Foreign Threats to U.S. Elections

Election Security Information Needs

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

Foreign Threats to U.S. Elections: Election Security Information Needs

Foreign intelligence entities likely view U.S. elections as an opportunity to undermine confidence in our democratic institutions and processes, sow divisions in our society, weaken our alliances, and promote their political, economic, or ideological agendas. These entities operate in the seams of our democratic system to advance their interests, using the tools of traditional espionage in combination with cyber operations and influence campaigns. Foreign attempts to interfere with our elections fall into five distinct categories:

1. Cyber operations targeting election infrastructure,
2. Cyber operations targeting political parties, campaigns, and public officials,
3. Covert influence operations to assist or harm political organizations, campaigns, or public officials,
4. Covert influence operations to influence public opinion and sow division,
5. Covert efforts to influence policymakers and the public.

This threat might take many forms, such as spreading disinformation, conducting hack-and-leak operations, or possibly manipulating data in a targeted fashion to influence the elections, and involves a wider range of foreign state and non-state actors than we have seen in the past, to include ideologically motivated entities and foreign cyber criminals.

Also complicating the election landscape is the range of tools available today that can magnify the impact of our adversaries' activities and further obfuscate their origin: nontraditional forms of espionage that do not use professional intelligence officers to acquire information or gain access to critical infrastructure; new sensors and surveillance technologies; supply chain operations; and, indirectly, foreign direct investments, joint ventures, and mergers and acquisitions of election-related businesses and suppliers that could provide an adversary with access to key systems, networks, and information. As machine learning technology continues to advance, we are particularly concerned about foreign threat actors employing "deep fakes"—the use of technology to create false but convincing image, video, and audio—to augment influence campaigns and erode public confidence in our elections.

Countering the complex and wide-ranging threats expected in these elections must be a core obligation of the entire USG and will require a whole-of-society approach, including support from the private sector and the active engagement of an informed public.

The National Counterintelligence and Security Center is working closely with the Department of Homeland Security (DHS), the ODNI Election Threats Executive, the Federal Bureau of Investigation (FBI), the Election Assistance Commission, and other federal agencies to assess and mitigate the plans and activities of foreign governments to interfere in U.S. elections.

I encourage those who are involved with elections to report to DHS or FBI detailed information regarding indications that foreign actors may be interfering in U.S. elections by providing a brief description of what occurred, what systems and/or processes were affected, what mitigation actions were taken, and the effectiveness of those efforts. Potential foreign adversary activities of particular interest are listed on the following pages as Election Security Information Needs.

William R. Evanina
Director, National Counterintelligence and Security Center

Election Security Information Needs

1. Unauthorized entry or attempts to gain access to facilities used to store election and voting system infrastructure, including those located on public or private property, as well as to polling places and voter centers.

2. Incidents of spear-phishing or attempts to hack voter registration systems, including efforts against seemingly unrelated state or local government entities, such as Departments of Motor Vehicles or civic organizations responsible for registering voters.

3. Attempts to access, alter, or destroy systems used to qualify candidates, produce and deliver ballots, procure, manage, and prepare voting equipment, process requests for absentee ballots, and store and manage election administration processes and procedures.

4. Unauthorized access, or attempts to access, information technology (IT) infrastructure or systems used to manage elections, including systems that count, audit, or display election results and systems used to certify and validate post-election results.

5. Attempts to hack, spear-phish, or compromise personal or professional e-mail accounts and social media accounts of elections officials, staff, and volunteers.

6. Attempts, successful or otherwise, to hack into political parties, campaign organization IT systems, or the personal IT devices of candidates, staffs, or associated consultants and contractors.

7. Attempts to access, hack, alter, or disrupt the infrastructure that receives and processes absentee ballots, such as tabulation centers, web portals, e-mails, or fax machines. Also, any attempts by foreign entities to interfere with votes sent through the U.S. Postal Service.

8. Compromises of networks and/or systems, including hardware and/or software, by cyber actors, including the tactics, techniques, procedures and impact on election-related networks and systems. Also, any evidence of interference detected on state networks or systems, or cyber security indicators of compromise.

9. Instances of any unexplained disruption at polling stations or training locations for voting officials, including early voting locations, which alter voter turnout. Disruptions may include social media posts, text messages, or robocalls falsely reporting closed or changed locations of polling stations, or physical incidents at polling stations, including the distribution of false information there. Other disruptions could include hijacked television broadcasts or manipulated online exit polling data.

10 Foreign adversary disinformation efforts, including on social media or media websites, or other online sources to alter or shut down government web sites, or deliver "deep fake" content in an effort to foment social unrest, influence voter perceptions, decisions, or actions, or alter voter turnout.

11 Unauthorized entry at centralized vote counting or tallying locations, or into electronic systems or networks used by states and localities to count absentee, military, and Election Day voting ballots.

12 Efforts to impact critical infrastructure that would limit access to polling stations, such as power, water, internet, telephone (cellular), and transportation (traffic controls) outages.

13 Suspicious behaviors by foreign members of election observation teams, such as those associated with the Organization for Security Cooperation in Europe (OSCE) observation mission for the 2020 U.S. elections, including probing questions directed at election officials that are outside of the scope of the observer mission.

14 Any indication that adversaries, especially Russia and China, are collecting on or analyzing plans by U.S. states to employ block chain technology in U.S. elections.

15 Direct or indirect attempts, successful or otherwise, by known or suspected foreign entities to lobby or donate to select political candidates, parties, or political action organizations in an effort to shape the outcome of an election, potentially in violation of U.S. campaign finance laws.

16 Direct or indirect efforts by known or suspected foreign entities or foreign-linked entities to discredit or smear the reputation or credibility of a political candidate or party, to include leaking data (real, altered, or fictitious) to embarrass the individual or group targeted.

17 Direct or indirect activities and messaging by U.S.-based foreign proxy organizations to mobilize U.S. voters, to include U.S. businesses and organizations at the local, state, and national level, in support of a particular candidate or political party.

18 Known or suspected foreign efforts to covertly or discretely promote or support fringe U.S. ideological movements and anti-establishment groups to sow societal discord.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE