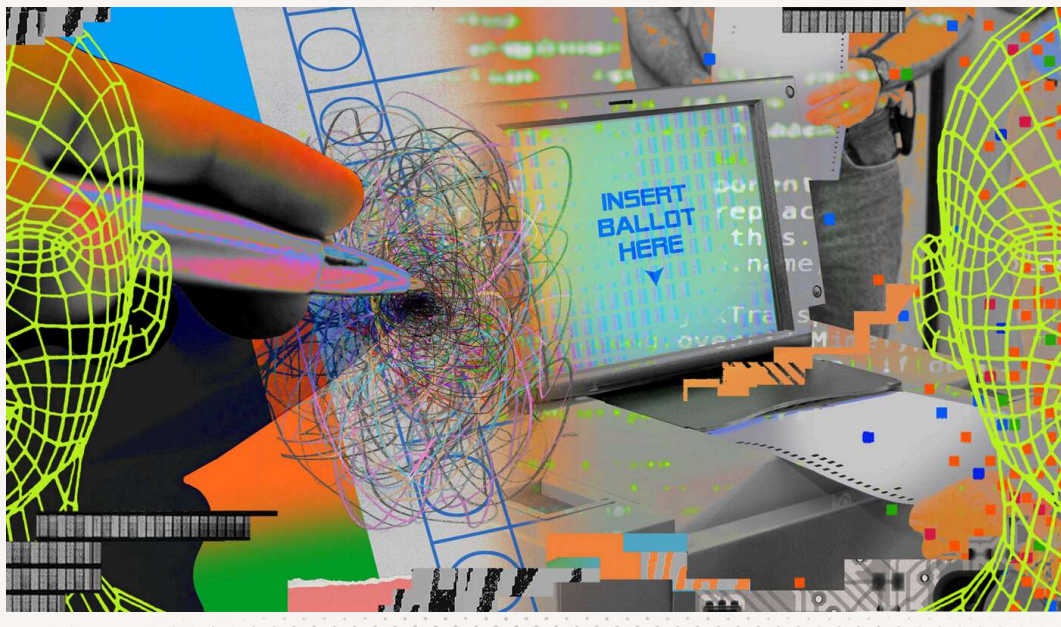
EXPERT BRIEF

Artificial Intelligence and Election Security

To protect election infrastructure and personnel from AI-generated threats, election offices and vendors must implement the best practices that experts have been urging for over a decade.



Chris Burnett

Lawrence Norden

Gowri Ramachandran

PUBLISHED: October 5, 2023

Defend Our Elections

- Election Security

View the entire *AI and Democracy* series ▶

In the course of writing this article, we have spoken to numerous election officials and security experts about their apprehensions and ambitions regarding **generative artificial intelligence**. Within the elections community, many officials have expressed grave concerns about what generative AI might mean for election security. That sentiment aligns with **recent media discourse** highlighting the dangers posed by AI. An illustrative May 2023 **article** in the *Washington Post* described an increase in phishing attacks attributed to AI, noting that such attacks are "just the beginning . . . as attackers use artificial intelligence to write software that can break into . . . networks in novel ways, change appearance and functionality to beat detection, and smuggle data back out through processes that appear normal."

Other commentaries recount the ways that AI may make it easier to **impersonate election officials, offices, and system vendors** in order to infiltrate election infrastructure and mislead the public. Meanwhile, some election officials worry that excessive emphasis on AI's frightening capabilities itself breeds more peril. David Triplett, the elections manager for Ramsey County, Minnesota, wonders if "all this talk about AI's power is fueling even more paranoia and confusion about the trustworthiness of elections." Such concerns seem valid given **recent sensationalist narratives** stoking public fears to propagate **baseless claims** of **AI-driven election rigging**.

How much should election offices and vendors worry about the security threats posed by advances in AI, and what steps should they take to prepare for them? This article is the inaugural piece in a series delving into AI's potential effects on American democracy. It examines generative AI's capacity to disrupt the security of election offices and election system vendors. Specifically, we look here at how AI changes (and *does not* change) the cybersecurity situation for election offices and election infrastructure. We also look at the threat that generative AI poses to the ability of election offices to function as authoritative sources of election information and records. We then detail measures that government, the private sector, and the media must take to guard against AI's risks and build public confidence in the integrity of election outcomes in the AI age.

Later pieces in this series will consider, among other issues, AI's effects on manipulated media in political advertising, election administration, voter suppression efforts, and the public comment process.

