What to expect when you're electing:

What Talos learned after 4 years of research and hands-on experience

By Matthew Olney | Director, Threat Intelligence and Interdiction

Talos
Cisco Security Research

What to expect when you're electing:

What Talos learned after 4 years of research and hands-on experience

Cisco Security Research

TABLE OF CONTENTS

INTRODUCTION

Shortly after the June 14, 2016 Washington Post report[1] that first detailed how adversaries breached servers for one of America's two major national political parties, monitored staff chats and exfiltrated thousands of emails and documents, Talos initiated what would become a long-running investigation into election security issues. Like many researchers, we weren't familiar with the specifics of how American elections operate, much less the security issues that were particular to those systems. We made an early decision to learn as much as we could from the people that actually ran the elections. So our first step was to reach out to every Secretary of State's office – or equivalent – in the United States and start asking questions. We believe there are important lessons worth sharing from what we have learned since then.

Given this was in the run-up to the 2016 general election, we were not surprised that few were particularly interested in answering questions from researchers who they had never heard from before. But we did find some experts who made themselves available. We asked questions, listened and eventually accepted an opportunity to observe one state as they ran the 2016 election. This was the start of a journey that would lead us to spend hours in conversations with administrators and defenders of election systems across the United States, to fly to state capitols we might otherwise never have gotten to visit, to learn the story of how a well-meaning law created a whole new set of threat surfaces for attackers, how average, everyday Americans in every community across the country suddenly found themselves defending their community's voice from state-sponsored attackers and how these same Americans are so often grossly under-resourced to do so.

This paper represents our current understanding of the election security space. We'll cover the basic technical elements of American election architecture, how American political theory complicates the space, how far we've come since 2016 and things we still have to overcome. It is intended to be a primer for the security professional who wishes to help address the challenges American election administrators face.

There is a lot to cover, but there are three things a helpful researcher must never forget: The first is that every state – and in many states, every county – is different. As we were told early on: "If you've seen one election system, you've seen one election system." The second is that while many things will look familiar, this isn't enterprise security. This is how Americans distribute power – and that colors everything in this space. Finally, we are convinced that not only is it vital to maintain the integrity of the election system, but also to convey to the public the strength of the system and the investments necessary to achieve that result.

OBJECTIVES AND DECIDING DEFENSIVELY

When most people think about election security, they think about the end: Does the final tally accurately reflect the will of the voters? But foreign adversaries have forced Talos to broaden the set of concerns we discuss with our partners. It isn't just the core integrity of individual elections that we are

1 https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html

worried about, we are also worried about the faith and trust the electorate has in state institutions to fairly administer the elections.

We've talked about this more broadly in our July 2019 blog post "Let's Destroy Democracy."[2] In short, a key geopolitical objective of our adversaries is to weaken the faith that American voters have in American democracy, and to weaken the faith the world has in western-style democracy in general. Because of this, the mere appearance of a problem is sufficient to advance some actors' goals. It also means that everyone involved, from local precincts to those involved in federal efforts and even those in the private sector need to consider how their decisions, words and actions play into this objective.

The decisions of everyone involved in elections, from county commissioners to the politicians running for office plays into how Americans and the world perceive the integrity of our elections. Every action and statement that raises doubts about the integrity of our elections is both a win and an opportunity for our adversaries, and as such should be carefully considered.

In May 2019, years after the 2016 general election, Florida state officials were finally briefed by the FBI on breaches that occurred in 2016 in two Florida counties. Although the counties knew in 2016, the FBI decided not to brief state officials. Gov. Ron DeSantis was forced to defend an election that took place before he became governor, saying, "There was no manipulation or anything but there was voter data that was able to be had. Now that voter data I think was public anyways, nevertheless those were intrusions."[3] Any time an elected official has to explain why an intrusion did not undermine election results — even if it is completely correct — it is a win for our adversaries.

In light of our understanding of our adversaries' objectives, we would argue that the decision in 2016 not to brief the Florida government on foreign adversary operations affecting their voting systems created a difficult situation. Most obviously, it cuts the state out of its essential role as part of the security ecosystem of Florida voting. But the critical issue is that it resulted in taking a win by the adversary — gaining access to certain parts of Florida voting infrastructure — and making it worse by creating the narrative that the federal government wasn't an effective partner, at least for Florida, in securing the elections process. Finally, it created a situation where officials were defending election integrity years after the election in question, which is obviously problematic.

We don't have all the information necessary to state that the federal government acted incorrectly in not briefing Florida state officials. But it is clear to us that the decisions made in 2016 resulted in a win for foreign adversaries in May 2019. Without the adversary doing anything more, events unfolded that called into question the ability of Florida to secure its elections,

It isn't just the core integrity of individual elections that we are worried about, we are also worried about the faith and trust the electorate has in state institutions to fairly administer the elections.

