2024 Election Threat Landscape

October 2024 • White Paper 2024-02

TLP: CLEAR

Introduction

The 2024 election threat landscape represents one of the most dynamic and complex threat environments U.S. election officials and organizations have faced. As a result, the Multi-State Information Sharing & Analysis Center (MS-ISAC), the Elections Infrastructure Information Sharing & Analysis Center (EI-ISAC), the Electricity Information & Analysis Center (E-ISAC)[a], the Faith-Based Information Sharing & Analysis Organization (FB-ISAO), and the Water Information Sharing & Analysis Center (WaterISAC), have published this White Paper, highlighting threats to elections infrastructure in the lead up to the November General Election. This paper discusses threats from the cyber, physical, and hybrid perspectives and includes recommendations for election offices and associated parties to implement to improve their preparedness.

Key Findings

- A wide array of cyber threat actors (CTAs) are likely to target election offices, election officials, and voters using opportunistic and targeted campaigns as well as leverage emerging technologies, such as generative artificial intelligence (Generative AI), and developments in more common tactics like phishing.
    - Observed malicious campaigns included election-specific lures and the use of stolen election correspondence to increase the likelihood of success.
    - Ransomware attacks pose a threat to election offices, even if they are not the direct target of the attack.
- CTAs will increasingly aim to sell election-related information online leading up to the 2024 U.S. general election, taking advantage of the increased interest surrounding the election.
- Politically motivated hacktivists are highly likely to increase elections-focused targeting throughout the 2024 election cycle due to the hacktivism resurgence brought on by the Israel-Hamas and Russia-Ukraine wars.
- Election officials and poll workers are likely to be targeted with physical threats online and in-person. False narratives regarding elections infrastructure will likely influence and direct threat actors (TAs) to target the U.S. electoral system and companies facilitating elections. Supporters of these narratives may become motivated to take physical action.

[a] The E-ISAC would like to thank Areeza Rizvi, Elvin Ramirez, Taylor Oldaker, Joseph Januszewski, and the E-ISAC Physical Security Analysis Team for their contributions to this white paper.

Cyber-Specific Threats

The authoring agencies assess with high confidence that CTAs will focus their malicious cyber campaigns on election offices ahead of, during, and following the 2024 U.S. election cycle. CTAs often take advantage of heightened interest during election cycles to increase the likelihood of success in their attacks. These campaigns include ransomware attacks, Business Email Compromise (BEC), and data exfiltration, followed by extortion. CTAs can deploy malware or aim to disrupt critical election systems and processes as part of opportunistic and targeted campaigns. Furthermore, cyber attacks on sectors and industries unrelated to the election could result in second or third-order impacts on Election Infrastructure (EI), such as disruptions to EI connectivity due to a city network infected with ransomware or service disruptions following a cyber or physical attack against critical infrastructure.

Incidents reported to the EI-ISAC throughout 2024 continue to match patterns in member reporting observed during previous election cycles. Spam and phishing have historically led member reporting, with this trend continuing throughout 2024. Many of these reports involved generic malware campaigns (malspam) employing common themes, frequently sent to targets in all industries, including impersonation of known individuals or organizations and requests to open malicious documents. While these types of generic malspam may not specifically target election offices, they still pose a risk if end users interact with them and can lead to a network compromise or data theft. Scanning and reports of suspicious network activity are also frequently reported by members, both historically and throughout 2024. Suspicious traffic can include reports of attempted brute-force attacks or other reports of malicious IP addresses. Scanning activity often includes reports of known IP addresses that frequently scan networks. These can be automated programs, which researchers periodically use, or malicious actors seeking network vulnerabilities.

EI-ISAC member threat reporting aligns with reporting observed in other sectors and reflects how network and email-based attacks are among the most common methods leveraged by CTAs, both state-affiliated actors and cybercriminals, to access systems.

Evolutions in Phishing

Phishing tactics continue to evolve in response to new steps taken by network defenders. The authoring agencies have observed an increase in the use of thread hijacking, where CTAs steal legitimate correspondence from compromised accounts, and incorporate pieces of the conversation into emails to appear legitimate.

In September 2022, the MS- & EI-ISAC CTI team released SFAR-2022-4, as well as a blog post, detailing how Microsoft’s move to block macros in files from the internet by default caused CTAs to change their initial access techniques for malware delivery. Microsoft implemented this change because CTAs abused macros to gain access to their targets and deploy malware. In response, CTAs shifted to using OneNote files and other non-macro tactics. In Q1 2023, the EI-ISAC saw an increase in the use of OneNote file attachments, corresponding to open-source reports of attackers adapting their techniques in response to new security measures from Microsoft.

The example below shows the malicious OneNote file indicates it requires user interaction with an open “button” before the content can be seen clearly.

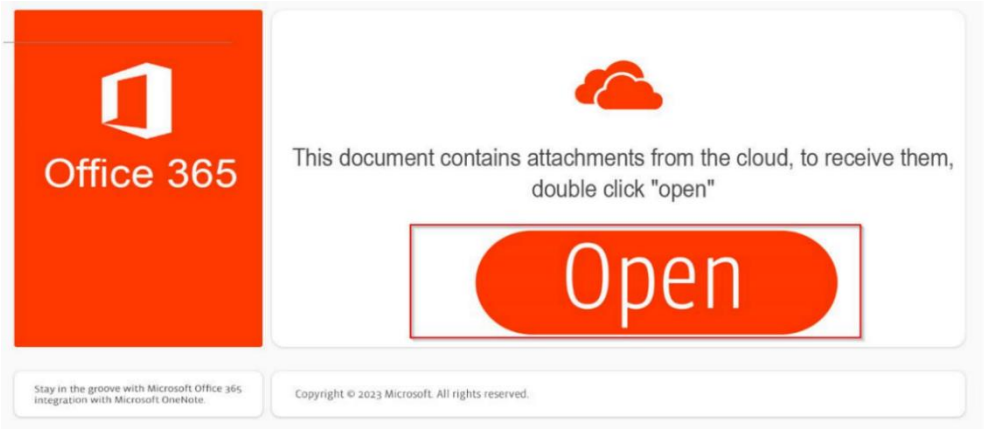

Figure 1 - Malicious OneNote file with "Open" button

This open “button” is a non-functional graphic covering a malicious script icon. Users are tricked into double-clicking and executing malicious scripts masked by this button. This example features a hidden malicious HTML application (HTA) file named “Open.hta.”

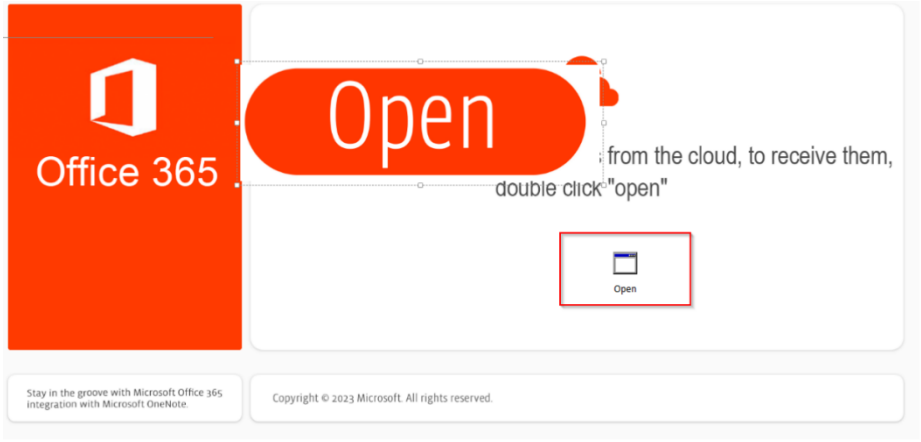

Figure 2 - Non-functional "Open" button moved to reveal a malicious HTA file, Open.hta.

