CIRCADENCE

Protecting Democracy from Election Hacking

A Five-Step Implementation Strategy to Address Global Election Integrity in the Wake of Digitalization

Abstract

This white paper discusses key recommendations from the Campaign Cybersecurity Playbook to reduce the risk of a cyberattack on election infrastructure and identifies a five-step implementation strategy to preserve the integrity of global election processes. The Russian cyberattack on the 2016 U.S. presidential election spurred mass distrust in the democratic voting process, which inspired the questions: what can be done to better secure the election process and how can we prevent attacks like this in the future? The use of antiquated voting technology, inadequate integration across systems, and patchwork election administration models widen the entry points for new-era threats to take hold. Previous cybersecurity solutions on the market have provided dull, on-site, expensive training courses for professionals that attempt to upskill cyber teams. However, the escalated investment and lackluster learning outcomes have rendered traditional training solutions fruitless. Circadence proposes an adaptable and measurable verification platform that places the technology, processes and people involved in the end-to-end election system at the forefront of resolution. It recommends that training to protect, detect and respond to cyberattacks must include reaching personnel at ALL levels from the voting registration volunteer to the key government leader who would be involved in responding to an incident. Circadence's suite of training and education platforms leverage AI and machine learning, which scale, adapt, and deliver measurable ROI—keeping data secure in the intelligent cloud or on-premise. By engaging in realistic training in a virtual world with actual systems, threats and emulated user traffic, election officials can restore voter confidence, detect and defeat threats, and preserve the integrity of the democratic process.

Introduction

Since the 2016 election, numerous reports have cited concerns of vulnerabilities in the voting ecosystem, detailing attempts by nation states such as Russia to exploit these. To assist in securing the critical infrastructure of elections, Congress provided federal funding under the recent 2018 Consolidated Appropriations Act Election Reform Program[1], authorized by the 2002 Help America Vote Act (HAVA). This funding grants states additional resources to make improvements in election security[2]. The HAVA act inspires this white paper, which discusses key recommendations in the Campaign Cybersecurity Playbook to reduce the risk of a cyberattack on the election infrastructure[3] and identifies a five-step implementation strategy to begin acting on the key recommendations now.

Effective cybersecurity is no longer localized to the Information Technology (IT) support team or the realm of technical specifications for voting machines. Success in maintaining the integrity of our democracy requires a holistic approach to cybersecurity that broadens its reach to all individuals in the process. One core element across the list of recommendations is the need to develop skilled personnel. This training to protect, detect and respond to cyberattacks must include training personnel at ALL levels from the voting registration volunteer to the key government leader who would be involved in responding to an incident. Before diving into implementation strategies to preserve election integrity across the globe, we must first understand the current state of election security, its structure, process, and vulnerabilities.

1. Securing the human element
2. Using secure communication methods
3. Restricting account access and management
4. Controlling access to devices
5. Monitoring and protecting the networks
6. Addressing Information Operations/Public Facing communications
7. Planning for incident response

Figure 1 - Cybersecurity Campaign Playbook Recommendations

The Current State of Election Security

After revelations of the Russians attempting to change the outcome of U.S. elections in 2016[4], the governments and voting system industry have been working to prevent a repeat (and potentially worse scenario) before the next election. Unfortunately, hackers have grown increasingly sophisticated during this time and it is likely that they will use their lessons learned from the past to be even more effective. Exacerbating the current situation is the use of antiquated technology (over 80 percent of state voting systems in the U.S. are more than a decade old[5]), inadequate integration across

[1]Halderman, Alex, *"I Hacked an Election. So Can the Russians.,"* New York Times, 5 April 2018.
[2]Election Assistance Commission, *"2018 HAVA Election Security Funds,"* Accessed 14 August 2018.
[3]Mook R., Rhoades, M., Rosenbach, E., *"Cybersecurity Campaign Playbook,"* November 2017.
[4]Office of the Director of National Intelligence, *"Background to 'Assessing Russian Activities and Intention in Recent US Elections:' The Analytic Process and Cyber Incident Attribution,"* National Intelligence Council, 6 January 2017.
[5]Norden, L., Vandewalker, I., *"Securing Elections from Foreign Interference,"* Brennan Center for Justice, 2017.

systems, and patchwork election administration models that widen the entry points for new-era threats to take hold. While technological advances have contributed to the ease of communication and transfer of election data, those advances have inadvertently created a bigger digital threat[6] than ever before. Further complications arise from the decentralization of U.S. election processes[7]. Although the federal government provides national-level guidance, state and local governments are responsible for figuring out how to best conduct localized elections and those with fewer security resources are likely more vulnerable targets for adversaries.

Several weaknesses in the election ecosystem have been discussed in the notable election attacks in the United States and abroad. This has led to many nations across the globe questioning the ability to ensure digital integrity.

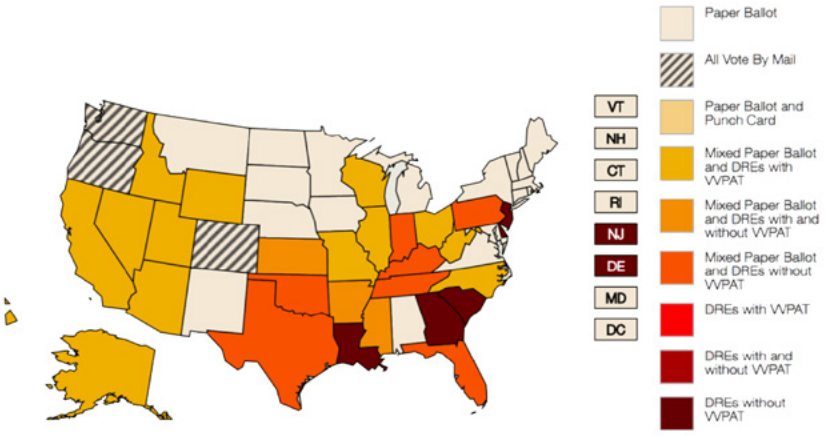
- 2008 & 2012: Chinese hackers breached U.S. presidential Democratic and Republican campaigns for intelligence gathering[8].
- 2016: Russia hackers allegedly penetrated a U.S. election software vendor in attempts to gain data for a spear-phishing campaign against election officials[9].
- 2017: A court in Kenya says it nullified election over possible hacking[10] and the French report hacking in their national elections.[11]
- June 2018: A presidential candidate in Mexico was hit with a DDoS attack during a debate.[12]
- Taiwan is preparing for a spike in cyberattacks that will coincide with the country's local elections in November 2018[13].

These attack examples illustrate a determined effort by adversaries, which has led the public to question the legitimacy of the democratic process.

