Department of Justice

STATEMENT OF

ADAM S. HICKEY
DEPUTY ASSISTANT ATTORNEY GENERAL
DEPARTMENT OF JUSTICE

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY
COMMMITTEE ON OVERSIGHT AND REFORM
U.S. HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED

"SECURING U.S. ELECTION INFRASTRUCTURE AND PROTECTING POLITICAL DISCOURSE"

PRESENTED

MAY 22, 2019

STATEMENT OF
ADAM S. HICKEY
DEPUTY ASSISTANT ATTORNEY GENERAL
DEPARTMENT OF JUSTICE

BEFORE THE
SUBCOMMITTEE ON NATIONAL SECURITY
COMMITTEE ON OVERSIGHT AND REFORM
U.S. HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED
"SECURING U.S. ELECTION INFRASTRUCTURE AND PROTECTING POLITICAL DISCOURSE "

MAY 22, 2019

Good afternoon, Chairman Lynch, Ranking Member Hice, and distinguished Members of the Subcommittee. Thank you for the opportunity to testify on behalf of the Department of Justice concerning our efforts to ensure the safety and security of our nation's election infrastructure and to combat malign foreign influence.

Protecting our Nation's democratic processes, including our elections, is among the Department's top priorities, and malign foreign influence operations targeting those processes are among the most pressing threats our Nation faces. The Department appreciates the Subcommittee's interest in making sure that we have 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. Malign 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 "malign foreign influence operations" and provide examples of operations we have observed in the past. Second, I will discuss how the Department has categorized recent malign foreign influence operations targeting our elections. Third, 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 malign foreign influence operations.

I. Background on Malign Foreign Influence Operations

For these purposes, malign 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 objectives.

Malign foreign influence operations aimed at the United States are not a new problem. These efforts have taken many forms across the decades, from covertly 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, malign foreign influence operations have targeted U.S. elections. Indeed, elections are a particularly attractive target for malign 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 to previous operations."[1] Russia's malign 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.'"[2]

Russia's malign foreign influence campaign did not end with the 2016 election. On the eve of the 2018 midterm election, ODNI, the Department of Homeland Security, the Department of Justice, and the Federal Bureau of Investigation ("FBI") informed the public: "Americans should be aware that foreign actors — and Russia in particular — continue to try to influence public sentiment and voter perceptions through actions intended to sow discord. They can do this by spreading false information about political processes and candidates, lying about their own interference activities, disseminating propaganda on social media, and through other

[1] 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 14, 2019).

[2] ODNI Report at 2.

tactics."[3] After the election, the Director of National Intelligence confirmed: "Russia, and other foreign countries, including China and Iran, conducted influence activities and messaging campaigns targeted at the United States to promote their strategic interests."[4]

Malign foreign influence operations are not limited to elections and voter perceptions. They also attempt to influence public policy, including by leveraging businessmen, exploiting credible surrogates like law firms, using media organizations, and targeting student organizations and funding on our college campuses. China, in particular, has been working to influence American public opinion in its favor. As the Vice President said last fall, quoting the Intelligence Community ("IC"): "China is targeting U.S. state and local governments and officials to exploit any divisions between federal and local levels on policy. It's using wedge issues, like trade tariffs, to advance Beijing's political influence."[5] The Department remains "concerned that Beijing may use its economic leverage over businesses to covertly influence American policy, may covertly influence student groups on campus to monitor or retaliate against fellow students, or may exercise undisclosed control over media organizations in the United States."[6] Malign foreign influence operations, from any adversary, require a strong response.

II. Types of Foreign Influence Operations

To help identify how the Department can more effectively accomplish its mission in this vital and evolving area, the Department recently drafted an analysis of the types of foreign influences that can target democratic and electoral processes as well as the Department's responses to counter them. That analysis is included in the first chapter of the Report of the

---

[3] Joint Statement on Election Day Preparations (Nov. 5, 2018), available at: https://www.dhs.gov/cisa/news/2018/11/05/joint-statement-election-day-preparations (last accessed May 14, 2019).

