Mini Simulation

Foreign Cyberattacks and Election Security

Last Updated:
March 14, 2024

Overview

Intelligence shows that foreign actors are already interfering in the 2024 U.S. election. How should the United States respond?

The Situation

Free and fair elections are essential to a functioning democracy. However, ensuring the integrity of U.S. elections is a growing national security challenge. As cyber capabilities become more advanced, foreign actors are increasingly targeting elections around the world through cyberattacks and disinformation campaigns in order to influence results, aggravate social and political tensions, and undermine confidence in democratic processes. Election interference not only threatens U.S. sovereignty but can also sow instability that hinders the government's ability to operate effectively. The U.S. intelligence community has concluded that Russia interfered in the 2016 U.S. presidential election, the 2018 midterm elections, and the 2020 U.S. presidential election by accessing state election systems and voter data, hacking and leaking Democratic National Committee emails, and spreading disinformation on social media. In addition to Russia's interference, China orchestrated election influence activities in the 2022 U.S. midterm elections. It does not appear that hackers directly manipulated any voter data, and it is difficult to know how successful the disinformation campaign was. But foreign interference struck a blow at confidence in U.S. elections. Analysts fear that if policymakers cannot ensure public trust in future elections, even the threat of interference could erode democratic systems and aggravate domestic divisions, weakening national security.

Intelligence agencies and security experts warn that foreign interference may affect the 2024 U.S. presidential election. Possible actors include Russia, China, and Iran. Public reports so far indicate social media accounts from China posting on partisan issues ahead of the 2024 election; Meta has since disabled these accounts. The attacks reported so far may or may not be state-sponsored, and there may be more that are not publicly known. Election interference is expected on multiple fronts. Most directly, foreign actors could launch cyberattacks on U.S. election infrastructure by hacking voting systems to manipulate votes. They could also attack voter registration systems in order to remove certain voters from the rolls, target them for disinformation, or impede their access to the polls. Cyberattacks could target specific campaigns or parties as well in search of damaging information to leak. Furthermore, disinformation campaigns on social media threaten to influence the outcome of an election and exacerbate partisan divisions. Even a small-scale or failed attack on an election would create mistrust in the democratic process. With elections fast approaching, policymakers face a renewed challenge to safeguard U.S. elections against foreign threats and to determine how to respond to actors seeking to interfere in the United States' democracy.

Decision Point

The U.S. intelligence community expects that foreign actors, including Russia and China, have mountedcampaigns to interfere in the upcoming 2024 U.S. election. These are likely multipronged efforts involving disinformation campaigns and cyberattacks on election infrastructure or candidates. If not addressed, these efforts could

undermine U.S. election integrity and damage public trust in democratic systems, potentially for years to come. The National Security Council (NSC) is meeting to advise the president on how the government should safeguard U.S. national elections. Members will need to do contingency planning, deciding which measures to take when foreign influence is detected.

NSC members should consider any combination of the following options:

- *Prepare to employ cyber counterattacks and sanctions against perpetrators.* Offensive measures could safeguard future elections, but they risk diplomatic fallout and may not secure current election systems. Furthermore, attributing cyberattacks to specific countries can be a challenging task.
- *Provide federal funding to bolster election infrastructure and establish a task force* to oversee preelection testing on ballot machines, and provide cybersecurity training and support. This option enhances security but requires significant funds.
- *Take executive action to regulate disinformation on social media and create a public awareness and media literacy campaign to educate voters.* This option would address disinformation but not election infrastructure. In addition, regulations on social media could face criticism for limiting freedom of expression.
- *Maintain current election practices while continuing to monitor and disclose threats.* This option would require the least commitment of resources but may not improve the security of upcoming elections, because even with monitoring, cyberattacks may not be detected.

Elections and Disinformation Are Colliding Like Never Before in 2024 New York Times
China Increased U.S. Election Influence in 2022, Intelligence Report Says New York Times
Election Interference Demands a Collective Defense Foreign Affairs