FORD SCHOOL OF PUBLIC POLICY
SCIENCE, TECHNOLOGY AND PUBLIC POLICY
UNIVERSITY OF MICHIGAN

ELECTION SECURITY PERSPECTIVES FROM INTELLIGENCE AND ELECTION CYBERSECURITY EXPERTS

Intelligence and Cybersecurity Experts

Javed Ali

J. Alex Halderman

Student Research Assistants

Terry Nguyen

Molly Sherry

Cyrus Soonavala

Introduction

Deterring election interference remains an ongoing challenge for national security institutions and election administration agencies. Interference is defined as "any covert, fraudulent, deceptive, or unlawful actions or attempted actions of a foreign government, or of any person acting as an agent of or on behalf of a foreign government, undertaken with the purpose or effect of undermining confidence in, or altering the result or reported result of, the election, or undermining public confidence in election processes or institutions." The primary areas of concern are voter registration databases, voting machines, and outdated election infrastructure standards that are vulnerable to malign foreign interference. Javed Ali, associate professor of practice at the Gerald R. Ford School of Public Policy, and J. Alex Halderman, the Bredt Family Professor of Engineering and a professor of Electrical Engineering and Computer Science, agreed to share their expert insights into the state of U.S. election security. Professor Ali expressed his confidence in the intelligence community and in improvements made to cyberinfrastructure and inter-agency coordination to deter cybersecurity threats. Professor Halderman encouraged greater state, local, and federal agency cooperation to implement uniform election infrastructure standards. He also urged election administration agencies to implement both defensive and deterrent measures to counter any election interference attempts. An evolving threat landscape presents a variety of security challenges, but Americans can be confident that their vote was safeguarded this election cycle. Despite known attempts at interference, they were not large or effective enough to alter election results.

HOW DOES VOTING WORK IN THE UNITED STATES?

The United States electoral system is highly decentralized and often managed at the county level, with more than 10,000 election jurisdictions across the country. As a result, there is significant variation in how elections are conducted. The National Voter Registration Act of 1993 (NVRA) mandates that each state appoint a chief election official to oversee the administration of elections. The United States Election Assistance Commission (EAC) provides guidance to election officials but does not possess regulatory oversight over the conduct of elections.

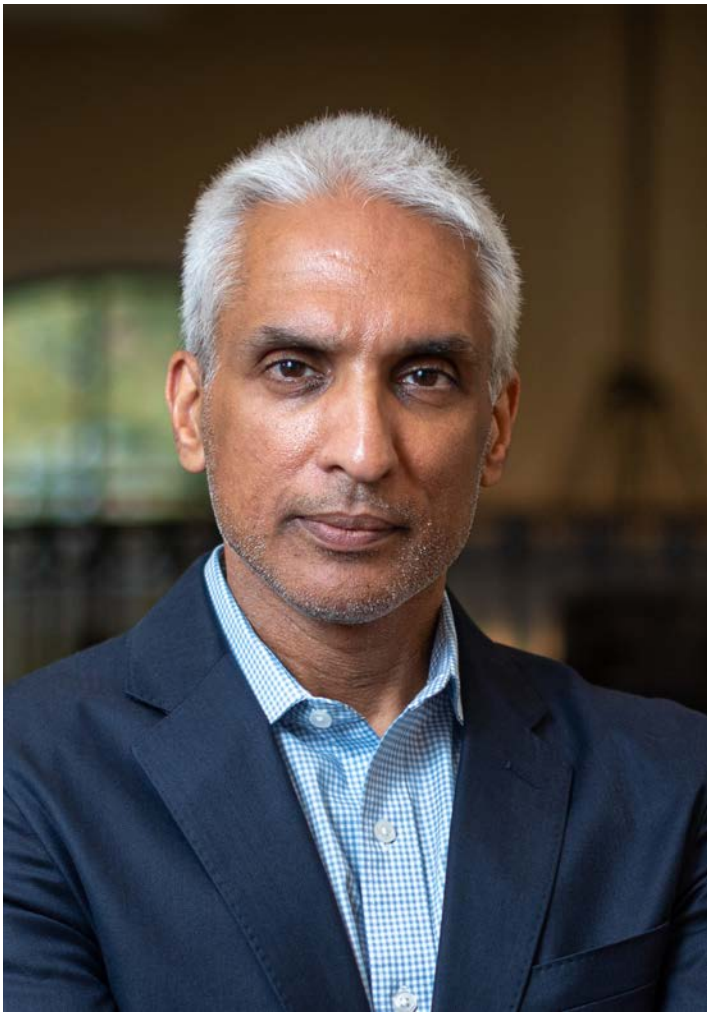
Systems of voting vary by state and jurisdiction; however, each state utilizes one or a combination of the following systems:

- Hand-Marked Paper Ballots: Voters mark their selections by filling in an oval, box, or similar shape on a paper ballot, which is then scanned either at the polling place or at a central location.
- Ballot Marking Devices (BMDs): BMDs present the ballot electronically, allow voters to make their selections digitally, and produce a human-readable paper ballot. Initially designed for voters with disabilities, BMDs are now used by all voters in certain locations.
- Direct Recording Electronic (DRE) machines: DRE systems record votes directly into the computer's memory using touchscreens, dials, or mechanical buttons. Some DRE systems include Voter-Verified Paper Audit Trail (VVPAT) printers to create paper records for potential audits or recounts.

Investment in paperless electronic voting machines surged after the 2000 Bush v. Gore election. In that election, Florida voters used styluses to punch out paper chads. This process led to "hanging chads"—ballots that were not completely punched through—which raised doubts about the accuracy of voter intent. These issues eroded confidence in the paper voting system among election officials.

Russian interference in the 2016 election, however, raised concerns about security vulnerabilities in electronic election systems when Russian Advanced Persistent Threat (APT) groups scanned voter registration systems for vulnerabilities. While U.S. government inquiries found no evidence of altered election results, to safeguard against potential breaches and ensure the integrity of election outcomes, many election officials came to see the need to back up electronic voting with paper ballots. Currently, only Louisiana and Texas contain counties with completely paperless voting systems. Election-deciding swing states—Arizona, Georgia, Michigan, Nevada, North Carolina, Pennsylvania, and Wisconsin—all maintain paper records, which are used in post-election audits in 48 states. To maintain the security and integrity of our electoral system, election administrators should migrate the remaining legacy systems to modern voting systems.

ELECTION SECURITY PERSPECTIVES FROM INTELLIGENCE COMMUNITIES: IN CONVERSATION WITH JAVED ALI



JAVED ALI

Professor Javed Ali is an associate professor of practice at the Gerald R. Ford School of Public Policy where he delivers courses on counterterrorism and domestic terrorism, cybersecurity, and national security law and policy. Professor Ali brings more than 20 years of professional experience in national security and intelligence issues in Washington, DC. He held positions in the Defense Intelligence Agency and the Department of Homeland Security before joining the Federal Bureau of Investigation. While at the FBI, he also held senior roles on joint duty assignments at the National Intelligence Council, the National Counterterrorism Center, and the National Security Council under the Trump Administration. The following responses are paraphrased from interviews conducted with Professor Javed Ali on October 23, 2024 and November 6, 2024. Direct quotations are indicated by quotation marks.

Q: WHAT THREATS WERE PRESENT DURING THE 2020 ELECTION? WERE THE 2024 ELECTION RESULTS SAFE FROM FOREIGN INTERFERENCE?

Despite foreign interference and influence operations attempts from Russia, Cuba, and Iran to sway voter opinions through social media disinformation and propaganda, multiple federal agencies, including CISA (Cybersecurity and Infrastructure Security Agency), the FBI (Federal Bureau of Investigation) and NCSC (National Counterintelligence and Security Center) concluded that no foreign actor successfully compromised or manipulated vote tallies or election infrastructure in 2020. According to the declassified Intelligence Community Assessment, no foreign actors successfully altered any technical aspects of the voting process in the 2020 U.S. elections. The intelligence community (IC) found no indications of interference with voter registration, ballot casting, vote tabulation, or reporting results.

Proactive defensive measures enacted by IC agencies such as firewalls, patching, cybersecurity training, and separation of election systems prevented system compromise attempts. The IC assessment concluded that Russia did not make persistent cyber efforts to gain access to election infrastructure as it had in 2016. Iran exploited a vulnerability to compromise some U.S. election-related entities in early 2020, but this was assessed to be part of a broader targeting effort rather than intended for election interference.

Despite attempts at interference from foreign nations, the 2024 election was more secure than ever. Jen Easterly, head of the Cybersecurity and Infrastructure Security Agency (CISA), expressed confidence in the integrity of the election infrastructure:

> "As we have said repeatedly, our election infrastructure has never been more secure and the election community [has] never [been] better prepared to deliver safe, secure, free, and fair elections for the American people. This is what we saw on November 5th in the peaceful and secure exercise of democracy. Importantly, we have no evidence of any malicious activity that had a material impact on the security or integrity of our election infrastructure."

Director Easterly noted that no specific cyber activity targeting election systems was detected, and various security measures, like paper vote records, maintained transparency and reliability. Although foreign actors attempted to interfere, they did not succeed in altering election outcomes on a scale

Photo Credit: LPETTET

Q: HOW DID THE U.S. HOMELAND SECURITY AND INTELLIGENCE AGENCIES COMBAT ELECTION INTERFERENCE?

Our homeland security and intelligence agencies are the first line of defense against election interference and influence from foreign adversaries. The fact that these intelligence operations are rarely noticeable is an indicator that they are intercepting threats before they materialize into noteworthy incidents.

CISA is responsible for the government's federal, state, and local election infrastructure security and is a sub-element within the larger Department of Homeland Security (DHS). The agency is tasked with conducting regular testing and vulnerability assessments on voting equipment to address any weaknesses ahead of time. Over 97% of voting jurisdictions use paper ballots, which provide a verifiable record to support recounts or audits.

The National Counterintelligence and Security Center (NCSC) within the Office of the Director of National Intelligence (ODNI) spearheads the government's information-sharing and foreign threat-detection operations. They share information on foreign influence tactics and educate election officials, political campaigns, and the public on recognizing these tactics and countering them with reliable information.

As the lead federal law enforcement and domestic intelligence agency in the United States, the Federal Bureau of Investigation (FBI) would have responsibilities to investigate any possible attempts by foreign adversaries to conduct election interference operations as part of its broader cybersecurity responsibilities, assisted by intelligence and information from other partners in the IC. Likewise, the National Security Agency (NSA) and the US military's cyber command (CYBERCOM) established an Election Security Working Group in 2022 to help detect signs of possible foreign adversary interference operations and respond to possible intrusions.

Photo Credit: Sergeant Matt Hecht from Rawpixel

Q: WAS THE U.S. GOVERNMENT WELL EQUIPPED TO ADMINISTER AN ELECTION FREE FROM FOREIGN INTERFERENCE IN 2024?

Policy and computer science professionals agree that the government was well-positioned to administer an election free from malign foreign interference. Improvements in cyberinfrastructure and inter-agency coordination, as well as valuable lessons learned from 2016, prepared election officials well to administer a free and fair election:

> "We've had several years now to anticipate those kinds of threats and to harden our system, both physically and technically, and raise the awareness that these foreign adversaries are trying to do what they have done in the past. So I'd like to think that we were in a much better [position] going into the 2024 elections, but as I say in counterterrorism, you're never going to have a hundred percent security in anything."

This preparedness was demonstrated by the effective response by intelligence community members and election administrators to Russia's false reports of bomb threats aimed at disrupting the electoral process.

U.S. election officials navigated Russian-linked interference on Election Day with preparedness, effective responses, and clear communication. As hoax bomb threats originating from Russian email domains targeted polling sites in key battleground states—Georgia, Michigan, Arizona, Wisconsin, and Pennsylvania—officials coordinated evacuations, secured emergency court orders to extend polling hours, and swiftly resumed voting. Polling locations in Georgia's Fulton and DeKalb counties, which faced over two dozen threats, were evacuated but quickly reopened, ensuring minimal voter access disruptions. Georgia's Secretary of State, Brad Raffensperger, attributed the disruptions to Russian attempts to "get us to fight among ourselves," emphasizing that divisive tactics failed to derail election operations. Former DHS cyber agency head Chris Krebs commended the resilience of election workers, calling them "natural emergency managers" adept at handling unforeseen challenges. Arizona Secretary of State Adrian Fontes echoed this sentiment, highlighting that officials were prepared to maintain order despite efforts to intimidate voters. The FBI found no credible bombs at the sites and allowed voting to continue safely. High early voting turnout also mitigated the impact of Election Day disruptions. With over 80 million votes secured ahead of time, the temporary evacuations and delayed reopenings at polling sites on Election Day affected fewer voters than they might have otherwise. The early voting buffer allowed officials to focus on swiftly resolving Election Day issues without compromising overall voter access and turnout, reinforcing the resilience of the election process against interference attempts.

