Department of Justice

STATEMENT OF

ADAM S. HICKEY
DEPUTY ASSISTANT ATTORNEY GENERAL
DEPARTMENT OF JUSTICE

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

AT A HEARING ENTITLED

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

PRESENTED

JUNE 12, 2018

Statement of
Adam S. Hickey
Deputy Assistant Attorney General
Department of Justice

Before the
Committee on the Judiciary
United States Senate

At a Hearing Entitled
"Election Interference:
Ensuring Law Enforcement Is Equipped to Target Those Seeking to Do Harm"

June 12, 2018

Good morning, Chairman Grassley, Ranking Member Feinstein, and distinguished Members of the Committee. Thank you for the opportunity to testify on behalf of the Department of Justice concerning our efforts to combat election interference.

The Attorney General identified this issue as a priority when he created a Cyber-Digital Task Force earlier this year and directed it to address "efforts to interfere with our elections," among other threats. That Task Force is expected to submit a report to the Attorney General by the end of this month and will issue a public report in mid-July. The Department appreciates the Committee's interest in making sure that law enforcement has the tools we need to target those who may seek to do us harm by interfering in our elections.

As I describe below, the Department's principal role in combatting election interference is the investigation and prosecution of Federal crimes, but our investigations can yield more than criminal charges to protect national security. Foreign influence efforts extend beyond efforts to interfere with elections, and they require more than law enforcement responses alone. I will cover three areas in my testimony today. First, I will describe what we mean by the term "foreign influence operations" and provide examples of operations we have observed in the past. Second, I will discuss how the Department has categorized recent foreign influence operations targeting our elections. Third, and finally, I will explain how the Department is responding to those operations and how our efforts fit within the "whole of society" approach that is necessary to defeat foreign influence operations.

I. Background on Foreign Influence Operations

Foreign influence operations include covert actions by foreign governments intended to affect U.S. political sentiment and public discourse, sow divisions in our society, or undermine confidence in our democratic institutions to achieve strategic geopolitical objectives.[1]

Foreign influence operations aimed at the United States are not a new problem. These efforts have taken many forms across the decades, from funding newspapers and forging internal government communications, to more recently creating and operating false U.S. personas on Internet sites designed to attract U.S. audiences and spread divisive messages. The nature of the problem, however — and how the U.S. government must combat it — are changing as advances in technology allow foreign actors to reach unprecedented numbers of Americans covertly and without setting foot on U.S. soil. Fabricated news stories and sensational headlines like those sometimes found on social media platforms are just the latest iteration of a practice foreign adversaries have long employed in an effort to discredit and undermine individuals or organizations in the United States.

Although the tactics have evolved, the goals of these activities remain the same: to spread disinformation and to sow discord on a mass scale in order to weaken the U.S. democratic process, and ultimately to undermine the appeal of democracy itself.

As one deliberate component of this strategy, foreign influence operations have targeted U.S. elections. Indeed, elections are a particularly attractive target for foreign influence campaigns because they provide an opportunity to undermine confidence in a core element of our democracy: the process by which we select our leaders. As explained in the January 2017 report by the Office of the Director of National Intelligence ("ODNI") addressing Russian interference in the 2016 U.S. presidential election, Russia has had a "longstanding desire to undermine the U.S.-led liberal democratic order," and that nation's recent election-focused "activities demonstrated a significant escalation in directness, level of activity, and scope of effort compared

[1]Foreign influence operations, though not always illegal, can implicate several U.S. Federal criminal statutes, including (but not limited to) 18 U.S.C. § 371 (conspiracy to defraud the United States); 18 U.S.C. § 951 (acting in the United States as an agent of a foreign government without prior notification to the Attorney General); 18 U.S.C. § 1001 (false statements); 18 U.S.C. § 1028A (aggravated identity theft); 18 U.S.C. § 1030 (computer fraud and abuse); 18 U.S.C. §§ 1343, 1344 (wire fraud and bank fraud); 18 U.S.C. § 1519 (destruction of evidence); 18 U.S.C. § 1546 (visa fraud); 22 U.S.C. § 618 (Foreign Agents Registration Act); and 52 U.S.C. §§ 30109, 30121 (soliciting or making foreign contributions to influence Federal elections, or donations to influence State or local elections).

to previous operations."2 Russia's foreign influence campaign, according to ODNI, "followed a Russian messaging strategy that blends covert intelligence operations — such as cyber activity — with overt efforts by Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users or 'trolls.'"[3]

Although foreign influence operations did not begin and will not end with the 2016 election, the operations we saw in 2016 represent a significant escalation in the directness, level of activity, and scope of efforts aimed at the United States and our democracy, based in large part on the utility of the Internet for conducting these operations. They require a strong response.