How to Counter AI Threats to Election Security

AI THREATS	MITIGATIONS
More sophisticated phishing attacks against election offices and vendors	• Implement Cybersecurity and Infrastructure Security Agency (CISA) trainings for election offices and vendors on how to spot and prevent AI generated phishing attacks • Election offices and vendors should remove data on the internet that could be used to personalize phishing attacks
More advanced malware	• Build more security and resiliency into election systems, such as paper ballots, audits, backups, expanded use of multifactor authentication • Provide more technical support to election offices, such as state cyber navigator programs and cyber security advisors from CISA • Create federal regulation of election vendor security practices • Create federal standards for use of AI by vendors and election offices • The federal government should invest in tools to defeat AI generated cyberattacks and infrastructure to distribute new tools to election offices nationwide
Impersonation of election offices and vendors	• Move election websites to .gov • CISA/Election Assistance Commission (EAC) should create government verified handles for election office social media accounts
Misuse of open records processes to disrupt election offices' work	• Implement CAPTCHA verification tests for open records requests, allowing accommodations for accessibility • Publish all unique open records responses on government websites • CISA should pilot use of authentication tools for official election related documents
Increased mistrust in elections due to ignorance about AI	• Journalists should take extra steps to verify election-related content • EAC and CISA should collaborate with election officials to enhance public awareness and confidence in election system security • EAC and CISA should promote accurate information from election officials • CISA should strengthen and expand its information sharing networks, using them to create public awareness campaigns around misinformation • Traditional and social media companies should promote accurate and authenticated election information • Technology companies, including AI developers and social media companies, should invest in tools that promote a healthy election information environment and increase security, confidence and transparency in elections • Chatbots should make clear their limitations on spreading accurate election information and redirect users to official, authoritative sources • AI developers should collaborate with social media companies on development of AI-generation detection tools

Challenges

This section looks at how AI will (and won't) change the election security landscape for election offices and election system vendors. Security experts we interviewed asserted that election offices nationwide can effectively counter AI-related cybersecurity risks leading up to the 2024 elections. These risks mirror those cautioned against over the past two decades. Essential safeguards involve robust cyber hygiene; preempting, identifying, and recovering from breaches; ensuring paper backups of voter choices; and regularly auditing software tabulations. Although many of these measures are already in place across the country thanks to substantial investments in election security, much more needs to be done ahead of 2024.

Looking further ahead, experts agree that AI will change how software is engineered. It can make cyberattacks bigger, quicker, sneakier, and better able to outsmart existing software security tools. But it also holds the promise of new defensive capabilities. As the National Science Foundation's Jeremy Epstein framed it, AI "is going to have an impact on both the offensive and defensive sides of the game. The net outcome is wildly uncertain."

Generative AI poses a major and immediate threat to election offices and election system vendors. It excels at imitating authoritative sources, making it easier to deceive specific individuals or the general public by impersonating election officials or forging official election documents. Worse, it can do so on a massive scale. As Ron Rivest of the Massachusetts Institute of Technology observed, "Generative AI is really an *amplifier* — an adversary can produce more high-quality output with less effort than before."

That adversary could be an individual domestic antagonist, who in coming elections will be able to harness AI to attack election offices with far fewer resources than ever before; or it could be a nation-state **like China**, **Russia**, or **Iran**, all of whom have meddled in recent American elections, and all of whom are developing their own AI technologies capable of targeting American networks. Microsoft analysts have **warned** that Chinese operatives have already used artificial intelligence to "generate images . . . for influence operations meant to mimic U.S. voters across the political spectrum and create controversy along racial, economic, and ideological lines."

Below we look at four examples of how AI might be used to support — and thwart — some of the most menacing attacks against election offices and infrastructure. Our adversaries' goals in each case could be anything from changing vote totals to undermining confidence in electoral outcomes to inciting violence.

The goal of this article and this series is to examine in detail the promise and potential peril of AI for American democracy in the coming years, so as to equip government, election officials, and civil society with the information needed to tackle the most urgent new challenges head-on.

More Sophisticated Phishing Attacks (but More Powerful Tools to Defeat Them)

Phishing is the practice of sending fraudulent messages that appear to be from a trusted source to obtain sensitive data or trick the recipient into downloading **malware**. Phishing attacks have been used to target election officials and election system vendors going back to at least 2016. A 2017 National Security Agency (NSA) **report** details a cyberattack on a U.S. election system vendor perpetrated by Russian military intelligence a few days before the 2016 presidential election. The attack allowed the hackers to create seemingly valid vendor email addresses and send phishing emails containing malware to 122 local election officials. The NSA determined that, if opened, the corrupted attachments gave the hackers unlimited access to the affected computers; the attackers could then install malware, survey user activity, and steal documents and proprietary information. The FBI **confirmed** in 2019 that two county elections departments fell victim to the attacks and were successfully breached. In Washington County, Florida, hackers accessed voter files, though **no evidence** indicates that files were compromised or that vote tallying was affected. More recently, in October 2021, the FBI **warned** that a phishing campaign designed to obtain login credentials and access to voting systems had targeted election officials in nine states.

New AI tools enable more widespread attacks on election systems with fewer resources. The use of **large language models** (the technology underlying chatbots) eliminates all but a few humans from the process of creating phishing emails, which means that hackers can employ generative AI to send out such missives faster and on a larger scale. This ease will result in more phishing emails targeted at election officials and vendors than we have seen in the past. The network security company Zscaler reported a **47 percent surge** in phishing attacks nationally in 2022 and identified AI technologies as a major contributing factor to this dramatic rise.

Attacks themselves are also becoming more sophisticated. **Phishing emails generated by new AI tools** are unlikely to contain the telltale spelling and grammar mistakes that earlier attempts became notorious for. Scammers can now use AI software to clone voices and assume trusted identities (e.g., chief election officials or private tech companies' leaders) to try to steal protected passwords or other confidential information. And AI can pull data from the internet about scam targets or their workplaces that may make messages seem more realistic or urgent.

