Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations

May 8, 2018

Overview

In 2016, cyber actors affiliated with the Russian Government conducted an unprecedented, coordinated cyber campaign against state election infrastructure. Russian actors scanned databases for vulnerabilities, attempted intrusions, and in a small number of cases successfully penetrated a voter registration database. This activity was part of a larger campaign to prepare to undermine confidence in the voting process. The Committee has not seen any evidence that vote tallies were manipulated or that voter registration information was deleted or modified.

- The Committee has limited information about whether, and to what extent, state and local officials carried out forensic or other examination of election infrastructure systems in order to confirm whether election-related systems were compromised. It is possible that additional activity occurred and has not yet been uncovered.

Summary of Initial Findings

- Cyber actors affiliated with the Russian government scanned state systems extensively throughout the 2016 election cycle. These cyber actors made attempts to access numerous state election systems, and in a small number of cases accessed voter registration databases.
    - At least 18 states had election systems targeted by Russian-affiliated cyber actors in some fashion.[1] Elements of the IC have varying levels of confidence about three additional states, for a possible total of at least 21. In addition, other states saw suspicious or malicious behavior the IC has been unable to attribute to Russia.
    - Almost all of the states that were targeted observed vulnerability scanning directed at their Secretary of State websites or voter registration infrastructure. Other scans were broader or less specific in their target.
    - In at least six states, the Russian-affiliated cyber actors went beyond scanning and conducted malicious access attempts on voting-related websites.[2]
      In a small number of states, Russian-affiliated cyber actors were able to gain access to restricted elements of election infrastructure. In a small number of states, these cyber actors were in a position to, at a minimum, alter or delete voter

[1] These numbers only account for state or local government targets. DHS did not include states which may have witnessed attacks on political parties, political organizations, or NGOs. In addition, the numbers do not include any potential attacks on third-party vendors.
[2] In the majority of these instances, Russian government-affiliated cyber actors used Structure Query Language (SQL) injection - a well-known technique for cyberattacks on public-facing websites.

registration data; however, they did not appear to be in a position to manipulate individual votes or aggregate vote totals.

- The Committee found that in addition to the cyber activity directed at state election infrastructure, Russia undertook a wide variety of intelligence-related activities targeting the U.S. voting process. These activities began at least as early as 2014, continued through Election Day 2016, and included traditional information gathering efforts as well as operations likely aimed at preparing to discredit the integrity of the U.S. voting process and election results.

- The Committee's assessments, as well as the assessments of the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI), are based on self-reporting by the states. DHS has been clear in its representations to the Committee that the Department did not have perfect insight into these cyber activities. It is possible that more states were attacked, but the activity was not detected. In light of the technical challenges associated with cyber forensic analysis, it is also possible that states may have overlooked some indicators of compromise.

- The Committee saw no evidence that votes were changed and found that, on balance, the diversity of our voting infrastructure is a strength. Because of the variety of systems and equipment, changing votes on a large scale would require an extensive, complex, and state or country-level campaign. However, the Committee notes that a small number of districts in key states can have a significant impact in a national election.

Actors and Motive

- The Committee concurs with the IC that Russian government-affiliated actors were behind the cyber activity directed against state election infrastructure.

- While the full scope of Russian activity against the states remains unclear because of collection gaps, the Committee found ample evidence to conclude that the Russian government was developing capabilities to undermine confidence in our election infrastructure, including voter processes.

- The Committee does not know whether the Russian government-affiliated actors intended to exploit vulnerabilities during the 2016 elections and decided against taking action, or whether they were merely gathering information and testing capabilities for a future attack. Regardless, the Committee believes the activity indicates an intent to go beyond traditional intelligence collection.

DHS Efforts to Bolster Election Security

- The Committee found that DHS's initial response was inadequate to counter the threat. In the summer of 2016, as the threat to the election infrastructure emerged, DHS attempted outreach to the states, seeking to highlight the threat for information technology (IT) directors without divulging classified information. By the fall of 2016, as the threat

became clearer, DHS attempted a more extensive outreach to the states with limited success.