[4] Daniel R. Coats, Director of National Intelligence, Statement on the Intelligence Community's Response to Executive Order 13848 on Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election (Dec. 21, 2018), available at: https://www.dni.gov/index.php/newsroom/press-releases/item/1933-dni-coats-statement-on-the-intelligence-community-s-response-to-executive-order-13848-on-imposing-certain-sanctions-in-the-event-of-foreign-interference-in-a-united-states-election (last accessed May 14, 2019).

[5] Vice President Mike Pence's Remarks on the Administration's Policy Towards China (Oct. 4, 2018), available at: https://www.hudson.org/events/1610-vice-president-mike-pence-s-remarks-on-the-administration-s-policy-towards-china102018 (last accessed May 14, 2019).

[6] *China's Non-Traditional Espionage Against The United States: The Threat And Potential Policy Responses: Hearing before the Senate Judiciary Committee* (Dec. 12, 2018) (statement of John C. Demers, Assistant Attorney General for National Security), available at: https://www.judiciary.senate.gov/imo/media/doc/12-12-18%20Demers%20Testimony.pdf (last accessed May 14, 2019).

Attorney General's Cyber-Digital Task Force, released last summer.[7] It includes a framework for categorizing the types of foreign influence activity our adversaries could engage in:

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,[8] 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.

---

[7] Countering Malign Foreign Influence Operations, in Report of the Attorney General's Cyber-Digital Task Force, at 1-21 (July 2, 2018), available at: https://www.justice.gov/ag/page/file/1076696/download (last accessed May 14, 2019).

[8] "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.

Governments can disguise these outlets as independent, while using them to promote divisive narratives and political objectives.

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

The Department of Justice, including the FBI, has a significant role in investigating and disrupting foreign government activity inside the United States that threatens U.S. national security. Through our own authorities and in close coordination with our partner Departments and agencies, the Department can act against threats posed by malign foreign influence operations in several ways.

First, as an intelligence-driven organization and member of the IC, the FBI can pursue tips and leads, including from classified information, to identify, investigate, and disrupt illegal foreign influence activities. With both law enforcement and intelligence authorities, the FBI is the lead Federal agency responsible for investigating foreign influence operations. The FBI has established the Foreign Influence Task Force ("FITF") as its central coordinating authority to identify and combat malign foreign influence operations targeting U.S. democratic institutions. Integrating FBI personnel, resources, and expertise across the agency, the FITF targets key foreign influence leaders, enablers, and actors and seeks to identify their plans, intentions, and activities to deter, mitigate, and impose consequences on their conduct more effectively. The FBI also works closely with its IC partners, as well as the Department of Homeland Security ("DHS"), to detect and disrupt cyber threats to election infrastructure, including by monitoring real-time election incidents and providing real-time reporting.

Second, the Department assists election officials, other public officials, candidates, and social media companies in hardening their own networks, products, and platforms against malign foreign influence operations. For example, the FBI, DHS, and ODNI have developed joint briefings — both in-person and online — for election officials, other public officials, and candidates. These briefings help increase awareness of foreign adversary intent and capabilities and provide officials and candidates with steps they can undertake to mitigate those threats. The FBI has also developed a "Protected Voices" initiative to mitigate the risk of cyber influence operations targeting U.S. elections, raising awareness among election officials and candidates about the best ways to fend off possible attempts to infiltrate their infrastructure.[9] Moreover, as appropriate and in coordination with DHS and the IC, the FBI shares cybersecurity threat information from its investigations and operations with campaigns and the cybersecurity community writ large to help them detect, prevent, and respond to computer hacking and other criminal activities.

The Department's engagement with social media platforms is a key component of our strategy to harden U.S. targets against malign foreign influence operations. Primarily through the FITF, the Department maintains strategic relationships with social media providers, which are responsible 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

[9] FBI, Protected Voices, available at: https://www.fbi.gov/investigate/counterintelligence/foreign-influence/protected-voices (last visited May 14, 2019).

malign foreign influence activity, to enforce terms of service that prohibit the use of their platforms for such activities, and to refer identified malign foreign influence operations back to the FBI. (This approach is similar to the Department's approach in working with social media providers to address terrorists' use of social media.) For example, on the eve of the 2018 midterm election, Facebook posted information noting that "US law enforcement contacted us about online activity that they recently discovered and which they believe may be linked to foreign entities" and that Facebook's ensuing investigation identified more than 100 accounts to block and investigate.[10] Twitter has also credited federal agencies and law enforcement for assisting its efforts to protect the integrity of its platform leading up to the 2018 midterm elections.[11]