> *"The history of national defense shows that threats are constantly evolving. When the United States was attacked at Pearl Harbor, we took action to protect our fleet. When we were attacked on 9/11, we took action to upgrade transportation security and protect our ports and other vulnerable targets. We were attacked in 2016. The target was not ships or airplanes or buildings, but the machinery of our democracy. We will be attacked again. We must act again — or leave our democracy at risk."*
>
> *~ Former Director of the Central Intelligence Agency, Amb R. James Woolsey*

[6]Rhoades, Matt, "U.S. elections are under threat from cyberattacks—and so are yours," Politico, 22 May 2018.
[7] Harvard Kennedy School, "Defending Digital Democracy," Belfer Center for Science and International Affairs, February 2018.
[8,9]Lipton, E., Sanger, D., Shane, S., "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.," The New York Times, 13 December 2016.
[10]Freytas-Tamura, Kimiko, "Kenya Court Says It Nullified Election Over Possible Hacking," New York Times, 20 September 2017.
[11]Hautala, Laura, "Russian hackers target French presidential candidate," CNET, 24 April 2017.
[12,13]Limbago, Andrea, "No time for stalling: The urgent need for an election hacking response," GCN, 24 July 2018.

Moreover, concerns around hacking elections are broader than the technical success or failure of an attack; the larger issue is voter confidence and a potential impact on election turnout[14]. The level of covert activity, unknown system vulnerabilities and digitalization of the election process contribute heavily to the state of election security today—which we can say with confidence is full of uncertainty and risk.



A Diverse and Expansive Attack Surface

The election infrastructure for the United States is selected, procured and maintained by over 8,000 individual jurisdictions[15] in counties, cities and towns. Voting machine technologies vary from Optical Scanning to Direct Recording Electronic (DRE) machines to paper ballots and hybrid systems, each with their own unique vulnerabilities and concerns. In addition, it's not just the voting machines at risk but the entire process from voter registration to casting votes, tabulating results, reporting the outcome and auditing the process. The process encompasses the machines themselves, the enterprise they are a part of and the people who install, administer and use them.

> *The process encompasses the machines themselves, the enterprise they are a part of and the people who install, administer and use them.*

It might seem that the variability in equipment and process is a plus for security because there are so many disparate systems and unknowns that will impact the attacker but at the same time, the variability of opportunity to infiltrate and attack is equally problematic in creating an integrated defensive response. On one hand, diversity could be working for us, better safeguarding election data, and by the same note, working against us. Obscurity or obfuscation can seem safer, however, in our election infrastructure, we actually have a diverse but well-known and published mesh of outdated systems that must operate together for proper election results. With multiple ways to breach the process and the diversity and expansiveness of the attack surface, voting integrity is a major challenge.

[14]*Hawkins, Derek, "The Cybersecurity 202: Voters' distrust of election security is just as powerful as an actual hack, officials worry," Washington Post, 5 June 2018.*
[15]*Center for Internet Security, "A Handbook for Elections Infrastructure Security," February 2018.*

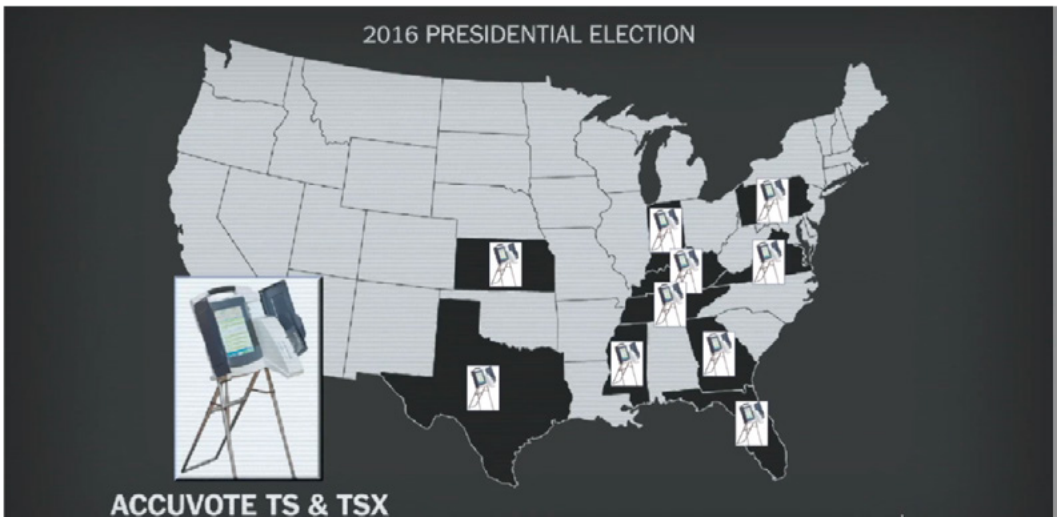


Figure 3 – Map of where Accuvote TS & TSX equipment is used and vulnerability to same attack

The non-profit Verified Voting Organization provides a web site[16] that lists the make, model and type of equipment used in each county, making it that much easier for a hacker to isolate an attack. Furthermore, an attack developed for one region can be tested and perfected on multiple other counties across the nation. Consider the example of the AccuVote TS and TSX touch-screen voting machines. In April 2018, a professor of computer science in the University of Michigan demonstrated how to hack this specific system. That system[17] was not only used in the state of Wisconsin but in several other critical battle grounds to include Texas and Florida[18].

To plan an attack, an adversary can purchase specific equipment to develop attacks on different machines or go after the credentialing process that signs the votes being transmitted to the central reporting system, or attack the firewalls protecting the voting machines or even modify data via the router on the internet[19].

To address voting system security gaps, The U.S. Election Assistance Commission provides a certification program for the equipment used in these counties and districts. However, states still face issues integrating election hardware among their districts, securing the data exchange between the state, vendors, counties, and districts, and handling the varying maturity of IT systems security to implement training within their state.

> *The highly distributed nature of election systems does not necessarily protect the system as a whole, because even small-scale attacks, or hacks in highly contested districts, can cast doubt on the legitimacy of the final election results.*

[16]*Verified Voting, "The Verifier – Polling Place Equipment," November 2018.*
[17]*Halderman, Alex, "I Hacked an Election. So Can the Russians.," New York Times, 5 April 2018.*
[18]*Atanesian, Grigor, "Voting systems in Wisconsin, a key swing state, vulnerable to hackers, security experts say," Journal Sentinel, 30 July 2018.*
[19]*Zetter, Kim, "The Myth of the Hacker-Proof Voting Machine," New York Times, 21 February 2018.*

The highly distributed nature of election systems does not necessarily protect the system as a whole, because even small-scale attacks, or hacks in highly contested districts, can cast doubt on the legitimacy of the final election results. It is for this and other safety reasons, countries including France, Britain, Germany and the Netherlands have opted to hand count ballots[20] in efforts to prevent an attack affecting the outcome, however this is not the most feasible or efficient solution for counties, states or districts with limited staffing and resources. To address this breadth of attack possibilities, we need an adaptable and measurable verification process that includes the **technology, processes and people** involved throughout the end-to-end election system.

