BRENNAN CENTER FOR JUSTICE

IFTF Institute for the Future

The Elections Group

How Election Officials Can Identify, Prepare for, and Respond to AI Threats

By David Evan Harris, Lawrence Norden, Noah Praetz, and Elizabeth Howard with multimedia by Toshi Anders Hoo MAY 8, 2024

Brennan Center for Justice at New York University School of Law
Institute for the Future
The Elections Group

Table of Contents

STAY CONNECTED TO THE BRENNAN CENTER

Visit our website at
brennancenter.org

Introduction: A Case Study from Arizona

As potential artificial intelligence threats to elections have grown increasingly dire, many election officials worry that they have little awareness of the risks, nor practical guidance for how to prepare for this new technology and the threats it poses to election security. In particular, they feel limited in their ability to communicate with voters about possible AI-driven disruptions to the 2024 elections.

In recent weeks, the Cybersecurity and Infrastructure Security Agency (CISA) provided election officials with a risk analysis that details ways in which AI might be used maliciously against election processes, offices, officials, and vendors and provides invaluable suggestions for mitigating these risks. CISA also released an assessment of foreign malign influence operations targeting elections, including how foreign adversaries might leverage AI, which similarly included suggestions for countering such threats.

Mere awareness of the ways that AI might threaten elections is no substitute for actually seeing how it could do so. On December 15–16, 2023, the office of Arizona Secretary of State Adrian Fontes, in collaboration with the Brennan Center, the Elections Group, and the Institute for the Future, conducted a first-of-its-kind tabletop exercise on how AI could disrupt election operations in 2024. The goal of this exercise was to prepare officials at all levels of government for AI-generated or supported attacks against election offices and infrastructure.

This two-day tabletop exercise was a crisis scenario planning exercise in which participants practiced responding to simulated emergency situations. Among the scenarios were an attempt to harvest county office login credentials using AI-generated emails and text messages that appeared to be from the state's election security office; an audio deepfake from a state official directing offices to keep polling locations open because of a nonexistent court order; and AI-generated photos that purported to show an election official involved in criminal activity circulating on social media. In all cases, the AI tools used were available on the web for free or at low cost and did not require special technical skills to operate. AI tools were used in other ways during the tabletop exercise as well, including to create deepfake videos using material from the secretary of state's X (formerly Twitter) account.

The tabletop exercise included participants from 14 of 15 Arizona counties, including county election officials and representatives from county information technology (IT) offices, law enforcement, emergency management services, federal and state agencies (such as CISA and the National Guard), and other members of the elections community. Most participants were broken into 10 teams of 8 to 10 people each. Most approached the exercises from the vantage point of their current employment (e.g., county recorder, emergency manager, information officer, or board of supervisors member). Each team was given a fake county name and its own table. There were individual teams for secretary of state employees, law enforcement, and vendors.

At the beginning of the first day, participants were given a budget to purchase security and resiliency items, ranging from anti-phishing training to backup communications capability (for phone and internet) to multifactor authentication systems. Their budgets were intentionally not enough to pay for all the security and resiliency measures that were offered. The scenarios each team faced were recalibrated based on the risks they used their budgets to mitigate. For example, if a team purchased anti-phishing training, then the phishing scenario and consequences were removed from that table's experience. At the end of each day, participants debriefed on lessons learned and additional steps they might have taken to prepare for and address the emergency scenarios.

For the most part, participants did not learn that deepfakes and other AI-generated material were inauthentic or AI-generated until the end of the second day. But skepticism about what could be trusted grew over the course of the two days, and by the second day, many participants were asking for credentials when contacted and using group chats they created with the secretary of state's office and law enforcement to confirm the accuracy of information they were receiving.

This scenario planner will delve deeper into the lessons that participants learned during the tabletop exercise to help their counterparts around the country understand, identify, prepare for, and respond to various AI-related threats that may arise during the upcoming elections. One major insight was the importance of reinforcing fundamental security measures, such as implementing multifactor authentication, securing essential communication channels, conducting regular impersonation checks, and creating rapid-response communications plans. As Harvard University professor Bruce Schneier has noted, artificial intelligence will increase the "speed, scale, scope, and sophistication" of threats to our democracy. Put another way, many of the threats are not new, but they could become more dangerous in the rapidly evolving AI environment.

The scenarios participants faced during the tabletop exercise were frightening for their realism but also reassuring, making clear that election officials and others already have many tools at their disposal to combat AI threats. As one participant put it, "I appreciated learning about AI threats and experiencing the mock [scenarios] that may happen. The chaos was disorienting at first but easier to deal with by the second day." Michael Moore, the secretary of state's chief information security officer, emphasized that these kinds of exercises are exactly what election officials and those supporting them need in the coming months, noting that "AI is going to increase the quality, quantity, and urgency of [mis-, dis-, and malinformation]. Training events like this are one of the best ways we can ensure we are ready for what's coming."

Seven Ways to Prepare Today

Taking lessons from the Arizona tabletop exercise, this scenario planner defines AI threats and lists actions that election officials can take to mitigate them. The list below includes the top seven steps that officials can take to make the coming election as safe and secure as possible:

1. Understand what AI can do. Review the resources, watch and listen to the demos, and try the AI tools in the "Understand What AI Can Do" section below. Train your team to be aware of these threats.

2. Take control of your online presence. Verify that you have access to all your social media accounts and that you can quickly make edits to your .gov website. If you don't directly control your website, identify the person who has the ability to make updates and ensure that you have their current and accurate contact information. If you don't have social media accounts on major platforms, consider creating them even if you don't plan to use them and putting a link to your official .gov website in each profile to make it harder to impersonate your office. Control publicly accessible data, including personal and organizational information that can be used to facilitate attacks. Conduct regular impersonation checks by searching for your office and staff names on major platforms.

3. Prepare for rapid-response communications. Develop a crisis communications plan, ensuring that all relevant stakeholders in the office understand their roles. Publicly available plans for election officials are highlighted below. Do a practice run of the plan, seeing how quickly you can post messages to all your social media accounts and update your website. You should be able to do this in under 30 minutes. Ensure that your team has secondary channels to communicate internally to confirm facts before communicating to the public. Meet with representatives of local community organizations and share your response plan. Ask for their assistance to amplify accurate information and agree on a plan for notifying these groups as part of your crisis communications plan.

4. Adopt cyber and physical security best practices. Set up a password manager and enable multifactor authentication for all your accounts, including social media, email, website administration, and phone and internet services. Make CISA cybersecurity training mandatory for staff and volunteers with access to any information systems, effective immediately. Ensure that all officials, poll workers, and vendors are aware of ways to double-check information or requests that come from suspicious emails or phone calls.

5. Build and strengthen relationships with local media and other partners. Contact local news media far in advance of the election and let them know who you are, what your official phone and email contact information is, what official social media accounts you plan to use (if any), and that you're available to talk to them throughout the election and postelection period if they have any questions or concerns about election information. Relationship-building is paramount, as journalists may quickly become critical figures if you face AI threats. This outreach strategy also applies to community organizations and law enforcement.

6. Create escalation plans. Many types of AI threats will require you to escalate an incident by seeking support from state or federal agencies and/or other external parties like your internet service provider or social media companies. Your existing incident response or continuity of operations plans likely already account for escalation in the event of cyber or physical incidents. If an AI-related attack occurs, escalation is the process of alerting all relevant parties to mitigate potential harm. Make a contact list for your team containing your escalation channels. This list should include everyone on your team, the chief state election official's office, law enforcement, federal election support agencies, civil society resources, and emergency staffing contacts.

7. Prepare legal support networks. Meet with your local attorney. Identify the threats associated with AI and ask them to review the legal remedies available in your state and jurisdiction to each one, using the scenarios in this planner to guide your conversation. Ensure that your attorney is available on Election Day and in the period leading up to the election. Your local attorney should be an important partner in your efforts to protect against and respond to AI-related threats.

Types of Generative AI Outputs: Audio, Images, Text, Video, and Malware

When it comes to AI threats, officials must be prepared for five main types of generative AI outputs: audio, images, text, video, and malware. This section provides an overview of the characteristics and uses of each type.