Starting in Q4 2023, the MS- & EI-ISAC CTI team received reports of emails with Quick Response (QR) codes, also known as “quishing.” Quishing is a significant concern to election offices because it is an increasingly popular technique that combines social engineering with defense evasion. This technique was first reported to the EI-ISAC in October 2023 after an opportunistic CTA sent a quishing email to an election office employee’s enterprise email account. Quishing emails have been identified as initial stages of credential harvesting campaigns that used tactics often seen in other phishing campaigns, such as portraying a sense of urgency. Recipients of one email were directed to scan a QR code with their mobile device to “complete the due task,” which had a deadline of the next day (Figures 3 and 4). The attacker intended to evade defenses by transitioning user activity off secure systems and networks, where the email was opened and the QR code was displayed, and onto a potentially unsecured and unmonitored mobile device. This transition may increase the difficulty for defenders to prevent or detect attacks and potentially increases the likelihood of a successful attack.

Figure 3: A quishing email report to the EI-ISAC

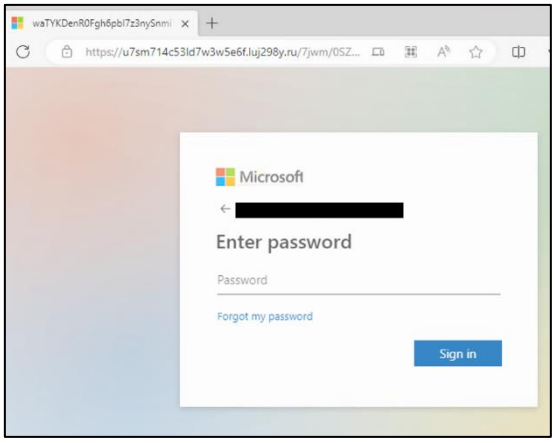

Figure 4: The spoofed login page from the quishing email

Criminal groups and state-sponsored CTAs continue to employ phishing in their malicious campaigns. A Microsoft report from August 2024, documenting activity by Iranian groups, noted that a group referred to as Mint Sandstorm used spear-phishing against a "high-ranking official of a presidential campaign."[1] Spear-phishing typically targets specific individuals or groups with customized messaging to increase a campaign's chances of success. Spear-phishing has been commonly employed by multiple state-sponsored affiliated groups and cybercriminals. In some cases, spear-phishing campaigns have also leveraged legitimate but compromised email addresses, which are often used to impersonate real people and to avoid raising suspicions. Following the establishment of rapport and trust, initially gained through a benign email (e.g., requests for input), CTAs deliver malicious content.[2]

Smishing, the use of SMS text messages as the phishing delivery method, is likely to increase in the lead up to the November 2024 election based on historical trends and CTAs taking advantage of increased interest in the elections process. Smishing is used to deploy malware, harvest information, and spread inaccurate electoral information. Previous election cycles have seen the use of election themes in smishing campaigns to increase the likelihood of success. In some cases, smishing campaigns are the result of organizations mistakenly sending inaccurate information to voters. In 2024 multiple text messages were sent to voters across a state that contained incorrect polling location, which was the result of an error and not malicious activity.[3]

Ransomware

Ransomware attacks continue to impact nearly all critical infrastructure sectors, including healthcare, emergency services, and government entities, such as municipalities and public education. The authoring agencies have not seen reports of ransomware groups claiming direct targeting election offices, however, ransomware attacks on local governments can still cause disruptions to election officials. For example, in 2024, the EI-ISAC received a ransomware incident report for a county that also affected the county clerk's office, where one of their roles is administering elections. Additionally, open-source reporting has noted some cases where ransomware attacks at the county level have led state-level departments to cut services to ensure the ransomware does not spread.[4]

There were 70 state, local, tribal, and territorial (SLTT) ransomware incidents reported to the MS-ISAC in Q2 2024, which is a 22.8% increase from the 57 reported incidents in Q1. LockBit continued to be the most prevalent ransomware variant for SLTTs in Q2 2024. LockBit uses the Ransomware-as-a-Service (RaaS) model, where recruited affiliates conduct ransomware attacks using LockBit's infrastructure and tooling.[5] LockBit ransomware attacks have also leveraged double extortion where the victim's data is exfiltrated prior to encryption. The LockBit group then threatens to post the data on a leak site unless the ransomware is paid, along with holding the decryption key for ransom. [6] The MS-ISAC also received substantial reporting in Q3 2024 of threats to SLTTs from the RansomHub, BlackSuit, Rhysida and LockBit ransomware groups.

Many of these groups have a history of targeting several sectors. The E-ISAC publishes weekly cybercrime and ransomware reports regarding risks impacting the energy sector, as well as monthly open source intelligence (OSINT) reports to include ransomware leak sites alongside current trends. In February of this year, a member notified the E-ISAC about a cybersecurity incident resulting from BlackCat (aka ALPHV) ransomware. Only the member's corporate environment was impacted by the incident, and they have since returned all business systems to operational status. The BlackCat ransomware group, one of the most prolific as of this paper's publication, is a RaaS group that allows freelance hackers, or affiliates, to join the ransomware group in a non-contractual agreement, allowing them to work within other RaaS groups simultaneously. Since November 2021, the group has historically exploited internet-facing applications via secure shell SSH or compromised user credentials to gain initial access of entities within critical infrastructure organizations, government, and other key infrastructure, predominantly within the U.S. In early 2024 the BlackCat group ceased its operations, though its affiliates are likely continuing to carry out other ransomware operations.

Data Theft

The authoring agencies assess with moderate confidence that CTAs will increase the frequency of online sales of election-related information leading up to the 2024 U.S. general election.[7] This data can include, but is not limited to: voter registration databases, election official and poll worker data, and campaign voter files. CTAs have previously taken advantage of the increased interest in elections to sell election-related information.

The authoring agencies have previously observed CTAs posting data that is legally available to individuals or organizations. Additionally, CTAs looking to improve their reputation, or increase their profit margin, have used already-leaked election data. We have observed a limited set of cases where the data posted online was sourced to a legitimate data leak. In some cases, this leaked data was traced to incidents that occurred months, or years, prior and was simply being recycled by CTAs seeking a financial gain.

In 2022, the EI-ISAC was informed about a series of online posts regarding a system misconfiguration that exposed sensitive election-related data. In this situation, the CTA stole data about poll workers and election officials in multiple U.S. states. To prove the data was legitimate, the CTA provided a small sample of the data that included personal information. The EI-ISAC did confirm the data leaked was legitimate and informed impacted members.

Hacktivist Activity

The authoring agencies assess with high confidence that politically motivated hacktivists are highly likely to increase efforts to leverage cyber tactics and Information Operations (IO) to undermine the 2024 U.S. presidential election. Hacktivist groups use cyber means to further "an ideological, social, or political cause," oftentimes "following high-profile political, socioeconomic, or world events."[8] Although hacktivist groups were historically rooted in anti-establishment ideologies and considered to have low capabilities, the onset of the Russia-Ukraine and Israel-Hamas wars have resulted in a hacktivism resurgence. This resurgence is marked by politically motivated hacktivists that are aligned to or supported by hostile foreign states involved in these conflicts. Targeting has expanded to include

not only organizations directly in opposition to specific sides of the conflict, but also loosely associated third parties.[9] According to Mandiant, hacktivists are also coupling traditional hacktivist activity with IOs to "maximize the real or perceived impact of attacks or gain attention to advance their agendas."[10] Other CTA groups, including those involved in state-sponsored and financially motivated activity, are also using hacktivist personas in attempts to obfuscate their activity and take advantage of geopolitical conflicts.[11, 12] Additionally, election seasons have historically coincided with surges in distributed denial of service (DDoS) attacks, which is a favored hacktivism tactic.[13]

"Faketivists" and State-Backed Hacktivists

"Faketivists" refer to state-sponsored or affiliated actors employing the guise of hacktivist groups or persona identities to operate with plausible deniability. Some state-sponsored groups also use hacktivist personas to publicize or claim responsibility for attacks, as a form of a post-intrusion influence operation IO.[14] This "blurring of the lines" between hacktivist and state-sponsored or affiliated CTAs is likely to continue, especially given the geopolitical backdrop of the Israel-Hamas and Russia-Ukraine wars.