    - At the outset, DHS was not well-positioned to provide effective support to states confronting a hostile nation-state cyber actor.
    - In addition, members of the Obama administration were concerned that, by raising the alarm, they would create the very impression they were trying to avoid—calling into question the integrity of election systems.

- DHS and FBI alerts to the states in the summer and fall of 2016 were limited in substance and distribution. Although DHS provided warning to IT staff in the fall of 2016, notifications to state elections officials were delayed by nearly a year. Therefore, states understood that there was a cyber threat, but did not appreciate the scope, seriousness, or implications of the particular threat they were facing.

    - Many state election officials reported hearing for the first time about the Russian attempts to scan and penetrate state systems from the press or from the public Committee hearing on June 21, 2017. DHS's notifications in the summer of 2016 and the public statement by DHS and the ODNI in October 2016 were not sufficient warning.
    - It was not until September of 2017, and only under significant pressure from this Committee and others, that DHS reached out directly to chief election officials in the targeted states to alert the appropriate election officials about the scanning activity and other attacks and the actor behind them. (However, the Committee notes that in the small number of cases where election-related systems had been compromised, the federal government was in contact with senior election officials at the time the intrusion was discovered.)

- The Committee found that DHS is engaging state election officials more effectively now than in the summer of 2016. Although early interactions between state election officials and DHS were strained, states now largely give DHS credit for making tremendous progress over the last six months.

    - States have signed up for many of the resources that DHS has to offer, and DHS has hosted meetings of the Government Coordinating Council and Sector Coordinating Council, as required under the critical infrastructure designation. Those interactions have begun to increase trust and communication between federal and state entities.
    - DHS hosted a classified briefing for state chief election officials and is working through providing security clearances for those officials.
    - An Election Infrastructure Information Sharing and Analysis Center has been established, focused on sharing network defense information with state and local election officials.

Ongoing Vulnerabilities:

Despite the progress on communication and improvements to the security of our election process, the Committee remains concerned about a number of potential vulnerabilities in election infrastructure.

- Voting systems across the United States are outdated, and many do not have a paper record of votes as a backup counting system that can be reliably audited, should there be allegations of machine manipulation. In addition, the number of vendors selling machines is shrinking, raising concerns about supply chain vulnerability.

    - Paperless Direct Recording Electronic (DRE) voting machines—machines with electronic interfaces that electronically store votes (as opposed to paper ballots or optical scanners)—are used in jurisdictions in 30 states and are at highest risk for security flaws. Five states use DREs exclusively.

- Many aspects of election infrastructure systems are connected to and can be accessed over the internet. Furthermore, systems that are not connected to the internet, such as voting machines, may still be updated via software downloaded from the internet.

    - These potentially vulnerable systems include some of the core components of U.S. election infrastructure, including systems affiliated with voter registration databases, electronic poll books, vote casting, vote tallying, and unofficial election night reporting to the general public and the media. Risk-limiting audits are a best practice to mitigate risk.

- Vendors of election software and equipment play a critical role in the U.S. election system, and the Committee continues to be concerned that vendors represent an enticing target or malicious cyber actors. State local, territorial, tribal, and federal government authorities have very little insight into the cyber security practices of many of these vendors, and while the Election Assistance Commission issues guidelines for Security, abiding by those guidelines is currently voluntary.

Summary of SSCI Recommendations

The Senate Select Committee on Intelligence has examined evidence of Russian attempts to target election infrastructure during the 2016 U.S. elections. The Committee has reviewed the steps state and local election officials have taken to ensure the integrity of our elections and agrees that U.S. election infrastructure is fundamentally resilient. The Department of Homeland Security, the Election Assistance Commission, state and local governments, and other groups have already taken beneficial steps toward addressing the vulnerabilities exposed during the 2016 election cycle, including some of the measures listed below, but more needs to be done. The Committee recommends the following steps to better defend against a hostile nation-state who may seek to undermine our democracy:

1. **Reinforce States' Primacy in Running Elections**
    - States should remain firmly in the lead on running elections, and the Federal government should ensure they receive the necessary resources and information.

