STATEMENT OF

KENNETH L. WAINSTEIN

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

CONCERNING

ELECTION INTERFERENCE: ENSURING LAW ENFORCEMENT IS EQUIPPED TO TARGET THOSE SEEKING TO DO HARM

PRESENTED ON

JUNE 12, 2018

STATEMENT OF

KENNETH L. WAINSTEIN

CONCERNING

ELECTION INTERFERENCE: ENSURING LAW ENFORCEMENT IS EQUIPPED TO TARGET THOSE SEEKING TO DO HARM

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

June 12, 2018

Chairman Grassley, Ranking Member Feinstein, and distinguished Members of the Committee, thank you for the invitation to appear before you today. It is an honor to be here with my distinguished fellow panelists to discuss our capacity to meet a fundamental and growing threat to our democracy.

I. INTRODUCTION

You are doing a real service by having this hearing, as much of the political controversy over the past year and a half has obscured the most important lesson from the 2016 election – which is that we face a serious and growing threat to our democratic institutions that demands a strong and resolute response by our legislative and executive branches.

In January 2017, the Intelligence Community assessed that elements of the Russian government directed a multifaceted campaign to influence our 2016 federal elections – an assessment that has since been buttressed by reports issued by the intelligence committees of both Houses of Congress and by the Minority Staff of the Senate Foreign Relations Committee and by the Special Counsel's indictment of Russia's Internet Research Agency, two other Russian organizations, and 13 Russian nationals in February of this year for various offense relating to their interference in the 2016 election. That campaign involved the use of several different methods of influence and disruption, to include:

1. Cyber intrusions into state and local election board systems;

2. The penetration of systems in primary campaigns, lobbying groups and the Democratic National Committee and the release of material they thought would influence the election in their desired direction;

3. The use of Internet trolls to spread disinformation and amplify stories and

themes that supported the campaign narrative they were propounding; and

4. The launching of a general propaganda campaign that echoed that narrative around the world.

The Intelligence Community Assessment concluded that these efforts represented a "significant escalation" of activity over that seen in any previous American elections and a "new normal" as to what we can expect to see in future elections both here and around the world. With its perceived success in roiling the 2016 elections, Russia and other hostile countries will likely be emboldened to ramp up such efforts in future elections, including in the mid-term elections that will take place a short five months from now.

II. GOVERNMENT CAPABILITIES FOR RESPONDING TO THE THREAT

Having established the growing threat we face, the question is how we can most effectively respond to it. The government has a number of tools it uses against this threat. The following is a non-inclusive summary of some of those tools:

1. Investigative Methods

First, the government has a range of investigative tools that it can use to detect and identify these influence activities. Since this threat emanates from a foreign power, the Intelligence Community can use the whole arsenal of national security tools – including orders from the Foreign Intelligence Surveillance Court to electronically surveil the perpetrators and national security letters to acquire relevant records (such as financial and communications records) that may identify the perpetrators and their plans. The government can also use criminal tools like search warrants and grand jury subpoenas to investigate those activities that are criminal violations as well as the technical investigative techniques for establishing attribution for cyber wrongdoing, which the Special Counsel apparently used in the investigation leading to the indictment of the Internet Research Agency.

2. Criminal Prosecution

In those cases where it can assemble sufficient admissible evidence, the government can bring a prosecution against those who commit criminal violations in the course of political interference efforts, as we saw with the Special Counsel's recent indictment.

A number of criminal violations could apply to those efforts, ranging from violations of the Computer Fraud and Abuse Act for hacking into protected computer systems to violations of the Foreign Agent Registration Act, which mandates criminal penalties for those who intentionally engage in domestic political or lobbying activities on behalf of a foreign entity without registering as a foreign agent (and also provides the government with the civil remedy of securing an injunction against such violative conduct). The government also can bring cases under 18 U.S.C. § 951, which allows the prosecution of agents of foreign governments who work in a non-diplomatic and non-official capacity without registering with the Justice Department.