Both Iran and Russia reportedly leverage hacktivist personas or groups as fronts for state-sponsored activities. For example, APT44 is a sophisticated CTA linked to "Unit 74455...within the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU)."[15] According to Mandiant, the group has "actively engaged in the full spectrum of espionage, attack, and influence operations," including attacks on "western electoral systems and institutions."[16] APT44 commonly leverages hacktivist personas, such as "Solntsepek," to "[amplify] the narrative of successful disruption" and "claim responsibility for and leak stolen information."[17]

Mandiant also assesses the operators of APT44 "have the ability to direct and influence" the activity of another hacktivist group known as Cyber Army of Russia Reborn (CARR).[18] CARR is a Russian hacktivist group that began launching DDoS attacks against targets in Ukraine and pro-Ukraine countries in late 2022. In late 2023, the group also began taking credit for attacks on industrial control systems (ICS) used by critical infrastructure operators in the U.S. and Europe. This included claiming responsibility for ICS compromises at two U.S. water facilities and a U.S. energy company's SCADA system in January 2024.[19] According to Mandiant, APT44-attributed infrastructure was used to create CARR's YouTube channel and to exfiltrate data from victims the group claimed credit for targeting in their Telegram channel.[20] This relationship demonstrates the "faketivist" phenomenon wherein state actors launder activities through hacktivist groups for obfuscation and amplification purposes.

A similar example is "CyberAv3ngers," a hacktivist group linked to Iran's Islamic Revolutionary Guard Corps (IRGC).[21] In November 2023, CyberAv3ngers began targeting Israeli-made programmable logic controllers used in U.S. Water and Wastewater systems (WWS). The group first gained initial access to victim WWS systems via compromised default credentials followed by anti-Israel defacement messages on victims' equipment claiming that any Israeli-made device is a target.[22] CyberAv3ngers' attacks also highlight an increasing trend wherein hacktivists target third parties allied against their declared organizational or governmental allegiances. In this case, the pro-Hamas and anti-Israel CyberAv3ngers targeted U.S. water facilities because of the U.S.'s allegiance to Israel. In addition, the Iranian government has leveraged the group to further its IO objectives. Microsoft reported that "after [the CyberAv3ngers] claimed cyberattacks against Israel's railway system [in September 2024], IRGC-linked media almost immediately amplified and exaggerated their claims."[23]

Hacktivist Tactics, Techniques, and Procedures (TTPs) - Denial of Service (DoS)

DDoS activity has historically increased during election seasons.[24] Several hacktivist groups have also already indicated their intent to attack elections during the 2024 cycle.[25] This includes "NoName57(16) crew," a pro-Russia hacktivist group that threatened in early June that it, along with several other hacktivist groups, intended to launch

attacks against European elections.[26] A social media account (Daily Dark Web) shared a post by the group that claimed the attacks would be in retaliation for the "Russophobia and double standards of European authorities."[27] "HackNet," which was one of the groups the NoName57(16) Crew listed in its threats, later claimed responsibility for DDoS attacks against Dutch political party websites on June 5-6, 2024.[28, 29] Other groups listed included CARR, KillNet, and Anonymous Russia.[30]

NoName57(16) Crew is also known for developing DDoSia, a crowdsourced botnet that launched in early 2022 and gained over 10,000 followers on Telegram. Cybercriminals that volunteer to participate in campaigns receive a .zip file with the DDoSia toolkit and are paid based on their contribution.[31] NoName57(16) Crew recently announced the DDoSia project is now aligned with CARR, stating that the merger aims to increase the effectiveness of their attacks and benefit from the combination of resources and knowledge. The announcement also stated that new targets of attack will include government and public institutions, in addition to large companies.[32]

NoName57(16) Crew and CARR also belong to the "Holy League" alliance, which was formed in 2024. According to the group's Telegram, the alliance was formed in accordance with goals related to "the destruction of the NATO alliance….and its partners from Ukraine, Israel, India, and the United States."[33] The coalition, which consists of over 70 pro-Kremlin, pro-Palestinian, and pro-Iranian groups, is the result of a merger of two coalitions, "The High Society" and "7 October Union."[34] The Holy League emerged in late July and joined in NoName57(16) Crew's call for a "holy war" against Spain following the arrest of three individuals associated with the group.[35,36] According to NetScout, from July 22-23, 2024 "at least a dozen hacktivist groups" conducted DDoS attacks on Spanish infrastructure, "attacking more than fourteen industries with a specific focus on Government and Transportation."[37]

It is important to note that hacktivists tend to exaggerate the actual impacts of their attacks.[38] The pro-Russia hacktivist group "Killnet," for example, has targeted multiple US government websites with DDoS attacks that had limited impacts on operations.[39]

Hacktivist TTPs - Website Defacements

Website defacements are the unauthorized modification of web pages, including the addition, removal, or alteration of existing content. Defacements of election websites can keep voters from accessing the information they need or cause reputational issues. CTAs could also use website defacements to change key information like voting times or places to spread inaccurate information. However, the EI-ISAC has not previously observed this type of defacement in practice.[40] In 2020, Iranian-affiliated CTAs accessed a local government's election reporting website. While the attack was disrupted before it could be carried out, the CTAs could have altered the website to post inaccurate results.[41]

Hacktivist TTPs - Hack and Leak Operations

Hack and leak operations refer to attacks in which CTAs gain unauthorized access to a system, exfiltrate sensitive information, and then leak the exfiltrated information with the aim of influencing target audiences.[42] For example, Resecurity, a cybersecurity company, reported in May 2024 that hacktivists targeted India's general election season with hack and leak campaigns. Resecurity observed multiple leaks on the dark web and Telegram of Indian citizens' personally identifiable information, including multiple leaks of Voter ID Cards. Although "the source of this data remains unclear," Resecurity assessed that "it may be linked to compromised third party entities" rather than from election systems.[43] However, CTAs could still use this leaked information "to generate a narrative that Indian election systems are insecure and vulnerable to cyberattacks."[44] A recent Public Service Announcement by CISA and FBI noted that "One of the most common tactics involves using obtained voter registration information as evidence to support false claims that a cyber operation compromised election infrastructure."[45]

In August, suspected Iranian CTAs targeted former President Donald Trump's campaign in a hack and leak operation that resulted in the release of what appeared to be the internal communications of a senior campaign official. On August 19th, the Director of National Intelligence (ODNI), FBI, and CISA confirmed the campaign was targeted and blamed Iran for the attack.[46]

Generative Artificial Intelligence

Cyber Threat Actors' Malicious Use

The authoring agencies have not received reports indicating that CTAs are leveraging Generative AI to conduct novel cyber attacks. Reporting indicates that CTAs are currently experimenting with Generative AI, and testing how to best incorporate this technology into their ongoing tactics, techniques, and procedures (TTPs). Many Generative AI platforms are publicly available at either low or no cost. This ease of access helps lower the barrier to entry for CTAs to leverage them.