2 https://blog.talosintelligence.com/2019/07/lets-destroy-democracy.html

3 https://abcnews.go.com/Politics/voter-databases-florida-counties-hacked-2016-governor/story?id=63052842

the role of the federal government in securing elections, the effectiveness of federal/state and state/local partnerships and the safety of voter data in Florida. Our point is that these decisions made in 2016 should have considered the objectives of our adversaries, and the possible damage that would occur down the line.

In January 2020, the FBI announced a policy change that they would notify states if local election systems were breached.[4] It was explained that past decisions were made based on FBI policies that protected the identities of hacking victims. It is important to note that these will still not be made public, and it will be up to the individual election entities to decide whether to disclose to the electorate they were attacked.

DEFENDING FAITH

Everyone involved in politics and elections has a role in working against adversaries on their core objective. Unforced errors, such as unsubstantiated accusations of voter manipulation, administrative incompetence, censorship, partisan bias or voter fraud should be avoided and condemned. Each of these accusations chip away at the faith of the American electorate and serves the interests of our adversaries.

On the flip side, success and progress in security should be aggressively communicated. States should be open about their investments, timelines and policies. Localities should do likewise, and work to educate their citizens about the day-to-day work done to secure their vote. We cannot rely on citizens to passively trust that the various layers of government are at work to protect democracy, they need to be actively engaged and assured that their elections are being looked after. The public should understand the investments necessary in terms of time, money, personnel and equipment to ensure free and fair elections and that those investments are being made.

Finally, all levels of government should work on crisis communications. In our discussions with states, we frequently discuss the situation of the Secretary of State at the podium. First we work to avoid this by hardening systems and processes, but we also spend time talking about the failure condition. When something goes wrong,

Everyone involved in politics and elections has a role in working against adversaries on their core objective.

what is said and to whom is a critical decision. Foreign adversaries and their information operations are always looking for opportunities to twist statements and actions to show them as indications of a failing democracy. To counter this activity, we run tabletops where the scenario revolves around successful compromise of components of the larger election system and as part of that concentrate on communications. We always advocate for taking time to construct the right message and erring on the side of transparency. These recommendations work directly against the adversary's ability to construct misleading narratives based on official statements.

THE SYSTEM AND THE PIECES

In our work, we've come to approach our evaluations in two ways: looking at the whole system – from registering the voter to displaying the results of an election, and then drilling into the minutiae of how each component works. Security issues can be found from both views, and to understand the role of each component, you must understand the role of the whole. It is also important to understand that a passing knowledge of the general principles of elections is not a replacement for the time spent understanding the intricacies and idiosyncrasies of any given election system. Each implementation is different, and each must be approached with a fresh curiosity and desire to dive into technical details. In this section, we'll discuss the systemic approach, detail the role of vendors in U.S. elections and dig into some of the basic components that are commonly seen in election systems today.

