, they weren't integrating what the various companies were seeing, and developing a pattern. As the Chairman said and I said to you last year, the private companies were each touching a piece of the elephant and not seeing the whole. I also think that there was a tendency in the U.S. Intelligence Community to look only at classified information. And the necessary integration of open source and classified information was not happening the way it needed to. So, we were as a government not as aware of what was happening in the private sector.

Vice Chairman WARNER. Mr. Daniel.

Mr. DANIEL. And I would just, also, building on top of that, my position was cybersecurity coordinator, focused on the protection of information systems. We weren't set up then and we aren't really set up now to have a focused effort within the U.S. government to counter information operations, many of which were not carried out through using malware or stealing credentials. In many cases, for example, the Russian agents that you talked about just signed up for Facebook accounts. That's not a cybersecurity problem. That's an information operations problem. And while those two things can often be blended—and the Russians are very good at combining their cyber capabilities with their information operations capabilities—those are actually separate things and, in many ways, require separate disciplines in order to counter.

Vice Chairman WARNER. I know my time's about up. But you just said certain companies were aware that Russians were interfering prior to the election. What I think is remarkable is that none of those companies acknowledged that ahead of time. As a matter of fact, in our immediate aftermath of the election, when public officials raised the concern that Facebook and others could have been misused by the Russians, actually the leadership of many of those companies dismissed that notion wholeheartedly. And it literally was months and months and months before these social media companies acknowledged they'd been misused.

Thank you, Mr. Chairman.

Chairman BURR. Senator Risch.

Senator RISCH. Thank you. First of all, Ambassador Nuland, thank you for your well-thought-out recommendations. I think those are serious and deserve serious consideration.

I want to summarize here a little bit. Both of you have indicated, and I think it's well documented, that this whole thing started in spring of 2016 and gradually grew through the year, to the point where, in September at the G20 summit President Obama con-

fronted Mr. Putin and disclosed to him that we knew what they were doing. Obviously, that was classified information, but I am not criticizing him for that. That's a President's job to do that. I think also, Ambassador Nuland, your description is that confrontation may have slowed him down briefly, but just briefly, and they continued on the direction they were headed. Is that a fair statement?

Ambassador NULAND. That appears to be fair based on what we know. Obviously, we don't have full knowledge of the Kremlin's thinking.

Senator RISCH. Okay, thank you. And one of the things that puzzles me is that while the government—in fact, the next month, in October, DNI went public with the fact that we knew all about—we knew what the Russians were doing and people need to pay attention to it, at least to some degree.

This is a question I have for you, Mr. Daniel, and this puzzles me. There's a quote I want to read you from an article that appeared of what happened in late August of 2016.

At his morning staff meeting, Daniel matter-of-factly said to his team it had to stop working on options to counter the Russian attack. Quote, "We have been told to stand down." That's a quote from you. Daniel Prieto, one of Daniel's top deputies, recalled, quote, "I was incredulous and in disbelief. It took me a moment to process. In my head I was like, did I hear that correctly?" End quote. Then Prieto asked, quote, "Why the hell are we standing down? Michael, can you help us understand?" End quote.

Is that an accurate description of what happened?

Mr. DANIEL. So that is an accurate rendering of the conversation at the staff meeting. But the larger context is something that we can discuss in the classified session. But I can say that there were many concerns about the widespread—how many people were involved in the development of the options. And so, the decision at that point was to neck down the number of people that were involved in developing our ongoing response options. And it's not accurate to say that all activities ceased at that point.

Senator RISCH. What about your area of supervision? Did it completely cease as far as that was concerned?

Mr. DANIEL. No. We shifted our focus in that September and October timeframe to focus heavily on better protecting and assisting the states in better protecting the electoral infrastructure and ensuring that we had as great a visibility as possible into what the Russians were doing and developing our—essentially an incident response plan for Election Day.

Senator RISCH. And you've described that. But as far as your cyber response, you were told to stand down. Is that correct?

Mr. DANIEL. We were—those actions were put on the back burner, yes, and that was not the focus of our activity during that time period.

Senator RISCH. What cyber options did you recommend? And which ones were taken and which ones were rejected?

Mr. DANIEL. Again, this is actually something we will have to discuss in the classified session. And I am more than happy to describe some of those there. But it was a full range of potential actions where we could use to use our cyber capabilities to impose

costs on the Russians, both openly, to demonstrate that we could do it as a deterrent; and also clandestinely, to disrupt their operations, as well.