There are practical limits on the effectiveness of criminal prosecution as a tool to prevent or deter this type of activity. First, it can be very difficult to attribute criminal conduct over the Internet to specific, identifiable individuals who can be named and charged in an indictment. Second, even where the government can identify and build a prosecutable case against a particular individual operating on behalf of a foreign government, it is often difficult or impossible to extradite that person so that he or she can be brought into court to face charges.

Nonetheless, criminal prosecution can have an important deterrent effect on both foreign governments and their operatives. As for the operatives, a criminal charge means international exposure as a criminal and probably a life without travel outside of their home country for fear of being arrested on an Interpol notice and taken into custody in a third country. As for the foreign government, a criminal charge against one or more of its agents has a naming-and-shaming effect that could lead the government to moderate its behavior in the future. In 2015, we saw a hopeful sign that this form of deterrence may work when the Chinese government finally agreed not to engage in cyber theft for commercial advantage after our Justice Department charged five uniformed members of its People's Liberation Army with stealing American trade secrets for the commercial benefit of Chinese companies. While there are reports that the Chinese government continues to engage in such activities, the intensity has reportedly diminished.

3. Economic and Trade Sanctions

A more immediate and direct deterrent measure is the application of sanctions through the Office of Foreign Assets Control in the Treasury Department. That office has long exercised the authority to impose sanctions such as the blocking of assets and the imposition of trade and travel restrictions in furtherance of our national security and foreign policy goals. By executive order in 2015, President Obama authorized the imposition of sanctions on individuals and entities engaged in cyber activities that threaten the national security, foreign policy or economic health or financial stability of the United States. After disclosure of Russia's meddling in the 2016 election, President Obama amended that order to incorporate the imposition of sanctions against individuals or entities for "tampering, altering, or causing a misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions."

Based on that new authority, President Obama promptly designated and imposed sanctions on five Russian entities, including Russia's two leading intelligence services – the Main Intelligence Directorate (GRU), which was primarily responsible for the sanctioned activity, and the Federal Security Service (FSB), which assisted the GRU – and three entities that provided support to the activity, along with four high-level officials from the GRU. In March 2018, President Trump imposed additional sanctions on five more Russian organizations and nineteen individuals for the election interference efforts charged in the Special Counsel's indictment and for other cyber attacks dating back to March 2016.

Given the failure of existing sanctions to rein in Russian adventurism in Ukraine, it is hard to predict whether the sanctions by Presidents Obama and Trump will have a strong or lasting impact on Russian enthusiasm for election meddling around the world.

4. Diplomatic Responses

Another direct response is to censure an offending foreign government by ejecting from the United States (or declaring "persona non grata") some number of that government's diplomatic staff. President Obama ejected 35 suspected Russian intelligence operatives and closed two official Russian facilities simultaneous with the imposition of sanctions in December 2016. In March of this year, President Trump also expelled 60 Russian diplomats following the attack on a former Russian spy and his daughter with a nerve agent in the United Kingdom.

Although this persona non grata measure can have a strong shaming effect, it can also simply devolve into a tit-for-tat with both countries ejecting each other's officials, as happened routinely between the Soviet Union and the United States during the Cold War and again just recently when Russia responded to our expulsion of Russian diplomats by expelling 60 US diplomats and ordering the closure of our consulate in Saint Petersburg.

5. Campaign Finance Laws

Recent news reports have suggested that Russian nationals made illegal contributions in our 2016 election. This conduct would certainly fit a pattern, given prior reports of such Russian activity around the world, including that French far-right party presidential candidate Marine Le Pen received funding from Russia in part as a reward for her supporting Russia's actions in Crimea.

Our campaign finance laws prohibit any foreign national from directly or indirectly contributing, donating, or spending funds in connection with any federal, state, or local election in the United States, and violations may lead to criminal prosecution. It is critical that we effectively enforce these campaign finance laws in the face of the growing foreign threat to the integrity of our election processes.

6. Protection of Electoral Systems

Although the Intelligence Community Assessment cited no evidence that Russian intelligence elements in any way compromised the vote-tallying in the 2016 election, it did find that they had accessed the voter-registration databases (as opposed to the vote-tallying systems) in a number of states. In response to these findings, Secretary of Homeland Security Jeh Johnson announced that election processes will henceforth be designated as "critical infrastructure" and therefore eligible to receive the same federal assistance and protections currently enjoyed by other critical infrastructure sectors like the energy grid and the telecommunications networks. While it is too early to assess its practical impact, this designation is a clear recognition of our reliance on state and local election processes and the need to protect that infrastructure against foreign interference.