CTAs are highly likely to increasingly leverage Generative AI platforms to aid in phishing email generation, malware development, and financial crimes. Generative AI platforms can enable the creation of phishing emails that lack typical hallmarks, like spelling and grammatical errors, and generate a convincing storyline with little effort from the CTA. Following the launch of ChatGPT, according to SlashNext Threat Labs Intelligence, there was a 1,265% increase in phishing email activity from Q4 2022 to Q3 2023. The increase in phishing activity suggests CTAs are likely exploiting Generative AI platforms for criminal phishing activities.[47, 48] Additionally, although Generative AI is not yet proficient at producing fully functioning malware, it can assist CTAs with debugging code and lowers the barrier of entry for less sophisticated actors seeking to introduce malware into their criminal activities.[49, 50]

The Office of the Director of National Intelligence (ODNI)'s 2024 Annual Threat Assessment noted that "Russia's influence actors have adapted their efforts to better hide their hand, and may use new technologies, such as generative AI" to improve their capabilities.[51] Similarly, the report noted that China was "experimenting" with Generative AI as it seeks to improve its influence campaigns.[52] A Microsoft report had similar findings, noting that "cybercrime groups, state-sponsored threat actors, and other adversaries are exploring and testing different AI technologies as they emerge."[53] The report explored how specific CTAs were employing Generative AI, and found some common themes included help with reconnaissance, coding, and learning other languages.[54] Additionally, OpenAI disrupted five IOs in May, including online campaigns run by Russian, Chinese, Iranian, and Israeli actors, whose operators leveraged OpenAI's platforms to generate or translate longform, articles, debug code, generate social media comments, create website tags and headlines, and research current events.[55]

On September 23rd, the ODNI released an election security update stating foreign actors, including Russia, Iran, and China are leveraging GenAI to "boost" election IO efforts.[56, 57] The update states Generative AI "is helping to improve and accelerate aspects of foreign influence operations but thus far the IC [intelligence community] has not seen it revolutionize such operations."[58] The report noted that GenAI election risks emanating from hostile foreign actors is dependent on the hostile foreign state's ability to successfully circumvent AI platform restrictions, remain undetected, and develop independent sophisticated models to strategically target and disseminate content. ODNI specifically noted that Russia has created the most content generated by AI targeting the upcoming U.S. election, including text, images, audio, and video, while Iran is leveraging AI to create content for both social media posts as well as to populate websites that claim to be legitimate media sources.[59] The report also noted China, while not focusing on specific election outcome, is using AI to promote and influence global opinions that are in alignment with China's geopolitical goals as well as to amplify divisive U.S. political issues.[60]

Voice Cloning

Artificial intelligence platforms create voice clones by dissecting patterns of speech from audio clips to create copies of someone's voice.[61] These AI platforms are often built on large language models (LLMs) and based on datasets of real voices.[62] These datasets are used alongside uploaded audio clips to train the AI to recognize and synthesize components of someone's speech, including elements like intonation and accents. An end user then provides a script for the voice clone either by typing it into a prompt (text-to-speech) or verbally submitting it through an audio recording (speech-to-speech).[63]

This lower barrier to entry is attractive for those using voice clones for legitimate or malicious purposes. Malicious actors can abuse these platforms for authentication in banking fraud attempts, malign influence campaigns, music and copyright infringement, family emergency scams, executive impersonation, and callback scams.[64]

On January 21, 2024, a robocall impersonating President Biden's voice was used as part of a voter suppression effort ahead of the New Hampshire primaries. According to the New Hampshire Office of the Attorney General, the call "directly encouraged recipients" to not vote.[65] A former consultant for a political campaign admitted to commissioning the voice clone and claims that he did so to demonstrate the dangers of AI.[66] The incident demonstrates how malicious actors may leverage these tools in the 2024 U.S. election cycle and continue to abuse them despite the implementation of security measures.

Threats to Voting Infrastructure

Consistent with narratives observed during the 2022 U.S. midterm elections, inaccurate information surrounding voting machines has originated primarily from U.S. domestic sources on alternative media websites and social media platforms. However, motivated CTAs, particularly foreign state adversaries, may attempt to exploit legitimate voting system vulnerabilities in attempts to impact election outcomes or delegitimize the democratic process.

To compromise election infrastructure, hostile foreign state adversaries may leverage a variety of tactics in attempts to compromise election infrastructure. For example, reports allege that in 2016 Russia's GRU targeted an election technology vendor with a spear phishing campaign to compromise employee credentials.[67] Although the vendor denied that CTAs were successful, the NSA stated "'It is unknown whether the aforementioned spear-phishing deployment successfully compromised all the intended victims,… However, based on subsequent targeting, it was likely that at least one account was compromised.'"[68] Posing as the vendors employees, CTAs then targeted 122 election officials nationwide with malicious documents. Several months later an official encountered technical difficulties while updating poll books to flash drives, resulting in the same election technology vendor remotely accessing the software to troubleshoot. On election day, "some crashed or froze. Others indicated that voters had already voted when they hadn't. Others displayed an alert saying voters had to show ID before they could vote" resulting in state officials ordering the use of paper voter lists for check-in.[69] Although the cause of the technical issue associated with the pollbooks remain unclear, suspicions of the GRU's involvement persist due to the previous targeting of both the election technology vendor and that vendor's election clients. Although targeting pollbooks would not grant a CTA the opportunity to adjust voting results, it could result in a disruption to the voting process, and be used by malicious actors to spread doubts about the electoral process.[70]

Cellular modems used for voting machines are under increasing scrutiny. Modems transmit voting data in real time from precincts to central offices using cellphone networks. However, officials recognize that the transference of data creates vulnerabilities and provides an attack landscape, particularly if a nation-state or an individual CTA specifically targeted infrastructure systems.[71] Currently, there is no indication that modems have been attacked in previous elections.

Information Operations (IOs)

IOs are increasingly leveraged by TAs, often adversarial state-sponsored groups, seeking to manipulate, instill fear, sow discord and division, undermine the U.S. election process, and confuse voters.[72] IOs include leveraging inauthentic of fraudulent news outlets and online personas impersonating members of a targeted community to disseminate messaging in alignment with each nation's objectives.[73, 74]

Many IOs are incorporating AI, appearing authentic and increasing the speed and spread of content creation.[75] TAs are more effectively using native languages, including colloquial usage, effectively blending in with their targets while exploiting divisive topics that are most likely to elicit a desired reaction. Malign operations can swiftly exploit current events. This is integral to IOs because it captures the audience's attention, particularly surrounding divisive topics, and grants adversaries a greater opportunity to ensure targeted messaging is disseminated amongst a wider audience.