Senator RISCH. And were any of those accepted?

Mr. DANIEL. So, I can't really go into that here.

Senator RISCH. I got it. How about you, Ambassador Nuland? What did you recommend? And what did they take and what did they trash?

Ambassador NULAND. Again, I think it's more appropriate to do specific recommendations in the closed session. What I will say is that we were aware as—I was aware as early as December 2015 that the DNC had been hacked. We didn't know by whom at that point, but it bore a lot of signatures of other activity we'd seen from the Russians in other parts of the world.

And then as we saw more hack activity during the spring, those of us on the Russia account pushed very hard internally to put more intelligence resources on this to better understand what was going on. We didn't know at that point whether this would take the form of intelligence-gathering during an election period or whether it would be used for influence and of what kind before or after the election.

We became more alarmed when throughout the spring, and in June my team was authorized by Secretary Kerry to begin working internally at State and interagency on what kinds of deterrence opportunities there might be, whether in the cyber realm or using other tools, like economic tools. We developed a full suite of options in July and then we understood that this issue would be taken up again after the election, but we were authorized to continue our work on what might be effective in the August and September period. And we did that so that we were ready for the formal conversations when President Obama authorized them after the election.

Senator RISCH. My time's up. Thank you.

Chairman BURR. Senator Wyden.

Senator WYDEN. Thank you, Mr. Chairman.

So, thank you both. The Chairman has called an important hearing, because we're talking about policy responses to the Russian attack on our democracy. And I have felt for a long time that one of the best ways to be able to push back on Russian attacks on our democracy is to have a lot of allies close to us, allies who are going to stand with us.

And if you're going to focus on that, it is certainly relevant to discuss President Trump's behavior toward the Russians and towards our allies. So, at the G7—I think I'll do this for you, Ms. Nuland, if I could—at the G7, not only did the President criticize our allies, both individually and collectively, he was unhappy that Vladimir Putin had not been invited. And this week apparently he is trying to undermine the German government by making false claims about migration and crime. So, at every step of the way on these key kinds of questions—climate change, trade, Iran, basic issues of human rights—it seems to me the net effect is that the President has isolated us from allies that we very much need to help us stand up to Russia and the attacks on our democracy.

So, given your background, how important in your view are these alliances to be able to push back against the Russians? And what's your take? How would you evaluate the President's recent actions that I have described?

Ambassador NULAND. Senator Wyden, in my professional experience and study in history, the U.S. alliance system has served our Nation superbly in terms of security, in terms of prosperity, in terms of defense of the values in our Constitution and Declaration of Independence, for more than 70 years. We don't always think our allies are doing enough. We sometimes have frictions. We have in every decade, whether it was over Suez or whether it was over Vietnam or whether it was over Iraq. But it is important that we work together to get through those as a family. And fundamentally, the system we have in place is a collective security system, where we jointly pay for it and jointly execute against our common enemy, and a shared prosperity system where we push for maximum openness so that we can all benefit and all prosper.

Obviously, adjustments are always needed. We adjusted NATO after 9/11 to go to Afghanistan. And I would remind that allies bore more than half of the combat burden for most of the Afghanistan mission throughout the period. So, I am concerned.

Senator WYDEN. What's your take on the President's recent actions that I've described?

Ambassador NULAND. I am very concerned when America's adversaries appear to get better public and private treatment than America's closest friends. And we certainly should not be in the business of interfering in internal politics. I am also quite concerned on the trade side that if we are not careful we could set off a renewed recession in Europe and perhaps even in the United States.

Senator WYDEN. I'm glad that you've pointed out this kind of double standard. And it's a double standard that cuts against America's security interests, in my view, when people who have been hostile to us appear to get better treatment than those who have not. So, I appreciate your pointing it out.

One last question on the remainder of my time, Mr. Daniel. So, your position was eliminated, as you know, recently—the cybersecurity coordinator—at a time when it seems to me you have more and more cyber threats of a wide variety. I mean, we saw press reports with respect to hacks from North Korea during the middle of these discussions. These were in our publications.