7. Coordination with the Private Sector

Given how much of this subversive activity is perpetrated over various on-line platforms, it is critical that the government work closely with the communication providers that control the

different platforms. It has been particularly gratifying to see the level of cooperation over recent years with Facebook, Twitter and others in the effort to prevent their platforms from being used by violent criminals and terrorists. Although these companies could have done more to investigate the source of campaign advertisement purchases prior to the 2016 election, it is clear that they are now improving their defense mechanisms, with Google and Facebook each recently introducing new measures to authenticate the citizenship of individuals purchasing campaign ads. While these measures are commendable, the social media providers must continue to consider ways to prevent their platforms from being used to undermine our democracy.

III. ADDITIONAL CAPABILITIES

Those are a number of the tools and capabilities that the U.S. government can bring to bear against this threat of foreign political interference. Given the increasing severity of this threat, however, it would be wise for Congress to consider ways to strengthen or augment these capabilities. I would like to highlight five recommendations – four specific additional authorities and one general approach for combating foreign influence campaigns – that are now being discussed in the aftermath of the 2016 presidential election.

1. Provide the Government Authority to Seek Civil Injunctions Against Botnets

"Botnets" are networks of computers taken over and often used by malicious actors to launch disruptive attacks, and they can be used to sow disruption for political purposes, as we saw with the Russian denial of service attacks in Estonia in 2007. While the government is currently authorized to seek civil injunction orders against parties committing cyber-enabled theft under the Computer Fraud and Abuse Act, it has no such authority to enjoin denial of service attacks that do not involve any theft or "fraud." As such, the government has no legal recourse to these disruptive attacks, even when the circumstances clearly demonstrate that they are being undertaken for political reasons. Congress should consider expanding the government's authority to allow prosecutors to seek civil injunctions against botnets being used for such a purpose.

2. Amend the Foreign Agent Registration Act

As I mentioned above, the Foreign Agent Registration Act (FARA) is designed to expose foreign influence in our political system by imposing a registration requirement on those who engage in political or lobbying activities in the U.S. on behalf of a foreign government, entity or individual. For a variety of reasons, the criminal provisions of this statute have rarely been enforced, with only a handful of criminal prosecutions thereunder over the past 50 years. One of those reasons is the lack of an effective means of requiring potential violators – i.e. suspected unregistered foreign agents – to produce the business records that would reveal whether they are in fact taking political actions on behalf of foreign entities.

As the law currently stands, the Justice Department lacks authority to compel the production of such records, short of empanelling a federal grand jury and using a grand jury subpoena. As such, Justice Department officials find themselves in a Catch-22 situation: They cannot obtain the subpoena authority to investigate a potentially unregistered foreign agent without establishing the factual predicate of a FARA violation necessary to convene a grand

jury, yet they cannot establish that factual predicate without the authority to secure the records that would reveal such a violation in the first place.

In recent reports, the Justice Department Inspector General and the Project on Government Oversight both explained how this authority gap is handicapping the Justice Department's ability to effectively enforce the statute. To address this problem, the Inspector General supported a proposal to give the Justice Department the authority to issue Civil Investigative Demands (CIDs) in a FARA investigation – much like it can do in securities, RICO, antitrust, false claims and other investigations – so that it can compel an individual or entity to produce documents, answer interrogatories, or submit to testimony where there is "reason to believe" that the person may have information relevant to a FARA investigation. On two occasions in the 1990's, Justice Department officials proposed the addition of CID authority to FARA, but neither proposal became law. It is my hope that Congress consider conferring that authority, as it would greatly strengthen the Justice Department's ability to investigate and prosecute unregistered foreign agents, thereby shining a brighter light on the role of foreign individuals, governments and other entities in our political system.