> *To address this breadth of attack possibilities, we need an adaptable and measurable verification process that includes the technology, processes and people involved throughout the end-to-end election system.*

Technology: Understanding the Voting Ecosystem

Reducing the risk of a cyberattack on our election infrastructure requires an assessment of the full, end-to-end process, including the systems used and the personnel involved throughout. In many cases, the cyber risk outcomes from database and system integration must depend on proper configuration and system administration.

The below technology-driven components detail the phases of the entire election process at a high level to outline further the infrastructure ecosystem and demonstrate the complexity of the voting process.

Voter Registration. The voting process starts with voter registration. This is done either via mail, or in some states online. Registration takes place at the county and state level and involves verifying the validity of the registrant's identity and their meeting of eligibility requirements.

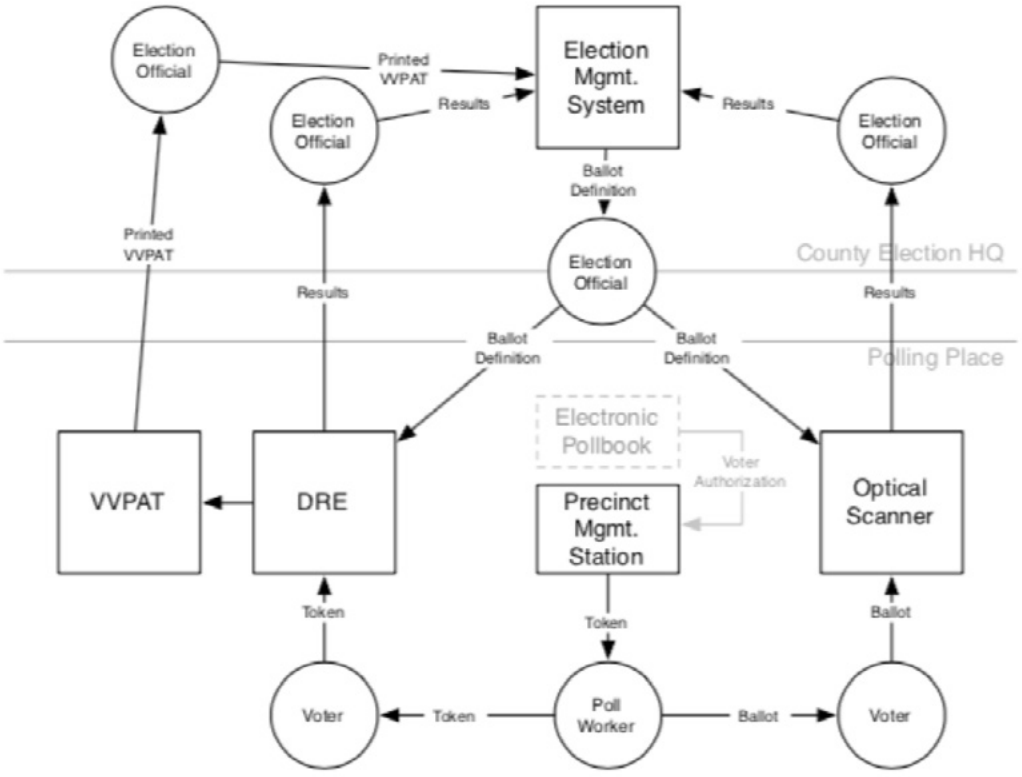
Casting the Vote. Voting is conducted in a variety of means. The voter may cast their vote during an early election, at their assigned voting site, or by mail. While voting in person there are four primary means through which their vote will be cast: hand-counted paper ballots, ballot-marking devices and digital equipment to include Direct Recording Electronic (DRE) systems and Optical Scan paper ballot systems.

[20] *Fidler, David, "Transforming Election Cybersecurity," 17 May 2017.*

Tabulation of Results. After the vote has been cast, it must be tabulated. The tabulation is done either at the precinct level, or the central (county) level. The means of tabulation is somewhat dependent on the vote casting method and is either completed manually or with automation. Depending on the system, there may or may not be a Voter-Verified Paper Audit Trail (VVPAT) to accompany electronic votes.

Auditing the Process. Auditing is a critical function to ensure the process is operating properly. Unfortunately, it is not consistent between election jurisdictions. Auditing is dependent on the state's policy and some systems lack any paper back-up capability at all.

The Everest Report[21], commissioned by the Secretary of State of Ohio provides a reference model for analysis of election systems. The reference model can be used to create a complete set of training tasks, conditions and standards to train the different personnel in all the work roles involved in the process.



[21] *Pennsylvania State University, "EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing," EAC.gov, 7 December 2007.*

The model identifies many different pathways of information flow at the county and district level. Outside of the model, there are additional systems that house and exchange voter registration data at the state level. Many of the pathways between county systems, election officials, vendors, and precincts occur over both networks and off-line removable media, and the complete set of pathways defines the potential attack surface for election hacking, which includes:

- State web-applications providing registration and verification of voters.
- State computers with access to voting registration systems.
- State computers that network with county election-board systems or load off-line removable media for distribution to counties.
- Election Management Systems at state, county or district levels, via networks or removable media.
- Intermediate networks and systems that house these computers.
- Contractors that provide ballot definition and loading services for counties and districts.
- Vendors that provide election machines and support services.

With many points of interaction and potential vulnerability, it is critical for states to conduct thorough risk-analysis and mitigation to find the system interactions and data exchanges. This includes both networked and removable media-based exchanges.

> *With many points of interaction and potential vulnerability, it is critical for states to conduct thorough risk-analysis and mitigation to find the system interactions and data exchanges.*

As discussed in detail below, using realistic Virtual Environments of these systems for testing and training provides a unique opportunity for personnel to see how footholds are established through web-based vulnerabilities, phishing, or use of removable media, and how these types of attacks can propagate through an environment both directly and off-line.

Process: Building Trust Across Systems

The decentralized election process assumes a large amount of trust among election systems, which creates additional opportunities for attackers. States and counties inherently trust the information they exchange and physical media is automatically trusted due to a chain of custody between districts and the county and state.

Unfortunately, air-gapped networks are not 100 percent secured as long as data is transferred from one network to the other[22]. If malware has been introduced through a compromised host, the chain of custody only assures that it hasn't been tampered by direct access, not indirectly by other computers and malware.

To mitigate this, election officials should train staff on how to implement strategies to verify data instead of implicitly trusting systems. Best practices to train personnel include processes that:

- Limit where systems connect and what they are used for. If a trusted machine connects with untrusted networks or media, it is no longer considered trusted.
- Ensure patches and known vulnerabilities are addressed. Unpatched systems are untrusted.
- Confirm security products are up to date and properly configured to detect attacks via email, web surfing, removable media insertion or network-based attacks.
  - » Scan any device that connects to the system via a peripheral port (e.g., CD/DVD/BlueRay, USB, PCMCIA memory cards).
  - » Apply security processes to address removable media best practices.
- Protect data stored on any device using strong encryption, such as AES 128/256 bit. Maintain a backup copy located in a secured, off-site location.
  - » Conduct risk-limiting audits, such as suggested by the UC-Berkley working group[23]. This ensures that processes are effective, builds a behavioral baseline, and facilitates incident response preparation. Do not consider any control as properly enforced until an audit has confirmed compliance or non-compliance through log data.