Audio

Audio technology allows users to choose from a catalog of voices (e.g., British male, Australian female) and make the voice say whatever they want via text prompt. This threat can be used against election officials and other public figures by mimicking their voices to say something they never actually said. This technology leverages existing audio recordings, which makes politicians and public officials incredibly vulnerable given the sheer volume of publicly available voice recordings. This tactic could be employed to mislead the public about voting or election workers in an attempt to steal data or disrupt activity. Example threats include:

- **Overt impersonation:** As seen in New Hampshire, malefactors can create voice clones to mimic politicians' voices over the phone with the intent to disrupt electoral processes. Voice-cloning technology can also create fake audio recordings of politicians, as seen in Slovakia, to spread misinformation or to hurt a rival candidate or party.

- **Covert impersonation:** Voice clones of known and trusted figures can be employed to gain instant trust in election administration circles and get election workers or election officials to do something outside of standard operating procedures.

Images

Tools like DALL-E (now incorporated into ChatGPT) can produce high-quality images from text prompts and modify existing images with high levels of detail. These tools can modify people's faces, change backgrounds, and even add or remove objects from photos. This technology gives agitators a means to create false or misleading images, potentially with the intent to misinform voters. Example threats include:

- **Website generation:** These advanced tools allow adversaries to create extremely realistic images and write the code to produce fake websites or news articles with the intent of undermining elections.

- **Impersonation:** These tools can be used to create phony images of politicians, election workers, and other figures, known as deepfakes. This fake AI-generated content can disrupt elections by, for instance, showing election workers in compromising situations or otherwise mispresenting them to the public.

Text

Text-based content is generally created through chatbots, such as ChatGPT. This technology lets users prompt the bot with a statement, a question, or a casual conversation, to which they are provided replies, answers, documents, and code, among many other outputs. As with audio deepfakes, this technology can be used to mislead the public or election workers. Example threats include:

- **Impersonation:** Users can command the bot to write in the style of an election official or known politician, or to simply create fake profiles of what appear to be real people for the purpose of creating and spreading rumors about elections and voting.

- **Phishing**: Agitators can generate a massive amount of cogent text in any language, even if they do not speak the language themselves.

- **Misinformation**: This technology can be used to undermine elections by generating false or misleading content about the election quickly and in large quantities.

Video

Video technology allows users to create content by uploading a video or asking AI to create a video based on a text prompt. An otherwise time-consuming process, malefactors can now generate videos with ease and minimal expense that can be used to confuse voters and elected officials. This technology can also modify existing videos: a user can simply upload an existing video and ask AI to modify it. An example threat is provided below:

- **Overt impersonation:** Videos that impersonate people (another type of deepfake) can be leveraged against public figures, as seen recently, to sow confusion and spread false information.

Malware

As mentioned above, AI can also write computer code, which hackers can use to develop novel or improve existing malware (software designed to harm or take control of a computer or network). This malware could target election infrastructure to undermine electoral processes. While this threat is not new, AI technology allows attackers to write large amounts of code quickly, potentially increasing the amount of malware threats facing election officials. Example threats include:

- **Targeting voter data:** Malware can be used to obtain repositories of voter data that hackers may threaten to leak to the public, enabling future doxing incidents and violations of people's privacy and sowing doubt about the electoral process.

- **Damaging voting infrastructure:** Malware can also target election infrastructure, including voting machines, causing them to malfunction or change outcomes; these attacks may not become apparent or correctable until audits and canvasses are conducted days after preliminary results are posted.

Primary Attack Methods and Hypothetical Scenarios

Below, we offer a series of hypothetical scenarios in which the technologies discussed above could be used to disrupt elections. These AI-assisted scenarios fall into three main categories: misleading the public about the electoral process; tricking election workers into aiding cyberattacks or disrupting election administration; and harassing election workers in ways that interfere with their work.

Method 1: Misleading the public

Election officials and offices are rightly among the most trusted sources of information about elections, especially in the period immediately before an election. For this very reason, they make an attractive target for those seeking to disrupt our elections.

Though these types of attacks may be difficult to stop altogether, careful preparation can minimize the disruptions they sow. In particular, by taking control of your online presence and being prepared for rapid-response communication, election offices can reduce the effects of these threats.

Scenario 1.1: Election official deepfaked in a public post

Background

Deepfakes created with AI may be the most talked-about threat from this new technology. A particular concern for election officials — being among the most trusted voices for election information — is that they or their colleagues will be deepfaked in a video or audio clip that voters believe to be real.

We have already seen deepfakes of public figures and politicians. In 2022, a manipulated video of Ukrainian President Volodymyr Zelenskyy telling Ukrainian troops to surrender their weapons went viral. A recent TikTok also went viral that used an AI-generated audio clip of President Joe Biden saying, "if we have to [. . .] wage war against Texas, so be it." These deepfakes were quickly debunked, in part because they were imitating internationally known figures making outlandish statements that were inconsistent with what people know about them. Deepfakes of election officials and workers may be more difficult to debunk, especially if the information is at least somewhat believable to a public that has little understanding of the intricacies of election administration.

How It Could Happen

In this hypothetical situation, a foreign adversary gathers publicly available video of an election official and uses the audio and visuals to train an AI system. With this training, the adversary can create a deepfake video depicting the official giving false information designed to trick voters, including falsehoods about how to vote. It could be targeted at members of a specific political party, gender, race, or ethnicity. The deepfake below is an AI version of Arizona Secretary of State Adrian Fontes and was produced as part of a statewide election security tabletop exercise with his consent and cooperation. But such AI-generated videos could be created of any election official *without* their permission, using anything from a years-old video recording of a city council meeting that the election official spoke at for only minutes, to a television interview an election official conducted just days ago. The danger is that the video looks and sounds

Video created by Toshi Hoo of the Institute for the Future using AI content generator GenAI

so authentic that people believe it is real, and it impacts their ability to vote or undermines their trust in the democratic process.

How to Prepare

- *Take control of your online presence.* Ensure that your website is on a .gov domain. Get verified social media accounts with consistent profiles. Doing so ensures that you'll be in a stronger position to respond through trusted, official channels.

- *Prepare for rapid-response communications.* By rehearsing the process of responding to a situation like this, you will be prepared to quickly debunk the deepfake on all available platforms.

- *Build and strengthen relationships with local media.* If you already have connections with local news media, you can shape coverage of the story to be accurate.

- *Prepare legal support networks.* Ask your attorney if state law provides legal options for responding to a deepfake of you, your staff, poll workers, or volunteers. For example, does your state law prohibit impersonating a governmental official acting in an official capacity? If so, are poll workers and/or volunteers covered? Work with your attorney to create a legal response plan in the event of a deepfake, which should designate responsible parties for collecting documentation and for contacting, if appropriate, website hosting companies and social media companies.

How to Respond

- *Document the attack.* Document carefully from the moment the attack is first observed with screenshots, screen recordings, hyperlinks, and downloads of audio, video, and image files. Work with your attorney to determine responsibility for searching to find every possible instance of the content, collecting the information, and cataloging it. Before any response action is taken, confirm that the video is a manipulation. Observe the media and look closely for visual artifacts. You will likely observe an unnatural desyncing between the subject's spoken words and their mouth movements. Beyond this, look closely at the video for a noticeable disconnect between the upper and lower parts of the face, an unnatural perspective, out-of-place shadows on the face, unnatural smoothness of the face, and a subject that does not turn their head. Listen closely to the audio and search for robotic speech patterns, unnatural vocal inflections, and electronic wavering in the voice as if a phone call is losing connection. Use deepfake detection tools like the one offered by TrueMedia.org, but note that such tools are not 100 percent reliable.

- Implement online damage control. Some social media platforms and some states may have laws expressly prohibiting this type of content. You or your attorney should immediately notify all social media platforms that have posts containing the deepfake. Always send hyperlinks and screenshots in case links cease to function and to facilitate rapid location of offending content.

- *Activate communications plan.* If the content appears to be gaining traction, you will want to issue a public statement on your website and through your official social media accounts and email lists, and contact trusted media outlets as quickly as possible. Your email lists should include civil society leaders in your community so they are aware of and can amplify your messaging, and your law enforcement, public emergency, and other relevant government counterparts so they are aware that you are facing such attacks and can, if appropriate, also amplify your messaging.

- *Escalate to appropriate authorities.* Contact your local attorney, the Federal Bureau of Investigation (FBI), the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), your chief state election official's office, and social media companies so they can ensure that others who may be affected by similar deepfakes are on alert.