We've seen this kind of attack in recent years. In 2022, the Federal Trade Commission (FTC) **reported** more than 36,000 incidents of people being scammed by hackers pretending to be friends or family. The 15

percent of those scams conducted over the phone resulted in over $11 million in losses. Scammers only need a short audio clip of someone's voice — even **shorter than a 30-second TikTok video** — to convincingly clone a voice. As one expert told the *Washington Post*, "Two years ago, even a year ago, you needed a lot of audio to clone a person's voice. . . . Now . . . if you have a Facebook page . . . or if you've recorded a TikTok and your voice is in there for 30 seconds, people can clone your voice." One AI start-up even offers this service for free depending on the amount of audio required.

While AI raises the risks associated with phishing and other scams, effective tools for catching and flagging these attacks can also leverage AI technology. Filters that seek to identify malicious emails can be trained on large data sets of known legitimate emails. Such filters use **natural language processing and machine learning** to separate phishing attempts from legitimate content with ever-increasing efficacy. Similarly, large language models could be trained to **identify unsafe** websites that phishing emails or text messages direct users to seeking to trick them into divulging sensitive information. Whether AI will ultimately be a net benefit or harm in terms of phishing attacks is still unclear; in the near term, election officials must watch this threat vector carefully.

More Advanced Malware (but Potentially Better Defenses Too)

Gaining access to a system is not necessarily enough to allow someone to disrupt it with **malware**. But here too, generative AI can inflate security risks by giving those who do gain unauthorized access more powerful tools to use once they're in. Developers have already **begun selling access** to chatbots such as WormGPT, which for approximately $70 per month claims to assist in creating malware and pulling off sophisticated phishing attacks.

To demonstrate the threat posed by AI-enhanced malware, HYAS Institute cybersecurity expert Jeff Sims recently developed a **proof of concept** called BlackMamba. The BlackMamba malware infiltrates a target system (perhaps through a **spear-phishing attack**), then uses AI to create new code every time it runs on the system. It also secretly records the system user's keystrokes, using ChatGPT to identify which ones are important (e.g., sensitive information like names or addresses typed into a webform or passwords used to access confidential files). The malware sends these important keystrokes back to the attacker, while less significant keystrokes (e.g., that generated by typing emails or searching social media websites) are ignored.

Some of the security experts we spoke to did not consider BlackMamba itself particularly dangerous for elections, but all of them agreed that generative AI will change how software is engineered. Yet several noted that although AI — and generative AI in particular — heightens the malware risk to election systems, AI (including non-generative or traditional AI) should also *improve* cyber defenses. Traditional AI should boost the ability to accurately classify software as malware. Researchers have endorsed a number of classifying systems that utilize **machine learning**, including **image-based** binary **representations**, as competitive with or even exceeding the performance of previously state-of-the-art classifiers.

Impersonations, Deepfakes, and Spoofed Official Websites

Voters **widely trust** and rely on election officials and their websites for accurate information in the weeks before and after Election Day, which makes those officials and their websites attractive targets for impersonation and spoofing.

Generative AI makes it easier to simulate election websites by producing HTML code, stock images, extremely realistic portrait photos, and website text. It also allows an antagonist to create **fake video and audio content** with just a few minutes of video and even a few seconds of voice capture from the target of the impersonation. In performing their duties, most election officials make public appearances to explain election procedures and initial results to the public, thus creating the source material needed to generate fakes.

As countless **deepfakes of public officials** have shown in recent months and years, this threat is not just theoretical. In March 2023, a **deepfake video** of Sen. Elizabeth Warren saying that Republicans should be restricted from voting went viral. These spoofs may be easy to spot when they involve a public official with a large following and vast communications resources, but fast and far-reaching rebuttals would be much more challenging for many of the nearly 10,000 local election officials who have no support staff or public information officer to assist.

The threat of impersonation extends to fake social media accounts as well. After X (formerly known as Twitter) changed its verification rules, a wave of imposter accounts flooded the platform posing as agencies such as the **IRS** and the **Illinois Department of Transportation**. Election **offices may qualify** for the platform's new gray checkmark feature for government accounts, but the accounts of many of the country's most populous counties are still not verified as of this writing.

Of course, voters turn not just to election officials for accurate election information but also to official content issued by election jurisdictions, often conveyed on official election websites. Security experts have long proclaimed the dangers of spoofed election websites masquerading as official government sources to spread misinformation about everything from how and where to vote to election results. Indeed, the FBI and the **Cybersecurity and Infrastructure Security Agency (CISA)** have expressly warned of foreign antagonists **using** phony election websites as a disinformation tactic. This type of attack has already occurred against **election** and other government websites. For example, in 2020, the **FTC sued a company** that had set up hundreds of fake websites using names like DMV.*com* to mimic public agencies. These sites falsely promised public benefits to deceive people into divulging personal information. Such attacks will probably escalate in the future, as generative AI can simply read a target website's code and create scores of copycat sites.

Misuse of Open Records Requests Processes to Disrupt Election Offices' Work

Mark Earley, the elections supervisor for Leon County, Florida, echoed many election officials we spoke to when he told us his concern that AI would make an already difficult situation — excessive and frivolous Freedom of Information Act (FOIA) and other open records requests — even worse through deliberate deception. Since the 2020 elections, election fraud conspiracy theorists have **inundated** election officials around the country with open records requests. In many such cases, activist groups have submitted the same requests multiple times to different localities, seeking to substantiate baseless claims of mass voter fraud. These burdensome requests divert election offices from essential election administration work, particularly in the weeks and months prior to Election Day.