4 https://apnews.com/dca69532127c625956be9e8d6e6a5c2b

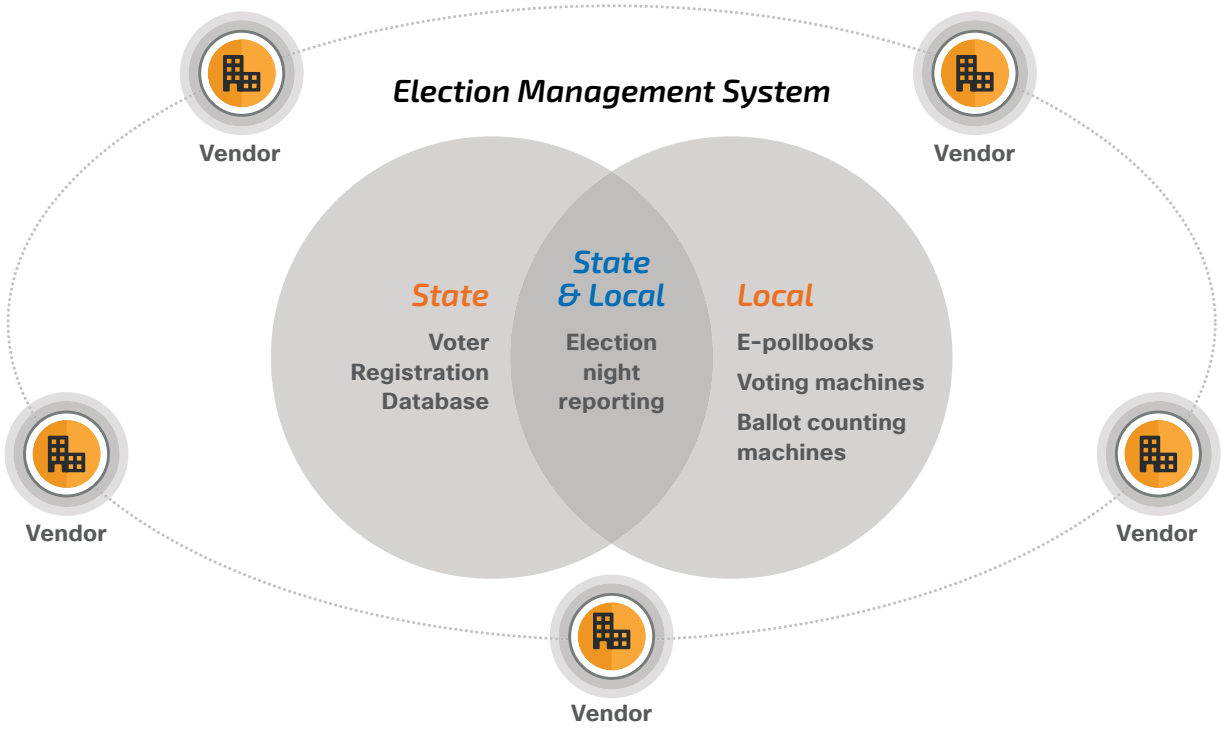

Figure 1. *Common distribution of responsiblities for key election technologies. It's important to note that the state itself is usually responsible for operating the EMS.*

THE ROLE OF VENDORS

Voter technology vendors are critical to the democratic processes in the United States. While localities can develop their own systems, such as Iowa's homegrown Precinct Atlas e-pollbook solution[5], vendors are central to the systems that enable elections. The relationship between these vendors and election officials can go back more than a decade, and a great deal of trust has been built during this time. Security practitioners should respect this relationship, but also push to ensure that statements match reality and that states are asking everything they should be of vendors.

While partners, including voting technology vendors, are critical to ensuring the security of the election, ultimately the responsibility for a secure election rests with the government. Security practitioners should look for places where election officials have lost visibility into critical pieces of the election system and highlight them so that change orders and future requests for proposals can be modified to ensure that there are sufficient security technology present, that the election officials have sufficient access and visibility into the systems and that auditing of both user and administrative functions are present.

This is particularly problematic when vendors provide cloud or hosted services. These wholly vendor-provided solutions can be opaque to election officials, with poorly understood security monitoring, little-to-no reporting and limited ability to verify and test the security of the systems.

At a minimum, contracts should be written to require that vendors disclose security incidents that affect the systems or the employees involved in administering those systems that election officials rely on. State-sponsored adversaries are quick to abuse the trust relationship between vendors and their preferred targets, and there are known past

5 https://www.iowacounties.org/programs/iowa-precinct-atlas-consortium/

incidents of adversaries targeting election vendors.[6] Elections officials need to know when there has been an incident so they can validate that activities in their own systems haven't been affected.

Vendors are not the enemy, they are critical components of how we conduct elections. But as profit-motivated entities with risk exposure, their motivations and concerns may not always be aligned with the election officials who retain them. Controls must be written into contracting to ensure that election officials maintain the ability to verify and enforce security controls, including external testing and coordinated incident response policies. Security practitioners should provide guidance to election officials as they seek to update their vendor contracts.

SYSTEMIC REVIEW

None of the devices we describe below exist in a vacuum. They are all part of a set of policies, procedures, devices and humans that interact to determine the will of the electorate. While reviewing the security of each of these point systems independently is almost certainly the most effective way to move forward to start, stepping back and reviewing the system as a functioning whole is also necessary.

Adversaries have objectives, and will spend as much time as necessary analyzing and mapping out the systemic nature of elections to locate the most effective and viable route for them to achieve their goals. It isn't just technological failures that can be exploited, but also failures in training, processes and procedures and in the humans that run the election. Security practitioners must at all times be looking for places where controls are weak, where humans can fail to follow procedure, where hardware can fail and ensure that there are operational controls to catch that failure.

An August 2019 article by Kim Zetter[7] shows an excellent example of this. Both election officials and election technology vendors frequently highlight the fact that devices aren't connected to the Internet as a key reason they are secure. The article calls into question how accurate these claims are, and highlights some examples where claims didn't match up with reality. A quote from Kevin Skoglund, a security researcher, is telling:

"In some cases, [the vendor was] in charge [of installing the systems] and there was no oversight. Election officials were publicly saying that their systems were never connected to the internet because they didn't know differently."

Three things from this quote: First, again, election officials need to be in a position where they can audit and check the claims of voting technology vendors. Second, If Mr. Skoglund determined this remotely, then state-sponsored actors can as well. Finally, any time election officials make statements that ultimately turn out to be incorrect, there is damage done.

One of the key roles of the security practitioner is to have the eyes and ears of an attacker. Listen carefully to what you are told should happen, and then verify empirically that it does indeed happen. Ensure that if that doesn't happen, that fact is easily determined by the IT staff working with the election officials. Think constantly like the attacker, poke at assertions, look for seams in process, and harden not just the systems, but the systems watching the systems.