So, tell me in your view what capabilities do you think are lost with respect to the elimination of your position? In other words, I was going to ask you for your assessment of threats today. But I said, well, Mr. Daniel is in a position where he doesn't have that kind of current sort of situational awareness, I guess, would be one of the technical terms. But tell me, if you would, what capabilities are lost by the elimination of your position?

Mr. DANIEL. Thank you, Senator. It's not so much the capabilities, but the ability to integrate those capabilities and employ them. The departments and agencies are the ones that develop and maintain those capabilities, and those are still extant. But given the relative newness still of the law and policy, and interagency cooperation on cyber-related issues and the use of our cyber capabili-

ties, I think it is still very important to have a senior official at the NSC—at the White House—that's actually driving policy and driving operational collaboration in that area.

Senator WYDEN. I'm over my time. Thank you, Mr. Chairman.

Chairman BURR. Senator Rubio.

Senator RUBIO. Thank you. Thank you both for being here.

Mr. Daniel and Ambassador Nuland, throughout the campaign, the Administration took a few steps to attempt to warn Russia against additional activity. I think that includes the October 7th statement and direct warnings from the President, from Director Brennan, and over the cyber hotline. Do you believe any of these efforts had any deterrent effect at all?

Ambassador NULAND. Thanks, Senator Rubio. I think it's pretty well unknowable what the total effect might have been. It appears that there may have been a slowing of Russian activity in September, after the President directly warned President Putin. But clearly by the middle of October that activity had resumed in full force.

Mr. DANIEL. I would agree that it's essentially unknowable. I think that it did. I believe it prompted them to shift some of their focus away from trying to penetrate State-level voter systems and focus more on the influence operations. But again, I think that it's a very difficult question to answer.

Senator RUBIO. Well, in that context, you both—I think the date you pointed to is October, when you said you thought it might have restarted up, even had been a different direction, mid-October?

Ambassador NULAND. I think the Russians were constantly reevaluating the opportunity that this operation gave them and seeing more and more advantage. I think by mid-, late-October, they may well have changed their calculus about the outcome of the election and accelerated their influence operation accordingly.

Senator RUBIO. So, in that context—and this happened after the President's warning—the later release of the Podesta emails, do you ascribe that to kind of moving in a different direction, in particular towards the influence campaign that Mr. Daniel referred to, as opposed to attacks on State systems and the like?

Ambassador NULAND. I wasn't involved in working with the states, obviously. I was only involved in the Russian piece of it. I think what we saw was a move from the release of the emails into our political conversation among ourselves moving later in the campaign to the acceleration using the bot networks and using the internet accounts that they had established to push false narratives that were popular on the fringes of U.S. politics and to try to mainstream those.

Senator RUBIO. I forgot the exact quote, but you had said a moment earlier that if you push and you hit something hard, you stop, and if you feel mush, you keep pushing. In that context, why did Vladimir Putin think he could get away with treating the United States the way he treats countries in his near-abroad, that they think they should be under Russia's control and under their thumb? Why did he feel, in your opinion, that he could get away with that—or treating us in the same way?

Ambassador NULAND. In my experience with this particular leader, if you don't make these aggressive moves cost directly for him and his circle in his own context, then he will keep pushing.

Mr. DANIEL. I don't really have anything to add on top of what the ambassador has said.

Senator RUBIO. But ultimately, I guess it sounds what you're saying, or to rephrase it is, he has a cost-benefit analysis. Here's the price of doing this. Here's the benefit of doing it. I believe the benefit outweighs the cost, and therefore I'm going to do it.

Ambassador NULAND. I think it's probably the case that the Russians expected deterrent measures and didn't see them and so felt they could keep pushing.

Senator RUBIO. Well, in that context—and I know this is kind of a hindsight 20/20 situation—but, Ambassador Nuland, if you could do it over again, if we could go back to 2015 and 2016 and try to deter this activity, as you said that they were expecting, what would you do? What language do you believe he would have understood? What could we have done differently? Part of this inquiry is to learn about what our policies should be moving forward and whether there should—in addition to the rhetorical one obviously—the actions that we would take. But what would have worked, in your opinion, looking back now?

Ambassador NULAND. Again, we can talk a little bit more about this in classified session. But I think part of the problem that we had was that, as I said in my opening, we didn't have sufficient integration of information to understand fully how their campaign was structured.