Many critical steps in the existing process rely on human interaction with the different components of the system including validating voter registration, entering election data, configuration of voting equipment, voting tabulation/processing, results consolidation and reporting. The process presents greater opportunities for attackers to act within and around those human interactions. And if the personnel are not trained to quickly identify suspicious activity, hackers will sneak right past them.

Movement of removable media

One situation to consider begins by targeting the board of elections personnel or contractors. These personnel are trusted to maintain and support the system used prior to and during the elections while also performing their regular duties in a production system. Attackers can target these users via spear phishing campaigns to gain initial access to the network. Another similar scenario involves the trusted unwitting insider with bad judgment who takes a flash drive in the cafeteria, bathroom or parking lot and decides to insert it into his desktop computer at work.

[22] *ISC-Cert, "USB Usage," U.S. Department of Homeland Security, 26 April 2010.*
[23] *Bretschneider, Jennie, "Risk-Limiting Post-Election Audits: Why and How" Risk-Limiting Audits Working Group, October 2012.*

Once inside the network, the attacker identifies critical systems by enumerating, becoming familiar with voting systems suites by data mining documents provided by the equipment vendor for user, maintenance and administrative personnel. He spends time analyzing and learning processes required to operate these specialized systems and compromise key systems to launch the attack[24]. Segregated networks or air-gapped systems (i.e. networks that aren't physically connected) are still at risk when data movement is done via removable media[25].

This presents an opportunity to manipulate removable media and loading malicious code during the transfer of legitimate files. Once the removable media is connected to the non-updated system, malicious code is released, infecting the host. The movement of removable media from system to system provides a transport mechanism for an attacker to tamper with votes, tabulation or results consolidation.

Insider Risk

A less sophisticated yet effective attack relies on a willing or coerced trusted insider to penetrate the network. Data published by the National Cybersecurity and Communications Integration Center cites local area network access as the top vector for insider threats and misuses (71 percent), physical access (28 percent) and remote access (21 percent)[26]. The inside personnel enable adversaries to perform a wide range of actions as discussed earlier. Detecting this type of a threat can be challenging yet indicators in human behavior can be detected by a properly trained workforce.

People: Establishing a Secure Approach

The threat is real and already identified as sophisticated[27]. Compounding the challenge is the lack of a federal standard to implement a complete security solution, leaving each jurisdiction trying to figure it out for themselves. Working within and across the states to certify the personnel on a secure approach within a standard training framework is one effective method to educate the personnel accessing the systems as well as personnel involved in the processing of such critical information.

Virtual Environments for Testing and Training

Testing and Training on specific systems is possible using Virtual Environments, which can be designed to mimic specific voting jurisdictions network models and equipment. Circadence has developed an immersive, gamified cybersecurity training platform called

[24] *Group-IB. (2017, Dec). Money Take: 1.5 Years of Silent Operations.*
[25] *Gonzales & Ramirez, (2017, Jul 13) Hidden Network: Detecting Hidden Networks created with USB Devices.*
[26] *National Cybersecurity and Communications Integration Center, "Combating the Insider Threat," U.S. Department of Homeland Security, Accessed 8 August 2018.*
[27] *Alperovitch, Dmitri, "Bears in the Midst: Intrusion into the Democratic National Committee," Crowdstrike, 15 June 2016.*

Project Ares® that presents different emulated environments under a range of attacks, complete with a synthetic internet and virtual real-world users. This platform prepares cybersecurity professionals by offering: pre-engineered missions with varied attack vectors; an Artificial Intelligence-powered advisor, umpire for objective assessments and opponents modeled from real-world threat actors; on-demand help and feedback for all levels to facilitate progress; and persistent, 24/7 availability in a secure cloud to train anytime, anywhere. This allows all personnel who interact and engage with any aspect of the election data usage and transfer process to be trained or assessed on actual cyberattacks, resulting in higher confidence of the training provided. This can lead to specialized certifications or requirements for personnel employment.

Example vulnerabilities and scenarios that can be built into the Virtual Environment include:

- Voter registration systems manipulated to:
  - » Drop voters from the polls, preventing them from voting
  - » Mark voters as felons, preventing them from voting
  - » Invalidate voter records (age, address, etc.) preventing record validation
  - » Theft and release of voter registration data

- Election equipment manipulated to cause:
  - » Changed votes
  - » Invalid vote counts
  - » Removal or manipulation of audit data
  - » Denial of service

- Denial of Service Attacks that:
  - » Prevent voter registration pre-election
  - » Prevent access to voter records through ransomware
  - » Prevent/Slow polling place throughput

Likewise, governments should ensure all their workers and contractors are trained to avoid phishing attacks, which can provide footholds into governments and election systems. System administrators need training on risk-assessment, network enumeration, segmentation, vulnerability management, and security configuration baselines to prevent attacks and limit their scope and propagation. Circadence's inCyt™ can support all knowledge levels of cybersecurity election training and awareness through the use of gamified activities where network emulations create authentic training environments for learners regardless of knowledge or skill level.

Implementation Strategy to Prevent Election Hacking

Consistent with the recommendations in the Cybersecurity Campaign Playbook[28], Circadence developed a five-step implementation strategy to immediately begin protecting the digital integrity of the election system. These steps address the technology, processes and people involved in election security and support near-term capabilities and longer-term strategies to handle the evolving threat.

Step 1. Adopt a holistic, continuous learning approach

With almost 90 percent of cyberattacks caused by human error or behavior[29], it is imperative that election security officials take strides to educate every person involved in the campaign process from volunteers and contractors to the participating candidates themselves. Unfortunately, there have been documented instances of untrained personnel who have knowingly and unknowingly jeopardized the security of elections thus far. Notably, one of the first cryptic signs of cyberespionage came when the Democratic National Committee (DNC) help desk contractor ignored repeated calls from the FBI who were reporting a computer system hack conducted by a Russian group referred to as "the Dukes[30]." The article notes the contractor "was no expert in cyberattacks," and couldn't differentiate the call from a prank call.

While cybersecurity professionals know threats are imminent and technology alone or training alone will not protect them from hackers, there still seems to be a lag in adopting a more integrative, holistic approach to cybersecurity where all parties are involved in securing their environments. Fortunately, with the passing of the Election Reform Program, now is the time for election security professionals to dedicate the resources necessary to address all aspects of cybersecurity that affect a strong cyber posture. This includes having the proper equipment and security protocols in place, employing a trained team who can identify and combat threats quickly, deployment of cyber resilience when attacks do occur, and much more.

