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.