We didn't have sufficient agreement in the interagency as to what the deterrence tools were and what the effect on us might be if the Russians chose to escalate, because we haven't studied it hard enough and we weren't unified enough. We weren't working closely enough with the companies to know what might be possible, as well. And we were beginning the work with our allies, but we hadn't done enough.

So, if you look at the more successful counteroperation that French President Macron later did in the following years, some of which built on our experience that we shared, what he was able to do was to, much more quickly than we were, identify Russian influence operations, to call them out, and to put a legal structure in place to counter them. So, he essentially neutered the influence by telling his people that this was Russia. It was not part of the debate in France.

So, one concrete example, there was a poll about a month out from the French election which showed Le Pen, the far-right candidate, in the lead. It was a Russian operation. It was not a true poll. And the French were able to prove that both in terms of the origin of the information, heading back to Russia, and in terms of their own data. And within the same news cycle, virtually, or within a week, they were able to debunk it publicly, and therefore they blunted the weapon.

We've got to be in the same situation at least, if not in terms of countermeasures inside Russia and other adversaries, so that they know that this is going to cripple them, as well. We can talk about those later.

Chairman BURR. Ambassador, let me just say, the Vice Chairman and I many times have wondered what we would have done if we had the same ability that the French do to pull down the media three weeks before the election. To some degree, it shows you the vulnerabilities, but we are challenged to live within the First Amendment, and clearly, they had some tools that we didn't have.

Ambassador NULAND. And, Chairman, I'm obviously not recommending that. But I do think that, you know, information is the best. Sunshine is the best disinfectant, right?

Chairman BURR. But it is very obvious that it changed the campaign for Russia as it related to France.

Senator King.

Senator KING. Well, I'd like to follow up on that point. In talking to people in Eastern Europe who have been living this for years, Ambassador, I have asked them, what's the best defense? What do you do? You can't cut off television, take down the internet. They said the best defense is for the public to understand that it's happening and then they can discount it, and say, oh, it's just the Russians again. And that's why I think what we're doing here is so important: to inform the American people that this is real and that it's going to continue, because then they're better prepared. Would you agree with that?

Ambassador NULAND. Senator, I would completely agree with that, because no population, no citizen wants to think that a foreign entity is controlling their election. It should be a national and sovereign right of every citizen to elect their leaders.

And so, when you explain and expose exactly how these campaigns work, and that the information they're getting is manipulated by somebody outside of our country, not only does it change their processing of the information, it actually radically turns them off to that information, because they feel appropriately that they have been manipulated.

Senator KING. When did you two first meet in person?

Ambassador NULAND. I don't remember. I mean, we certainly were part of meetings in the summer and fall of 2016. Did we meet before that?

Senator KING. That was really the point of my question. There were meetings. You were in similar meetings. But I want to go to your first recommendation, which is a fusion center. It seems to me that one of the problems with that response to cyber generally is a lack of a central focus. I believe it should be a person, not just a fusion center, but someone who has overall responsibility. I just listed nine agencies that have a piece of this. And right now, I'm getting frustrated. I hear the term whole of government, and to me that means none of government, because there's no one in charge.

Do you believe that there should be some central authority, somebody in government whose responsibility it is to think about cyber and protecting this country?

Ambassador NULAND. Senator, there obviously has to be somebody who looks at cyber. Cyber is obviously bigger than the issue of malign state actors affecting politics.

Senator KING. Yes.

Ambassador NULAND. In the concept of the fusion center that I put forward, presumably there would be a director, as there is for the National Counterterrorism Center, who would be the single bellybutton for leaders to hold this together.

Senator KING. As Mr. Daniel pointed out, someone to integrate the data. And that was one of the problems early on in our response, was it not? That we had data coming into the FBI and the NSA and various places, and we didn't really have a full picture of the magnitude of this attack until fairly late in the summer or early fall. Is that correct, Mr. Daniel?

Mr. DANIEL. I would actually argue that we didn't have a full appreciation for the scope of what was going on until actually well into 2017—that, in fact, in the fall of 2016, the full extent of the Russian information operations, everything that they were doing on social media, and the vast number of trolls and activity that they had going on—I don't think we fully understood that even in the fall of 2016. And it's a picture that has continued to evolve over time, as committees like this have done their work, and I think that was, as the ambassador pointed out, part of the problem was that we didn't actually have a complete understanding of the campaign that was being carried out against us.