> *Now is the time for election security professionals to dedicate the resources necessary to address all aspects of cybersecurity that affect a strong cyber posture.*

[28] *Mook, R., Rhoades, M., Rosenbach, E., "Cybersecurity Campaign Playbook," November 2017.*
[29] *Kelly, Ross, "Almost 90% of Cyber Attacks are Caused by Human Error or Behavior," Chief Executive magazine, 3 March 2017.*
[30] *Lipton, E., Sanger, D., Shane S., "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.," New York Times, 13 December 2016.*

When looking at election success as a whole, it is not just one component of the election (e.g., TV ads, canvassing, rallies, events) that dictates a win for the candidate.

It is a combination of many elements: strategic planning, outreach, appearances, communication, advocates, endorsements, etc. When combined, those efforts best position candidates for a win. The same holistic thinking can be employed to election cybersecurity efforts. We need a big picture view of every element that touches cybersecurity from start to finish to be better prepared for the challenges to come.

A holistic approach not only benefits the election campaign overall, but equally important, it can restore public confidence in voting. According to a 2016 Gallup poll, 66 percent of voters[31] are very or somewhat confident that votes will be cast and counted accurately across the country, so clearly, there's room for improvement. Failure to adopt a holistic approach, according to an election official means "we would be saying to the public that we didn't have confidence in the integrity of our voting system[32]."

Circadence's approach to cybersecurity supports a continuous learning model that gives training access to users at all knowledge levels through gamified, hands-on platforms available via desktop and mobile devices (including Project Ares and security awareness application inCyt). Practicing continuous learning with cybersecurity teams delivers the following benefits:

- Protects your company against evolving cyber threats
- Enables and empowers cyber teams to perform optimally and efficiently
- Increases productivity
- Expands knowledge of current hacker methods and understanding of ways to stop attacks
- Improves decision making
- Stimulates cognitive activity, keeping teams actively engaged and passionate about what they do

inCyt is a all-encompassing cyber awareness mobile application that lets teams compete in a multi-player game where they simultaneously protect their data while trying to steal their opponent's. The platform is reflective of and inspired by real-world cybersecurity offensive and defensive strategies and best practices. This game builds a culture where cybersecurity is everyone's responsibility in a fun and interactive way.

[31] *McCarthy, J., Clifton, J., "Updates: Americans Confidence in Voting, Election," Gallup, 1 November 2016.*
[32] *Lipton, E., Sanger, D., Shane S., "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.," New York Times, 13 December 2016.*

This active-learning style lets players practice strategies through demonstration and application, which improves information retention by 75 percent, as compared[33] to 5 percent in traditional classroom-based teaching styles. With intuitive game play, staff want to learn best practices in cyber so they can compete with their colleagues. The exercises are designed to provide useful information that employees can apply outside the workplace, such as using a Virtual Private Network (VPN) when connecting to public Wi-Fi.

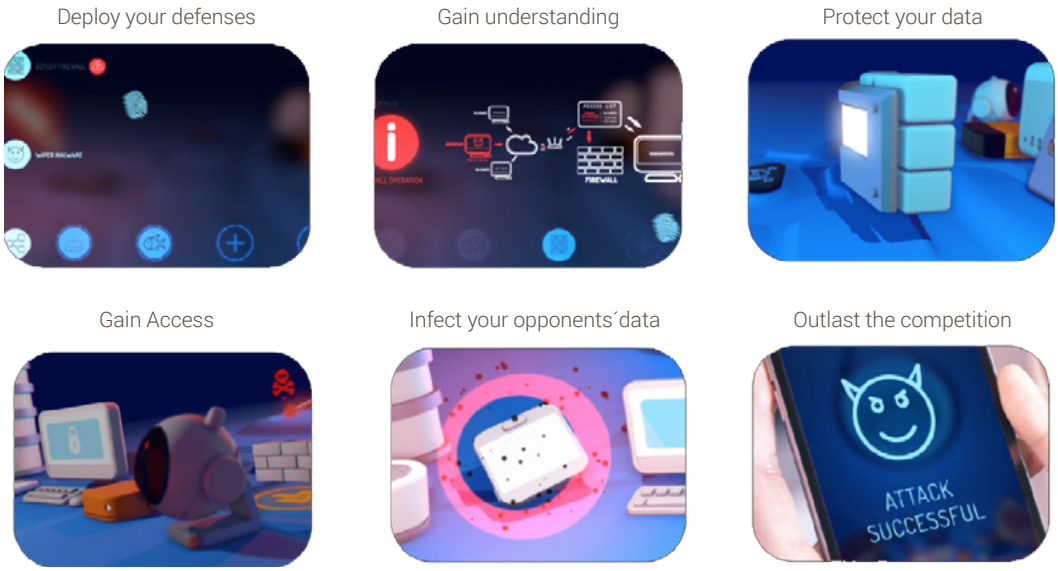


Figure 5 - inCyt game play is an example of "edutainment," or active learning

inCyt makes phishing, multi-factor authentication, spyware, password management, encryption, watering holes, man-in-the-middle attacks and many more relevant topics exciting and informative. The game is interactive and engaging, plus players compete with each other, bringing cybersecurity into the office dialogue. By providing this game to all employees, organizations can reach the non-technical workforce and convert them to be a part of the defensive strategy instead of the common cause of a successful breach.

> *By providing this game to all employees, organizations can reach the non-technical workforce and convert them to be a part of the defensive strategy instead of the common cause of a successful breach.*

[33] *Play to Teach, "Solving the training dilemma with game-based learning," Digitech, Accessed 28 August 2018.*

Figure 6 - inCyt helps everyone understand cyber technologies such as a VPN

About 60 percent of companies today use training to build security expertise[34] and 96 percent of cybersecurity professionals agree that they must keep up with their skills or the organizations they work for will be at a significant disadvantage[35]. Training and assessing personnel in the election process can begin today. As described below, additional election hacking scenarios and customized virtual environments can further advance the knowledge and evolve the training as the threat evolves.

> *Training and assessing personnel in the election process can begin today.*

Step 2. Analyze Attacks Previously Used to Understand Adversary Techniques

It is insufficient to solely analyze the specific attacks from the past few years but it is still important to see and understand the tactics and vulnerabilities exploited, particularly since voting machines are not upgraded often. In the words of philosopher George Santayana, "to know your future you must know your past." A strategic approach to boosting election security needs to include a thorough understanding of past threat actors, at minimum from the recent 2016 U.S. election. The New York Times visual depiction of state-sponsored hackers provides a high-level view and timeline of the election upheaval and effects[36].

Since threat actors evolve and build on past tools and approaches, security personnel must be familiar with and be able to protect, detect and respond against the already-known 2016 election attack groups Advanced Persistent Threat (APT) 28 Fancy Bear and APT29 Cozy Bear. Both of these groups are attributed to Russian nation state actors[37] and their attack methods have been analyzed in detail.