Scenario 1.2: Public intentionally misinformed about where to vote

Background

WhatsApp has close to 100 million users in the United States, and it is possible that it has already had a significant effect on our elections — though it's hard to know for sure because it is an encrypted platform. iMessage, Signal, and Telegram also offer encrypted messaging, which means that the companies operating the platforms cannot read the messages that people send and receive. A notable exception to this rule is that if a user reports content for violating platform policies or breaking the law, the platform can see the reported content as it was originally shared.

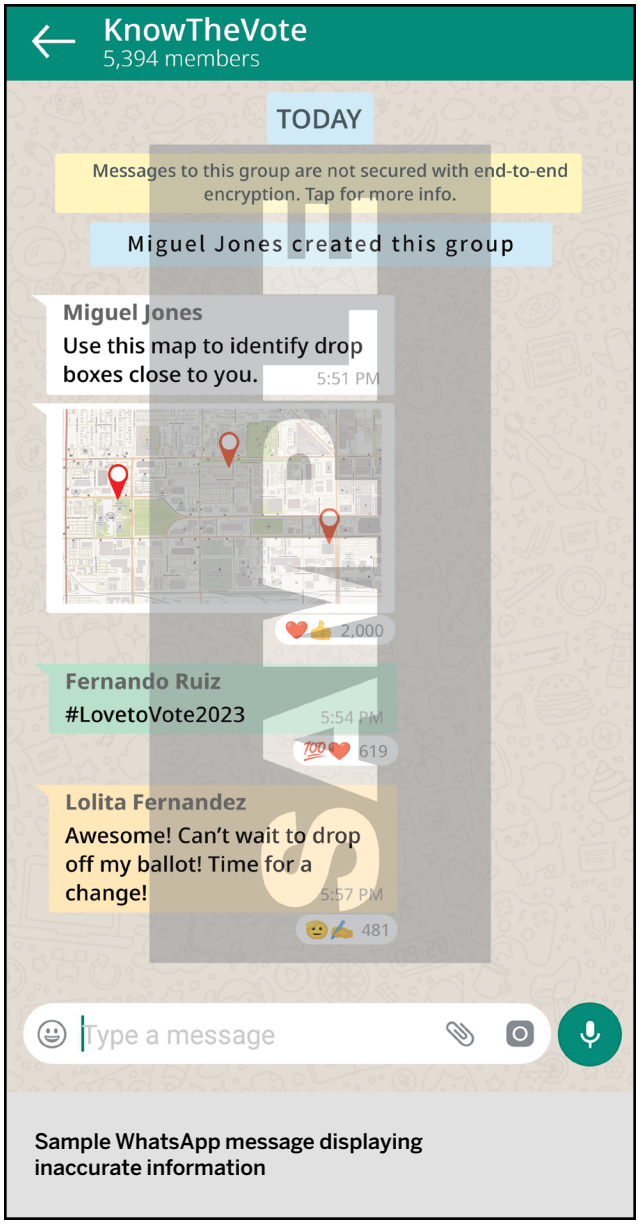
These encryption standards make WhatsApp and other encrypted communications tools ideal for spreading massive amounts of AI-generated, personalized, and even interactive chatbot-based misinformation about elections.

How It Could Happen

A large WhatsApp group chat displays inaccurate drop box locations throughout a county. The information seems to be spreading fast among the local Latino population.

How to Prepare

- *Take control of your online presence.* Ensure that all correct election information is publicly available and



Sample WhatsApp message displaying inaccurate information

easily accessible in languages used in your jurisdiction, and in a format that is easy to access on mobile devices, even for people with low literacy or digital literacy levels. Ensure that your website is on a .gov domain, establish official social media accounts, and routinely search for impersonating websites and social media accounts. If you do not have the resources to do this from your office, contact companies and nonprofits that can offer this service at low or no cost.

- *Prepare for rapid-response communications.* Establish a plan to communicate accurate information, including in the relevant languages. In jurisdictions where staff doesn't speak those languages, make contacts ahead of time with translators and community organizations to help with fast-turnaround translation needs.
- Build and strengthen relationships with local media. Establish contact with local news outlets and journalists, including those that report in languages that are common among your voters. Supply them with links to your official online and social media accounts, and share official ways for voters to contact your office so that their reporting can reference those official channels.
- *Prepare legal response network.* Review this scenario with your attorney and ask whether state law provides any legal remedies. For example, has your state criminalized the knowing and intentional communication of false and misleading information about the time, place, or manner of voting? Ensure that your attorney is aware of your existing documentation collection plans and public communications plans under these circumstances.

How to Respond

- *Document the attack.* Save links to and screenshots of fake websites and screenshots of chat messages that contain false information.
- *Activate communications plan.* If the false information gains traction, consider issuing a public statement that provides accurate information. Work with your local civil society organizations to amplify this statement.
- *Escalate to appropriate authorities.* Have contact information for social media and website hosting companies readily available to notify them about misleading information on their services and platforms. Notify your attorney.

Scenario 1.3: False reports warn of ICE showing up at polling places

Background

Agitators trying to suppress voters have historically used deceptive practices to keep people away from the polls. During the pandemic, political operatives ran a robocall scheme targeting thousands of Black voters in Ohio, telling them that if they submitted a mail-in ballot, their personal information would be added to a government database and they would be monitored by the authorities. Fake images of voters being arrested by U.S. Immigration and Customs Enforcement (ICE) went viral in 2016, and false rumors that immigration authorities will be at the polls are evergreen on social media. Disinformation campaigns often target racial groups that have been subjected to real oppression by the government, framing electoral participation as a dangerous activity. AI is likely to make such deceptions easier and more widespread.

How It Could Happen

A fake post purporting to originate from an election office

says that people without citizenship documentation may be subject to detention and interviews by ICE if they are at or near a polling place. The post appears as a social media screenshot and includes a fake website that looks just like the election office website but ends in .com instead of .gov. The account itself uses an official-sounding username and even has platform verification, which is available to purchase on specific platforms.

How to Prepare

- *Take control of your online presence.* Work ahead of time to ensure that the media, community groups, and your voters know how to get accurate information from your office if they have any questions about what they see online. In particular, ensure that your website is on a .gov domain and establish official social media accounts that they can turn to. Consider whether you can "prebunk" rumors you know are likely to spread during election season through an official "rumor control" page.

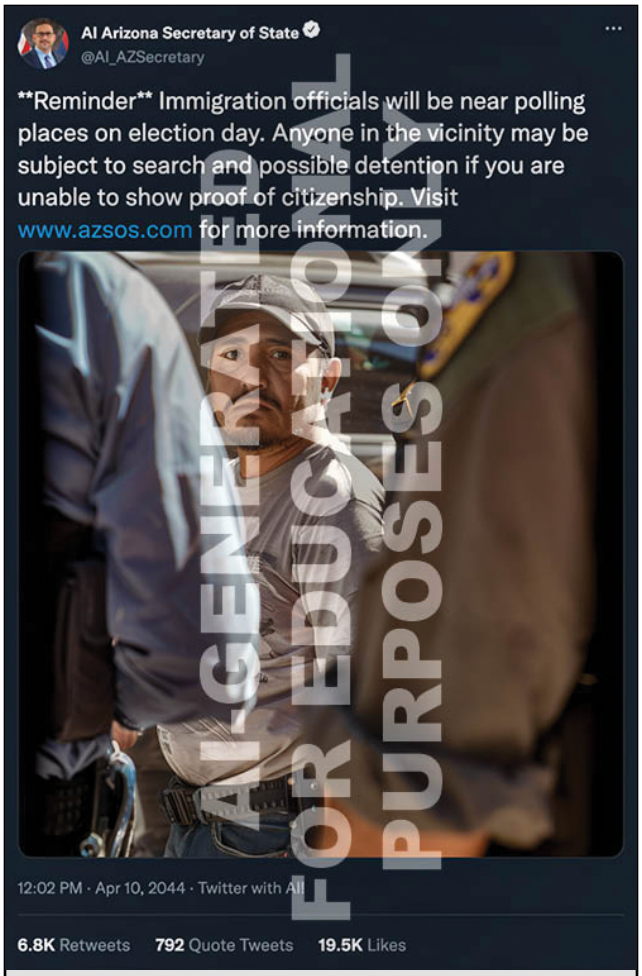


Image created using AI content generator TweetGen

- *Prepare for rapid-response communications.* Prepare the plan and designate the team members to provide rapid communications within your team and to the public to debunk the misleading posts. Review this scenario with representatives of local community organizations. Ensure that notifying these groups is part of your communications plan, and ask for their assistance to amplify accurate information under these circumstances.