TTPs Consistent with IOs include the following:

- **Account takeover:** TAs combine hacking and IO to compromise legitimate accounts and websites, which are then used to disseminate inauthentic content in alignment with targeted influence operations.[76]
- **Encrypted messaging apps (EMAs):** Malicious actors use EMAs, such as WhatsApp, to target diaspora communities, who often perceive EMAs as trustworthy.[77]
- **Information laundering:** To lend credibility to IOs, information or narratives are laundered to lend credibility to misleading or inauthentic media. Narrative laundering methods include posting content to proxy networks including websites, individuals, social media accounts, and organizations appearing to be independent news sources.[78]
- **Impersonation of a targeted group:** Impersonating a group to leverage their reputation to advance IO and cyber-related narratives. For example, Iranian state-sponsored CTAs deployed operation "Tears of War," which impersonated Israeli activists to spread anti-Netanyahu messaging, on various social media and messaging platforms, reportedly resulting in legitimate Israeli activists hanging branded "Tears of War" banners in Israeli neighborhoods.[79]
- **Partisan narratives hijacked:** IOs leverage legitimate partisan narratives in deceptive campaigns which may assist in driving traffic, building a user base and trust amongst users, and to promote messaging supportive of specific goals. According to Meta, TA activity from China and Iran implement "copypasta" techniques, or the verbatim usage of legitimate posts authored by real people, including influential political figures.[80]
- **Plagiarism and manipulation of news articles:** Altering legitimate news articles to fabricate content or misrepresent information. Websites mimicking legitimate news outlets may also be created to lend credibility to manufactured narratives.[81]
- **Short-form video content:** Short-form video content (TikTok, Instagram Reels, YouTube Shorts, etc.) is used as a means of disseminating false or misleading information and narratives regarding volatile subjects, often meant to elicit emotional responses, including anger and fear.[82]

State-Sponsored IOs

A July 2024 ODNI report titled "100 Days Until Election 2024," outlined how hostile foreign state governments are continuing to leverage state-sponsored groups and affiliates to deploy IOs and malign cyber activity targeting the U.S. and allies. Their motivations include sowing social discord and civil unrest, encouraging violence, influencing economic interests, eroding public support for U.S. allies (i.e. Israel and Ukraine), undermining confidence in trusted

democratic U.S. processes, and influencing voters to further a nation's strategic geopolitical goals, or to distract from ongoing domestic and international tensions or conflicts.[83] IOs, such as those from Russia and Iran, frequently leverage cyber-enabled tactics, or those blending traditional malicious cyber methods alongside IOs and social engineering.

The ODNI report specifically mentioned Russia, China and Iran. While Russia "remains the predominate threat to U.S. elections" Iran has continued efforts to "fuel distrust in U.S political instructions and increase social discord." The report also noted that China "probably does not plan to influence the outcome of the US presidential election" but did not rule out the possibility of future action.[84]

TTPs mentioned in the report included the use of commercial firms, such as marketing and public relations companies, as well as organic user engagement where "witting and unwitting Americans to seed, promote, and add credibility to narratives that serve the foreign actors' interests."

Recent IO Activity

In early September, researchers at the Foundation for Defense of Democracies exposed a network of 19 covert Iranian websites, several of which targeted U.S. audiences, including specific communities and groups.[85] Microsoft and OpenAI previously attributed five of the sites in the network to Iran.[86] The sites receive limited web traffic and have not generated significant engagement on social media.

On September 4th, the U.S. Department of Justice (DOJ) announced the seizure of 32 internet domains operated by the Russian government in violation of U.S. money laundering and criminal trademark laws.[87] According to the DOJ, the domains were a component of an ongoing Russian state-sponsored IO, commonly known as "Doppelganger," targeting the U.S., and other countries, in an effort to influence U.S. public opinion and the outcome of the 2024 U.S. presidential election. Doppelganger focused on exploiting current events, developing false or misleading narratives, creating inauthentic online personas, using influencers to disseminate narratives, impersonating legitimate and trusted news sources and journalists, and creating inauthentic media organizations intended to appear to be operated by Americans.

On August 19th, the ODNI, FBI, and CISA released a joint statement regarding the Iranian government's continued efforts to influence the 2024 U.S. election cycle leveraging cyber operations.[88] The joint statement indicated Iran is seeking to sow discord and undermine confidence in the U.S. election cycle, as well as stating Iran has demonstrated a continued and "longstanding" interest in exploiting U.S. social tensions, including through the use of cyber operations to gain access to and exploit sensitive election related information. Additionally, the ODNI, FBI, and CISA stated "Iran perceives this year's elections to be particularly consequential in terms of the impact they could have on its national security interests, increasing Tehran's inclination to try to shape the outcome." The report also noted increasingly aggressive Iranian activity, including targeting presidential campaigns.

On August 16, 2024, OpenAI issued a report detailing an Iranian IO's use of ChatGPT. The CTA, referred to as "Storm-203,5" created content related to U.S. presidential candidates, politics, and global events which was shared on social media as well as websites posing as news outlets.[89] OpenAI identified a dozen inauthentic accounts on X and one on Instagram, none of which attained "meaningful levels of engagement."

Physical Election Threats

Supported by both historical and current reports, the authoring agencies assess with high confidence that prior to, and possibly following, the 2024 election, election officials, poll workers, candidates, and other high profile individuals nationwide will be increasingly targeted with threats online and in-person.[90, 91, 92] Additionally, online rhetoric is likely to influence CTAs to target the U.S., and private companies supporting the election process.

Potential targets of physical attacks include voter registration and election offices in-person voting locations, vote counting centers, ballot tabulators, drop boxes, and U.S. Postal Services facilities, including mailboxes. Motivations to take physical action range from acts of violence to physical actions supporting cyberattacks (e.g., inserting flash drives into computers). Previously observed physical attacks have included a fire set in a ballot drop box, and the physical harassment of election workers.

A Department of Homeland Security (DHS) National Terrorism Advisory Summary released in May 2023 noted that "factors that could mobilize individuals to commit violence include their perceptions of the 2024 U.S. general election cycle and legislative or judicial decisions pertaining to sociopolitical issues."[93]

Election Officials, Candidates, and Other Influential Individuals

These threats can potentially intimidate, escalate to physical harm, disrupt events, discourage individuals from joining election efforts, and influence current officials to resign.[94] A 2024 Brennan Center survey found that "38 percent of local election officials report experiencing threats, harassment, or abuse," and 54% were concerned about their colleague's safety in future elections.[95] False or misleading narratives spread online frequently directs the targeting of these threats. Tactics used to target individuals associated with U.S. election processes include doxing, swatting, and harassment. Locations where large gatherings are expected could also become targets.

TAs also leverage doxing (the publishing of private information about an individual) to harass election officials. A recent example of doxing occurred in early July, when an individual harassed and took videos of election workers, later posting the video on YouTube and doxing some of the staff's personal information. ABC News reported that local officials indicated the video "resulted in 'dozens of calls and emails' to election workers."[96]

Swatting and Bomb Threats

Based on recent trends in targeting, there is a high likelihood that swatting will continue to be used before, during, and after the 2024 election cycle to target political figures of both parties, election officials, and others associated with the electoral process. Swatting creates both highly dangerous situations as well as creating a pervasive atmosphere of intimidation. Since 2021, the FBI has reviewed 2,000 incidents of election worker harassment or threats.[97]

Some recent examples of individuals being targeted with swatting include:

- In January 2024, a Secretary of State was the victim of a swatting incident and additional incidents targeting election officials have been reported in other states.[98]
- In December 2023, the director of the Cybersecurity and Infrastructure Security Agency (CISA), Jen Easterly, was the target of a swatting incident, followed by additional swatting calls to public officials and judges across the U.S., including White House officials.[99]
- Public officials were swatted in August 2024, including a Secretary of State, who revealed on August 12th via X that they were swatted twice in 48 hours.[100] This followed reports of swatting incidents targeting current and former U.S. House Representatives on August 8th and August 9th.[101, 102]

Swatting and bomb threats have been leveraged to target government and community institutions, including hospitals, schools, and religious organizations. In October 2023, reports revealed more than 500 schools were targeted in active shooter hoax calls over the previous year.[103] In December 2023, the FBI reported that more than 200 synagogues and Jewish schools were targeted in one week, which were all traced to foreign actors.[104] Additionally, multiple state capitol buildings, courthouses, and other government facilities were sent hoax bomb threats on January 3rd and 4th 2024, resulting in disruptions in at least 12 states.[105, 106, 107, 108, 109, 110] Multiple delegate

hotels were also sent bomb threats during the 2024 Democratic National Convention, which took place between August 19-22.[111]

