The Changing Landscape of U.S. Election Security

Protecting the sanctity of the ballot box against cyberthreats depends on legislation, enforcement, and sharing up-to-date threat intelligence data.

The United States is the longest-lasting federation of self-governing states, each of which operates its own elections for statewide office and oversees those of constituent municipalities. These disparate election systems operate with little standardization and no unified oversight, making them particularly vulnerable in the face of growing cybersecurity threats.

One saving grace of the U.S. election system is that the diversity and separation of election infrastructure across 50 states, plus territories, decrease the chances that a threat actor could be able to conduct a widespread disruption of the election process. To actually disrupt elections on a widespread basis, threat actors or groups would have to deploy significant resources to target hundreds, if not thousands, of municipalities. But it may take only one or two small successes—or even just evidence of actual attempts—for the integrity of elections to be undermined.

Amid growing evidence that foreign-sponsored entities and other threat actors have scanned and probed these electoral systems for vulnerabilities and attempted to sow discord among the electorate—and are continuing to do so—governments at the local, state, and federal level face the threat that emboldened malevolent hackers may attempt to manipulate results or disrupt the voting process.

According to a 2018 U.S. Department of Justice (DoJ) report on national cyberthreats and how it is working to combat them, "Elections are a particularly attractive target for 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."

To ensure that all constituents have confidence that their votes will count, government entities will need to ensure that every citizen has the right to a secure vote. This will take legislation; heightened security measures; and information sharing that provides up-to-date threat intelligence to officeholders, law enforcement agencies, and election systems administrators.

REAL THREATS TO ELECTION SYSTEMS IN THE UNITED STATES

Until the 2016 U.S. presidential election, voter registration and accurate tabulations were the primary issues driving news coverage about the mechanics of counting votes. But just weeks before citizens headed to the polls, reports began circulating that the FBI had issued a flash-alert warning to election officials nationwide that it had "uncovered evidence that foreign hackers penetrated two state election databases."

In July 2018, the Department of Justice's Special Counsel's Office, headed by former FBI Director Robert S. Mueller III, disclosed federal grand jury indictments alleging efforts to interfere in the 2016 U.S. presidential election by a dozen members of a Russian military intelligence agency.

The indictment charges that members of Russia's Main Intelligence Directorate of the General Staff (GRU) conspired "to hack into the computers of U.S. persons and entities responsible for the administration of 2016 U.S. elections, such as state boards of elections, secretaries of state, and U.S. companies that supplied software and other technology related to the administration of U.S. elections." In addition, those agents hacked into the computers of a U.S. vendor "that supplied software used to verify voter registration information for the 2016 U.S. elections."

Those efforts were accompanied by an aggressive disinformation campaign via social media aimed at meddling with the election. This type of disruption is now seen as such a global threat that, in 2017, countries such as the Netherlands, France, and Germany took preemptive steps to prevent interference. In the United States, the threat continues, with leaders of U.S. national security agencies warning in August 2018 that Russia was engaged in a campaign to impact the current Congressional midterm elections.

Cyberattacks, whether mounted by foreign intelligence services or nongovernmental actors, don't have to modify any votes to disrupt elections. "If our adversaries can successfully shake the confidence of the American people in their government, in their processes and institutions, and in the selection of their leaders,

then that is a successful assault on liberal democracy," Susan Hennessey of the Brookings Institution testified to Congress. She warned that "a malicious actor needs only to penetrate systems such that experts and election officials can no longer express sufficient certainty in the integrity of a system or result."

READINESS AT THE STATE AND MUNICIPAL LEVELS

In the United States, each state oversees its own elections, no matter whether citizens are voting for national officeholders, state officials, or municipal officials. The result is a fragmented system with multiple methods of voting—from electronic to mechanical, to paper-based—often overseen by part-time election officials.

In March 2018, Congress appropriated $380 million for improving election infrastructure, but it is being apportioned to states based on a 2002 formula that focuses on population rather than actual risks.

Officials at the state and local levels are taking notice, but not uniformly. "All 50 states have taken at least some steps to provide security in their election administration," the Center for American Progress reported in a comprehensive assessment of efforts at the state level. Nonetheless, "all states have room for improvement," the organization concluded. Among its findings:

- Fourteen states use paperless direct recording electronic (DRE) machines in at least some jurisdictions, whereas five states rely exclusively on DRE machines.
- Postelection audit procedures are unsatisfactory in 33 states, and at least 18 do not legally require postelection audits or require jurisdictions to meet certain criteria before audits may be carried out.
- Thirty-two states allow regular absentee voters and/or U.S. citizens and service members living or stationed abroad to return voted ballots electronically, a practice deemed insecure by election and cybersecurity experts.
- At least 10 states do not provide cybersecurity training to election officials.

DEFENSIVE STARTS AND STOPS

In March 2018, Congress appropriated $380 million for improving election infrastructure, but it is being apportioned to states based on a 2002 formula that focuses on population rather than actual risks.

Despite that budget appropriation, Congress has failed to come up with a consensus approach to address the issue nationally. Efforts to add more funds have failed to pass, and broader, more strategic efforts have not gained the broad partisan support needed for enactment.

The federal executive branch has not articulated an overarching strategy and plan of action to protect election systems. Individual agencies such as the Department of Homeland Security (DHS), DOJ, FBI, and the Department of Defense have taken steps on their own and in task forces to increase awareness of threats and offer advice and services to state and municipal officials. But the elimination of a cybercoordinator from the White House national security staff has added to concerns that the executive branch is "rudderless" when it comes to election cybersecurity.

