Congressional Research Service
Informing the legislative debate since 1914

INSIGHT

Election Security: Issues in the 2018 Midterm Elections

August 16, 2018

In the wake of assessments about foreign interference in the 2016 presidential election, concerns have been mounting about the security of the 2018 midterm elections. Security efforts are complicated by the complex, multidimensional election life cycle, with each dimension involving a broad array of components. The main dimensions can be thought of as election administration, campaign activities, and media coverage.

Traditionally, concerns about election security have focused largely on election administration. In the wake of the 2016 election, the Department of Homeland Security designated election-administration infrastructure as a critical infrastructure (CI) subsector. That made the state and local offices and private-sector entities involved in running elections eligible for enhanced federal technical assistance and information sharing on both physical- and cyber-security.

The CI designation expressly applies only to the election-administration dimension. However, malicious actors are unlikely to respect such limitations. The increasing use of internet connectivity in all three dimensions is creating a convergence of security risks not only within the dimensions but across them

- Attacks on election infrastructure might involve registration databases, voting systems, reporting of results, or other components or processes. The goal might be to exfiltrate (surreptitiously obtain) information such as voter files, to disrupt the election process, or even to change vote counts and results.
- Attacks on political parties and campaigns might involve exfiltration of candidate information or communications, disruption of events, or other goals. For example, data from the information networks of a political party could offer a foreign adversary insights into the prospective operations, priorities, and vulnerabilities of an incoming government, should the party prevail at the polls.
- Exploits involving media coverage, especially social media, might include, for example, spreading false or misleading information to voters with the aim of affecting their votes or eroding confidence in the election outcome. Voter information obtained through attacks on political party or government entities, or by other means, could be used to target voters considered susceptible to such misinformation. For example, Cambridge

Congressional Research Service
https://crsreports.congress.gov
IN10955

> Analytica reportedly acquired and used data on more than 50 million Facebook users to influence voters in the 2016 U.S. presidential election and Brexit referendum. Although Facebook maintains that the case did not constitute a data breach, the legality of how such information was and is obtained, as well as its potential impacts, remains controversial. Both House and Senate committees have held hearings on the topic.

Recent events indicate that attempts at interference are continuing in the run-up to the November 2018 midterm elections. For example, on July 31, Facebook revealed that it detected a campaign by "bad actors" that appeared to target those upcoming elections. The campaign used a mix of fake accounts, ads, and pages from both Facebook and Instagram. The company referred to these and previous activities as an "arms race" and vowed to invest in people and technology to address the threats.

Facebook did not attribute the activity to a specific entity but noted similarities to methods that the Russia-based Internet Research Agency (IRA) has been alleged to have employed in an attempt to influence the 2016 presidential election. In that campaign, fake accounts, bots, and trolls sought to further polarize the U.S. population on already divisive social issues, such as race and immigration. In one reported case, IRA agents attempted to organize a rally posing as activists from Black Lives Matter and other organizations. Thirteen Russian nationals said to be working with the IRA were indicted in February 2018 for their attempts to interfere with elections and the political process. Further indictments were issued in July 2018 against 12 other Russian nationals for cyber operations against political party and campaign organizations before the 2016 election.

Such methods and activities are consistent with Russian information warfare doctrine, which involves "a conflict between two or more States in the information space" and employs a mix of propaganda, misinformation, and disinformation to achieve an environment of permanent unrest, chaos, and conflict within an adversary nation state.

Some analysts contend that technical solutions and hardening of potential targets will fail to keep pace with the evolving tactics of such adversaries and that criminal indictments fall short of the level of deterrence that is needed. These analysts suggest that given the success of past efforts and the absence of sufficient deterrence, Russia will continue to pursue election-related information operations. Director of National Intelligence Dan Coats said in February 2018, "there should be no doubt" that Russia sees the 2018 U.S. midterm elections as a target. "We expect Russia to continue using propaganda, social media, false-flag personas, sympathetic spokesmen and other means to influence, to try to build on its wide range of operations and exacerbate social and political fissures in the United States." Facebook did not attribute to Russia the information operations described in its July report. However, it noted that the actors behind the recent activity took greater steps to obscure their identities than in the past, making attribution more difficult.

Other recent media reports have described alleged recent attacks on political campaigns and local election offices. Most public attention has focused on Russian activities, but other potential malefactors, whether foreign or domestic, could use similar methods in attempts to interfere with future elections at various points in the election life cycle.

More than 60 bills introduced in the 115th Congress have provisions related to election security. Most address concerns about the security of election administration, with others focusing on deterring foreign interference. A few have provisions on campaign security. Addressing broader concerns about election interference and security would likely require a whole-of-life-cycle approach to election integrity; that would need to balance meeting legitimate security needs with maintaining protections for free expression and other requirements for proper functioning of the democratic process.

Author Information

Catherine A. Theohary
Specialist in National Security Policy, Cyber and Information Operations

Eric A. Fischer
Senior Specialist in Science and Technology

Disclaimer