2. **Build a Stronger Defense, Part I: Create Effective Deterrence**
    - The U.S. Government should clearly communicate to adversaries that an attack on our election infrastructure is a hostile act, and we will respond accordingly.
    - The Federal government, in particular the State Department and Defense Department, should engage allies and partners to establish new international cyber norms.

3. **Build a Stronger Defense, Part II: Improve Information Sharing on Threats**
    - The Intelligence Community should put a high priority on attributing cyberattacks both quickly and accurately. Similarly, policymakers should make plans to operate prior to attribution.
    - DHS must create clear channels of communication between the Federal government and appropriate officials at the state and local levels. We recommend that state and local governments reciprocate that communication.
    - Election experts, security officials, cybersecurity experts, and the media should develop a common set of precise and well-defined election security terms to improve communication.
    - DHS should expedite security clearances for appropriate state and local officials.
    - The Intelligence Community should work to declassify information quickly, whenever possible, to provide warning to appropriate state and local officials.

4. **Build a Stronger Defense, Part III: Secure Election-Related Systems**
    - Cybersecurity should be a high priority for those managing election systems.
    - The Committee recommends State and Local officials prioritize the following:
        - Institute two-factor authentication for state databases.
        - Install monitoring sensors on state systems. One option is to further expand DHS's ALBERT network.
        - Identify the weak points in the network, including any under-resourced localities, and prioritize assistance towards those entities.
        - Update software in voter registration systems. Create backups, including paper copies, of state voter registration databases. Include voter registration database recovery in state continuity of operations plans.
        - Consider a voter education program to ensure voters check registration well prior to an election.
        - Undertake intensive security audits of state and local voter registration systems, ideally utilizing an outside entity.
        - Perform risk assessments for any current or potential third-party vendors to ensure they are meeting the necessary cyber security standards in protecting their election systems.

    - The Committee recommends DHS take the following steps:
        - Working closely with election experts, develop a risk management framework that can be used in engagements with state and local election infrastructure owners to document and mitigate risks to all components of the electoral process.
        - Create voluntary guidelines on cybersecurity best practices and a public awareness campaign to promote election security awareness, working through the U.S. Election Assistance Commission (EAC), the National Association of

Secretaries of State (NASS), and the National Association of State Election Directors (NASED).
    - Maintain and more aggressively promote the catalog of services DHS has available for states to help secure their systems, and update the catalog as DHS refines their understanding of what states need.
    - Expand capacity to reduce wait times for DHS cybersecurity services.
    - Work with GSA to establish a list of credible private sector vendors who can provide services similar to those provided by DHS.

5. **Build a Stronger Defense, Part IV: Take Steps to Secure the Vote Itself**
    - States should rapidly replace outdated and vulnerable voting systems. At a minimum, any machine purchased going forward should have a voter-verified paper trail and no WiFi capability. If use of paper ballots becomes more widespread, election officials should re-examine current practices for securing the chain of custody of all paper ballots and verify no opportunities exist for the introduction of fraudulent votes.
    - States should consider implementing more widespread, statistically sound audits of election results. Risk-limiting audits, in particular, can be a cost-effective way to ensure that votes cast are votes counted.
    - DHS should work with vendors to educate them about the potential vulnerabilities of both voting machines and the supply chains.

6. **Assistance for the States**
    - States should use federal grant funds to improve cybersecurity by hiring additional Information Technology staff, updating software, and contracting vendors to provide cybersecurity services, among other steps. Funds should also be available to defray the costs of instituting audits.

###