AI compounds this issue in two ways. First, groups can use AI to become more disruptive, easily generating hundreds or even thousands of varied open records requests to multiple jurisdictions in lieu of the current copy-and-paste method. When multiple election officials all receive the exact same request, coordinated responses can save time and resources. State officials can provide local offices with uniform guidance or assume the task of responding themselves. Election officials can also share information and turn to each other or to their state associations to determine how best to manage such requests efficiently. Those kinds of synchronized responses become far more difficult when mass-produced requests are written differently and cover a diffuse set of topics — which generative AI makes possible.

Second, as already discussed, one of AI's perils is that antagonists can spoof websites, fabricate videos, and forge or doctor official documents so easily. Election officials we spoke to raised concerns that watermarked documents or videos of election workers doing their jobs, submitted in response to open records requests, can be manipulated to create convincing fakes and thereby cast doubt on election results. For example, an altered **certificate of electors** could use AI to convincingly preserve the original watermark but incorporate text naming false electors. Likewise, authentic video of election workers performing their duties can be manipulated to appear to show them **destroying ballots**. Election deniers could use such deceptions to lend legitimacy to fraud claims.

Election offices must comply with FOIA requests in accordance with the law, but the records they deliver need some sort of authentication to make faked versions identifiable. While versions of these attacks may have been possible before recent advances in generative AI, the new technology's excellent image-generating capabilities could make such attacks far more sophisticated, making the job of debunking them more difficult.

Mitigations

There is no silver bullet for the additional security risks wrought by AI technology's rapid advances and increased availability. Broadly, however, government and the private sector must take action in five areas to mitigate the heightened threat: building more secure and resilient election systems; providing election officials with more technical support to safeguard election infrastructure; giving the public ways to

authenticate election office communications and detect fakes; offering election workers AI-specific trainings and resources; and effectively countering false narratives generated by or about AI.

Build More Security and Resilience into Election Systems

Although the nation has made substantial progress on election security in the last decade, the likelihood that AI will supercharge security threats makes it even more critical to adopt existing safeguards — some of which themselves leverage AI technology — and to devise new ones to help election officials prevent, detect, and recover from cyberattacks on election infrastructure.

Some jurisdictions still need to expand their use of **multifactor authentication**, which CISA director Jen Easterly has **called** the most consequential step that users can take to combat cybersecurity threats. Multifactor authentication entails requiring users to present a combination of something they know (e.g., a password or personal identification number), something they have (e.g., an authenticator app on a cell phone that receives a code or request to verify), or some form of biometric identification (e.g., a fingerprint, palm print, or voice or face recognition).

While an attacker might be able to obtain passwords used by an election worker to access sensitive files like registration databases or ballot programming files, multifactor authentication requires access to that worker's phone or another separate device as well. Security experts have long **recommended** multifactor authentication, but its **uptake** has not been universal. State and local officials must ensure even wider adoption of this essential security measure.

Effective resilience planning is also imperative. Even if an AI-aided cyberattack succeeds, it cannot be allowed to stop voters from casting ballots or officials from accurately tallying votes. States have made remarkable strides in enhancing system resilience over the last decade, including by moving overwhelmingly to voter-marked paper ballots. Paper ballots are independent of vote-counting software and can be used as a check against malware or software glitches. The Brennan Center has **estimated** that in 2022, 93 percent of voters — including nearly all voters in the major battleground states — cast their votes on paper ballots.

But **gaps** in election system resilience remain. For instance, paper is only a useful security measure when used as a check against election software. More states need to embrace postelection audits, which compare a subset of paper ballots with electronic tallies. As of 2022, **eight states** still do not require postelection audits of any kind. And even among the 42 that do, the audits' efficacy as a tool to detect cyberattacks and technical errors differs widely. **Only 33** of these states require election workers to hand-check sample ballots during an audit versus using a separate machine. Just **five states** require risk-limiting audits, which rely on statistical principles to determine the random sample of ballots that must be checked to confirm that overall election outcomes are accurate.

Election system vendors are **targets** too. The Brennan Center has previously **detailed** ways in which the federal government could mandate election security best practices — including stronger security and resilience planning — for vendors in the elections space as it does for vendors in other federal government sectors designated critical infrastructure. These standards should include guidelines for the use and disclosure of AI in election vendors' work to identify potential security risks.

Provide Local Election Offices with More Technical Support to Protect Election Infrastructure

In the decentralized U.S. election system, target-rich, resource-poor local jurisdictions with limited capacity to address cybersecurity issues present one of the most concerning vulnerabilities. These election offices have little or no dedicated cybersecurity expertise and are often dependent on other offices in their counties or municipalities for IT support. In fact, **nearly half** of all election offices operate with one full-time employee at most, and nearly a third operate with no full-time staff at all. Yet election officials who serve these offices have the same monumental task of serving as frontline national security figures.

This challenge will only grow as the barriers to launch sophisticated cybersecurity attacks diminish. The federal and state governments must do more to protect local jurisdictions from these attacks.