Senator KING. Ambassador Nuland, a different tack. President Obama has been criticized for not acting soon enough, strong enough. What was the thinking, without revealing classified conversations? But what was the President's thinking, insofar as you know, in terms of how to respond to this? And what were the risks and what were the benefits? For example, why wasn't there a strong classified sanction or some activity as opposed to a stern admonition at the G20 summit?

Ambassador NULAND. Senator, we can talk a little bit more about this in classified session, as we did last year. I think some of the reasons have been ventilated here. You know, there was incomplete information at the right moment, which I think is a fault of the systems that we had in place to integrate, as you said, including the ability to integrate between the government and the private sector, between classified and unclassified.

There was already, by late July and early August, accusation by Candidate Trump that the election would be rigged. And I think there was a concern that if this wasn't handled properly, any move publicly would be seen as President Obama playing into those accusations. There were concerns about how this might escalate. If we took countermeasures, there could be escalatory measures, because one Russian goal was obviously to undercut the integrity of the electoral system. So, not wanting to play into that.

And I think there was a perception that this could be dealt with after the election in a more fulsome way and that whomever was elected would continue the work that the Administration started to get to the bottom of it more fully.

Senator KING. Thank you. Thank you, Mr. Chairman.

Chairman BURR. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Mr. Daniels, how did the Administration view WikiLeaks? For example, did you view it as a news organization, as a social platform like Facebook, or in essence a hostile intelligence service?

Mr. DANIEL. Senator, I would actually say that in many ways it was sort of all-of-the-above at various points. I mean, certainly, as someone who had spent a large amount of time working with the Intelligence Community over my career, certainly we did not view a lot of what WikiLeaks was doing as favorable.

You know, I think that our view was always split as to exactly how witting a lot of the people that were involved were with what was going on. Again, that's something we can explore in more detail in the classified session. But clearly, the Russians used them to great advantage.

Senator COLLINS. Exactly. Do you think that realization existed in 2016? Or is that only a realization that we have looking back?

Mr. DANIEL. I don't think that we fully appreciated the scope and scale of the Russian influence operations. And at the time, certainly that was part of what prompted our initial work, was the release of information into WikiLeaks with the persona that was called Guccifer 2.0.

But in many ways, we were very much—certainly on the cybersecurity side—we were very focused on the activity aimed at the State and local electoral systems. And it wasn't until I think later in the year, and even actually after the change of Administrations, that we became fully cognizant of the scope and scale of the influence operations.

Senator COLLINS. You mentioned the State and local electoral systems. We have received from the Department of Homeland Security inconsistent and varying numbers on the number of states whose systems were scanned by the Russians. How likely do you think it is that Russian cyber actors at least scanned all 50 states?

Mr. DANIEL. I think it is highly likely. It was always my judgment that given the number that we reached, where we had pretty good evidence of that, led me to believe that there was no reason why they wouldn't have at least attempted reconnaissance against all 50. And it was more likely that we hadn't detected it than that it didn't occur.

Senator COLLINS. I really appreciate your being forthright about that, because I believe that if states understood that, they'd be more receptive to the help that I know Secretary Johnson offered, and the help that they're being offered now, since certainly that threat continues.

Ambassador Nuland, in 2016, the FBI was complaining to this committee that Russian diplomats in the United States were not following the established rules about travel and they were not notifying the State Department. And it seemed that they were traveling to odd locations on short notice.

Were you aware at the State Department of the FBI's concerns?

Ambassador NULAND. Yes, Senator. As I testified in classified session a year ago, and as I think we should review again in the closed session, we had significant conversations with the FBI about their concerns and took some actions and prepared others as early as July and August of 2016 with regard to their concerns. They also, as they've I'm sure told you, had a severe understaffing problem in terms of their ability to do their job in identifying when the Russians didn't obey the rules and make it painful in those encounters.

Senator COLLINS. Do you think that that travel was related to the Russian active measures against our electoral system?

Ambassador NULAND. I do.

Senator COLLINS. Thank you.

Chairman BURR. Senator Manchin.

Senator MANCHIN. Thank you, Mr. Chairman, and thank both of you all for being here. And don't think there's any question that the Russians were attempting to be as involved as they possibly could at a higher level than they've ever done before.