- *Build and strengthen relationships with local media.* A strong relationship with local media makes it more likely that they will turn to you before amplifying false information.

- *Create escalation plans.* Create a plan to work with your secretary of state's office to report fake and misleading content to the relevant social media and web hosting companies.

- *Prepare legal support networks.* Review this scenario with your attorney and ask whether your state provides legal remedies. Agree on responsibilities for documentation collection and notification of social media platforms and web hosting companies.

How to Respond

- *Document the attack.* Be sure to collect both screenshots and links to all social media content and the offending website.

- *Escalate to appropriate authorities.* Escalate to your chief state election official's office, the EI-ISAC, CISA, your attorney, and social media platforms.

- *Implement online damage control.* Have a plan for notifying social media platforms and website hosting companies of false or misleading information that could disenfranchise voters.

Scenario 1.4: Elections website spoofed with fake results

Background

Voters turn not just to election officials for accurate election information, but also to local election office websites for everything from how to register to election night vote totals. Security experts have long proclaimed the dangers of spoofed elections websites masquerading as official government sources to spread misinformation. Indeed, in 2020, the FBI and CISA expressly warned that foreign adversaries may use phony elections websites to spread false information about the electoral process. This type of attack has also occurred against other government websites. For example, in 2020, the Federal Trade Commission sued a company that created hundreds of fake websites using

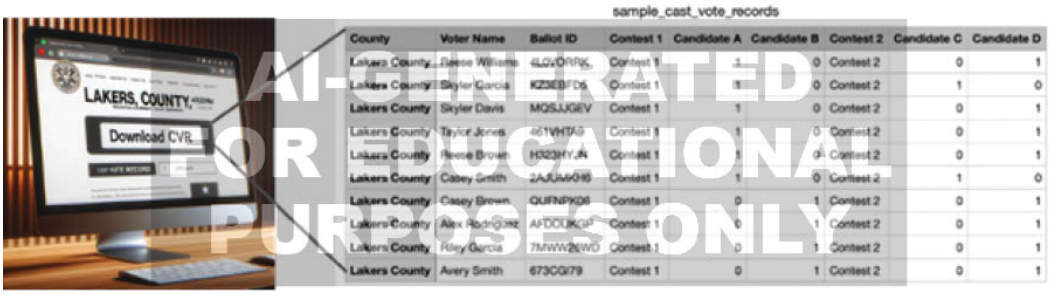


Image created using AI content generators DALL-E and ChatGPT

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 AI can simply read a target website's code and create scores of copycat sites.

How It Could Happen

A county elections website is spoofed and fake cast vote records with names of individuals are posted. Numerous groups from both parties are up in arms that this occurred. Election officials suspect that ChatGPT or a similar tool was used to create this phony website.

How to Prepare

- *Take control of your online presence.* Work with your IT department or the person in charge of your online presence to ensure that your website's code and any sensitive personal data about voters cannot be easily revealed and spoofed, and make sure that your official website and all official information is on a .gov domain.
- *Build and strengthen relationships with local media.* Supply media and community partners with links to your official online and social media accounts and official ways for voters to contact your office so that they can promulgate these accurate information sources.
- *Prepare for rapid-response communications.* Prepare a plan that identifies the internal staff members who need to be notified and their responsibilities, which may include posting a notice on the jurisdiction's website or notifying the website hosting platform in the event of such a threat.
- *Create escalation plans.* Create a well-documented plan to escalate to your state election office and your local and state IT departments if a fake website or websites are identified.
- *Prepare legal support networks.* Review this scenario with your attorney and ask whether state law provides any legal remedies. If it does, agree on responsibilities for documentation, evidence collection, and notification of web hosting companies.

How to Respond

- *Document the attack.* Save links to and screenshots of the fake website(s).
- *Implement online damage control.* Work with your secretary of state's office and local and state attorneys to notify website hosting services to take down any fake websites that are hosted on their platforms.
- *Activate communications plan.* Communicate accurate results to the public and include where they can find official information.
- *Escalate to appropriate authorities.* Notify your attorney and the state chief election official immediately. The FBI and the EI-ISAC should also be notified.

Method 2: Misleading election workers to aid cyberattacks and disrupt election administration

Microsoft recently reported that foreign adversaries such as Russia, China, North Korea, and Iran are using OpenAI's large language models to improve their hacking and spying operations. Foreign adversaries and other malefactors are reportedly using AI tools for help with coding to gain personal information about targets and to translate and use foreign languages. Election offices are almost certainly among those targets.

By systematically preparing for these attacks, election officials can harden their defenses and effectively deter most of these efforts. That preparation includes taking the latest cybersecurity trainings and implementing

protocols to respond to attacks. In some cases, election officials will need to be prepared to escalate incidents to state and federal agencies. Having an advance plan for how to do this will facilitate a more rapid response, which will in turn help to reduce harm.

Scenario 2.1: Hackers send texts or emails phishing for credentials

Background

Spear-phishing attacks target individuals or organizations through deceitful emails or other forms of communication with the goal of stealing sensitive information or infecting IT infrastructure with malware. These types of attacks have been part of foreign adversaries' playbooks for years, and there's no reason to think that 2024 will be any different. In 2016, Russian military intelligence sent spear-phishing emails to more than 100 U.S. election officials. The emails pretended to come from an e-voting vendor and lured officials into opening Microsoft Word documents that contained malware.

In 2022, phishing emails targeted Pennsylvania election workers before the state's primary. Arizona saw a 291 percent increase in phishing emails before its primary. The FBI warned election officials in 2022 of a widespread phishing campaign, and CISA recommends a multitude of resources to protect against phishing attacks.

2024 may see even more such attacks. AI can help hackers write and disseminate more sophisticated phishing emails and texts in greater numbers with fewer resources.

How It Could Happen

Election officials receive fake emails from people pretending to be with the secretary of state's office or the Department of Homeland Security directing them to configure two-factor authentication for the state election system. The AI-generated messages appear particularly convincing because they contain sensitive information and they use language appropriate to the region. In reality, although the messages look personalized and handcrafted, they are based on stolen databases and information publicly available on social media.

How to Prepare

- *Understand what AI can do.* Learn about how AI systems can be used to gather and process information from across the internet about people, their education, their travel, and even up-to-date weather conditions and sports in their areas.

- *Adopt cybersecurity best practices.* The latest CISA trainings and resources will help your team understand the degree to which AI can be used to customize spear-phishing campaigns. Talk with your IT department about installing software designed to mitigate spear-phishing.

- *Prepare legal support networks.* Review this scenario with your attorney and ask if state law protects you and your office against this threat. For example, does state law prohibit impersonating a governmental official acting in an official capacity? If yes, work with your attorney to

From: AZ Secretary<secretary@azsos.com>
Sent: February 2, 2024
To: Liz<lizrocks@ymail.com>
Subject: Two-Factor Requirement

Dear Liz,

It was great seeing you in Phoenix last month. I hope you and your family had a refreshing and memorable vacation in Telluride last week! There's nothing quite like exchanging our Arizona warmth for some scenic mountain coolness to recharge the batteries. Hope you stayed dry--I heard there was a lot of rain in the rockies last week! As you settle back into the desert rhythm, we have an important update that requires your attention and action.

While you were gone, we introduced a mandatory two-factor authentication (2FA) system to enhance our cybersecurity measures. Adapting to 2FA is a crucial step in ensuring our digital environment is as secure and resilient as possible.

By 5pm today, please take a moment to enroll in our 2FA program. Think of it as your digital sunscreen--essential under the Arizona sun.

1. Visit azsos.com/2fa to start the setup. It's as straightforward as following a well-marked trail.
2. Complete the setup steps, and you'll be all set. Remember, you'll need your username and password to start the process, and those are the same as the credentials you use to login to Microsoft Office 365.

We're here to support you, so if you have any questions or need assistance, please reach out to Michael on our IT support team for help.

Last but not least, hope you're watching the game on Sunday--go Wildcats!

Warm regards,

Sample email that could be used as part of a phishing scheme

create a legal response plan, which should designate responsible parties for collecting documentation and contacting, if appropriate, the companies hosting fake websites that could be used to collect usernames and passwords.

How to Respond

- *Escalate to the appropriate authorities.* Escalate to your state's chief election office and IT office if you suspect that a communication is fraudulent. Notify your attorney. Do not take the steps mentioned in the communication.