1. Develop State Cyber Navigator Programs

Several states — including Florida, Massachusetts, Michigan, Minnesota, and Ohio — are working to tackle cyber vulnerabilities at the local level by creating cyber navigator programs. These programs employ cybersecurity and election administration professionals who work closely with election officials to assess system security, identify potential vulnerabilities, and devise tailored strategies to mitigate risks. Other states should follow suit.

2. Offer Targeted Assistance from CISA

At the federal level, the most critical agency in the fight against cybersecurity threats is CISA, which provides state and local election officials with risk assessments, information sharing, and **security guidance**. The agency recently **announced** its intention to hire 10 regional election security advisers to help communicate various election security best practices, including AI-supported cyberattack countermeasures, which the Brennan Center and other election security experts have **urged**. These hires are a crucial first step in reaching the jurisdictions that need the most help.

The Brennan Center has also called for more cybersecurity advisers — trained cybersecurity experts who can assist state and local officials — to prioritize outreach to under-resourced local election offices. An April 2023 Brennan Center **survey** of election officials demonstrated the need for this increased outreach: only 29 percent of local election officials said they were aware of CISA's cybersecurity vulnerability scans, which are a vital tool for identifying election system weaknesses that generative AI can help attackers pinpoint and exploit.

3. Focus Resources on Defending AI Already Used in Elections

While this article mainly examines how hackers can use AI to hone and intensify their attacks against elections, we have also noted that it can bolster election defenses. Another article in this series will explore how AI is already being used to strengthen cybersecurity and for basic election administration tasks like signature matching and voter registration list maintenance. Undoubtedly, both election offices (especially those short on resources) and vendors will look to AI to improve their services in the coming years.

As election officials expand their use of AI, they must also consider that AI-supported systems will be **targets for attack** given the widespread damage that hackers can accomplish by corrupting such systems. It isn't difficult to imagine, for instance, how attackers could manipulate AI to discriminate in its signature matching or list maintenance functions, or how they could **corrupt AI functions** that filter phishing attacks and other spam to breach the systems that those functions are meant to protect.

Election offices using AI need to implement additional security protocols to protect these systems. Another article in this series will offer more extensive recommendations for how to do so; for now, suffice it to say that CISA and state agencies responsible for protecting election infrastructure must identify jurisdictions that have incorporated AI into their security and administrative systems and proactively help them minimize their risks. One place to start would be for CISA to create a document that lists security and other matters for election officials to consider when incorporating AI into their operations. This guidance could borrow from the National Institute of Standards and Technology's ***Plan for Federal Engagement in Developing Technical Standards and Related Tools*** and the Department of Homeland Security's ***Artificial Intelligence Strategy***.

4. Invest in AI to Protect Election Infrastructure

Cybersecurity is a race without a finish line. In the coming years, AI is likely to offer attackers more powerful tools for hacking into our election infrastructure. It is just as likely to offer powerful tools to defend it, but only if the government works to ensure that election officials have access to such tools and understand how to use them.

In August 2023, the Office of Management and Budget (OMB) and the Office of Science and Technology Policy (OSTP) published a memorandum outlining multiagency **research and development priorities** for FY 2025. Among other recommendations, the memo urged federal agencies to prioritize funding initiatives that would support and fulfill multiple critical purposes, including "build[ing] tools . . . for mitigating AI threats to truth, trust, and democracy."

Election officials urgently need AI-supported tools to address ever-more sophisticated and frequent cyberattacks. The federal government should prioritize developing such tools and working to guarantee

sufficient infrastructure that they can be implemented in election offices around the country.

5. Seek Tech Company Investment in Free and Low-Cost Tools That Increase Election Security, Confidence, and Transparency

Companies developing AI should not wait for government mandates or for AI's most dangerous threats to democracy to be realized — they should strive not to accelerate these threats even in the absence of regulation. At the same time, they can actively help election officials navigate the risks we've outlined above. When foreign antagonists have targeted democracies in the past, companies like Microsoft, Google, and Cloudflare provided election security tools both in the United States and abroad at no cost to help improve resilience against attacks. Microsoft held **virtual education and training sessions** for U.S. election officials in 2020; Google sister company Jigsaw issued a suite of **free security tools** for campaigns and voter information websites in 2017; and Cloudflare offered **free services**, also in 2017, to help keep official election websites functioning in the event of cyberattacks or technical difficulties.

These and other vendors — especially those that stand to profit from AI development — should consider how their work can influence the cybersecurity landscape, including election security, and expand their offerings and proactive contributions to foster a healthy election information environment. Among other things, they can invest resources in nonprofits and programs such as the **Election Technology Initiative**. The initiative assists election administrators by providing and maintaining technology that builds public confidence in elections.

Technology companies behind AI tools (such as large language model chatbots) that the public may use in 2024 to get election information have a particular responsibility to ensure that these chatbots provide accurate information. AI is not equipped to accurately answer questions about how and where to vote or whether the latest election conspiracy theory is accurate. Chatbots should be trained to make their limitations clear and to redirect users to official, authoritative sources of election information, such as election office websites.

Authenticate Election Office Communications and Help the Public Spot Impersonations

Election offices and officials were a critical bulwark against the stolen election lie in 2020. Those seeking to undermine confidence in American democracy thus continue to view them as valuable targets, attacking their credibility with falsehoods, harassing them, and threatening them with criminal prosecution and physical harm.