II. Types of Foreign Influence Operations

In advance of the 2018 mid-term elections, the Department is mindful of ODNI's assessment that Russia, and possibly other adversaries, likely will seek to interfere in the 2018 midterm elections through influence operations.[4] Such operations could include a broad spectrum of activity, which we categorize as follows. Importantly, these categories are just a way to conceptualize the types of foreign influence activity our adversaries *might* engage in; they are not an indication that foreign governments actually have engaged in each described category of activity.

---

[2]Office of the Director of National Intelligence, Assessing Russian Activities and Intentions in Recent U.S. Elections, at ii (Jan. 2017) ("ODNI Report"), available at: https://www.dni.gov/files/documents/ICA_2017_01.pdf (last accessed May 31, 2018).

[3]ODNI Report at 2; *see also* U.S. House of Representatives Permanent Select Committee on Intelligence, Report on Russian Active Measures, at viii (March 2018) ("In 2015, Russia began engaging in a covert influence campaign aimed at the U.S. presidential election. The Russian government, at the direction of Vladimir Putin, sought to sow discord in American society and undermine our faith in the democratic process."), available at: https://intelligence.house.gov/uploadedfiles/final_russia_investigation_report.pdf (last accessed May 31, 2018); U.S. Senate Select Committee on Intelligence, Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations, at 1 (May 2018) ("In 2016, cyber actors affiliated with the Russian Government conducted an unprecedented, coordinated cyber campaign against state election infrastructure . . . This activity was part of a larger campaign to prepare to undermine confidence in the voting process. The Committee has not seen any evidence that vote tallies were manipulated or that voter registration information was deleted or modified."), available at: https://www.burr.senate.gov/imo/media/doc/RussRptInstlmt1-%20ElecSec%20Findings,Recs2.pdf (last accessed May 31, 2018).

[4]*Worldwide Threats: Hearing before the Senate Select Comm. On Intelligence*, 115TH CONG. (Feb. 3, 2018) (statement of Daniel Coats, Director of National Intelligence; Admiral Michael Rogers, National Security Agency Director; and Lieutenant General Robert Ashley, Defense Intelligence Agency Director).

1. ***Cyber operations targeting election infrastructure***. Such operations could seek to undermine the integrity or availability of election-related data. For example, adversaries could employ cyber-enabled or other means to target election infrastructure, such as voter registration databases and voting machines. Operations aimed at removing otherwise eligible voters from the rolls or attempting to manipulate the results of an election (or even just disinformation suggesting that such manipulation has occurred) could undermine the integrity and legitimacy of elections, as well as public confidence in election results. To our knowledge, no foreign government has succeeded in perpetrating ballot fraud,[5] but raising even the doubt that it has occurred could be damaging.

2. ***Cyber operations targeting political organizations, campaigns, and public officials.*** These operations could seek to compromise the confidentiality of private information of the targeted groups or individuals, as well as its integrity. For example, adversaries could conduct cyber or other operations against U.S. political organizations and campaigns to steal confidential information and use that information, or alterations thereof, to discredit or embarrass candidates, undermine political organizations, or impugn the integrity of public officials.

3. ***Covert influence operations to assist or harm political organizations, campaigns, and public officials.*** For example, adversaries could conduct covert influence operations to provide assistance that is prohibited from foreign sources to political organizations, campaigns, and government officials. These intelligence operations might involve covert offers of financial, logistical, or other campaign support to, or covert attempts to influence the policies or positions of, unwitting politicians, party leaders, campaign officials, or even the public.

4. ***Covert influence operations, including disinformation operations, to influence public opinion and sow division***. Using false U.S. personas, adversaries could covertly create and operate social media pages and other forums designed to attract U.S. audiences and spread disinformation, or divisive messages. These messages need not relate directly to campaigns. They may seek to depress voter turnout among particular groups, encourage third-party voting, or convince the public of widespread voter fraud in order to undermine confidence in election results.

5. ***Overt influence efforts, such as the use of foreign media outlets or other organizations to influence policymakers and the public***. For example, adversaries could use state-owned or state-influenced media outlets to reach U.S. policymakers or the public. Governments can disguise these outlets as independent, while using them to promote divisive narratives and political objectives.