- *Stop the attack and secure infrastructure.* If you accidentally engaged with the communication before you realized it was fraudulent, such as by clicking on a link in a phishing email, immediately notify your IT department or the person responsible for your network so that they can prevent or mitigate any damage to infrastructure.

Scenario 2.2: Voice-cloned audio misinforms election workers about polling place hours

Background

Microsoft has confirmed that foreign adversaries are experimenting with large language models to improve their hacking efforts. It is probable that malicious state actors are testing other tools, including ones that can imitate election officials by voice or image. Indeed, both Russia and China have been accused of creating deepfakes to interfere in elections in Slovakia and Taiwan. Election offices should consider how deepfakes of their workers or officials could be used to target their operations.

How It Could Happen

An AI-generated voice clone of an election official is used to leave a voicemail for election workers, telling them that the office has received a court order to keep the polls open for an extra hour.

How to Prepare

- *Adopt cybersecurity best practices.* Among other steps, establish a phone number that election staff and polling place captains can call if they receive an unusual or urgent request to confirm that the request or order is legitimate.

Audio created using AI content generator Elevenlabs

- *Create escalation plans.* Create a well-documented plan for your team to escalate to your state's chief election office and relevant agencies.

- *Prepare for rapid-response communications.* Have a plan in place to be able to rapidly respond by informing your staff, voters, and local news media of actual voting hours. Prepare a secondary channel for your team members to confirm whether any such voicemail messages are real.

- *Build and strengthen relationships with local media.* Establish contact and relationships with local journalists and news outlets in advance in case rapid communications are needed.

- *Prepare legal support networks.* Review this scenario with your attorney and ask if state law protects you and your office against this threat. For example, does state law prohibit impersonating a governmental official acting in an official capacity? If yes, work with your attorney to create a legal response plan, which should designate responsible parties for collecting documentation and for contacting, if appropriate, telecom companies.

How to Respond

- *Document the attack.* Save the fraudulent voicemail(s) and record all details.

- *Escalate to appropriate authorities.* Contact your attorney, the FBI, the EI-ISAC, and CISA.

- *Activate communications plan.* Put out a statement reaffirming accurate voting hours.

Method 3: Harassing election workers to interfere with their work

Election workers and offices are, unfortunately, no strangers to harassment. As with other threats discussed above, AI could amplify this kind of attack, increasing the quantity and sophistication of harassment to interfere with administering elections.

The past few years have prepared election officials to address such attacks through countermeasures ranging from installing CAPTCHA (completely automated public Turing test to tell computers and humans apart) and anti-spam filters on office websites to prevent nonhuman users from overwhelming systems to increased cooperation and planning with local law enforcement.

Scenario 3.1: Phone lines jammed with AI-generated calls

Background

In August 2023, talk show host Charlie Kirk called for

people to "break the phone lines" of the New Hampshire Secretary of State's office to demand that Donald Trump remain on the primary ballot, even though Secretary of State David Scanlan had no plans to remove him. The office was soon flooded with hundreds of calls. Handling large volumes of calls demands precious time and resources, which are already limited by election offices' budgets and staffing constraints. Organized campaigns to deluge offices with phone calls can easily overwhelm election officials.

Similarly, denial-of-service attacks — in which attackers inundate a website or network with traffic and make it inaccessible to users — shut down websites and caused service interruptions in multiple state and local election offices in 2022. A number of elections websites were briefly compromised on Election Day that year. CISA advises election offices to plan and train for denial-of-service incidents. Even when non-malicious, large amounts of traffic on a voter registration portal or other elections website can cause major outages.

How It Could Happen

The election office phone line and staff's cell phones begin receiving regular calls asking questions about the election, such as polling place hours, addresses, and details about ballots and how to fill them out. Each call individually could be a real constituent, but the number of calls overwhelms staff resources and is far beyond what the office has seen before. When asked to identify themselves, the callers use names from actual voter rolls. Occasionally, there are suspiciously long pauses during the calls, and sometimes names of streets or last names seem to be pronounced strangely. The election office staff begins to suspect that the calls are AI-generated.

Audio created using AI content generator Elevenlabs

How to Prepare

- *Adopt cybersecurity best practices.* Ensure that public phone numbers are separate from internal and operational lines distributed to staff and emergency services so that at the very least, this kind of denial-of-service attack does not compromise your team's ability to communicate with each other. You should maintain a confidential list of alternative contact numbers for election workers to reach each other. If possible, provide core staff with dedicated work cell phones.

- *Communicate with your IT department and phone provider to discuss your office's current phone line capabilities and how to prepare for an overflow event.* Discuss with your phone provider how the phone lines will behave under heavy load so that a crisis can be quickly identified. Further, discuss ways that your office's phone preferences may be modified, such as by prioritizing relevant area codes. Collect contact information from the phone provider so that support can be reached quickly in case of a crisis.

- *Create escalation plans.* Create a plan for how to escalate when staff resources are being swamped and need to be adjusted. Create a process to efficiently document each call and what the call is about to make it easier to identify any patterns.

- *Prepare for rapid-response communications.* Be prepared to communicate to voters through other means if phone lines are overwhelmed, and to provide voters with legitimate questions a way to get the help they need, such as offering links to websites with voting information.

How to Respond

- *Document the attack.* Direct your staff to save voicemail messages and log call details, such as time, date, duration, and general questions asked as well as — if available — phone numbers used to call the office.

- *Escalate to appropriate authorities.* Contact your IT department, local telecom companies, the FBI, the EI-ISAC, and CISA to quickly investigate.

- *Activate communications plan.* Inform voters on your .gov website, social media accounts, and/or local news media that phone lines are receiving heavy volume and provide an alternate method for voters to access information they need. Contact civil society partners (such as chambers of commerce and voting rights groups) and local government counterparts (such as the county board of supervisors and law enforcement), informing them of the situation and asking them to amplify your public statement via their social media accounts and other communication channels.

Scenario 3.2: AI-generated social media posts call for armed protest at polling places

Background

Using social media to organize protests is not new. In 2016, Russia used Facebook accounts to organize over 60 protests on a variety of topics to deepen political discord. In December 2020, the Iranian government created a website called "Enemies of the People," which was disguised as a creation of far-right American activists and directed death threats at election officials and other public figures.

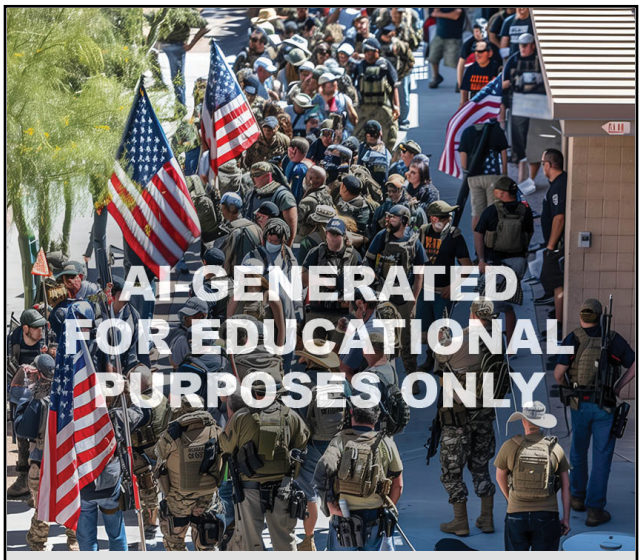


Image created using AI content generator Midjourney

While the scenario detailed here may not be a new threat, AI may make it dramatically easier for malefactors, including state actors, to create similar posts but in greater number and more convincingly (e.g., in multiple languages) than was possible just a few years ago. Russia, China, and Iran are already trying to weaponize OpenAI and Microsoft's AI tools, so election offices should be prepared for such attacks in 2024.

How It Could Happen

Angry and hostile posts are appearing at a rapid rate on social media, recruiting people to join protests. One post reads, "The fight for democracy is here! Fight off the deniers! Every vote must count! Protest starts at 8:00 a.m. at the vote counting center." Another post that was flagged and quickly removed said, "End the fraud! End the corruption! Arm yourself and be ready to defend our freedom! Early voting protest TODAY!" Some of the accounts posting the content appear suspicious — they were created recently, and some contain images that on close inspection appear to be AI-generated.

How to Prepare

- *Take control of your online presence.* Prepare posts on your social media accounts with updates to reassure voters that voting is proceeding smoothly and without fraud, to be posted ahead of and on Election Day. Make the public aware that your secured accounts are official.