AI-generated content offers a new way to attack the credibility of these essential information sources with a "**firehose of falsehood**" that purports to derive from those very sources, making the truth even more difficult for the average citizen to ascertain. Solving the problem of impersonation through AI-generated content requires multifaceted solutions. Election officials must act to secure their communication channels to make them harder to spoof, and all levels of government must reinforce these steps. Entities that seek to provide public information about elections must also verify content through official sources. The following urgent measures would help stem the flow of false information.

1. Move All Election Websites to .gov Domains

American election websites are far too vulnerable. In the lead-up to the 2020 election, the FBI **identified** dozens of websites mimicking federal and state election sources using easily accessible .com or .org domains. To guard against spoofing and interference, federal and state governments should work together to ensure that election offices adopt **.gov domains** — which only verified U.S.-based government entities can use — for their websites. When users see .gov in a website URL, they can be sure that the site is a trusted government source rather than a fake election website. Only **one in four** election office websites currently uses a .gov domain.

Leading up to the 2024 elections, CISA should double down on imparting the national security importance of .gov domains, in part through the **Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)**. States should mandate the use of .gov domains for local election offices, as **Ohio's secretary of state** did in 2019. Doing so would facilitate the transition for election officials who do not control their own websites and depend on their counties or municipalities for IT support. Registration for .gov domains is now

free for election offices verified by CISA. And states and localities can use federal funds from DHS's newly launched **State and Local Cybersecurity Grant Program** for other costs associated with transitioning to new domains.

2. Verify Accounts and Amplify Truthful Information

No .gov equivalent currently exists for social media, and generative AI makes it alarmingly easy to create and populate fake social media accounts that, among other problems, provide voters with inaccurate information about how and where to vote. Leading social media companies can intervene by identifying, verifying, and amplifying authentic election official content, as the Brennan Center and the Bipartisan Policy Center have previously **recommended**. At best, some companies like X (formerly Twitter) have taken a more passive approach, allowing election officials to apply for verification (albeit with lags between application for and grant of verification).

One solution is for the **Election Assistance Commission (EAC)** or CISA to create a dedicated server in the so-called **Fediverse**, a non-platform-specific federal clearinghouse for verified official accounts that can serve as a central distribution and syndication hub for social media communiqués. Posts with .gov handles could then be verified and batched, precluding the need for local election officials to publish content simultaneously across multiple platforms. Users, too, could then be sure of information's veracity.

In 2022, the German government's Federal Commissioner for Data Protection and Freedom of Information (BfDI) took a similar approach through Mastodon, which is currently the best-known entity in the Fediverse. More than 100 official accounts use the **BfDI server**, including the German weather service, the foreign office, and the federal court, which allows users to see posts from all these organizations in a single verified news feed. As one **commentator** put it, "When you read posts made by one of the https://social.bund.de accounts you inherently know from the domain name (web identity) that you're not following an impostor." A similar EAC/CISA feed would go a long way to dispelling election misinformation that ends up on social media.

3. Implement Methods to Ensure That Open Records Requests Are Authentic

As discussed above, AI makes it easier to bury election offices under mountains of deceptive open records requests that seem to come from different constituents. This challenge has no easy solution, but one important step would be for election offices to require every open records request to be filed by an actual person, and to use a version of **CAPTCHA** (which stands for "completely automated public Turing test to tell computers and humans apart") to prevent bots from using AI-generated open records requests to overwhelm an office. Although generative AI itself is increasingly **able to defeat** CAPTCHA tests, anything that might curb a potential flood of faux requests filed with election offices would be a step in the right direction. In instituting any such policy, offices should ensure that people with disabilities and those without access to high-speed internet or other technology have accommodations available.

Forthcoming articles in this series will discuss this threat of deceptive, AI-generated open records requests, as well as inauthentic public comments to election and other government officials more generally, in greater detail.

4. Explore How to Authenticate Sensitive Election Materials

Regarding the risk of videos or documents supplied in response to FOIA requests being manipulated to promote disinformation, election officials should consider posting on their websites the unaltered versions of every document produced for such requests. Unfortunately, this mitigation strategy would require resources that some already overburdened offices lack. A related option is for state election offices to create central repositories for all local FOIA responses, allowing election officials to point to original, unaltered documents in case hackers try to pass off distorted documents as true copies. **Hawaii** already does so.

Digital signatures and **cryptographic hash functions** also hold promise for authenticating digital records produced by election offices, but they may be less easily understood by the public — or even the election officials who need to implement to them. CISA could help here by educating election offices and the public about these tools. Cybersecurity advisers could also teach election officials how these tools can prove whether materials posted online (like cast vote records or ballot images) are real or altered.

5. Take Extra Steps to Verify Election-Related Content

Journalists should cultivate relationships with election officials and other authoritative sources on elections processes. Content that purports to be from these sources should be verified against content that can be authenticated — for example, videos and other information provided on a secure website with a current security certificate or, ideally, on a .gov site. In the case of breaking news, media sources should include nonpartisan experts who can assess the plausibility of content that may have been manipulated. Sources should also represent non-English-speaking and historically marginalized communities so that journalists can address specific and diverse items of confusion or misinformation.