So, I would ask, do you think that we have the assurances that we know exactly what they did, how they tried to do it, and are they still moving in that direction? Yes, go ahead.

Ambassador NULAND. Well, Mr. Daniels will speak from his experience. Among the reasons I put forward the five recommendations that I did is I do not think that we are yet organized, funded, structured——

Senator MANCHIN. How much do we know about their internet research area, basically in Saint Petersburg? Mr. Daniels, would that be you or——

Ambassador NULAND. I would simply say we know quite a bit about that one, with the help of the companies. What we don't know is how many more of those there are, whether in Russia or in other parts of the world.

Senator MANCHIN. Mr. Daniel.

Mr. DANIEL. And I would just say that I have too much appreciation for the capabilities of the Russians. They are an incredibly sophisticated actor both on the cyber side and on the information operations side. I have too much respect for that to believe that we've detected all of the activity that they either did do or are continuing to do.

Senator MANCHIN. With that being said, do you believe we should have a policy to treat cyberattack, if proven, to be sponsored by a foreign government—whether it be Russia or anybody else—as an act of war and automatically retaliate in cyberspace?

Mr. DANIEL. So, I think that as with any issue in the physical realm, I think what we have long argued and that I support, is that the same ideas and concepts of proportionality and the laws of war apply in cyberspace, just as they do in the physical realm. And so, that if you had a cyber-incident that rose to the same level of——

Senator MANCHIN. A use of force?

Mr. DANIEL [continuing]. That you should be able to respond using all the tools of national power, the same way we would to an incident in the physical world.

Senator MANCHIN. We have the midterms elections we're all concerned about because they're very critical for those of us who are involved and everybody else who's paying attention to it. And I'd like to know for the people in West Virginia that our systems are safe. If there is any indication that there might be an infiltration by a foreign actor to thwart the outcome, can they prevent that or can they detect it?

Ambassador NULAND. Senator, Mr. Daniel will speak to the technical capability, particularly in West Virginia. I would simply say that as a matter of U.S.-Russia policy, this would be a moment for

the President to first be working with his policy team to decide what the costs for Russia should be if there is proven interference in the 2018 election.

Senator MANCHIN. Why don't we just say the whole thing? Do you believe there should be the same alert that we have for a nuclear attack as a cyber-attack?

Ambassador NULAND. What I would say, I would repeat what Mr. Daniel said: that we want to make sure that any president can have a full toolbox of response options. In some cases, it may be that economic pressure is more effective, or more costly, to the adversary.

Senator MANCHIN. Let me ask this question to either one of you, or both of you. Do you believe there was anything the Obama Administration could have done to break through the pre-election political rhetoric and make people take that seriously, take that threat seriously? I mean, it got to the point that everything was after the fact, but they knew, you all knew, something before the fact.

Mr. DANIEL. I think, in my experience, it always takes an extended period of education and engagement—whether it's the financial sector, the electoral sector, the health-care sector—all of them followed a similar pattern to what we saw with the electoral infrastructure sector, in terms of it takes time for people to grasp and understand that the threat is real, that it's present, that it can affect them directly, and that then there are things that they can actually do to try to address it. And, in fact, actually I would say that timespan has actually been shortened in the electoral infrastructure. And people have gotten to that point much more quickly than they did in some of our other areas.

Ambassador NULAND. I believe that there were deterrence measures that we could have taken and should have taken earlier in 2016.

Senator MANCHIN. Should we have made the public aware?

Ambassador NULAND. I think obviously the public should be aware, but for a lot of reasons, some of which we'll discuss in the next session, we were not sufficiently aware ourselves at the right moment. But more importantly going forward, we know that they may very well do this again. So, now we need to be planning what the retaliation will be, and we need to be signaling it so that the cost is evident.

Senator MANCHIN. My time is running out. I'm just saying, you don't see the Russians or other foreign actors backing off at all? I mean, do you see their involvement at the same level, if not greater, Mr. Daniel?

Mr. DANIEL. So, not having access to classified information right now, certainly if you look at just the most recent activity associated with a piece of malware called "VPNFilter" that is almost assuredly associated with the Russian government, that targets routers and other things; it includes a destructive capability. It's a type of malware that we really hadn't seen before in the cybersecurity community. That shows quite clearly the intent of the Russians to continue using their cyber capabilities.

Senator MANCHIN. Thank you.