ELECTION MANAGEMENT SYSTEM

At its core, most American elections are local affairs. They are run by the counties and parishes across the country. Most states have an election management system (EMS) to coordinate the roles of the state and the localities. The roles of this system vary by state, but they can include jury pool management, voter registration, ballot creation and management, pollbook generation and election reporting.

These systems, which are typically custom created by specialist firms for states, are the standard mechanism for precincts to interact with voter data. As such, they are critical touch points in a security assessment. A deep dive is necessary, because these are custom coded and engineered systems that include interfaces for localities and state administrators as well as remote access for vendors to troubleshoot and administer the underlying systems.

In our experience, nothing replaces a hands-on demonstration of how these systems are used and administered to help scope the evaluation. This is because

6 https://www.rollcall.com/2019/04/22/mueller-report-russia-hacked-state-databases-and-voting-machine-companies/

7 https://www.vice.com/en_us/article/3kxzk9/exclusive-critical-us-election-systems-have-been-left-exposed-online-despite-official-denials

of the fuzziness of terms and the customized coding of these systems. For example, systems we observed had two-factor authentication, but that authentication ranged from bingo-cards with pre-printed access codes to SMS-based solutions to those that used more current commercial multi-factor solutions.

The EMS is a high-profile target for attackers, as it is the accepted way for localities to modify the voter registration database. Successful attacks would be less likely to show up using this system than they would through directly interfacing with the database. It is also deliberately set up for remote access, so it is easier to access than other components of the election system.

VOTER REGISTRATION DATABASE (VRDB)

The Voter Registration Database (VRDB) is the central database housing all the registration information about a voter and may also include additional information such as the last active voting date, jury duty activity and other information required by the individual state. The databases are required by the Help America Vote Act of 2002 (HAVA), and every state has one with the exception of North Dakota, which does not have voter registration.

When evaluating these components of the system, security practitioners should look for best practices for database security, but should also focus on the system as a whole as it relates to the VRDB. The VRDB is commonly wrapped in the election management system, so the connections to that system should be analyzed. It is also important to understand what other systems might interact with the database and how.

For example, the National Voter Registration Act of 1993 (popularly known as the "Motor Voter" law) allows voters to register at the same location they get their driver licenses. Also, in many states, there is a list of disqualifying felonies that disenfranchise those who are convicted of those offenses. How does the state system convey these changes to the VRDB? How does the system handle voter deaths, or voters who have moved out of state? How are these changes handled and is it secure? Does the threat surface of the election system extend out to other elements of the state network?

There are also additional behavioral controls that can be considered when looking at the VRDB. Several emerging approaches from companies like VoteShield[8] involve looking at change behavior in the database. These behavioral analysis systems can be useful not just for catching malicious behavior, but also for preventing human error events that can also cause concerns in the electorate.

Foreign actors largely targeted the VRDB in the past and it will be a target going forward.[9] For actors intent on disrupting election activity and causing difficulties at the polls, manipulating the VRDB, and by extension the pollbooks used by election workers, would be an effective approach. While voters affected by manipulation will typically be able to cast provisional ballots, a sufficiently scaled and targeted set of manipulations could cause long lines and delays aimed at specific verticals of voters. This is one of our standard scenarios for review during discussions with elections administrators.

ELECTION NIGHT REPORTING SYSTEMS

Election night reporting systems (ENR) are quality-of-life systems that centralize election results for review by interested citizens, press and politicians. They are not universal, with some states still simply posting results at precincts with runners from press organizations gathering the information and sharing the results. State-sponsored adversaries have targeted ENR systems in non-U.S. elections to display fraudulent data in the past, so we know that attacking ENR systems is in their playbook.

In some localities, ENR systems may not be the only location where election data is posted.

Counties may also choose to post the results on their own websites. These sites should also be considered, because if an actor can cause different data to be displayed on local websites than in the centralized ENR system, that would be problematic for the reasons outlined above. The perception of integrity is as important as the integrity of the system itself.

We've also observed that in some systems ENR is only deployed for certain elections, and results are posted to a local election website instead. Our recommendation in the past was to consider eliminating the practice of

8 https://www.voteshield.us/

9 https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers

dual-posting, and sending interested parties only to the centralized ENR system. This reduces the attack surface, makes disinformation campaigns more difficult and makes it easier for engaged citizens to track election activity.

Security practitioners should carefully trace the path of data from the election precinct through the ENR system until the point where it is displayed publicly. The overall process should include validation from the county level that the data was properly loaded into the system. The system can largely be analyzed as a standard enterprise information-processing system. Beyond those measures, practitioners should ensure that the process is robust and that it is mapped to the correct security controls, including auditing and multi-factor authentication. Finally, when planning for operational or security issues, ensure there are clear communications channels between the vendor, state and counties to ensure problems are handled quickly and information is properly disseminated.