ELECTION SECURITY PERSPECTIVES FROM CYBERSECURITY EXPERTS: IN CONVERSATION WITH J. ALEX HALDERMAN

J. Alex Halderman

Professor Alex J. Halderman is the Bredt Family Professor of Engineering and Professor of Electrical Engineering and Computer Science at the University of Michigan where he is also the Director of the Center for Computer Science & Society. Professor Halderman's research focuses on computer security and privacy, with an emphasis on problems that broadly impact society and public policy. Topics that interest him include software security, network security, security measurement, privacy and anonymity, election cybersecurity, censorship resistance, computer forensics, and online crime. He is also interested in the interaction of technology with law and policy, politics, and international affairs. These insights are based on an interview with Professor Alex Halderman, recorded on October 29, 2024. The content reflects the substance of his remarks, with language adapted for clarity and brevity.

Q: WHAT THREATS WERE PRESENT DURING THE 2016 AND 2020 ELECTION CYCLES? WHAT ATTACK VECTORS WERE USED?

The 2016 and 2020 U.S. election cycles faced a variety of threats aimed at undermining election integrity from state actors. In 2016, Russia conducted a multi-pronged attack targeting U.S. election infrastructure. It probed election-related systems in all 50 states and successfully breached voter registration system databases in at least two states. In at least one state, Russia gained the capability to alter or destroy state registration data. By August, Russian intelligence agencies had the capability to scramble voter registration records of voters in Illinois. The intelligence community assessed that Russia did not ultimately execute such an attack, not because of technical limitations, but due to a tactical decision by Russian leadership. This was the first time U.S. intelligence had been the victim of "sweeping and systematic" election interference that "violated U.S. criminal law." By 2020, the cyber threat landscape had expanded to include additional state actors such as Iran, China, and Cuba. Each of these state actors had a vested interest in swaying U.S. public opinion. Simultaneously, a domestic threat emerged: operatives with connections to the Trump campaign accessed election systems in multiple states, capturing data that could later be exploited to create "technically credible" false claims of election fraud. This access heightened the risk that even non-state actors could deploy tools originally designed by adversarial state actors. While substantial funds have been allocated to encourage election infrastructure security, uneven deployment across states has left critical security gaps, creating a patchwork of risk and resilience.

Photo Credit: LPETTET

Q: WHAT ARE GOVERNMENT AGENCIES DOING TO COMBAT ELECTION INTERFERENCE?

Agencies like the Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Homeland Security (DHS) are focused on collaborating with local election officials to improve election security, but their efforts are constrained. CISA provides training, resources, and guidance to help local officials better understand and manage cybersecurity risks, but it lacks regulatory authority over state and local election systems. The agency has faced challenges in coordinating with the vast number of local election offices and has had to focus on building relationships and encouraging best practices without the power to enforce compliance. This approach has made progress in guarding elections but has also led to inconsistent levels of security across jurisdictions. CISA's dual mission of combating election disinformation and addressing cybersecurity threats also creates a conflict, as publicly addressing security concerns could risk eroding public trust in elections. Admitting existing risks could erode public trust in the election system, yet minimizing or denying these risks could give a false sense of security. Since 2016, CISA and DHS have also worked to raise awareness of election vulnerabilities, pushing for stronger practices like using voter-verifiable paper ballots and conducting post-election audits. While CISA and DHS have advanced election security awareness and improvements, election administrators must do more to secure elections. Critical vulnerabilities remain in some systems, and without more authority, uniform standards, and targeted funding, achieving consistent, high-level election security nationwide remains a challenge.

Photo Credit: eyecrave productions

Q: WHAT WAS THE STATE OF OUR ELECTION INFRASTRUCTURE SECURITY THIS ELECTION CYCLE?

There remained infrastructure vulnerabilities and concerns about state and local preparedness during this election cycle. While there has been progress since 2016, including over a billion dollars in federal grants to states, the improvements have been uneven and insufficient. The current situation remains "a patchwork of strength and weakness when it comes to cyber security among the states." The problems were serious: days before the election, Professor Halderman reported a "devastating vulnerability" in one swing state's voter registration system that could have enabled a large volume of false votes. CISA has yet to make any statement addressing this vulnerability, and no registered voting machine manufacturers have publicly acknowledged releasing patches for any voting machines since then.