Chairman BURR. Thank you. Thanks, Senator.

Before I move to Senator Lankford, let me just ask both of you, at what point did the cyber indicators match up with the knowledge about Russia to form the complete picture of exactly what this threat was?

Ambassador NULAND. Chairman, as you know, since I was sitting at the center of government work on Russia, I was a consumer of all of the different intelligence information that there was.

Chairman BURR. Yes, this is more of a stovepipe question. At what point did the technical—the cyber indicators that, Michael, you were looking at on a constant basis—match with the knowledge that you had in the field or somebody at State? And were we able to put this together and see the complete picture?

Ambassador NULAND. My feeling about this is that it wasn't until the President ordered all of us to sit together and map what we knew that the full elephant came into view for all of us together. But even so, that was only an elephant that represented the government's holdings of information. As Mr. Daniel has said, we learned much later about the holdings that the companies had, the information.

Chairman BURR. And roughly that time when the President brought the team together, was——

Ambassador NULAND. December of 2016.

Vice Chairman WARNER. I don't want to interrupt Senator Lankford, but in other words, if the President had not asked for this bringing together of the information, there was no process in place that would have immediately aggregated this information on a regular, on a normal operating bases?

Ambassador NULAND. There should have been, but there wasn't. And that's why I advocate this fusion center and the second recommendation to also have a continuing conversation with the companies.

Chairman BURR. Michael, anything to add?

Mr. DANIEL. I would just add that, to the extent that, again, I would separate out some of the information on the influence operations and the information operations side, but on the targeting of the electoral infrastructure, the integration of that happened through the Cyber Threat Intelligence Integration Center within the Office of the DNI. And that was why that entity was created, to try to combine the cyber technical intelligence with the geopolitical intelligence, because you can't actually understand one without the other.

Chairman BURR. Senator Lankford.

Senator LANKFORD. Ambassador Nuland, tell me a little bit more about this second recommendation that you have to try to work with public and the private and to be able to work with entities. How do you think that should be formed?

Ambassador NULAND. I think this should be a presidentially directed commission, which meets at the technical level on an ongoing basis, but at the leader-level, monthly or thereafter.

After I left government and had an opportunity to talk to a lot of the big actors in the U.S. private cyberspace, it becomes clear that for reasons of company privacy, et cetera, proprietary business information, they don't want to talk to each other. They're not comfortable. They worry. But yet they're facing many of the same prob-

lems. And they're also having conversations with the government about what they're seeing, but it's limited to cyber experts. And it's not integrated with policy. And often it wasn't getting to a high enough level.

So, when I say the companies knew some of what was going on, on their platforms in Russia, Ukraine, and Europe, as early as 2014–2015, those were the cyber specialists, but not necessarily the leaders of the companies. So, this would be ideally a safe space where companies could speak to each other, where they could speak to government, and where common campaigns of action—whether they are regulatory, legal, policy—can be formed, and where the companies can also say what kinds of protection they need from government if they're going to take bold moves.

Senator LANKFORD. So, from this perspective, how often should they meet? And who do you think should be the primary actors to be there?

Ambassador NULAND. How often they should meet, I think, would be something we'd want to talk to both government and industry about. I would say that there should be an ongoing conversation, at least a virtual conversation at the working level. There should be mid-upper-level meetings at least monthly and probably senior cabinet-level meetings quarterly, unless there is an emergent crisis of the kind we saw in 2016.

Senator LANKFORD. Who? Who do you think should be at that table?

Ambassador NULAND. Again, I would want to do more work with the companies on this and more work with government to get a better sense of it. But on the company side, I would want to see both cybersecurity experts and policy experts to make sure they're integrating on the government side the same.

Senator LANKFORD. So, it is our great frustration, as you know well, that we've worked with several of these social media platforms, and they saw things and were taking in ads that were election related. They were aware of it and trying to figure out what to do with it, basically. They've now had some fairly significant changes in their policy. They're still trying to be able to address this, to figure out how to be able to monitor it, but obviously they saw it throughout the election, as well.

So why I'm pressing you on this is that that's one aspect. There will be others. That one's been tested. They're trying to be able to respond to it. There will be others. And our imagination can take us into places where they could go next.