Give Election Workers AI-Specific Training and Resources

Election office employees and election system vendors are appealing targets for anyone seeking to damage faith in American elections. This threat could come from foreign or domestic antagonists seeking to gain access to election infrastructure through phishing emails or other methods. CISA and other experts and organizations should do everything possible to help these offices and their staffs remove from public websites information that hackers might use to personalize AI-generated messages, and to help election workers identify such messages.

1. Remove Data That Could Be Used to Personalize AI-Generated Communications

Criminals already use data found on the web to dupe unsuspecting Americans out of money and to glean information they should not have. Election offices and vendors should review their websites for personal and organizational information (e.g., chain of command, employee email addresses, names of employees' relatives) that hackers seeking to obtain sensitive or confidential information could use to create personalized phishing emails or cloned voice messages.

CISA already makes recommendations for controlling personal information shared online to reduce the likelihood of doxing. The agency is well-positioned to create similar resources and trainings to help election offices and their workers analyze their websites to minimize the risk of personal information being used to facilitate attacks.

2. Help Election Workers Identify AI-Generated Content

For the moment, even as AI allows for more sophisticated phishing attacks and impersonations, there are often ways to spot such content. Among other clues, AI-generated text often includes very short sentences and repeated words and phrases; voices and images in AI-generated videos may not fully align.

The challenge for devising guidelines that election workers can use to spot AI-generated content is that generative AI's capabilities advance so quickly. Here again, CISA has the expertise to help. By keeping up with how AI is evolving and regularly communicating how to identify AI-generated content, the agency can help reduce the effectiveness of attacks against election offices and vendors that try to use such content to deceive them.

Push Back on False Narratives

As with other election security challenges, the problem of false narratives existed before the recent advances in generative AI's abilities. Yet rapidly developing AI technology threatens to exacerbate the problem, not only because it offers more tools to undermine confidence and spread lies, but because the use of those tools for crimes — and the inevitable publicity around those incidents — further undermines public confidence in the security of critical systems like those that support our elections.

All of us must push back on false narratives around election security. We must also recognize that AI's power to disrupt security will make this work even more challenging. Other articles in this series will discuss in more detail how to build resilience to election disinformation fueled by developments in AI, but here we note a few ways that government, the mainstream media, and social media platforms can help as we head into the 2024 election season.

Disinformation relies on core falsehoods that evolve and recirculate. Generative AI greatly increases the opportunities for these myths to perpetuate. Federal agencies like CISA and the EAC should collaborate with election officials to raise public awareness of and confidence in election system security. **Preemptive**

debunking of the sticky false narratives that we already know will underpin the lies and election disinformation in the weeks before and after Election Day is essential.

CISA and the EAC must vigorously promote the dissemination of accurate information from election officials and share best practices for strengthening societal resilience to the spread of false information, including falsehoods generated and enhanced by AI. One important step would be to follow the recommendations of CISA's Cybersecurity Advisory Committee (CSAC), which in a **2022 report** encouraged the agency to strengthen and expand its information-sharing networks and to use those networks to create public awareness campaigns focused on digital literacy, civics education, and bolstering information from authoritative sources. These networks could also be used to educate the public to spot AI-generated content.

Traditional and social media platforms alike must work to refute core misinformation themes and amplify accurate and authenticated election information, especially from election officials. Social media platforms should invest in detecting and removing coordinated bots to help prevent false information from influencing elections. And they should collaborate with AI developers to continually improve methods to detect AI-generated content.

Conclusion

When it comes to protecting election infrastructure and personnel from AI-generated threats, the most important thing that election offices and vendors can do is redouble (and in some cases implement for the first time) the election security best practices that experts in the government and academia have been urging for over a decade. Government, the private sector, and the media must evangelize the importance of those security measures to the integrity of our elections.

As to the threats of impersonation and other attacks that attempt to breach the security of election vendors or official offices or mislead the public, the solutions are both more complicated and novel and will require a whole-of-society approach. The recommendations offered in this paper are not enough to forestall the problems we have identified entirely, and we encourage state and federal agencies and the private sector to continue working to address them.

A number of new policies and regulations can better protect election officials and vendors from AI-supported attacks in the near and long term. We urge better regulation of election system vendors, including the development of new standards for the disclosure and use of AI in their work. Similar standards would be helpful for election offices. We also recommend targeted assistance to election officials from CISA, the EAC, and the OSTP to strengthen their resilience to AI-generated attacks. That assistance must include private-sector and government investment in AI tools that have the potential to defeat more sophisticated attacks against our election infrastructure and offices in the future. Finally, in light of the risk of impersonation and forgery that comes with new AI tools, states and federal agencies like CISA should help election officials take the steps necessary to be able to authenticate their digital records and communications with the public.