Third, the Department identifies and exposes foreign influence operations through the National Security Division's enforcement of the Foreign Agents Registration Act, 22 U.S.C. § 611 *et seq*. ("FARA"). FARA helps to ensure transparency in the activities of foreign entities and individuals, and makes it more difficult for those entities and individuals to hide their role in activities occurring in the United States. It requires persons who engage in certain conduct as agents of foreign principals to register with DOJ and to file periodic reports thereafter. The filings must disclose all aspects of the agent's relationship with the foreign principal, including activities by the agent within the United States on behalf of the foreign principal. FARA's purpose is to ensure that the American public and our lawmakers know the source of information that is provided at the behest of a foreign principal, where that information may be intended to influence U.S. public opinion, policy, and laws. The statute enhances the public's and the government's ability to evaluate such information.

While the Department has always enforced FARA, we have recently stepped up enforcement efforts, including by educating prosecutors nationwide about the importance of the statute, expanding our outreach to individuals and entities who may be obligated to register, and raising public awareness. Those efforts also include the use of civil enforcement actions, which the Department successfully utilized for the first time since 1991 to obtain a court order that requires the registration of a U.S. agent of a Russian state-owned media enterprise. The Department's efforts have resulted in the registrations of multiple foreign-media entities that had not fulfilled their FARA obligations, including the U.S. agents of Russian state-funded media networks RT and Sputnik and of China's state-controlled television network, CGTN. Increased FARA enforcement is also a critical prong of the Department's China Initiative. Under the Initiative, the Department educates American colleges and universities about potential threats to academic freedom and open discourse from covert Chinese malign influence efforts, raises awareness among the business community that acting as an agent of the Chinese government could trigger obligations to register under FARA, and continues to evaluate whether foreign

[10] Facebook, Election Update (Nov. 5, 2018), available at: https://newsroom.fb.com/news/2018/11/election-update (last visited May 14, 2019).

[11] Twitter, 2018 US midterm elections review (Jan. 31, 2019), available at: https://blog.twitter.com/en_us/topics/company/2019/18_midterm_review.html (last visited May 14, 2019).

media organizations operating under the editorial direction or control of a foreign government are complying with FARA.

Fourth, the Department's investigations may expose conduct that warrants criminal charges. Foreign influence operations, though not always illegal, can implicate several U.S. Federal criminal statutes. For example, FARA includes a criminal penalty for willful violations, 22 U.S.C. § 618, and the Federal Election Campaign Act criminalizes soliciting or making foreign contributions, donations, or expenditures to any candidate or political party in the United States, 52 U.S.C. §§ 30109, 30121.[12] Criminal charges uphold the Constitution's prescription that the President "shall take care that the laws be faithfully executed," U.S. Const. art. II, § 3, 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.

For example, in July 2018, a Russian national named Maria Butina was charged with conspiracy to act as a Russian agent within the United States for taking direction from the Russian government to develop backchannels of communication with Americans in an effort to influence them for Russia's eventual advantage.[13] She pleaded guilty and, last month, was sentenced to 18 months in prison.[14] And in September 2018, the Department filed a criminal complaint against Elan Alekseevna Khusyaynova, who is alleged to have been the chief accountant for the Internet Research Agency's Project Lakhta, a Russian malign influence

[12] Other statutes that the Department may use to prosecute unlawful foreign influence operations include, but are 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); and 18 U.S.C. § 1546 (visa fraud).

[13] *See* Department of Justice, Russian National Charged in Conspiracy to Act as an Agent of the Russian Federation Within the United States (July 16, 2018), available at: https://www.justice.gov/opa/pr/russian-national-charged-conspiracy-act-agent-russian-federation-within-united-states (last accessed May 14, 2019).