[34] Coursera, "Continuous Training Can Close the Cybersecurity Skills Gap," 22 November 2017.
[35] Oltsik, Jon, "The Life and Times of Cybersecurity Professionals," ESG and ISSA, November 2017.
[36] New York Times, "Following the Links from Russian Hackers to the U.S. Election," NYT, 6 January 2017.
[37] Office of the Director of National Intelligence, "Background to 'Assessing Russian Activities and Intention in Recent US Elections:' The Analytic Process and Cyber Incident Attribution," National Intelligence Council, 6 January 2017.

The group created an organization called DCLeaks operated by fake personas to deliver stolen email and documents to journalists[38] via Facebook. Fancy Bear also had a global effect, targeting military and political groups in Ukraine and Georgia and at NATO installations. As noted by the cybersecurity firm FireEye, "After compromising a victim organisation, APT28 will steal internal data that is then leaked to further political narratives aligned with Russian interests. To date these have included the conflict in Syria, NATO-Ukraine relations, the European Union refugee and migrant crisis, the 2016 Olympics and Paralympics Russian athlete doping scandal, public accusations regarding Russian state-sponsored hacking, and the 2016 US presidential election."

The group's use of malware and formal coding environments allowed for the creation and deployment of custom modules[39]. Approximately four key tactics have been identified by experts including "sending spear-phishing emails that either deliver exploit documents that deploy malware onto a user's systems, or contain a malicious URL designed to harvest the recipient's email credentials and provide access to their accounts.[40]" Tools like CHOPSTOCK, AZZY, OLDBAIT and other tools armed them with the resources they need to execute their tactics.

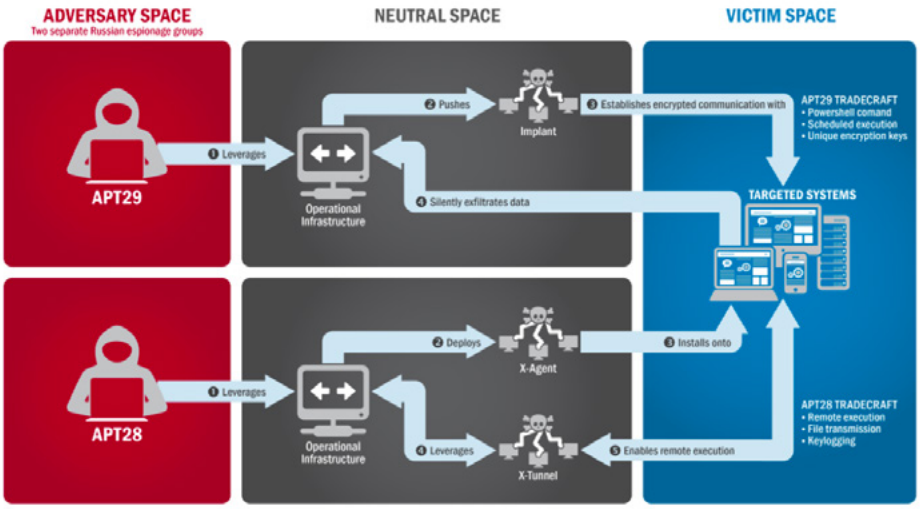


Figure 7 - The tactics and techniques of APT28 and APT29 can be virtualized for training

APT29 has also been observed crafting spear-phishing emails using web links to a malicious dropper; once executed, the code delivers Remote Access Tools (RATs) and evades detection using a range of techniques. APT28 is known for leveraging domains that closely mimic those of election organizations and tricking potential victims into entering legitimate credentials. APT28 actors relied heavily on shortened URLs in their spear-phishing email campaigns. Once APT28 and APT29 have access to victims, both groups exfiltrate and analyze information to gain intelligence value[41].

[38] *Constine, Josh, "Facebook shut down Russian APT28 trolls before the 2016 U.S. election," TechCrunch, 9 April 2018.*
[39.40] *Perez, Roi, "FireEye report: Hacking group APT28 and their tradecraft," SC Media, 12 January 2017*
[41] *NCCIC, "Grizzly Steppe – Russian Malicious Cyber Activity," Federal Bureau of Investigation, 29 December 2016.*

With real world threats and systems in a closed virtual world, personnel can safely observe and develop responses to practice with. Being able to handle APT28 and APT29 tactics in a Project Ares mission should be a core requirement for any defender of election systems. These cybersecurity professionals should be able to demonstrate highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence. This may include threat, exploitation, and forensic analysis.

Step 3. Assess Cyber Staff and Third Party Participants

With an understanding of past attacks and techniques, election officials and supporting organizations can begin assessing the skill level of their cyber teams and all involved in the election process to get a sense of their capabilities and how they would approach and prepare for a "Cozy Bear 2.0," for instance.

With HAVA allowing improvements to election security, officials may consider staff assessment tools to establish and promote a proactive security culture. Approaches may include facilitating a workshop where current policies and best practices are presented to election personnel to introduce the building blocks of cybersecurity. Leadership can take the lead with this effort to demonstrate a top down approach. Scheduled sessions reviewing adversary tactics (e.g., spear phishing, water holes, man-in-the-middle, whaling, spamming) and techniques exploiting elections systems as an extension of interconnected systems is another recommendation.

In addition to the aforementioned assessment approaches, assessments can also be conducted through Circadence's Project Ares platform. The virtual environments form scenarios or missions for cybersecurity personnel to handle that can be customized to mimic Cozy Bear and Fancy Bear attacks. For example, a Fancy Bear scenario would include phishing emails sent to simulated users in the election industry using the techniques and tools actually used by the Russians[42]. The key tactics include sending spear-phishing emails to deliver exploit documents that deploy malware onto a user's systems. A separate assessment pathway is available for trainees to demonstrate their knowledge in progressively difficult steps necessary for certification in one or more work roles.

[42] *Greenberg, Andy, "Everything we know about Russia's Election-Hacking Playbook," Wired magazine, 9 June 2017.*

Figure 8 - Project Ares is a virtual environment for training in cyber incorporated into an on-line game.