E-POLLBOOKS

Electronic poll books (e-pollbooks) are hand-held computing devices used to verify voter information during voter check-in at polling places. The use of electronic poll books not only provides an easy to use copy of the appropriate portion of the voter registration database, but it also allows for state and locality-specific processes to be converted to controls in the pollbook. Frequently, e-pollbooks will have functionality to walk poll workers through the appropriate checks as they process voters. The pollbooks have both data and process control functionality. The acquisition and administration of these devices are often handled by counties rather than states.

These devices can be tablets or laptops, can include accessories to scan identification and many implementations require a network component between the multiple devices at a single precinct so that check-ins are reflected across multiple devices. Evaluations should include not just the security of the devices individually, but also the security of the network, with particular focus on ensuring that the network activity is limited to only that which is necessary to support voting activity and all other activity is actively blocked.

While the security of the e-pollbooks and networks are important, the processes around how they are stored, configured, loaded with data and the environment in which they are used are all critical as well. Security practitioners should ensure that written guidelines for poll workers and administrators are complete and reflect the intent stated by election officials. For example, if officials say that wireless networking is not used, the images, configurations and processes should all come together to ensure that wireless networking is actually disabled, and that this outcome is verified.

VOTING MACHINES

Voting is different now than it was 20 years ago, almost entirely because of HAVA. This legislation resulted in the end of the use of punch card and mechanical lever systems and the rise of the use of computer systems in handling voting. This change was introduced in the wake of the 2000 general election, in which between 4-6 million ballots were not counted because the voter intent couldn't be determined. While that problem has largely been eliminated, the introduction of computing systems into the voting process has introduced new concerns.

Direct recording electronic (DRE) systems allow the voter to cast their vote directly at the system. The interface is varied, but one of the core concerns around these systems is that votes are recorded local to the machine and are then loaded onto memory cards or USB devices to be counted centrally. If the machine is interpreting the will of the voter and storing that in a way the voter can't verify, how can the voter be sure that their vote was correctly captured?

One solution here is adding a voter-verified paper audit trail (VVPAT) printer to the DRE. In this case, the voter can review the printout and ensure that it reflects their intent. Further, this allows recounts and audits to use this vote-verified print to check the results of the votes captured in the memory cards. Unfortunately, current research shows that most voters do not properly check the printout. More research into how to encourage voters to do this and how much compliance is needed to gain a security benefit still needs to be conducted. Either way, just knowing that the option to check results is available increases voter confidence in the voting system and should be carefully considered.

Another device that falls under this category is the ballot marking device. These devices allow the voter to indicate their voting preference and then generate a ballot on behalf of the voter that is tabulated elsewhere. These devices are broadly used as assistive devices for those voters who have some form of difficulty using the default voting system.

Much like with the DRE/VVPAT combination, it is important for voters utilizing these devices to ensure that the ballot is representative of their desires.

Voting machine security has been the focus of research for years and continues to be a hotbed of research today. Security practitioners venturing into this realm, even those familiar with evaluating similar technologies, should review key research and statements in this area. They should also be familiar with related procedural controls like risk-limiting audits and how those controls can be constructed using the voting technology they are evaluating.

BALLOT-COUNTING MACHINES

For localities that use hand-marked or machine-created ballots, ballot-counting machines rapidly tally the votes and provide results at the precinct level. Modern machines use digital scanning technology, and can identify ballots that have issues that require hand processing due to marking errors or other issues. These devices are typically not network connected and are in controlled environments.

Security practitioners should review the policy controls around the use of these systems, how ballots are delivered to the systems and how the resulting data is collected and provided upstream.

POLITICIANS

The words and actions of politicians are a key part of the election environment. Each person seeking or holding office has the opportunity to reinforce or damage the faith of the electorate in American democracy. One area that clearly shows this is accusations of election fraud. Clearly, when election misconduct occurs, it should be vigorously investigated and prosecuted. That activity contributes to the integrity of elections. However, unfounded claims of election fraud reduce faith in elections, endangers the peaceful transition of power and plays into the hands of our adversaries.

Leadership matters in this space, and Secretaries of State or the equivalent are situated in a position where they can take active steps to reinforce faith in the elections they administer. Actively communicating the work they are doing is key to this. In the state of Maryland, for example, posters were hung at voting locations detailing for voters what changes had been made to better secure elections.

Ohio is a case study in communication and leadership. Secretary of State Frank LaRose, who took office in January 2019, issued a directive to all 88 Ohio county boards of elections in June 2019 requiring each board to increase security at the county level of elections administration prior to the 2020 Primary Election. In addition to very publicly addressing the security issue through this directive, the office actively communicates security changes and adjustments to the challenges the COVID-19 pandemic presents. Even if one disagrees with the decisions made, the framing and active communication are key. Clear, accurate and pervasive messaging is a counter to future disinformation campaigns.

