OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
FROM THE OFFICE OF STRATEGIC COMMUNICATIONS

Avril Haines, Director of National Intelligence
Senate Select Committee on Intelligence
May 15, 2024

Chairman Warner, Vice Chairman Rubio, Members of the Committee, I appreciate having the opportunity to brief you on the intelligence community's election security work, alongside my colleagues at CISA and FBI, who are leading efforts to take action to secure our elections alongside the extraordinary state and local officials who are on the frontlines of this work.

The U.S. government's efforts to protect our elections have improved significantly since the 2016 presidential election and even as the threat landscape is becoming increasingly complicated, it is my view that the U.S. government has never been better prepared to address the challenge.

Protecting our democratic processes from foreign influence or interference is an absolute priority for the intelligence community.

Our efforts are effectively organized by the Foreign Malign Influence Center or "FMIC," which houses the Election Threats Executive.

The Election Threats Executive leads, coordinates and integrates the IC's activities, initiatives, and programs in this realm.

Fundamentally, we support the federal government – particularly CISA and the FBI – as they work to secure our elections, as well as state and local election officials across the country who actually manage and secure our election infrastructure on a day-to-day basis.

We do so by ensuring that our resources are aligned to promote collection and analysis so that we're able to identify and mitigate foreign threats to our elections and communicate our assessments to our federal partners, to you in the Congress, to state and local officials, and to the American people.

We also facilitate a notification framework that ensures that when relevant intelligence is collected concerning a foreign influence operation aimed at our election, appropriate notice is given to those who are being targeted so that they can take action.

While most of these notifications are non-public, there are scenarios in which public notifications are appropriate, if doing so would render the foreign influence operation less effective.

Of course, exposing a foreign actor's efforts is only one way in which we counter election threats. We support the law enforcement community as they disrupt election influence operations through legal action, including the disruption of illicit financial networks.

We also support CYBERCOM as it conducts a range of cyber operations to ensure that foreign adversaries cannot use our digital infrastructure to attack our elections.

Using every tool we have is critical, as the challenge is expanding. Over the last several years, we've seen three trends that make the threat landscape more diverse and complex:

First, there are an increasing number of foreign actors, including non-state entities, who are looking to engage in election influence activities;

Second, there are more commercial firms through which state actors are able to conduct election influence activities, often increasing the sophistication of such activities while making it more challenging to track down the original instigator of foreign influence efforts; and

Third, perhaps most obviously, relevant emerging technologies – particularly generative AI and big data analytics – are increasing the threat by enabling the proliferation of influence actors who can conduct targeted campaigns, reducing the cost of relatively sophisticated influence operations and content, and further complicating attribution.

For example, innovations in AI have enabled foreign influence actors to produce seemingly-authentic and tailored messaging more efficiently, at greater scale, and with content adapted for different languages and cultures.

In fact, we have already seen generative AI technology being used in the context of foreign elections.

In September 2023, two days before parliamentary elections in Slovakia, a fake audio recording was released online in which one candidate discussed how to rig the upcoming election with a journalist.

The audio was quickly shown to be a fake with signs of AI manipulation, but under Slovakia law, there is a moratorium on campaigning and media commentary about the election for 48 hours before polls open. Since the deepfake was released in that window, news and government organizations struggled to expose the manipulation. The victim of the deepfake ended up losing in a close election.

To position the IC to address generative-AI enabled foreign influence efforts we have an IC group focused on multimedia authentication that leverages DARPA's Semantic Forensics technology, among other tools, and enables those in the IC who are working on election security to rapidly access media forensic expertise to facilitate the authentication of foreign suspect media related to U.S. elections.

Members of this group regularly engage technical experts inside and outside government to ensure we are applying the latest techniques. If state and local officials have concerns, for example, about media that is suspected to be synthetic or manipulated and violates a law or is tied to a foreign actor, they can request authentication assistance through the FBI.

Of course, the most significant foreign actors who engage in foreign influence activity directed at the United States in relation to our elections are Russia, the People's Republic of China, and Iran.

Specifically, Russia remains the most active foreign threat to our elections. The Russian government's goals in such influence operations tend to include eroding trust in U.S. democratic institutions, exacerbating sociopolitical divisions in the United States, and degrading Western support to Ukraine.

Russia relies on a vast multi-media influence apparatus, which consists of its intelligence services, cyber actors, state media, proxies, and social media trolls.

Moscow most likely views such operations as a means to tear down the United States as its perceived primary adversary, enabling Russia to promote itself as a great power, whereas Beijing seeks to promote support for China's policy positions and perspectives, including in the context of specific elections; portray the U.S. democratic model as chaotic, ineffective, and unrepresentative; and magnify U.S. societal divisions.

The PRC also has a sophisticated influence apparatus through which they leverage emerging technologies, including generative AI, and they are growing increasingly confident in their ability to influence elections globally but remain concerned about possible blowback in the event their efforts are disclosed.

In fact, in 2020, we assessed that China did not deploy influence efforts intended to change the outcome of the U.S. presidential election, principally because of concerns regarding the blowback if caught. Thus far, we have no information to suggest that the PRC will take a more active role in this Presidential election than it did in 2020, even as they continue to engage in efforts to promote politicians at all levels who are taking positions favorable to China on key issues. Needless to say, we will continue to monitor their activities.

Finally, Iran is becoming increasingly aggressive in their efforts, seeking to stoke discord and undermine confidence in our democratic institutions, as we have seen them do in prior election cycles. They continue to adapt their cyber and influence activities, using social media platforms, issuing threats, and disseminating disinformation. It is likely they will continue to rely on their intelligence services in these efforts and Iran-based online influencers to promote their narratives.

We have also observed other countries attempt to support or undermine specific candidates but these efforts tend to be on a smaller scale. For instance, some other countries do things like direct campaign contributions to candidates they believe would promote their interests if elected and seek to obscure their support.

In brief, the election threat landscape is increasingly challenging but our capacity to manage the threat has also improved, as you will hear from my colleagues.

There is nothing more important or fundamental to our democracy than protecting our elections and I can tell you that we are focused and ready to do our part.

Thank you for your time and I look forward to your questions.