---

[5]"The term "ballot fraud" in this context includes fraud in the processes by which voters are registered or by which votes are cast or tabulated.

III. The Department of Justice's Role in Addressing Foreign Influence Operations

The Department of Justice has a significant role in investigating and disrupting foreign government activity inside the United States that threatens U.S. national security. With both law enforcement and intelligence authorities, the Federal Bureau of Investigation ("FBI") is the lead Federal agency responsible for investigating foreign influence operations, and the Department's prosecutors are responsible for charging and prosecuting any Federal crimes committed during a foreign influence operation. The FBI has established the Foreign Influence Task Force ("FITF") to identify and combat foreign influence operations targeting U.S. democratic institutions, with focus on the U.S. electoral process and the 2018 and 2020 elections. Through our own authorities and in close coordination with our partner Departments and agencies, the Department can act against threats posed by foreign influence operations in several ways.

First, as an intelligence-driven organization and member of the Intelligence Community ("IC"), the FBI can pursue tips and leads, including from classified information, to investigate illegal foreign influence activities and, in coordination with the IC and the Department of Homeland Security, share information from those investigations with State and local election officials, political organizations, and others to help them detect, prevent, and respond to computer hacking, espionage, and other criminal activities.

Second, through the FITF, the Department maintains strategic relationships with social media providers, who bear the primary responsibility for securing their own products, platforms, and services from this threat. By sharing information with them, the FBI can help providers with their own initiatives to track foreign influence activity and to enforce terms of service that prohibit the use of their platforms for such activities. (This approach is similar to the Department's approach in working with social media providers to address terrorists' use of social media.)

Third, the Department's investigations may expose conduct that warrants criminal charges. Criminal charges are a basic tool the Department uses to pursue justice and deter similar conduct in the future. We work with other nations to obtain custody of foreign defendants whenever possible, and those who seek to avoid justice in U.S. courts will find their freedom of travel significantly restricted. Criminal charges also provide the public with information about the activities of foreign actors we seek to hold accountable and raise awareness of the threats we face.

Fourth, the Department's investigations can support the actions of other U.S. government agencies using diplomatic, intelligence, military, and economic tools. For example, in several recent cases, the Secretary of the Treasury has imposed financial sanctions on defendants abroad under executive orders that authorize the imposition of sanctions for malicious cyber-enabled activity. (*See* E.O. 13694 (Apr. 1, 2015), *as amended by* E.O. 13757 (Dec. 29, 2016).) Treasury's action blocked all property and interests in property of the designated persons subject

to U.S. jurisdiction and prohibited U.S. persons from engaging in transactions with the sanctioned individuals.

Finally, in appropriate cases, information gathered during our investigations can be used — either by the Department or in coordination with our U.S. government partners — to alert victims, other affected individuals, and the public to foreign influence activities. Exposure of foreign influence operations ultimately may be one of the best ways to counter them. Victim notifications, defensive counterintelligence briefings, and public safety announcements are traditional Department activities, but they must be conducted with particular sensitivity in the context of elections, to avoid even the appearance of partiality.

In taking these actions, we are alert to ways in which current law may benefit from reform. By providing ready access to the American public and policymakers from abroad, the Internet makes it easier for foreign governments to evade restrictions on undeclared domestic activities and mask their identities while reaching an intended audience. We welcome the opportunity to work with Congress to combat foreign influence operations, including those aimed at our elections, by clarifying or expanding our laws to provide new tools or sharpen existing ones, if appropriate.

IV. Conclusion

The nature of foreign influence operations will continue to change as technology and our foreign adversaries' tactics continue to change. Our adversaries will persist in seeking to exploit the diversity and richness of today's information space, and the tactics and technology they employ will continue to evolve.

The Department plays an important role in combating foreign efforts to interfere in our elections. At the same time, it cannot and should not attempt to address the problem alone. There are limits to the Department's role — and the role of the U.S. government more broadly — in addressing foreign influence operations aimed at sowing discord and undermining our institutions. Combating foreign influence operations requires a "whole of society" approach that relies on coordinated actions by Federal, State, and local government agencies; support from the private sector; and the active engagement of an informed public.

* * *

I want to thank the Committee again for providing me this opportunity to discuss these important issues on behalf of the Department. We look forward to continuing to work with Congress to improve our ability to respond to this threat. I am happy to answer any questions you may have.