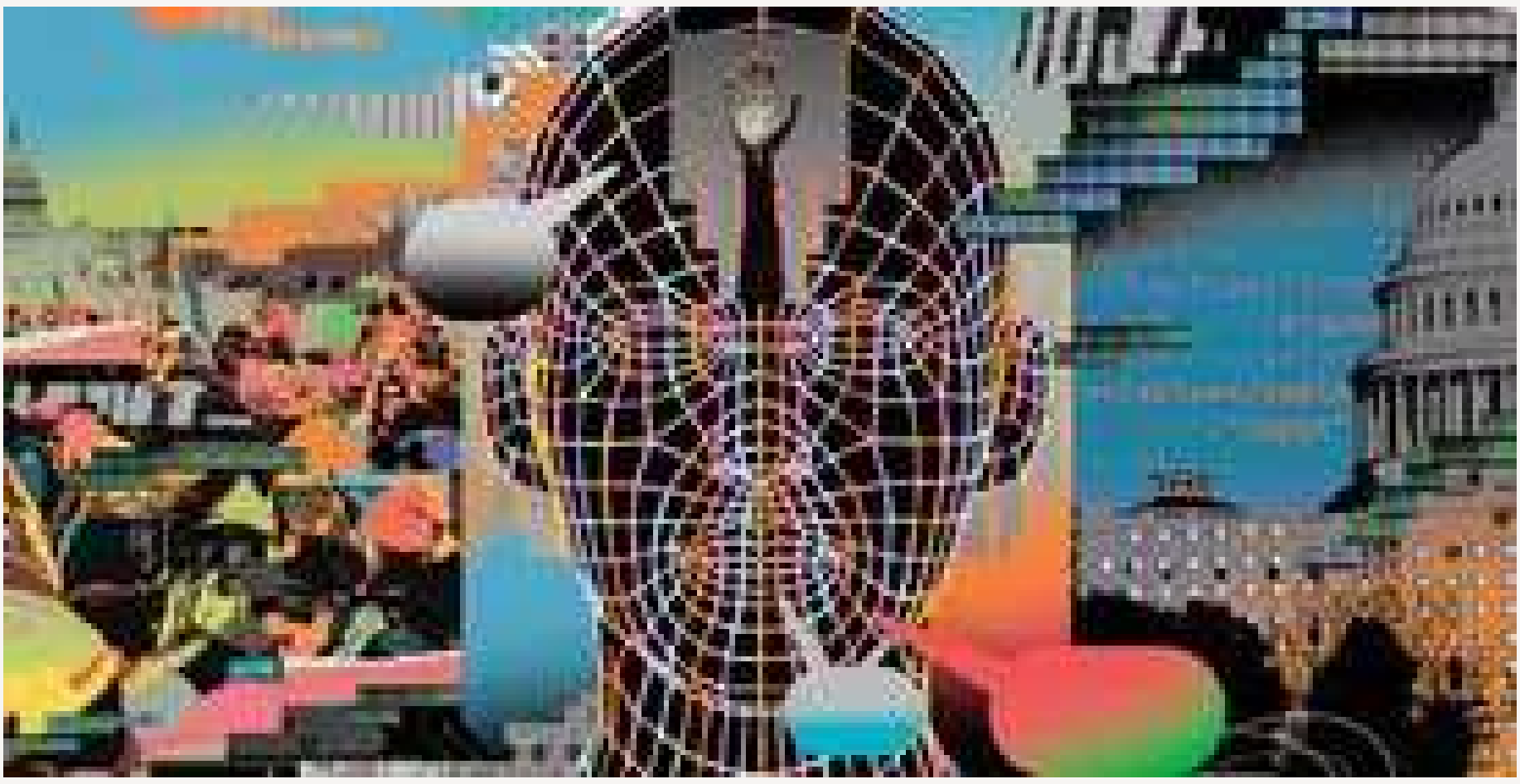
Many of AI's threats to our democracy writ large may be even more complex and novel than the ones discussed in this article. Those threats range from interactive generative AI changing the nature of disinformation and persuasion to technological advancements that could disrupt policymakers' ability to assess the public's interests and preferences. We will discuss those challenges — and possible solutions — in future articles in this series.

Acknowledgements

The authors thank the following individuals for their review and feedback: Ron Rivest, Institute Professor, Massachusetts Institute of Technology; Austin Botelho, research engineer, NYU Tandon School of Engineering; Jeremy Epstein, lead program officer, National Science Foundation; Frank Reyes, cloud solutions leader, Maximus; Lindsay Gorman, senior fellow for emerging technologies, Alliance for Securing Democracy, German Marshall Fund; Andrew Lohn and Josh A. Goldstein, Center for Security and Emerging Technology, Georgetown University; and Mekela Panditharatne, Democracy Program, Brennan Center for Justice. All mistakes are our own.*

** — For identification purposes only. Mr. Epstein's feedback was provided In his personal capacity and not on behalf of the National Science Foundation or the U.S. Government.*

More from the *AI and Democracy* series ▶



EXPERT BRIEF

Regulating AI Deepfakes and Synthetic Media in the Political Arena

Policymakers must prevent manipulated media from being used to undermine elections and disenfranchise voters.

Daniel I. Weiner, **Lawrence Norden** // December 19, 2023

READ MORE

EXPERT BRIEF

Safeguards for Using Artificial Intelligence in Election Administration

Adequate transparency and oversight can ensure AI tools in election offices are helpful and not harmful.

Edgardo Cortés, Lawrence Norden, Heather Frase, Mia Hoffmann // December 12, 2023

READ MORE

EXPERT BRIEF

Artificial Intelligence, Participatory Democracy, and Responsive Government

Government must implement safeguards against malicious uses of AI that could misrepresent public opinion and distort policymaking.

Mekela Panditharatne, Daniel I. Weiner, Douglas Kriner // November 3, 2023

READ MORE