[14] *See* Department of Justice, Russian National Sentenced to 18 Months in Prison for Conspiring to Act As an Agent of the Russian Federation within the United States (Apr. 26, 2019), available at: https://www.justice.gov/opa/pr/russian-national-sentenced-18-months-prison-conspiring-act-agent-russian-federation-within (last accessed May 14, 2019).

operation that included efforts to influence the 2018 midterm election.[15] The complaint alleged that the operation's goal was to sow division and discord in the U.S. political system, including by influencing the 2018 midterm election through "information warfare against the United States" conducted through fictitious U.S. personas on social media platforms and other Internet-based media. Over the last two years, the Department has brought several other cases against Russian actors exposing malign influence activities.[16]

Fifth, 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.[17] 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. Most recently, the Department worked with ODNI, DHS, and

---

[15] *See* Department of Justice, Russian National Charged with Interfering in U.S. Political System (Oct. 19, 2018), available at: https://www.justice.gov/usao-edva/pr/russian-national-charged-interfering-us-political-system (last accessed May 14, 2019).

[16] In February 2018, 13 Russian nationals and three Russian companies, including the Internet Research Agency and its alleged financier Yevgeny Prigozhin, were indicted on conspiracy charges related to a Russian malign influence effort designed to interfere with the 2016 election. *See* Department of Justice, Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System (Feb. 16, 2018), available at: https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere (last accessed May 14, 2019). In July 2018, 12 Russian officials of the Main Intelligence Directorate of the General Staff ("GRU") were indicted on charges related to the hacking and leaking of emails as part of the Russian effort to interfere in the 2016 election. *See* Department of Justice, Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election (July 13, 2018) https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election (last accessed May 14, 2019).

The Department's efforts in this regard are not limited to malign influence activities targeting elections. In October 2018, seven Russian officers in the GRU were indicted on computer hacking and other charges related to a Russian malign influence effort designed to undermine, retaliate against, and otherwise delegitimize the efforts of international anti-doping organizations and officials who had publicly exposed a Russian state-sponsored athlete doping program and to damage the reputations of athletes around the world. *See* Department of Justice, U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations (Oct. 4, 2018), available at: https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and (last accessed May 14, 2019).

[17] Executive Order 13694 (Apr. 1, 2015), as amended by Executive Order 13757 (Dec. 29, 2016).

other Federal partners to carry out its responsibilities under Executive Order 13848, *Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election* (Sept. 12, 2018). Pursuant to that Executive Order, the FBI provided information to support ODNI's classified assessment to the President of any information indicating that a foreign government, or any person acting as an agent of or on behalf of a foreign government, acted with the intent or purpose of interfering in the 2018 midterm election. Subsequently, on February 4, 2019, the Departments of Justice and Homeland Security submitted their own classified joint report to the President evaluating the impact of foreign activities identified in ODNI's assessment on the security or integrity of election infrastructure or the infrastructure of political organizations, campaigns, or candidates used in the 2018 midterm election. Thereafter, those Departments issued a joint public statement summarizing the classified report's conclusion, to wit, that there is no evidence to date that any identified foreign activities had a material impact on infrastructure used in the 2018 midterm election.

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 targets, other affected individuals, and the public to malign foreign influence activities. 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 foreign influence and elections. In many circumstances, exposing foreign interference operations can be an important means of rendering them less effective and maintaining confidence in our democratic processes and institutions. In some circumstances, however, exposure can be counterproductive or otherwise imprudent, for example, if it may amplify an operation or create undue public alarm, harm, or confusion. Given the countervailing considerations, the Department has adopted a policy for evaluating whether to disclose malign foreign influence activities.[18] The policy recognizes that exposing such activity may play an important role in mitigating the effect of malign foreign influence efforts, provides relevant factors for consideration, and requires that partisan political considerations must play no role in efforts to disclose malign foreign influence activities.

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 activities in the United States and mask their identities while reaching an intended audience. We welcome the opportunity to work with Congress to combat malign 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.

[18] *See* Justice Manual 9-90.730 (Sept. 2018), *adopting* DOJ Policy on Disclosure of Foreign Influence Operations, in *Report of the Attorney General's Cyber-Digital Task Force*, pp. 16-17 & nn.18-20 (July 2, 2018), available at: https://www.justice.gov/ag/page/file/1076696/download (last accessed May 14, 2019).

IV. Conclusion

The nature of malign 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 malign foreign influence operations aimed at sowing discord and undermining our institutions. Combating malign 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 Subcommittee 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.