- *Plan for rapid-response communications.* Reach out to local media in advance. Prepare a process and designate a point person on your team to handle rapid-response communications.

- *Create escalation plans.* Meet with local law enforcement; share information (such as the location and hours for all your polling locations and, if relevant, tabulation centers, warehouses, and other elections facilities) and develop a response plan. (See the Committee for Safe and Secure Elections' "Five Steps to Safer Elections" guidance and template memorandum of understanding between election officials and law enforcement.) Contact other supporting agencies that can assist if needed. Consider asking CISA for a physical security assessment for voter and counting centers.

- *Prepare legal support networks.* Review this scenario with your attorney. Share the response plan you've created with law enforcement.

How to Respond

- *Document the attack.* Document threats in detail. Include photos and video.

- *Escalate to appropriate authorities.* Given the imminent threat of violence, contact local law enforcement immediately. Take the steps mutually agreed upon with law enforcement to respond. Notify your attorney.

- *Implement online damage control.* Contact social media companies to notify them of the harmful content. Collect links to harmful or misleading content and share them with the social media platforms and with law enforcement.

Scenario 3.3: Election offices flooded with AI-generated FOIA requests

Background

In 2022 and 2023, conspiracy theorists who claimed they were seeking to validate unfounded allegations of widespread election fraud bombarded election officials with open records requests. In many instances, activist groups sent identical requests to multiple offices across the country. These often-excessive demands have sidetracked election offices from crucial election administration duties, especially in the lead-up to Election Day. In a 2023 poll of election officials, more than half said they were concerned about being harassed with bad-faith information requests in future elections.

AI can exacerbate this threat by allowing agitators to easily generate hundreds or even thousands of distinct open records requests targeting multiple jurisdictions. In the past, election offices turned to state offices or associations to coordinate responses and receive uniform guidance on how to respond. Such coordinated and synchronized responses become markedly more challenging when mass-produced requests vary in wording and cover a wide array of topics — capabilities that generative AI facilitates.

How It Could Happen

A local election office receives a series of Freedom of Information Act (FOIA) requests, each with slightly different wording, such that they each require different responses. They appear likely to have been generated by AI.

How to Prepare

- *Adopt cybersecurity best practices.* Institute CAPTCHA for election office portals that receive FOIA requests and public comments to prevent bots from using AI-generated open records requests or other opportunities for public comment to overwhelm an office. In instituting such tests, offices should ensure that those with disabilities or without access to high-speed internet are accommodated.

- *Create escalation plans.* Create a well-documented plan to escalate the incident and inform your state's chief election office and the local election official association.

- *Prepare legal support networks.* Review this scenario with your attorney. Share your escalation plans. Audit FOIA workflows to ensure maximum productivity. Consider communicating with statewide administrators about implementing self-service FOIA processes where feasible.

How to Respond

- *Document the attack.* Document the number of requests that you suspect are AI-generated, as well as any identifying details about the parties filing the requests.

Image created using AI content generator Ideogram

- *Escalate to appropriate authorities.* Because the onslaught may be a coordinated attack affecting other election offices, it is essential to alert your chief state election official, the EI-ISAC, and your local attorney.

- *Activate legal support network.* Your local attorney and other legal advisers may have advice about how to handle your response to this onslaught in a way that minimizes the ability of bad actors to disrupt your operations.

From: recordsnow@gatherer.net
Sent: August 22, 2024
To: ElectionsDirector<Elections@mi.county.gov>
Subject: Public Records Request for 2020/2022 Ballots

Dear Elections Director,

I hope this message finds you well. I am writing **again** to formally request access to public records related to the 2020 ballots cast in the jurisdiction you manage, pursuant to Arizona law.

Specifically, I am seeking the following information:

- Digital or physical copies of all ballots cast in the general election held in November 2020 and 2022.
- Any associated records, including but not limited to precinct counts, absentee ballots, and any related documentation regarding ballot tabulation and verification procedures.

Additionally, if there are any fees or costs associated with fulfilling this request, please inform me in advance. As a responsible requester, I assure you that the information obtained will be used solely for lawful and non-commercial purposes.

I kindly request that the records be provided in a digital format if possible. If there are any concerns or limitations regarding the accessibility of these records, please let me know, and I am willing to discuss alternative means of access. I understand and appreciate that fulfilling this request may take time. Thus, I would be grateful for an estimated timeline regarding when these records could be made available.

Thank you for your attention to this matter. Please acknowledge receipt of this request and inform me of any further steps required to proceed. I look forward to your prompt response and the opportunity to access the requested information.

Sincerely,

Citizens for Straightforward Elections
Maggie McMean

Sample email that could be used to overwhelm election offices with FOIA requests

Prepare for AI Threats

While AI threats cannot always be prevented, awareness and preparation will allow election officials to manage and mitigate these threats. This section lists several ways for election officials to prepare for any eventuality.

Understand What AI Can Do

Unless you and your team have a strong grasp of what AI technologies can do, you will be at a disadvantage when it comes to identifying and responding to AI threats to election security.

- Read this document thoroughly, especially the Identify AI Threats section.
- Try online deepfake detection tools like the one offered by TrueMedia.org, which, at the time of publication, appears to be the best tool available. Note that it requires an account, and although it is a free tool, there is a waitlist to get one. Keep in mind that there are currently no perfect or foolproof ways to identify AI-generated or modified content. AI technologies are constantly improving, so do not assume that you will always and conclusively be able to identify AI-generated content.
- Train your staff on the above.
- Test AI tools yourself by creating free accounts and/or watching demos on the following websites:
  - ChatGPT — The most popular AI chatbot and image generator
  - Google Gemini — A newer AI chatbot and image generator from Google
  - ElevenLabs — an AI tool for making fake voices
  - HeyGen — an AI tool for making fake videos of people speaking

Take Control of Your Online Presence

Your official online presence is your best defense against many types of AI threats. By controlling it in a secure and organized way, you are better positioned to counter these threats.

- Make sure that all official information is on a .gov website:
  - Ensure that all information is correct and up to date.
  - Establish and rehearse procedures for quickly correcting information and posting updates.
  - Provide answers to common questions in advance through multiple information channels, such as your website, social media account(s), prerecorded messages, and traditional media.
- Secure your website:
  - Work with your IT department or the person who manages your network to ensure that all cybersecurity best practices are met.
  - Implement a web application firewall (WAF), which can help defend against several types of cyberattacks. Certain cybersecurity companies offer free WAF services to election agencies.
- Secure and verify social media accounts on all major platforms:
  - Make the public aware that your secured accounts are official.
  - Ensure that your accounts are secure by using long passwords unique to each social media account, using a password manager to store passwords, setting up multifactor authentication when possible, minimizing who has access to each account, and changing passwords when an employee leaves.
  - Put a link to your official .gov website in the profile of all social media accounts.
  - Register social media accounts even on platforms that you don't plan to use, ideally with the same username you use on other platforms. Even if you

don't use them, it prevents others from using them and drives people back to your official website.

  - Use a consistent logo across all your social media accounts and websites so that they are not mistaken for impersonations.

- Conduct regular impersonation checks:

  - Set up a Google alert for your name and your office's name.

  - Scan social media to make sure that others are not impersonating your accounts. Ensure that scans take place at regular intervals. (Ideally, this practice should occur daily starting the week before voting begins.)

  - Search for your name (with variations) and that of your office and key staff members periodically. Include searches with quotation marks around the names.

- Conduct security checkups for all your personal and official social media accounts. Follow the instructions provided by the platforms:

  - Facebook: If upon logging into your account you see a notification on your newsfeed that prompts you to defend your account with Facebook Protect, select "Get Started." Facebook Protect provides security protections for certain elected and public officials. If there is no notification, perform a Facebook security checkup.

  - Instagram: Perform an Instagram security checkup.

  - Youtube: Perform a YouTube security checkup.

  - Google: Perform a Google security checkup.

- Consider developing a public service announcement campaign — leveraging paid social, digital, and search advertising, earned media, and your social media and other communication channels — both to warn voters that agitators may try to mislead them and to establish your office as the authoritative source of information on voting.

- Inform the public of your official websites, phone numbers, and social media accounts, and include links to frequently asked questions that can prebunk misunderstandings and misinformation about the voting process.

- Because developing and implementing such campaigns (including hiring communication professionals and marketing firms and paying for advertising) costs money, consider leveraging Help America Vote Act funds, which can be used for voter education campaigns.