Meanwhile, state legislators have been trying to plug gaps. The National Conference of State Legislators (NCSL) recaps a dozen laws enacted at the state level, including:

- Requiring adoption of regulations describing best practices for storage and security of voter registration information (California)
- Requiring local officials to report on the status of voting equipment and needs for replacement (Illinois)
- Dedicating funds to secure and monitor facilities where voting systems and electronic poll books are stored (Indiana)
- Establishing a chief information security officer to ensure compliance and coordinate executive branch cybersecurity efforts (Kansas)

FIRST LINE OF DEFENSE: INFORMATION

The dissemination of timely and accurate information is crucial to efforts to combat cyberthreats to election systems and counter misinformation that may undermine citizen belief in the integrity of voting tallies.

Malicious cyberactors frequently share tools and techniques, increasing their agility and precision in circumventing defenses. Collaboration among election officials can be a potent tool in defending against those threats. The most common place to begin collaboration is to share details about observed attacks, any relevant investigative work and analysis performed, and countermeasures taken to minimize the threat. This type of information is known as threat intelligence.

Many states have begun to take advantage of information sharing and analysis centers (ISACs) that provide threat-information-sharing collaboratives and partnerships. In 1988 Presidential Decision Directive/NSC-63 set out the goal of establishing ISACs to foster information sharing across critical infrastructures in the private sector. Subsequent directives have further encouraged information exchanges as well as standardization of ISACs.

Although the DHS is charged with overseeing critical infrastructure plans, it designates Sector-Specific Agencies (SSAs) to structure and manage each sector but has yet to designate an SSA for the elections sector. (The National Association of Secretaries of State says its members oppose the critical infrastructure designation for elections "based on the federal government's continued lack of transparency and clarity with chief state election officials on plans for implementing the designation.")

However, DHS's National Cybersecurity and Communications Integration Center (NCCIC) works with the Multi-State Information Sharing and Analysis Center (MS-ISAC), which was formed in 2003 by the nonprofit Center for Internet Security (CIS). MS-ISAC provides state, local, territorial, and tribal governments with key resources for cyberthreat prevention, protection, response, and recovery, including a 24 x 7 security operation center and incident response services to help election officials deal with attacks and disruptions.

In 2017, out of that MS-ISAC effort, the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) was formed, also under the auspices of the CIS, to support the cybersecurity

needs of the elections subsector. Through the EI-ISAC, election agencies can access an elections-focused cyberdefense suite, including threat intelligence products, incident response and remediation, threat and vulnerability monitoring, cybersecurity awareness and training products, and tools for implementing security best practices.

Also in 2017, the State of Colorado formed the Colorado Threat Intelligence Sharing network (CTIS), in partnership with Anomali, connecting state, county, municipal, and tribal governments to share, analyze, and better respond to threats. A comprehensive threat-sharing and analysis platform provides confidential information in one central location within a trusted circle of fully vetted users.

THREAT INTELLIGENCE TECHNOLOGY

Threat intelligence needs to be shared quickly and with as much context as possible to be effective.

Using sensors placed across the country provides a wealth of information regarding efforts to penetrate election systems and supporting infrastructure.

But there's a lot of threat data to absorb. DHS, through its continuous diagnostics and mitigation (CDM) program, makes available a suite of capabilities and tools—including network sensors—that enable network administrators to know the state of their respective networks at any given time. State, local, and tribal authorities can take advantage of the federal government's cooperative purchasing agreement to acquire pertinent tools. Additionally, DHS cybersecurity agents are available to help governments prepare for—and protect themselves against —cybersecurity threats.

These types of security technologies, along with peer-level information sharing, are crucial to staving off cyberthreats, says Roberto Sanchez, director of Threat Sharing & Analysis at Anomali. Using sensors placed across the country provides a wealth of information regarding efforts to penetrate election systems and supporting infrastructure. With a threat intelligence platform, computers quickly sift through huge volumes of data to provide analysts with actionable intelligence that can be quickly disseminated over networks or through ISAC alerts and forums.

SHORING UP CONFIDENCE

Prior to the Democratic and Republican presidential nomination conventions in 2016, the Gallup organization reported that "a record-low 30% of Americans expressed confidence in the 'honesty of elections'." Without more-rigorous efforts at every level of government, officeholders may be confronted by eroding trust in the sanctity of the ballot box and citizens' confidence in official tallies of their votes.

The fact that these small municipal entities usually end up being responsible for overseeing local election processes, with limited resources for protection, is a glaring weakness. These authorities generally don't have the resources to withstand a significant attack from a well-prepared adversary. Processes for proper testing and auditing voting mechanisms, voter registration, and mail-in or absentee ballots should be carefully developed and followed to ensure that election results are trustworthy and intact.

In the meantime, threat intelligence can help show where different states are, and where they need to be, to ensure the security and resilience of election systems. Enhancing situational awareness and timely dissemination of relevant threats can enable states to implement protective measures to thwart malicious actors and ensure free and fair elections. Ultimately, it's incumbent on election officials to take advantage of every available resource and put that information to work. It is essential to maintain public trust in the U.S. election process.

To learn more about government cybersecurity challenges, visit Anomali.