Coordinated swatting exhausts law enforcement resources and prompts unnecessary evacuations. To identify targets, malicious actors often use social engineering techniques to extract information, such as doxing, phishing, and social media research. The motives behind incidents vary but are likely intended to instill fear, panic, disrupt services, and inflict financial costs.[112]

Suspicious Powder Incidents

TAs are highly likely to continue sending letters containing suspicious powders to election officials, offices, or ballot counting centers in the lead up to, during, and after the November general election. Suspicious powder incidents involve both legitimate threats with hazardous material (fentanyl, ricin, etc.) or hoaxes with non-hazardous powder.[113]

In November 2023 suspicious letters, some laced with fentanyl, were sent to election officials in multiple states. One of the letters read "End elections now."[114] On September 17, 2024, secretaries of state, attorney general offices and state election offices in several states were sent threatening letters containing suspicious substances.[115] There have been no reports that any of the targets received hazardous materials, indicating the threat actor's intent was likely to cause panic and disrupt operations.[116] The FBI and the U.S. Postal Inspection Services are currently investigating the incidents.[117]

Impersonation of Election Offices, Vendors, and Organizations

The authoring agencies identified the risk of TAs impersonating election offices and vendors on social media as well as in person. TAs attempting to impersonate election offices will likely leverage social engineering efforts, such as emulating known and trusted entities, in an attempt deceive targeted organizations into providing sensitive information. One county reported an incident where a county resident with a legal voter registration was visited by two women claiming to come from a separate county's election office. The individuals carried ID cards and left the woman with an election complaint form.[118] The EI-ISAC received a report in September 2024 of an email sent to a local election office attempting to impersonate a national election organization.

Voter Intimidation and Roll Controversies

In 2020 and 2022, TAs targeted voters, a trend anticipated to continue with moderate confidence during the 2024 election cycle. For the 2020 and 2022 election cycles, the authoring agencies observed increased conspiratorial rhetoric regarding early voting and voting results, which appeared to influence in-person activity, such as targeting voters and unarmed and armed drop box monitoring.[119] Voters in minority communities have been specifically referenced in narratives and targeted with online and in-person activities.[120, 121]

Voters, voting rights, or similar groups accused of engaging in election fraud activities are expected to, with high confidence, be targeted through intimidation efforts, harassment, and doxing. TAs have previously shared images and videos of those purportedly involved in ballot trafficking or harvesting ("ballot mules") online and encouraged followers to uncover the individual's identity. Ballot harvesting refers to the collection and submission of completed ballots to a ballot collection site, which conspiracy theorists often believe have been stolen or are fraudulent ballots.

Other Threats and Targets

Domestic Violent Extremists (DVEs)

According to the DHS 2024 Homeland Threat Assessment, "Some DVEs, particularly those motivated by conspiracy theories and anti-government or partisan grievances, may seek to disrupt electoral processes. Violence or threats could target government officials, voters, and elections-related personnel and infrastructure, including polling places, ballot drop box locations, voter registration sites, campaign events, political party offices, and vote counting sites."[122] Moreover, DVEs from across the ideological spectrum are likely to view a wide range of entities directly and indirectly associated with elections as viable targets for violence. For instance, following the recent assassination attempt of former President Trump, DVEs called for violence against perceived ideological opponents.[123]

Critical Infrastructure

DVEs will likely continue to promote attacks on critical infrastructure with the intent to cause disruptions to the election process and incite panic.[124,125] The authoring agencies have observed social media chatter encouraging the destruction of electricity assets to disrupt upcoming elections. Examples often mention using firearms to shoot and destroy substation transformers.[126] Other threats include the promotion of attacking the electricity sector as a viable alternative to voting to enact change. Social media users have also been observed disparaging voting while providing links to multiple extremist publications that advocate and provide instructions for carrying out attacks against the electricity sector.[127] While electric substations are the primary target, maps of infrastructure locations including telecommunications hubs, water treatment plants, and natural gas pipelines are available online, providing DVEs with additional target opportunities.[128, 129]

Additionally, periods of civil unrest corresponding to the upcoming election could also serve as flashpoints for violent opportunists to commit acts of vandalism against utility personnel or assets. This also includes potential increased risk of communication infrastructure being targeted, specifically the targeting of fiber optic cabling, which can lead to the disruption of communications between critical equipment components. Beginning in May 2024, the E-ISAC observed a notable uptick in the number of incidents involving damage to fiber optic cabling based on historical trends since 2022. Cutting fiber optic cabling can disrupt communications between critical components that drive primary operations in electrical assets, which in some cases can cause generator unavailability until communication has been restored. This is a concerning tactic, and E-ISAC analysts are closely monitoring as it can result in kinetic impacts (such as generator unavailability or loss of service to customers) or network disruptions which can in turn impact IT/OT systems.

No matter the election outcome, the WaterISAC assesses individuals from across the ideological spectrum could be motivated to violence based on their perceptions of the election.[130] Consequently, there is potential for civil unrest and political violence in the lead-up to and after the U.S. elections. Critical infrastructure entities could be affected by civil unrest and incidents of significant violence in their communities, with potential impacts to their facilities, operations, and personnel. Government buildings, including courthouses and administrative facilities, have been the focus of, or near, large demonstrations and civil unrest. Infrastructure organizations have offices and personnel in these buildings which may be affected by these activities

Post-Election Threat Landscape

The post-election threat landscape is likely to result in challenges to several sectors, including election infrastructure. The following represents the most significant and high-priority threats that EI should be prepared for:

- Domestic unrest and political violence resulting from anticipated increases in heightened political polarization, with demonstrations – both peaceful and violent – likely to occur, particularly in contested or politically charged regions.
    - Extremist group activities may become more active after the election. These groups could target government buildings, public infrastructure, or elections, among others. In some cases, these groups may coordinate physical and cyberattacks to cause greater disruption, requiring impacted entities to be prepared for a variety of scenarios.
- Cyberattacks on critical infrastructure remain a constant threat, with both state-sponsored actors and organized criminal groups targeting critical, including, but not limited to, elections.
- The information operations post-election environment is expected to see a surge in malign campaigns, with both foreign and domestic actors seeking to sow confusion and distrust.

Recommendations

The recommendations below are applicable to all SLTTs and provide an overview of best practices organizations can take against a wide variety of threats.

- Review CISA's #Protect2024 page for a list of resources and information relevant to election offices.
- Review the CIS Critical Security Controls for recommendations on how to improve your organization's cyber security posture.
- Create, maintain, and exercise a basic cyber incident response plan and associated communications plan including response and notification procedures.

Phishing

- Conduct regular end-user awareness and social engineering training exercises. Awareness of social engineering techniques, including quishing, is the strongest protective measure available and is most likely to prevent attacks from succeeding.
    - For more information, see CIS Control 14 and the CISA guide on Avoiding Social Engineer and Phishing Attacks.
- Only visit trusted websites from expected emails and text messages.
    - Do not scan unexpected QR codes or click unexpected hyperlinks.
    - Verify the sender of the message prior to scanning QR codes and visiting hyperlinks. If an unexpected message is received, verify with the sender through another medium. Malicious QR codes have been observed coming from compromised email accounts (example in Figure 3).
    - Verify the URL prior to visiting websites. Smartphones may display the decoded URL and require user interaction prior to visiting websites. Shortened URLs may be encoded by QR codes and can be expanded using free, publicly available online tools.

Data Leaks

- Report suspected data posts/breaches to internal organization contacts and the EI-ISAC.
- Develop a response plan for data breaches impacting your office.
  - This plan should include notifying impacted individuals and responding to public inquiries.
  - Review the CISA elections security toolkit website: https://www.cisa.gov/cybersecurity-toolkit-and-resources-protect-elections
- Perform an audit of where information is stored.
  - Reference CIS Control 3 (Data Protection) for processes and technical controls to identify, classify, securely handle, retain, and dispose of data.
- Keep a record of data released in previous data leaks.
  - These records will be important if you are alerted to data posted online about your office by outside entities (EI-ISAC, media organizations, etc.).