Example activities for Project Ares related to hacking elections include:

1) Mini-games for security concepts and drills

- Team understanding of the threats
- Familiarization with operational procedures to enhance security protections
- Two factor authentication and strong password implementation
  - » Social media, Elections Access Portals and official correspondence accounts
- Principles of Access Controls and management of roles
  - » Least privilege concept
  - » Authorized personnel
  - » Management of active and inactive accounts

2) Battle Rooms for individual training on tools and tactics

- Emulating adversary tactics (e.g., spear-phishing, water holes, man-in-the-middle, whaling, spamming) and techniques exploiting elections systems as an extension of interconnected systems

- Vectors of attack by an adversary and how to prevent falling victim
  - » Servers, workstation and personal devices
- Insider Threats
- Configuration management and audits trail as part of a comprehensive solution to detect intrusions or systems operational anomalies
- Log and back up data practices
  - » Tracking changes to the voter registration database
  - » Backups as part of a business continuity plan
- Principles and implementation of Hardware/Software configuration management
  - » Updates
  - » Notification system

3) Missions as comprehensive scenarios of likely attacks

- Core missions discussed above for APT28 and 29 Tactics in the attack on the Democratic National Committee
- Attacks involving varying equipment types (DRE with and without auditing) and Optical Scanners
- Scenario attacking the credentials for transferring data on voting results for tabulation
- Hypothetical future scenarios designed to disrupt the auditing process

Other assessment items may include an evaluation of staff's ability to collect and analyze information that may be used to develop intelligence (e.g. operational planning, gathering evidence on criminal or foreign intelligence) to mitigate possible or real-time threats. The National Initiative for Cybersecurity Education offers a blueprint[43] to categorize, organize, and describe cybersecurity work into tasks and knowledge areas that can guide staff assessments and vendor evaluations.

Step 4. Develop and test new processes to implement

An election is much more than the actual voting day and begins months prior with campaigns to register voters, polling to suggest leaders and social media campaigns to influence participants. Imagine a coordinated attack to degrade public confidence and

[43] NICCS, *"NICE Cybersecurity Workforce Framework," Department of Homeland Security, Accessed 11 August 2018.*

spread dissent through a combination of technical attacks, as discussed above, combined with careful and persuasive messaging. An election hack could begin with an attack on a media outlet website reporting polling or a state's website on instructions for voting day.

Once early voting starts, a polling site could report falsified exit polls on election day, taking cues from actual polling, to adjust the narrative throughout the day. On feeds which "support" a particular candidate, the site could show them slightly trailing, thus driving more voters to polls, while on feeds which support the opposition, the hacked site could show the opposition with a sizable lead, thereby dissuading the opposition voters from feeling the need to vote.

After election day, a coordinated attack could include a messaging campaign hinting at falsified data or hacked systems. This would call into question the validity of the entire election and cause even more division. Such an attack would likely keep the false social media posts going and question facts and sources.

Figure 9 - Public and private partners gathered together in City of Houston for Jack Voltaic 2.0 Cyber Research Project.

Are counties, states and national organizations involved in the election prepared to handle this scenario? What happens when an attack is detected and a website is properly restored? How will the messaging to the public be managed?

Complicated scenarios like this one are well-suited for a combined cyber Table Top Exercise (TTX) with a supported Live Fire Exercise (LFX) in Project Ares to practice the incident response from protection, to identification, detection, and response. Recently, public and private entities have joined forces to prepare for cyberattack events across various municipalities and departments in efforts to avoid attacks and prepare for what may come. In one event involving the City of Houston emergency response to simulated cyberattacks on transportation, energy, water and government, senior leaders worked directly with technical cyber defenders to understand attacks and develop timely responses. This type of holistic approach should be undertaken in every voting

jurisdiction. There will always be risks, but cities and counties are realizing that the key is getting ahead of the attack and developing policies and procedures through realistic virtual environments to handle it. Running through these cyber exercises with multiple players helps leaders see apparent gaps in defense and offense techniques while reaffirming the practices that must take place to secure any type of infrastructure, IT or specialized voting system.

Step 5. Use adaptable, gamified training to stay current and future proof

Election officials looking for ways to strengthen their cybersecurity efforts will not find peace of mind with traditional classroom-based training. Studies show information retention rates of such programs peak at 5 percent[44], versus 75 percent when active-learning, hands-on models are used.

CHALLENGES IN THE CURRENT CYBERSECURITY TRAINING INDUSTRY		HOW CIRCADENCE'S CYBERSECURITY TRAINING SOLUTION SOLVES THESE INDUSTRY CHALLENGES
LIMITED AVAILABILITY Availability limitations due to finite number of: • Qualified instructors • Realistic physical environments • "Classroom" training times / schedules	✓	**ALWAYS AVAILABLE** • AI instructors and adversaries operate 24x7 • Boundless virtual space via public cloud scalability • Access to high-fidelity training platform any time and across devices
HIGH COSTS Prohibitive cost of: • Expert Instructors in Cybersecurity • Cyber Realistic Physical infrastructure • In-person training • Red Team Adversaries	✓	**BETTER INVESTMENT** • Continuing, ongoing education vs. one-time course • Curriculum curated by industry subject matter experts in cyber tradecraft and operations, threat intelligence and data analytics • Gives employers ability to determine employee skills objectively
SKILL RETENTION Lack of post-training practice environments; 80% of traditional instructor-led training is lost in 30 days	✓	**REFRESH ON DEMAND** • Engages learners individually or in teams • Active learning can increase retention by more than 75% • Retain and reinforce skills through repetition
OUTDATED THREAT SOURCING Training content is perishable and trainers are not capable of keeping up with the ever changing threat landscape	✓	**AGILE CONTENT** • Responsive to changes in threat landscape through automated artificial intelligence (AI) and machine learning (ML) threat data collection • Ecosystem feeds threat data to improve training • AI and ML augment cyber actions to ensures trainees are learning best practices to combat latest threats
DULL, STATIC LECTURES "Death by PowerPoint" classroom lectures or unexciting videos facilitate boring trainings; estimated that just 5% of classroom information is retained	✓	**GAMIFIED EXPERIENTIAL LEARNING** • Immersive, hands-on training via modern gamification • Competitive scoring and game reward systems keep students engaged • Realistic cyber missions based on modern threat scenarios

Table 1 - Use a gamified training platform to solve gaps in cybersecurity training

[44] *Play to Teach, "Solving the training dilemma with game-based learning," Digitech, Accessed 11 August 2018*

Unlike compliance-driven teaching methods, gamified teaching engages practitioners individually and in teams, through modern learning strategies. It works by deploying connected, interactive, social settings that allow learners to excel in competitive, strategic situations. One can imagine how useful this would be for election personnel who work individually and in teams to monitor vulnerabilities across systems and processes, making everyone's job much more fluid.

Game-based learning allows trainees to apply what they know to simulated environments or "worlds," creating a natural "flow" that keeps them engaged and focused. And we're not talking about simple Capture the Flag games, we're referring to cybersecurity exercises inspired by game-like activities to effectively engage learners.

According to Training Industry, gamified training programs are customizable based on an organization's needs; visually-driven through use of progress bars and milestones; and are usually time-bound to hold employees accountable for task completion[45]. Further, achievements, points, badges, trophies, and rewards/recognition of progress gives users a sense of accomplishment, keeping them motivated and engaged. Neuroscientist Eric Marr says the reason it works so well is because when an individual engages with gamified simulations, the brain releases dopamine[46], a chemical that plays a role in the motivational component of reward-driven behavior. Marr says "Dopamine helps activate the learning centers in the brain. If your brain releases dopamine while you're learning something, it helps you remember what you've learned at a later date."