Prepare for Rapid-Response Communications

Harms stemming from AI threats can spread rapidly. Your ability to respond quickly on your official channels will determine how effectively you can counter these threats. This requires, among other actions, building strong relationships with journalists, community leaders, and other government officials, as they may become important resources if you face misinformation or other threats that require you to quickly relay accurate information to reduce harm.

- Identify all communication channels and login credentials and keep a list of who has access to each.

- Reach out to local media, community partners, and other government leaders, such as fire and law enforcement, far in advance of the election. Let them know who you are, what your official phone and email contact information is, what official social media accounts you plan to use (if any), and that you're available to talk to them throughout the election period if they have questions. As part of these discussions, ensure that they are aware of potential AI threats to elections. Relationship-building is key, as journalists and civil society leaders — ranging from voting rights groups and unions to chambers of commerce and veteran groups — will be critical figures if you face AI threats.

- Develop a crisis communications plan, ensuring that everyone who potentially has a role — including communications, IT, legal, and leadership — is familiar with it and their duties.

- Use free crisis communications plans offered by the Elections Group and the Belfer Center at Harvard University, which include crisis communications exercises and can be used to develop a plan to respond to AI threats. As part of your plan, ensure that you:

  - Establish a communications lead for all rapid-response communications, as well as a support team. Ensure that all members of this team have access to all communication channels (social media, website, etc.).

- Create an on-call schedule so someone is always available to respond to incidents. Consider duplicating coverage during the election period.

- Prepare a secondary channel for your team members to confirm requests, even internal requests from staff members, before releasing sensitive information. Consider implementing identity verification for real-time communications. Protect against virtual impersonation attempts by adopting a rolling passphrase that only authorized personnel know, especially during active voting periods.

- Conduct crisis communications exercises with everyone who could be involved in such scenarios, focusing on rapid-response posting to social media sites and your website to correct misinformation or post updates.

  - Time practice runs using a message notifying your constituents that these are your official accounts and that your .gov website and verified social media accounts are the only places that they can get official information about the election. The goal is 30 minutes or less.

- Prepare proactive and responsive public communications about your secure practices. Develop talking points conveying fact-based evidence that your voters should have confidence in the security of your elections processes.

- Meet with local community organizations, including civil society organizations, to share the scenarios above and ask for their assistance in responding, when necessary, to these threats. Identify organizational points of contact and consider creating an email distribution list to quickly and easily distribute accurate information.

- Identify and meet with representatives of other local government agencies, such as law enforcement, IT, and communications, to share the scenarios below and ask for their help preparing for and, when necessary, responding to these threats. Identify organizational points of contact and consider creating an email distribution list so that you can quickly distribute accurate information.

Adopt Cyber and Physical Security Best Practices

Securing your technology systems fortifies your defenses and allows you to respond more quickly to AI threats. If you're not comfortable with the below recommendations, now is the time to request additional technical support from CISA, your cyber navigator program (if available), or your local or state IT office.

- Move toward zero trust security principles — a cybersecurity framework that requires continued authorization for all users — to prevent unauthorized access to data and services and make access control enforcement as specific and detailed as possible. Consult CISA's Zero Trust Maturity Model, which provides a scale of recommendations for implementation.

- Leverage password managers to keep all passwords secure, including for

  - website administration tools,

  - social media accounts,

  - email accounts and administrator tools,

  - your phone service provider,

  - your internet service provider, and

  - any other accounts that could be compromised.

- Enable multifactor authentication for all accounts. Whenever possible, do not share accounts between individuals — create a separate account for each person on your team and delegate appropriate access privileges to them.

- Update to the latest operating systems on all devices connected to the internet, including your team's personal phones and computers. Continuously review authentication tools to ensure that they are resilient to evolving capabilities (including AI-enabled capabilities) and employ tools that use so-called AI-hardened tasks or hardware-linked software actions (such as rotating a phone) to authenticate users.

- Implement CAPTCHA verification tests for open records requests, allowing accommodations for accessibility.

- Consider implementing CISA-recommended security systems, such as

  - endpoint detection and response (EDR) software, which continuously monitors devices used to access your system to detect and respond to cyber threats like ransomware and malware;

  - email authentication security protocols such as domain-based message authentication, reporting, and conformance (DMARC); sender policy framework (SPF); and DomainKeys Identified Mail (DKIM)

to better guard against email spoofing; and/or

  - cyber hygiene services, a proactive approach to cybersecurity that implements weekly vulnerability scanning, reports, and alerts.

- Talk to vendors about adopting provenance and authentication measures for election-related records. Consider using active authentication techniques such as watermarks, which mark and verify that a piece of content originated from your office and helps identify when files were altered after credentials were applied.

- Require staff and volunteers to complete CISA cybersecurity training programs.

- Request a CISA cyber assessment.

- Contact your regional CISA office to request a physical security assessment.

- Build more security and resiliency into election systems, such as using paper ballots, audits, and backups.

- Ensure that adequate technical support is available during the election period.

- Monitor election officials for potential insider threat behavior.

- Use secure calling channels (e.g., video calling, call authentication via email).

- Encourage staff to use services like DeleteMe to remove their personal information from online data broker websites. CISA recommends that you and your staff make your personal social media accounts private and delete old accounts.

- Establish authentication practices:

  - You and your staff must still be able to speak and exchange information by phone, text, and video conferencing. Authentication practices are ways to ensure that you are interacting with the actual person presenting themselves online, over the phone, over video chat, etc. Whatever method or methods you deploy, ensure that your team is informed on these new protocols.

  - A simple and effective practice is to establish a safe or code word before sharing secure, confidential, or sensitive information with a teammate over the phone or online. Share this safe word in person and then request it during your remote conversations. You can change safe words routinely or have them follow a convention.

  - Use knowledge-based authentication. Ask staff members a personal question that only legitimate personnel would know. You can also use predetermined security questions established in-office, similar to security questions for online banking.

  - Look for behavioral authentication. Voice synthesizers might mimic your voice range but not necessarily your speech patterns and behavior. Video bots are often very static in their head movements. Ask the caller to raise their hand or make a polite gesture.

  - Use out-of-band authentication. Whatever channel you use to communicate, use something else for verification.

Build and Strengthen Relationships with Local Media and Other Partners

Building strong relationships with journalists is crucial, as they may become important resources if you face misinformation or other threats that require you to quickly relay accurate information to your community to reduce harm.

- Let local media outlets know who you are and what your official contact information is (phone numbers, email, and social media accounts). Let them know that the lines of communication are open during the election period. Inform them of AI threats and encourage them to reach out to you directly if they see anything even slightly suspicious.

- Learn how to directly notify social media platforms of content on the electoral process — such as misleading information about when, where, and how to vote — that may violate their terms of service.

- Contact your hosting provider, such as Cloudflare, and establish a direct line of contact so that you know what to do in case of a security incident.

- Engage key community organizations and leaders in law enforcement, fire, and other agencies. As you do with media, ensure that these organizations know who you are, and that you have a direct line of communication in case you need to use it in an emergency.

Create Escalation Plans

Creating a well-documented plan for how to escalate AI threats will allow your team to respond more quickly and reduce harm if crises arise. Escalation plans should fit into existing continuity of operations plans or incident response plans. Consider identifying a contact person and gathering contact information for the organizations listed below to include in your existing continuity of operations or incident response plans. If your office does not currently have a continuity of operations or incident response plan, the resources below can help you create one. Ensure that escalation plans and emergency contact lists are available digitally and in printed physical form.

- Local resources
  - Your office IT department (or contact person)
  - Your phone service provider
  - Your internet service provider
  - Local law enforcement
  - Your attorney
- State resources
  - State chief election official's office
  - Your state fusion center (for counterterrorism reporting and information)
- National resources
  - CISA regional election security advisors and regional directors
  - EI-ISAC
  - FBI
  - National Guard
  - U.S. Postal Inspection Service
- Continuity of operations and incident response planning resources
  - Ready.gov — business continuity planning
  - EI-ISAC — incident response planning
  - CISA — incident response plan basics
- Practice
  - Create a fake incident and ensure that your team knows the correct escalation and communications channels and mitigation actions. Use the scenarios in the first section for inspiration.

