STATEMENT OF

KENNETH L. WAINSTEIN
PARTNER, CADWALADER, WICKERSHAM & TAFT LLP

BEFORE THE

COMMITTEE ON THE JUDICIARY
SUBCOMMITTEE ON CRIME AND TERRORISM
UNITED STATES SENATE

CONCERNING

THE MODUS OPERANDI AND TOOLBOX OF RUSSIA AND OTHER AUTOCRACIES FOR UNDERMINING DEMOCRACIES THROUGHOUT THE WORLD

PRESENTED ON

MARCH 15, 2017

STATEMENT OF

KENNETH L. WAINSTEIN
PARTNER, CADWALADER, WICKERSHAM & TAFT LLP

CONCERNING

THE MODUS OPERANDI AND TOOLBOX OF RUSSIA AND OTHER AUTOCRACIES FOR UNDERMINING DEMOCRACIES THROUGHOUT THE WORLD

BEFORE THE

COMMITTEE ON THE JUDICIARY
SUBCOMMITTEE ON CRIME AND TERRORISM
UNITED STATES SENATE

MARCH 15, 2017

Chairman Graham, Ranking Member Whitehouse and distinguished Members of the Subcommittee, thank you for the invitation to appear before you today. My name is Ken Wainstein, and I'm a partner at the law firm of Cadwalader, Wickersham & Taft. It is an honor to be here with my distinguished fellow panelists to discuss our government's capacity to meet a fundamental and growing threat to democracy around the world.

I. INTRODUCTION

I applaud the Subcommittee for calling a hearing that addresses the threat from Russia and other autocracies that undertake to interfere with the electoral processes of other countries and undermine democracy. You are doing a real service by having this hearing, as much of the news coverage and political controversy about last fall's election has actually served to obscure the most important lesson from this episode – which is that we are facing a serious and growing threat to the viability of democratic institutions around the globe.

As my fellow panelists eloquently testify, this subversive threat is real and has already manifested itself in various countries over the past decade, including:

- In the nations of Central and Eastern Europe, where, as CSIS has clearly described in its report The Kremlin Playbook, the Russian government has undertaken a campaign to corrode both those countries' democratic institutions and the political, cultural and economic ties they have developed with the West in the years since the Cold War, all in an effort to pull those states back under the Russian sphere of influence;

- In Estonia, where Russia-linked botnets and other computers engaged in a weeks-long distributed denial of service ("DDOS") attack against government, banking and news media web servers in response to Estonian efforts to distance their country from the Russian sphere of influence;

- In the Russian conflict with Georgia in 2008, where the Russians issued reports that the Georgians were engaging in genocide against South Ossetians as a means of justifying their invasion and undermining international support for Georgia; and

- Here in the United States, where the Intelligence Community assessed that elements of the Russian government directed a campaign against our political system in 2016 that 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.

As the Intelligence Community assessed in its report, the influence efforts of 2016 represent 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. They also represent a threat that will grow in severity as advances in technology and technological know-how continue to strengthen the hand of those who want to undermine Western society.

Finally, they represent the type of efforts we can expect to increasingly see from hostile governments other than Russia. Other countries have already engaged in analogous influence efforts, such as North Korea's launch of a cyber attack on Sony Pictures in retaliation for Sony's production of a movie lampooning supreme leader Kim Jong Un and Iran's sustained DDOS attack against 46 U.S. financial institutions in response to the imposition of economic sanctions by the United States and Europe. With Russia's perceived success in roiling the 2016 election campaign, these and other hostile countries will likely be emboldened to ramp up their own such efforts in future elections.

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, it has the 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 fall within Mr. Buchanan's expertise.

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 their political interference efforts. A number of criminal violations could apply to covert state-actor attempts to influence or subvert U.S. policies and/or elections, 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 state or entity without registering as a foreign agent. The government also can bring cases under 18 U.S.C. § 951, which allows the prosecution of agents of foreign governments working in a non-diplomatic and non-official capacity if they do not register 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 is often very difficult to identify and attribute criminal conduct to specific individuals who can be named and charged, especially where the violative conduct took place over the Internet. 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, the President then promptly designated as subject to sanctions 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. Given the failure of existing sanctions to rein in Russian adventurism in Ukraine, it is hard to predict whether these new sanctions will have an 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. A recent example was President Obama's decision to eject 35 suspected Russian intelligence operatives and to close two official Russian facilities simultaneous with the imposition of sanctions last December. 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 often happened between the Soviet Union and the United States during the Cold War.

The United States should also continue its efforts to assist those allies that are working to combat efforts by other countries to influence or disrupt their internal political processes. A good example was the passage of the Countering Disinformation and Propaganda Act last December, which provides support for the State Department's Global Engagement Center and its whole-of-government approach to fighting foreign disinformation campaigns.

5. Campaign Finance Laws

While there was relatively little discussion of Russian campaign funding in the 2016 election, it has long been a concern that other countries and their nationals will try to use contributions to influence American elections. 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. Violations of this law may lead to criminal prosecution and the imposition of fines or imprisonment, the most prominent historical example being the prosecutions arising from the investigation into foreign-national campaign contributions that were funneled to the Democratic National Committee and the Clinton-Gore campaign prior to the 1996 presidential election.

With the recent reports that French far-right party presidential candidate Marine Le Pen has received funding from Russia in part as a reward for her supporting Russia's actions in Crimea, there is heightened concern that Russia may make similar attempts to sway American politics with targeted campaign contributions. It is critical that we effectively enforce the campaign finance laws that would prevent this type of financial influence by foreign actors.

6. Protection of Electoral Systems

Although the Intelligence Community report issued this January 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 over half the 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. I expect these providers would be equally willing to assist the effort to protect our democratic processes and that the U.S. government is actively engaging with them to that end.

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, it would be wise to consider any recommendations for strengthening or augmenting these

capabilities. I would like to highlight three recommendations – two specific additional authorities and one general approach for combating foreign influence campaigns – that are now being discussed in the aftermath of the 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 or geopolitical 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 seven 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 they seek that authority again, 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 the Use of Countermeasures under International Law

In addition to these two specific recommendations, it is also worth considering the deterrence that is available under the concept of "countermeasures" under international law. Countermeasures are actions deemed unlawful under international law 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 whether Russia's activities in 2016 would or would not justify the use of such countermeasures under international law. 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 many 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 summary suggests, we do have certain tools and capabilities that can be effective in countering the threat of foreign interference in our political system. The real question for today, however, is not whether we have the capability to meet the threat, but rather, whether we have the single-minded focus and will to do so.

All too often, we as a country have failed to mobilize quickly enough in the face of a looming threat. We saw Al Qaeda strengthening and organizing itself, but did not get truly serious about fighting international terrorism until after the 9/11 attacks. Then, we saw the growing cyber threat in the 1990's and 2000's, but did not sufficiently respond until cybertheft had reached the point that it was famously characterized as "the greatest transfer of wealth in history."

It is my hope that we will not be late in responding to the threat to our democracy that is brewing today. The Russian interference in our 2016 presidential campaign was a wake-up call for all of us, and it is incumbent on both the Executive and Legislative Branches to respond to that call with a coherent strategy to protect our democratic 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 governments and actors that are trying to undermine our institutions and ideals. As we have heard from my co-panelists today, 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 democratic processes around the world.

I want to thank the Subcommittee 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 for me.