DDoS

- Establish and maintain effective partnerships with your upstream network service provider and establish what assistance they can provide you in the event of a DoS incident.
  - Some companies offer free DDoS mitigation services to election offices.
- Establish and regularly validate public-facing websites' baseline traffic patterns for volume and type.
- Review incident response and business continuity plans to ensure DoS incidents are covered, and educate staff on procedures for responding to a DoS incident.
- Refer to the MS-ISAC Guide to DDoS Attacks, the CISA No Downtime in Elections: A Guide to Mitigating Risks of Denial-of-Service, and the joint MS-ISAC, FBI & CISA Understanding and Responding to Distributed Denial of Service Attacks guides for more information on DDoS incidents and potential mitigations.
- The E-ISAC recommends members evaluate the use of geoblocking and/or a trusted dynamic list to help prevent similar adversarial activity, as affected members have historically reported successfully utilizing these methods to block most of the attempts.

Influence Operations

- Maintain situational awareness regarding IOs targeting elections infrastructure and elections more broadly.

Physical Threats[131]

- Maintain situational awareness regarding individuals and groups that might seek opportunities to target elections offices, elections employees, elections infrastructure, polling locations, etc.
- Implement procedures and policies for securing key locations including:
  - Exteriors to protect against intrusion.

- Implement access controls to ensure only individuals requiring access to sensitive areas are able to gain access.

- Develop and implement an incident response plan, including an election continuity plan in the event of disruptions.
  - Incident response should include procedures for handling suspicious mail and swatting/bomb threats.
  - Continuity plans should include responses to cyber or physical attacks targeting sectors that could impact election infrastructure, such as an attack targeting telecom or energy, which could result in confusion or panic amongst voters.
- Create or enhance redundancy (e.g., diverse fiber paths, a ring which can go either way, etc.), or implement a backup method of communication (e.g., cellular communication).

Influence Operations[132]

- Maintain situational awareness regarding IOs targeting elections infrastructure and elections more broadly.
- Establish or leverage communications to inform constituents, or any other relevant parties, and to provide necessary information regarding IOs. Establishing or maintaining effective communications may also enhance both security and public confidence in trusted organizations or entities.
  - Develop an incident response plan to combat possible impacts of an IO, which should include dissemination of information to constituents and other relevant parties.
  - Communications may include leveraging organizational websites, social media, public statements, press releases/media inquiries, among others.

MS-ISAC®
EI-ISAC®

Multi-State Information Sharing and Analysis Center (MS-ISAC)
Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722

Supported via cooperative agreement No. 23CISMSI00003-01-01 - 09/29/2025 awarded through the Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security (U.S. DHS). The analysis, findings, and conclusions or recommendations expressed in this document are those of the MS-ISAC & EI-ISAC.

References

[1] https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/5bc57431-a7a9-49ad-944d-b93b7d35d0fc.pdf
[2] https://www.microsoft.com/en-us/security/blog/2024/01/17/new-ttps-observed-in-mint-sandstorm-campaign-targeting-high-profile-individuals-at-universities-and-research-orgs/
[3] https://spectrumlocalnews.com/nys/central-ny/politics/2024/06/24/new-york-text-message-scam-election-polling-locations
[4] https://www.cnn.com/2024/04/26/politics/georgia-coffee-county-cyberattack-voter-system/index.html
[5] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a
[6] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a
[7] For more information, see the EI-ISAC's Short Form Analytic Report (SFAR) 2023-02: Cyber Threat Actors Selling Election Data Online Likely to Increase Leading up to the 2024 General Election – TLP:AMBER
[8] https://www.ic3.gov/Media/News/2022/221104.pdf
[9] https://cloud.google.com/blog/topics/threat-intelligence/global-revival-of-hacktivism
[10] https://cloud.google.com/blog/topics/threat-intelligence/global-revival-of-hacktivism
[11] https://cloud.google.com/blog/topics/threat-intelligence/global-revival-of-hacktivism
[12] https://www.infosecurity-magazine.com/news/hacktivism-financial-gain-threat/
[13] https://cloud.google.com/blog/products/identity-security/ddos-attack-trends-during-us-midterm-elections
[14] https://www.darkreading.com/cyberattacks-data-breaches/gaza-conflict-enters-third-month-how-involved-are-nation-state-attackers
[15] https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf
[16] https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf
[17] https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf
[18] https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf
[19] https://home.treasury.gov/news/press-releases/jy2473
[20] https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf
[21] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a
[22] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a
[23] https://blogs.microsoft.com/on-the-issues/2024/02/06/iran-accelerates-cyber-ops-against-israel/
[24] https://cloud.google.com/blog/products/identity-security/ddos-attack-trends-during-us-midterm-elections
[25] https://cloud.google.com/blog/products/identity-security/ddos-attack-trends-during-us-midterm-elections
[26] https://www.theregister.com/2024/06/07/russian_hacktivists_eu_elections/
[27] https://dailydarkweb.net/russian-hacker-group-noname057-announces-cyberattack-on-european-internet-infrastructure/
[28] https://www.theregister.com/2024/06/07/russian_hacktivists_eu_elections/
[29] https://www.bleepingcomputer.com/news/security/ddos-attacks-target-eu-political-parties-as-elections-begin/
[30] https://www.theregister.com/2024/06/07/russian_hacktivists_eu_elections/
[31] https://therecord.media/ddosia-pro-russian-hackers-upgrades
[32] https://t[.]me/noname05716
[33] https://t[.]me/h0lyleague/229
[34] https://cybernews.com/cybercrime/holy-league-hacker-alliance-attack-nato/
[35] https://www.netscout.com/blog/asert/ddos-attacks-spain
[36] https://cybernews.com/cybercrime/holy-league-hacker-alliance-attack-nato/
[37] https://www.netscout.com/blog/asert/ddos-attacks-spain
[38] https://www.infosecurity-magazine.com/news/hacktivism-financial-gain-threat/
[39] https://flashpoint.io/intelligence-101/killnet/#:~:text=Killnet%20seeks%20support%20from%20the,the%20pro%2DKremlin%20Russian%20media.
[40] https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-website-defacements
[41] https://www.washingtonpost.com/technology/2023/04/24/election-2020-iran-hacking/
[42] https://cloud.google.com/blog/topics/threat-intelligence/global-revival-of-hacktivism
[43] https://www.resecurity.com/blog/article/cybercriminals-are-targeting-elections-in-india-with-influence-campaigns
[44] https://www.resecurity.com/blog/article/cybercriminals-are-targeting-elections-in-india-with-influence-campaigns
[45] https://www.cisa.gov/sites/default/files/2024-09/PSA_Just_So_You_Know_False_Claims_of_Hacking_Voter_Reg_CISA_and_FBI-508.pdf
[46] https://www.cisa.gov/news-events/news/joint-odni-fbi-and-cisa-statement-iranian-election-influence-efforts