3. Consider a New Statute to Address Election-Related Disinformation Operations

As described above, the government has available to it a number of statutes – such as FARA, 18 U.S.C. § 951, and the Computer Fraud and Abuse Act – that criminalize aspects of the election interference we experienced in 2016. While those statutes currently provide a basis for prosecuting much of this activity, Congress should consider crafting a statute that specifically targets the disinformation activities that have been a central feature in Russia's election interference efforts around the globe. Besides highlighting our condemnation of this activity, the passage of such a statute would provide prosecutors a tool that can be directly and effectively used against these influence campaigns, which will become only more prevalent and insidious as our adversaries continue to hone their skills and use new technologies for their subversive ends.

4. Consider a Requirement of Intelligence Community Reporting Prior to Federal Elections

It is clear from a review of the 2016 election that the Obama Administration struggled with the question whether and how much information to provide the public about the Russian interference efforts they were detecting throughout the preceding summer and fall. Officials have publicly explained that they were torn between a desire to inform the public and the need to refrain from public announcements that could be construed as an attempt to affect the outcome of the election. In order to negate that concern for the next set of executive branch officials dealing with this sensitive issue, some have recommended that Congress pass legislation requiring the Director of National Intelligence to report at intervals leading up to a federal election (maybe 9 and 3 months prior to election day) whether the Intelligence Community is detecting any foreign interference with the upcoming election and the source and extent of that interference. That reporting would be publicly issued, consistent with the need to protect sensitive sources and methods. I would fully support a law requiring such pre-election reporting, as it would help ensure that voters are on the lookout for misleading propaganda and disinformation in the run-up to an election, which is the most effective way to neutralize a foreign influence campaign.

5. Consider the Use of Countermeasures under International Law

In addition to the above specific recommendations, it is also worth considering the deterrence that is available under the concept of "countermeasures" under international law. Countermeasures are offensive actions that a victim nation can lawfully take in order to compel another state to stop its unlawful actions against the victim nation. To employ countermeasures against an offending state, the victim nation must be able to attribute the unlawful actions to that state, and may undertake only those measures that result in damage to the offending state that is reversible and proportionate to the damage it suffered.

Some commentators have argued that Russia's subversive campaign to influence the U.S. electoral process violates the principle of non-intervention, which holds that states cannot interfere in the internal affairs of another nation, and would therefore justify the United States in responding with proportionate offensive actions – such as "hacking back" – in order to compel Russia to abandon its campaign.

I know there currently is a healthy legal debate in the academic literature as to what countermeasures would be justified under international law in light of Russia's subversive activities in 2016. It is also possible that our government has already done that analysis and taken appropriate responsive action that is not visible to us. Regardless of what is being done in the current situation, I would agree with those commentators who are encouraging the government to consider countermeasures as a means of responding to and deterring foreign state efforts to interfere in our elections in the future.

IV. CONCLUSION

As the foregoing suggests, we have a number of tools that can be effective to meet the threat of foreign election interference, and those tools can be bolstered in a variety of ways. The real question, however, is not whether we have sufficient capability, but instead whether we have sufficient will to undertake the hard work required to meet that threat. All too often, we as a country have failed to mobilize quickly enough in the face of a looming threat. For example, we saw Al Qaeda strengthening and organizing itself for many years, but failed to get truly serious about fighting international terrorism until after the 9/11 attacks. Similarly, we saw the growing cyber threat in the 1990's and 2000's, but failed to sufficiently respond until after cybertheft had reached the point of being famously characterized as "the greatest transfer of wealth in history."

It is my hope that we will not be late in responding to this most recent threat. The Russian interference efforts in our 2016 presidential campaign were a wake-up call for all of us, and we are fully on notice that they will continue in the campaigns and elections this year. It is therefore incumbent on both the executive and legislative branches to meet that threat with a coherent strategy for protecting our election processes.

Today's hearing is an important step in the right direction, but it is critical that we follow it up with resolute, sustained and decisive action against those foreign actors and governments that are trying to undermine our institutions and ideals. The threat is real, and it is not an over-

statement to say that there is a lot at stake – no less than the continuing viability of our democratic processes.

I want to thank the Committee again for holding this hearing and for giving me the opportunity to speak about this important matter. I look forward to answering any questions you may have.