Prepare Legal Support Networks

- Meet with your local attorney. Identify AI-associated threats and ask them to review the legal remedies available in your state and jurisdiction, using the scenarios in this document to guide your conversation.
- Ask your attorney to be available on Election Day and in the period leading up to the election. Your local attorney is an important partner to protect against and respond to AI-related threats to safe and secure elections.

Respond to AI Attacks

Document the Attack

A key part of responding to an AI threat is documenting everything so that lessons can be learned to prevent future attacks. This will help digital forensic analysts understand how the attack happened and how to fix any vulnerabilities.

- Collect hyperlinks, screenshots, and, in the case of video or audio, screen or audio recordings as well. This evidence collection ensures that durable documentation of screenshots and recordings exists, even if content is removed and hyperlinks no longer work. Once you get used to documenting, it should be a relatively quick process, only taking a few minutes. It is crucial to document before taking other steps because evidence can disappear quickly.

- Use deepfake detection tools like the one offered by TrueMedia.org to investigate possible deepfakes, then take screenshots of the reports so that you can show why you believe them to be fake. As mentioned, none of these tools are perfect. Be sure to use language that does not overstate your confidence in your assessment of the deepfake.

Escalate to the Appropriate Authorities

- Notify your attorney, local law enforcement, the FBI, the EI-ISAC, CISA, social media companies, and any other relevant entity if necessary. Alert these groups to the attack and seek their help identifying the perpetrator(s) and mitigating the harm caused by the attack.

- Contact law enforcement immediately if officials, staff, volunteers, or voters are being threatened with violence.

Stop the Attack and Secure Infrastructure

Once an attack is identified, make sure to stop it from causing any additional damage as soon as possible. Doing so might require help from outside agencies like those listed above, or from other local government IT departments. Your internet service provider may also be able to help.

- Immediately shut down any compromised systems or take them offline, then work with IT or other technical experts to determine the correct course of action.

Implement Online Damage Control

- Notify the relevant social media platform or web hosting service of the content through publicly available reporting tools or channels, as well as through any relationships that you have cultivated.

- Work with the chief state election official to notify social media sites of the content if their office has more direct means of communication.

- If the misleading content is a fraudulent website, Cloudflare and other hosting services also have procedures to notify platforms of content that may violate their terms of service.

Activate Communications Plan

- Implement your crisis communications plan to alert the public to the issue when necessary. This might look like issuing a public statement on your verified social media accounts, on your .gov website, and/or through local news media.

- Activate your network of local civil society organizations, community groups, and, where appropriate, state and local election offices and others who can ensure that your statement reaches as wide an audience as possible.

Activate Your Legal Support Network

- Move quickly to notify your attorney.

Conclusion

As the scenarios in this planner show, most of the current threats to elections posed by AI are not entirely novel. For the 2024 U.S. election, the real challenge is that AI provides agitators new tools to increase the scale of such attacks at little cost and in more sophisticated form than we have previously seen.

For years, experts have been warning about the threats that AI poses to elections — even before recent advancements — including those from misinformation directed at the public, phishing attacks against election offices, and denial-of-service attacks against election infrastructure. Many election offices have already implemented significant and successful steps to protect their infrastructure and staff from these threats. Our hope is that this scenario planner will help election officials build on their preexisting security plans to prepare for the more sophisticated and widespread attacks that AI may bring.

ABOUT THE AUTHORS

▶ **David Evan Harris** is Chancellor's Public Scholar at the University of California, Berkeley, and a senior adviser on AI and elections to the Brennan Center's Elections and Government Program. He previously worked as a research manager at Facebook (now Meta) on the responsible AI, civic integrity, and social impact teams. Harris is a frequent commentator on AI, misinformation, and technology and has been published or quoted by the *Wall Street Journal*, the *Washington Post*, the Associated Press, the *Atlantic*, the BBC, Bloomberg, the *Guardian*, and *Tech Policy Press*, among others.

▶ **Lawrence Norden** is senior director of the Brennan Center's Elections and Government Program, where he leads the Brennan Center's work on ensuring that U.S. election infrastructure is secure and accessible to every voter and protecting elections from disinformation and foreign interference. He served on the U.S. Election Assistance Commission's Board of Advisors from 2019 to 2023 and has testified before Congress and several state legislatures. Norden's work has been featured in outlets including the *New York Times*, the *Wall Street Journal*, Fox News, CNN, MSNBC, and NPR.

▶ **Noah Praetz** is president of the Elections Group and consults on election operations and security for local, state, and federal election partners. He formerly ran elections in Cook County, Illinois. In 2019, he left Cook County to support federal, state and local election security and administration efforts, and then cofounded the Elections Group in 2020. Praetz has testified before U.S. House and Senate committees on election security and is a lecturer at the University of Chicago and an adjunct law professor at DePaul University College of Law.

▶ **Elizabeth Howard** is deputy director of the Brennan Center's Elections and Government Program, where she focuses on election security. Prior to joining the Brennan Center, Howard served as deputy commissioner for the Virginia Department of Elections. She previously worked as general counsel at Rock the Vote, a nonprofit organization dedicated to engaging young people in politics, and as a senior associate at Sandler Reiff in Washington, DC, where she specialized in election law with a focus on voting rights, campaign finance, and postelection disputes.

▶ **Toshi Anders Hoo** leads Institute for the Future's Emerging Media Lab, where he explores the implications of rapidly evolving technologies that are transforming the ways humans communicate, collaborate, and connect. Hoo also leads IFTF's Technology and Media Foresight Council, advising leaders from both the public and private sectors, and he is a lead instructor for IFTF's Three Horizons of AI course, which explores the near-, mid-, and long-term implications of AI. His work examines not only the direct applications of emerging technologies but also their wider implications and impact on individuals, organizations, and society at large.

ABOUT THE BRENNAN CENTER

The Brennan Center for Justice at NYU School of Law is a nonpartisan law and policy institute that works to reform and revitalize — and when necessary defend — our country's systems of democracy and justice. The Brennan Center is dedicated to protecting the rule of law and the values of constitutional democracy. We focus on voting rights, campaign finance reform, ending mass incarceration, and preserving our liberties while also maintaining our national security. Part think tank, part advocacy group, part cutting-edge communications hub, we start with rigorous research. We craft innovative policies. And we fight for them — in Congress and the states, in the courts, and in the court of public opinion.

ABOUT THE INSTITUTE FOR THE FUTURE

Institute for the Future is the world's leading nonprofit futures organization. For over 55 years, businesses, governments, and social impact organizations have depended upon IFTF global forecasts, custom research, foresight education, and training to navigate complex change and develop future-ready strategies. IFTF methodologies and toolsets yield views of transformative possibilities across all sectors that together support a more equitable and sustainable future.

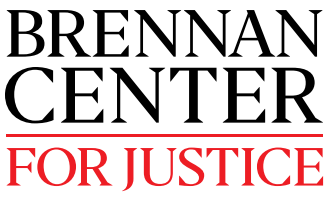
ABOUT THE ELECTIONS GROUP

The Elections Group is a non-partisan team of election experts supporting election professionals through collaboration, thought leadership, and elevating best practices. The Elections Group partners with state and local election jurisdictions, as well as nonprofit organizations, to help implement new programs or improve processes for voters and stakeholders.

ACKNOWLEDGMENTS

The Brennan Center extends deep gratitude to all our supporters, who make this report and all our work possible. See them at brennancenter.org/supporters.

The authors thank Arizona Secretary of State Adrian Fontes and his staff, particularly Assistant Secretary of State Keely Varvel and Chief Information Security Officer Michael Moore, for hosting the December 2023 tabletop exercise and providing insightful and constructive feedback on this report. We especially thank Toshi Hoo of the Institute for the Future for his assistance in creating many of the AI-generated video, audio, and images that were used in the tabletop exercise as well as in this report. We are grateful to Aaron Hayman, Matthew Tlachac, Michele Forney, and Andrew Haun, all of whom also assisted in the production of the tabletop exercise and were responsible for many of the AI-generated assets and other multimedia items used in that exercise and this report. We also thank Owen Doyle, Diane Chang, and Jackson Eilers for their substantial research, writing, and editing help, as well as Penny Mack, Derek Tisler, Julia Fishman, Marina Pino, and Shanze Hasan for cite checking and proofreading this report. Last but not least, thanks to Jiyoon Park for her assistance with the tabletop exercise.



Brennan Center for Justice at
New York University School of Law
www.brennancenter.org

Institute for the Future
www.iftf.org

The Elections Group
www.electionsgroup.com