What would you anticipate is the goal of this meeting time? Is it maintaining what we already have? Or trying to imagine what could be coming in the cooperation and sharing? As you know in the private sector, there's not a lot of cooperation and sharing between, "We're seeing this threat, are you?" They typically see this threat and they're trying to figure out how to be able to manage it, the same as government did during 2015 and 2016.

Ambassador NULAND. I mean, obviously, it's to do past forensics in order to inform future forensics and future policy. As I said in my opening, I think Russia has done pretty well with this tool, but other actors are starting to get even better, notably including China.

Senator LANKFORD. So, let me back up a little bit on this. And this is for both of you, to use your imagination. Ambassador Nuland, you know the Russians. You know that region extremely well. So, as you talk about other actors leaning into this, whether it be nation-states or whether it be just hacktivists that just want to be able to engage, or people that have a political beef and they want to try to be able to effect this, for you, and particularly with the Russians, and, Mr. Daniel, in a broader setting, what do you think the Russians' next move is? Where do you think they're going next, based on what you've seen? And I know you're not there all the time on it, but what do you think is the next move?

Ambassador NULAND. Well, I think we're already seeing some of the moves on the Russian side. There's obviously the electoral target. But over the course of 2017 and 2018, they've had great success turbocharging their efforts to divide the U.S. on race, on issues of gun control, on any of the seams that stretch us. So, I think they will accelerate that.

I don't know whether they will have a view about the 2020 election, but having been more successful than they anticipated the last time, I think you could see them be quite aggressive on both sides—both at primary time and at general election time—in trying to influence how Americans choose their next leaders.

Senator LANKFORD. Right. Mr. Daniel, any other view for other actors?

Mr. DANIEL. Well, I would certainly say that both the Russians and other actors, including China, Iran, North Korea, criminal organizations, terrorist organizations, hacktivists, all of them, are discovering that cyberspace is a great place to try to advance their agenda. And we are seeing a proliferation of capabilities across the globe, and we should expect that to continue. Our adversaries are also going to get better at integrating their cyber capabilities with other aspects of their national power. The Russians are already quite far along in that, but the Chinese and others are not far behind.

Ambassador NULAND. Senator, if I may just highlight one. There's also the risk that you'll have American-on-American violence in this space: that if we don't put the right laws and regulatory policy in place, that it will create a jungle in our own politics against each other.

Senator LANKFORD. Thank you.

Chairman BURR. Thank you, Senator Lankford. If no members are seeking any additional questions, I think we've come to the end of the open session.

I do have one final question, if I could, Ambassador. Can you provide us any insight as to why INR was not included in the team that comprised the ICA, the Intelligence Community Assessment?

Ambassador NULAND. I thought, Chairman, that they were included. Mr. Daniel would know better because he was closer. But I thought that they were included. They were certainly included in the work we did on potential deterrence steps.

Mr. DANIEL. To the best of my knowledge, they should have been included, because by definition, the ICA should be coordinated across the community.

Chairman BURR. We'll check.

Ambassador NULAND. I have a vague memory of their coming to us on the policy side thinking that things could be more rigorous at a certain point in December. So, I think they were involved in some way.

Chairman BURR. To the best of our understanding, the participants were FBI, NSA, and CIA. And again, it gets back to our ability to look forward and to figure out how we create a pathway that has no stovepipes where these things are instinctively created correctly.

Vice Chairman, do you have anything in closing?

Vice Chairman WARNER. No, Chairman.

Chairman BURR. Let me say thank you to both of you for your insight, for everything on this important issue. While we'd all like to look exclusively forward, our mission for this investigation was to fully review Russia's involvement and intentions in the 2016 election. You both played a pivotal role.

And I hope both of you will continue to stay engaged with the committee as we finish the investigation on areas that you might be able to provide some texture and clarity on. But I hope also you'll stay involved with the committee as it relates to future policies that, Ambassador, I assure you will be on the table.

Nobody would like to concentrate solely on oversight more than the Russia investigative team, I can assure you. So, it's my hope and it's my belief that this hearing has helped us get closer to the end than to the beginning. And you have helped us today better understand some of the issues that we've tussled with for the last 16 months now. So, we are grateful to you.

With that, I will adjourn this hearing with the intent to start the closed hearing at approximately 1:15 and would encourage you to seek nourishment during that period.

This hearing is adjourned.

[Whereupon, at 12:33 p.m., the hearing was adjourned.]

○