Figure 9 - Gamified exercises like Cylitaire engage trainees in hands-on activities that reinforce cybersecurity concepts and put them into practice.

[45]Wong, Johnson, "Gamification of Work," Training Industry, 25 September 2017.
[46]Kozera, Greg, "Gamification: The Power of Gaming Features in Corporate eLearning," Elm Learning, 5 December 2017.

Studies[47] outline the following benefits:

- Increased engagement, sense of control and self-efficacy
- Adoption of new initiatives
- Increased satisfaction with internal communication
- Development of personal and organizational capabilities and resources
- Increased personal satisfaction and employee retention
- Enhanced productivity, monitoring and decision making
- Development of personal and organizational capabilities and resources

With so many individuals of varying expertise levels working on elections, a method like gamified training can ensure every professional has the skills and knowledge to safeguard the data they're accessing. Circadence has identified solutions that ensure those who are handling election data have both the conceptual and experiential capabilities necessary to work on new systems and are amply prepared thanks to being trained in virtual environments.

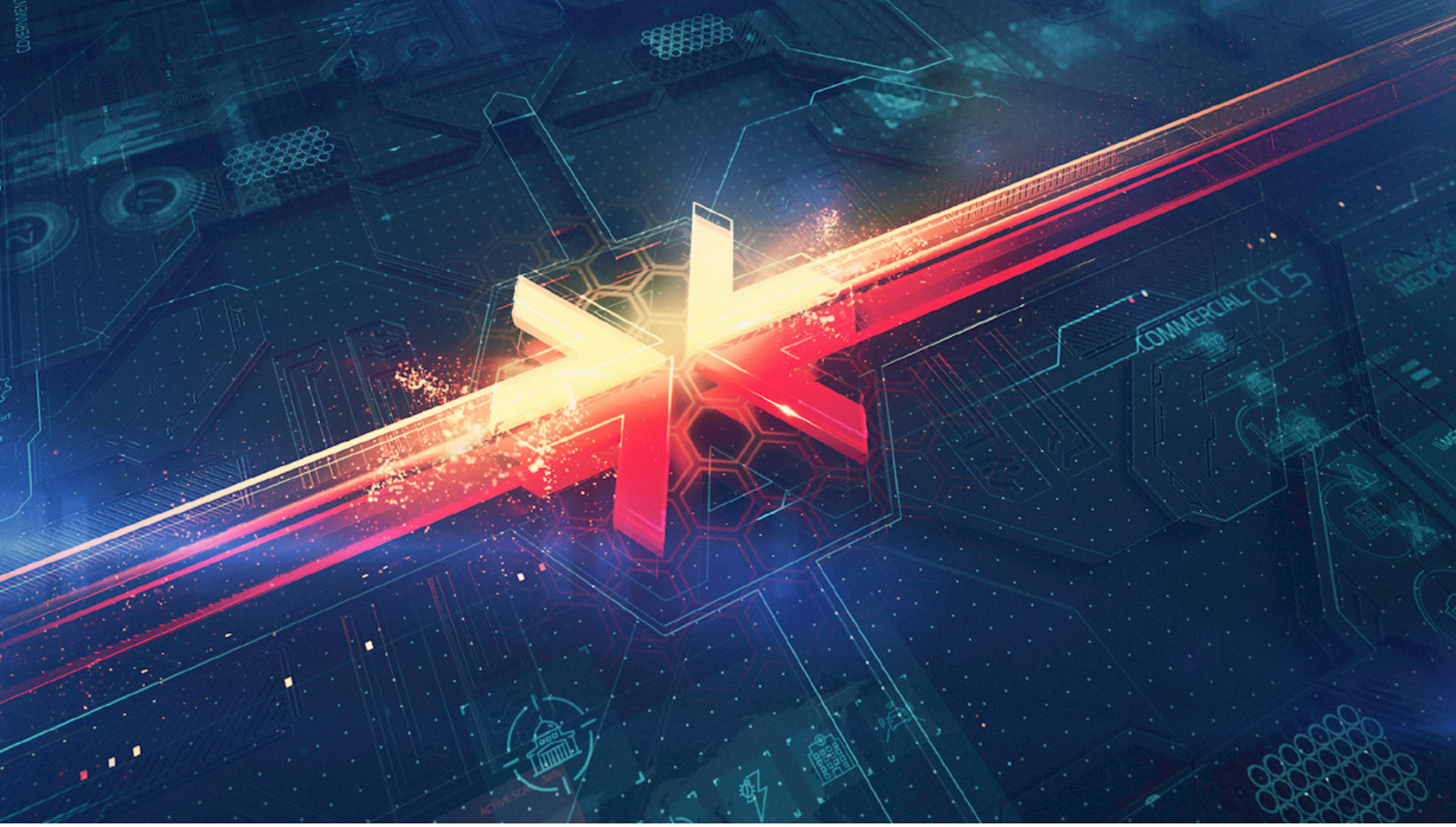
Project Ares can provide virtual environments in a gamified setting to raise awareness and teach the best practices in cybersecurity to protect, detect and respond to attacks within the voting ecosystem. It includes a tool called Orion™ that allows organizations to develop their own customized activities to address new voting systems, processes and the adaptability of the threat.

Conclusion

As election security officials plan for new ways to leverage the HAVA Election Security Fund to improve processes, they will be pressed with justifying such expenditures while also demonstrating that said security measures have indeed improved. Further, between the intelligence community's assessment of Russia's interference and what history has documented as proof of poor security measures, complacency is not an option as we move forward on future campaigns across the globe.

The recommendations we've proposed will make elections safer and protect public confidence in their legitimacy while preserving digital election integrity. Now is the time to take the reins to protect democracy once again. By using gamified training that focuses on our people, we not only improve infrastructure security but we lessen the likelihood of human error as dominant sources of cyberattacks.

[47] *Oprescu, F., Jones, C., Katsikitis, M., "I Play at Work—Ten Principles for Transforming Work Processes Through Gamification," U.S. National Library of Medicine, 30 January 2014.*



LOCATIONS

Headquarters – Circadence Corporation
1900 9th Street, Suite 300
Boulder, CO 80302

Advanced Research & Development Facility
398 E. Main Street, CDF Building, 2nd Floor
Tupelo, MS 38804

Center For Cyber Autonomy & Data Sciences
9665 Chesapeake Drive, Suite 401
San Diego, CA 92123

Washington, D.C. Sales Office
6715 Whittier Avenue, 3rd Floor
McLean, VA 22101

CIRCADENCE

Circadence® Corporation is a market leader in next generation cybersecurity education and training. Circadence's ecosystem is the first fully immersive, AI-powered cybersecurity training and assessment platform for government and enterprise organizations.

Circadence's solutions modernize outdated and largely generic cybersecurity training with an advanced online gaming platform that delivers persistent, immersive and real-to life experiences that match and adapt to a contemporary threat environment. Contact us at 303.413.8800 or www.circadence.com/contact