Election officials should work to provide standardized and verified communications paths to reach voters. If Twitter is used, it should be a standardized account for the office and verified by Twitter. There should be a standard, updated page for election news and results that voters can easily navigate to. Part of voter education should include where to go to report problems, learn about changes and validate claims.

Security practitioners working with politicians should ensure that accurate information is available and should highlight any gaps that exist in understanding a situation. Statements made, particularly during crisis, need to be based on facts, highlighting where investigations are still ongoing and what actions are being taken. They should craft incident response plans to generate the kind of information that politicians will need in responding to press queries and should test communications during tabletop exercises. The goal should be to allow no free wins for adversaries interfering with free elections.

VOTERS

As participants in the democratic process, voters should engage actively with information that comes their way. Information hygiene is critical today, and information needs to be vetted and not blindly shared with others. Claims should be viewed skeptically when presented without evidence.

Voters should understand that they are the target of disinformation campaigns: their opinions, anger or apathy is being weaponized by both foreign and domestic actors. They should be taught the disinformation mechanisms that are used, the psychology of handling information and how to be engaged voters given the current threat environment. Security practitioners should strive to remain neutral, and provide the tools and approaches to voters to handle disinformation campaigns.

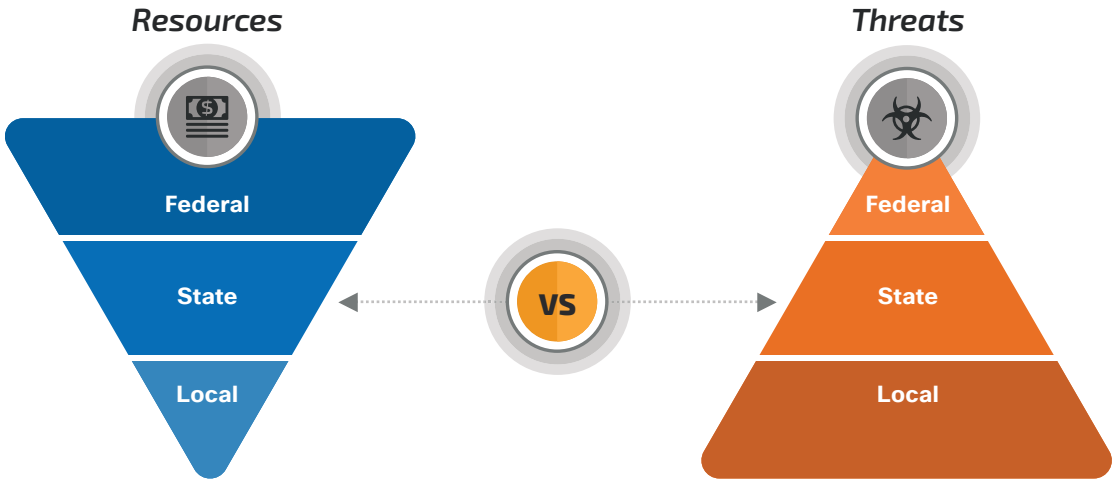

Figure 2. *The inverse pyramid relationship between resources and threats faced by federal, state, and local agencies.*

THE CURIOUS ARCHITECTURE OF AMERICAN DEMOCRACY

One of the first concepts that we ran into in our research was that it was almost impossible to hijack an election because the elections systems were different in each state and, in some states, different in each county. This is certainly a glass-half-full thought process, but it is built on the truth that elections in the United States are largely locally run, an architecture that's been in place since the beginnings of the United States. While the balance is different in each state, in many states, counties have an enormous say in process, protocol, equipment selection and administration.

We see three levels of involvement for elections: federal, state and local. We also see tension between each of these levels as the offices involved work to ensure that their position is respected. It takes active engagement with the realities of the architecture to best position everyone to play their role during a crisis.

We also see an inversion between targeting and resources when looking at these levels, as illustrated in Figure 2. From an election perspective, foreign adversaries would have the least to benefit from directly targeting federal agencies. On the other hand, local administration targets would be highly desirable for the same adversary. But the federal government is much better positioned to monitor, understand and engage with these adversaries. Ultimately the least resourced piece of the puzzle, the local administration infrastructure, is also the most likely to be targeted.

During one visit to a state, we brought along one of our experts from a country in Europe with a strong central government control of elections. After a day

Ultimately, the least resourced piece of the puzzle, the local administration infrastructure, is also the most likely to be targeted.

going through all of the ins and outs of the election setup, we were leaving on the elevator when he asked, "Is this really how Americans do this?". When we confirmed that all of this was common, he just shook his head and said, "Insane." What he was struggling with wasn't any patent defect in the operation, but the extreme difficulty in securing election infrastructure from the bottom up. But this is the reality of how we are built, and this is how we have to approach the issue – from the bottom up.