While federal money was provided to states, it came without effective standards for how it should be deployed, leaving states "to their own devices" about implementation. This led to a situation where some newly purchased election equipment was "well secured," while other equipment was "drastically under-secured." Local election administrators want more federal funding but resist new directives or standards. In the scenario where election outcomes in states were decided by less than 1% of votes, "simple human error might alter the results, let alone malicious, well-designed attacks." Although security risks to our election infrastructure will always exist, security risks are not the same as security breaches. Security experts distinguish between theoretical vulnerabilities and confirmed breaches. The 2024 election served as a prime example of this difference. Despite multiple attempts to interfere with the election by foreign adversaries, no credible evidence of election hacking that could have affected the outcome has ever emerged. Claims of widespread interference have consistently proven to be either

Photo Credit: Michelle R. Lee

POLICY RECOMMENDATIONS FROM CYBERSECURITY AND INTELLIGENCE EXPERTS

CYBERSECURITY STRATEGIES FOR ELECTION INFRASTRUCTURE

Election administration agencies should implement policies that focus on both defensive and deterrent measures. Leveraging all available U.S. government powers to disincentivize foreign adversaries from attempting cyberattacks against election infrastructure will be the most effective method of deterring foreign threats. Local governments should raise the security standards and practices within the election system. Election administrators should better utilize federal resources and standards to promote uniform, high-level security across states. Federal funding should also come with security requirements, creating more consistent cybersecurity practices nationwide. This approach would address vulnerabilities that remain under-addressed in some states and encourage efficient use of funds in ways that improve election security.

EXPANDING DETERRENCE STRATEGIES

To deter future attacks, IC members should expand the array of retaliatory measures available to counter foreign election interference. Building a deterrence framework requires approaches that extend beyond traditional diplomatic sanctions. Cybersecurity experts and policymakers propose expanding the toolkit to include targeted financial measures, counter-cyber operations, and strategic information campaigns. These tools allow democratic nations to impose proportional costs on malicious actors while maintaining control over escalation. We should also reduce the certainty requirement for identifying threat actors, enabling more proactive responses when attacks are likely attributed to state actors. While this approach may strain diplomatic relations, national security issues such as election integrity must take precedence. By implementing these comprehensive deterrence strategies, democratic nations can impose proportional costs on malicious actors while maintaining escalation control and protecting the fundamental democratic process.

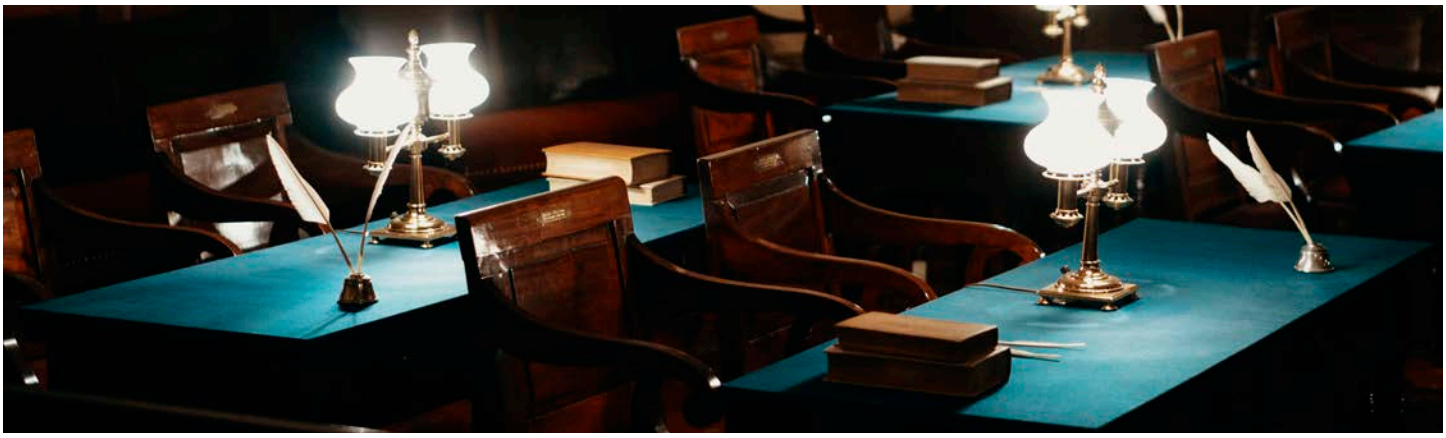


Photo Credit: Michael Savidge