STATE AND LOCAL

Many of our conversations over the past four years have centered on advocating for flexibility, trust and engagement between federal, state and local resources. The most important relationships in elections exist between the state and the local authorities. States tend to be better resourced and positioned to respond to an incident than those at the local level. They also are close enough to the local level to know the key players, know the constraints and capabilities and understand the legal requirements at the state level for handling elections.

Leadership is critical here, as is problem solving and relationship building. Understanding and respecting the roles and responsibilities for the administration of elections, while still finding a way to drive change is critical. Ultimately state and local elections infrastructure should be mapped to a common security roadmap, with coordinated incident response and the ability to shift resources and support as necessary. This takes years of patient work in both directions, and hours of practice. But leaving counties to fend for themselves in the face of state-sponsored activity is simply not a viable path forward.

When evaluating state and local interactions, we start by looking at the established support points. How do local election officials contact the state to troubleshoot issues. Then, we look at how (if they can) the state pushes down security requirements. We try to identify deficiencies in these capabilities and look for sustainable ways to improve those pathways. We also look to run tabletop exercises that involve both state and local resources to discover areas of friction. Finally, we try to establish a unified incident response plan for election systems that includes both state and local resources and highlights communications and support paths.

The most important relationships in elections exist between the state and the local authorities.

One last note at the local level: Our experience has shown a great deal of trust between individual counties. Frequently, the most important support for a county comes from other counties. For example, in Iowa there is the Iowa Counties Information Technology group[10], which provides a shared-resource model where a county that is lacking the resources in an area can request expertise from other counties. This group brings both pre-existing trust and an understanding of how the counties operate that is invaluable. This type of capability should be captured in incident response plans, and states should engage directly with this group to come to a collective understanding of the kind of response that can be provided.

FEDERAL

The direct role of the federal government in any given election, from the administration standpoint, is minimal. While the federal government has few specific authorities when it comes to the administration of elections, it does provide proactive security guidance, funding and intelligence. These services are largely opt-in, and require engagement from the states with the federal government. This engagement, which was problematic in 2016[11], is much stronger going into the 2020 general election.

HAVA funding is the most public of this support. After several years without funding, in 2018 $380 million dollars were allocated and with an additional $425 million dollars in 2020. While this funding is vital, some state officials we have

10 https://iowacountiesit.org/projects/

11 https://thehill.com/policy/cybersecurity/339734-investigation-shows-dhs-did-not-hack-georgia-state-computers

talked to have highlighted the lack of consistent funding as a key difficulty. One official went so far as to say that consistent funding at lower levels was preferred to the current uneven process.

This aligns with an early conversation we had with an academic expert in elections. This person highlighted the market economy of election systems – including the inconsistent funding from federal sources and investment at state and local levels – as a key issue in election security. This inconsistency leads to a dysfunctional market lacking high-end companies, slow product innovation and improvement and an uncertain capability to respond to security incidents.

The federal government is also well situated to provide consistent security guidance and other proactive services. The Cybersecurity and Infrastructure Security Agency (CISA), part of the U.S. DHS, provides several election services, including cyber security assessments, detection and prevention, information sharing and awareness, and training and career development.[12] One particularly critical component of this is regional specialists in intelligence and security that can build relationships with state and local authorities. We always ensure, both at the state and local level, that the personnel are aware of and in contact with these specialists.

States can, in theory, self-fund, and they also have security expertise of their own. But the federal government is uniquely situated to provide timely intelligence assessments and notifications to states and localities. In our discussions with state and local leaders, this is the area where the federal government can most improve. The various providers of intelligence and law enforcement services at the federal level must work to provide current intelligence to the defenders on the ground. There is simply no other dedicated option for election officials to use to gain an understanding into the motivation and actions of these state-sponsored adversaries.

FOUR YEARS OF IMPROVEMENT (2016 - 2020)

We, as a nation, did not do enough to ensure the perception of integrity in the 2016 election cycle. The relationship between the federal government and states was not strong enough to allow for effective cooperation.[13] This meant that even discussion of designating elections as critical infrastructure were problematic.[14] There had not been any HAVA funds allocated to states since federal fiscal year 2010.[15] At the state and local level, very little information was flowing down to them and at the federal level there were few policy options available to react to an emerging understanding of the

2020 itself is providing new challenges for elections officials:

A lot has changed in the few short months since our last visit with an election security partner. Whole new issues, like the potential for mail-in ballots, have arisen as the country struggles with the pandemic. While we haven't worked with mail-in ballots, we would approach this like we would any other technology. Look to states, like Colorado, Oregon and Washington, that have spent years successfully using mail-in ballot systems, carefully review the findings of security experts and then act based on your research, speaking carefully about your understanding and being certain not to raise alarm without cause and always being sure not to hand our adversaries unearned victories.

12 https://www.cisa.gov/election-security

13 https://www.cyberscoop.com/state-election-officials-resisted-federal-cybersecurity-assistance-during-2016-election/

14 https://www.politico.com/story/2016/08/election-cyber-security-georgia-227475

15 https://editions.lib.umn.edu/electionacademy/2018/08/27/eac-releases-details-on-states-plans-for-spending-new-380m-in-hava-funds/

scope of foreign interference.[16] While far from perfect, we are confident that our adversaries will find a different landscape in 2020.

Many of the changes are visible. HAVA funds have been allocated both in 2018 and 2020, totaling more the $800 million in investments. Elections are now critical infrastructure, which allows for increased funding and focus at the federal level. Specifically, CISA has taken on the role as the election security focal point for federal efforts and is offering popular services such as phishing testing and vulnerability scanning. In near record time, the Election Infrastructure ISAC (EI-ISAC) was stood up to coordinate information between election authorities and has widely deployed Albert intrusion detection and flow analysis systems to state and local authorities.

Organizations like the National Association of Secretaries of State and National Association of State Election Directors have partnered with federal agencies to bridge messaging and options to their members. Academic groups like the Belfer Center's Defending Digital Democracy and the Brennan Center for Justice are providing digestible security guidelines written in conjunction with election officials. After some stumbles, the security community and the election community are working more closely together. Researchers are being invited to share their expertise with election officials. Organizations like Defcon Voting Village are also emerging as important allies in moving toward more secure elections.

Some are less visible, but just as important. Reporters are specializing in election security and publications are specifically assigning reporters to the election security beat. State and local officials are more aware of cyber security issues and the efforts of foreign adversaries. Staff from CISA have criss-crossed the nation building trust and relationships and establishing an appropriate and important role for the federal government in election security. Work is being done to get critical information into the hands of defenders more quickly (see the previous FBI policy change on page 5).

CONCLUSION

Election security cannot be solved just by looking at individual components of the system. More than any other broad issue we've encountered, election security must be analyzed systemically and addressed in collaboration with a number of parties. States and localities cannot stand alone against state-sponsored actors, and there is no reason for them to do so. There are partnership opportunities across the board that can be taken advantage of. But leadership matters, and officials must make clear that security is critical and then act to build the relationships necessary to not only secure American elections, but also to cement the electorate's trust in the integrity of the elections.

The cyber security community is just one piece of the puzzle. Those of us who chose to work on this issue also shoulder the responsibility of building trust, of understanding all the viewpoints and to ensure that limited resources are expended where they will do the most good. We should also work to build bridges between other key partners, to share our understanding of how malicious actors work and to build out that understanding with those we are privileged to work with.

Beyond purely technical considerations, the security community should work to ensure that communications are a focus of incident response plans and exercises. Ultimately, what we are defending is the faith the electorate has in our institutions, and clear, honest and accurate communications both before and after incidents are a key action in reinforcing this faith. Practice, plan and execute with this objective in mind.

We are stronger in 2020 than we were in 2016, but we must continue to be vigilant and build up our defenses. Our adversaries are patient, and they will change tactics as it benefits them. Only with local, state and federal authorities working together and with private sector partners will we be successful.

16 https://www.washingtonpost.com/national-security/obama-teams-response-to-russian-election-interference-fell-short-senate-report-says/2020/02/06/93c2fdac-48f2-11ea-9164-d3154ad8a5cd_story.html

Talos
Cisco Security Research

About Talos

The Talos Threat Intelligence Group is Cisco Security's threat intelligence organization, an elite group of security experts devoted to providing superior protection for our customers, products, and services – as well as a vast collection of open source security products and tools. Talos is among the largest threat research teams in the world, encompassing seven key areas: Community & Open Source, Detection Research, Engineering & Development, Incident Response, Intelligence and Interdiction, Outreach, and Vulnerability Research & Discovery.

Talos detects and correlates threats as they happen, pushing coverage to customers globally within minutes to protect against known and emerging cyber security threats. With great visibility comes great responsibility – Talos also supports open-source security and often undertakes interdiction efforts to mitigate threats in the wild that pose significant risk to the internet at-large.

For more information, visit www.talosIntelligence.com.

ABOUT THE AUTHOR

Matthew Olney is the Director of Threat Intelligence and Interdiction for Cisco Systems. He leads a group charged with working with both public- and private-sector partners around the world to identify and address security threats. His group also provides intelligence support to Cisco's commercial incident response organization and manages Cisco's response to large-scale security events. This team took the lead in response to global events such as WannaCry, NotPetya and VPNFilter. Over the course of the past 13 years of working with Sourcefire and Cisco, his roles have also included vulnerability development, detection logic creation, and application development and has been awarded a patent for his work on cutting-edge security analysis engines.