[47] https://learn.cisecurity.org/examination-of-how-cyber-threat-actors-can-leverage-generative-ai-platforms
[48] https://slashnext.com/wp-content/uploads/2023/10/SlashNext-The-State-of-Phishing-Report-2023.pdf
[49] https://www.techtarget.com/searchsecurity/news/365531559/How-hackers-can-abuse-ChatGPT-to-create-malware
[50] https://www.trendmicro.com/en_us/research/23/k/a-closer-look-at-chatgpt-s-role-in-automated-malware-creation.html
[51] https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf
[52] https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf
[53] https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai
[54] https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai
[55] https://openai.com/index/disrupting-deceptive-uses-of-AI-by-covert-influence-operations/
[56] https://www.dni.gov/index.php/fmic-news/3998-election-security-update-20240923
[57] https://www.dni.gov/files/FMIC/documents/ODNI-Election-Security-Update-20240923.pdf
[58] https://www.dni.gov/files/FMIC/documents/ODNI-Election-Security-Update-20240923.pdf
[59] https://www.dni.gov/files/FMIC/documents/ODNI-Election-Security-Update-20240923.pdf
[60] https://www.dni.gov/files/FMIC/documents/ODNI-Election-Security-Update-20240923.pdf
[61] https://elevenlabs.io/voice-cloning
[62] https://cybernews.com/privacy/ftc-voice-cloning-challenge-ai-fraud/
[63] https://www.scientificamerican.com/article/ai-audio-deepfakes-are-quickly-outpacing-detection/
[64] https://go.recordedfuture.com/hubfs/reports/cta-2023-0518.pdf
[65] https://www.doj.nh.gov/news/2024/20240206-voter-robocall-update.html
[66] https://www.nbcnews.com/politics/2024-election/democratic-operative-admits-commissioning-fake-biden-robocall-used-ai-rcna140402
[67] https://www.politico.com/story/2019/06/05/vr-systems-russian-hackers-2016-1505582
[68] https://vox.com/new-money/2017/6/6/15745888/russia-election-hacking-leak
[69] https://www.politico.com/news/magazine/2019/12/26/did-russia-really-hack-2016-election-088171
[70] https://apnews.com/article/arizona-united-states-government-2022-midterm-elections-donald-trump-los-angeles-651d0e923973daf28ff3b9d6105b4d74
[71] https://www.politico.com/news/2022/10/14/wireless-modems-could-endanger-midterms-00061769
[72] https://blogs.microsoft.com/on-the-issues/2024/09/17/russian-election-interference-efforts-focus-on-the-harris-walz-campaign/
[73] https://blogs.microsoft.com/on-the-issues/2024/08/08/iran-targeting-2024-us-election/
[74] https://blogs.microsoft.com/on-the-issues/2024/09/17/russian-election-interference-efforts-focus-on-the-harris-walz-campaign/
[75] https://www.dhs.gov/sites/default/files/2023-09/23_0913_ia_23-333-ia_u_homeland-threat-assessment-2024_508C_V6_13Sep23.pdf
[76] Meta's threat disruptions | Transparency Center (fb.com)
[77] https://www.brookings.edu/articles/the-disinformation-threat-to-diaspora-communities-in-encrypted-chat-apps/
[78] https://www.state.gov/the-kremlins-efforts-to-covertly-spread-disinformation-in-latin-america/
[79] Ihttps://www.microsoft.com/en-us/security/business/security-insider/reports/iran-surges-cyber-enabled-influence-operations-in-support-of-hamas/
[80] Meta's threat disruptions | Transparency Center (fb.com)
[81] https://www.justice.gov/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence
[82] https://www.isdglobal.org/digital_dispatches/election-disinformation-thrives-following-social-media-platforms-shift-to-short-form-video-content/
[83] https://www.odni.gov/files/FMIC/documents/ODNI-Election-Security-Update-20240729.pdf
[84] https://www.odni.gov/files/FMIC/documents/ODNI-Election-Security-Update-20240729.pdff
[85] https://www.fdd.org/analysis/2024/09/05/fdd-identifies-19-websites-as-part-of-an-iranian-global-influence-operation/
[86] https://openai.com/index/disrupting-a-covert-iranian-influence-operation/
[87] https://www.justice.gov/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence
[88] https://www.fbi.gov/news/press-releases/joint-odni-fbi-and-cisa-statement-on-iranian-election-influence-efforts
[89] https://openai.com/index/disrupting-a-covert-iranian-influence-operation/

[90] https://www.cnn.com/2023/12/30/politics/maine-secretary-of-state-bellows-swatted/index.htmls
[91] https://www.nytimes.com/2024/01/04/us/politics/threats-election-officials-swatting.html
[92] https://www.cnn.com/2024/03/13/politics/swatting-election-officials-invs/index.html
[93] https://www.dhs.gov/ntas/advisory/national-terrorism-advisory-system-bulletin-may-24-2023
[94] https://www.brennancenter.org/our-work/analysis-opinion/poll-election-officials-shows-high-turnover-amid-safety-threats-and
[95] https://www.brennancenter.org/our-work/research-reports/local-election-officials-survey-may-2024
[96] https://abcnews.go.com/US/election-officials-continue-face-threats-harassment-ahead-november/story?id=112204734
[97] https://www.cnn.com/2024/03/13/politics/swatting-election-officials-invs/index.html
[98] https://www.cnn.com/2024/03/13/politics/swatting-election-officials-invs/index.html
[99] https://www.bloomberg.com/news/articles/2024-01-23/cisa-director-was-target-of-harrowing-swatting-incident?embedded-checkout=true
[100] https://x.com/JocelynBenson/status/1823120682114318728
[101] https://www.nytimes.com/2024/08/09/us/politics/elissa-slotkin-mike-rogers-swatting.html
[102] https://apnews.com/article/michigan-primary-senate-house-slotkin-rogers-539bec9d2ef95d5cc724c22feb7ff99f
[103] https://www.washingtonpost.com/nation/2023/10/04/school-swatting-hoax-active-shooter/
[104] https://thehill.com/homenews/state-watch/4370415-fbi-memo-suggests-swatting-spree-targeting-jewish-institutions-linked/
[105] https://www.nbcnews.com/politics/politics-news/state-capitol-buildings-evacuated-bomb-threats-rcna132099
[106] https://apnews.com/article/government-building-bomb-threats-3d3dd10b648d76e471d934a14b54b3b3
[107] https://www.courts.maine.gov/news/article.html?id=12233776
[108] https://x.com/GovHawaii/status/1742658221112991810
[109] https://www.nbcnews.com/politics/politics-news/state-government-buildings-face-bomb-threats-second-consecutive-day-rcna132299
[110] https://x.com/ACKCurrent/status/1742933739838341422
[111] https://www.fox32chicago.com/news/chicago-hotel-bomb-threat-nobu
[112] https://www.cisecurity.org/insights/spotlight/election-security-spotlight-swatting
[113] https://www.cisa.gov/resources-tools/resources/election-mail-handling-procedures-protect-against-hazardous-materials
[114] https://www.npr.org/2023/11/09/1212045794/envelopes-with-fentanyl-or-other-substances-were-sent-to-several-elections-offic
[115] https://www.nbcnews.com/politics/2024-election/fbi-investigating-threatening-letters-sent-elections-officials-several-rcna171464
[116] https://abcnews.go.com/US/wireStory/suspicious-packages-election-officials-5-states-113740474
[117] https://www.nbcnews.com/politics/2024-election/fbi-investigating-threatening-letters-sent-elections-officials-several-rcna171464
[118] https://www.news10.com/news/north-country/ny-election-staff-impersonators-knocking-on-doors/
[119] https://www.justice.gov/opa/pr/man-arrested-making-threats-maricopa-county-election-official-and-official-office-arizona
[120] https://www.nbcnews.com/news/nbcblk/misinformation-may-only-worsen-black-voters-lead-election-experts-warn-rcna26924
[121] https://www.nytimes.com/2022/10/25/us/politics/ohio-robocalls-wohl-burkman-guilty.html#:~:text=Wohl%20used%20a%20voice%20broadcasting,or%20went%20to%20voice%20mail
[122] https://www.dhs.gov/sites/default/files/2023-09/23_0913_ia_23-333-ia_u_homeland-threat-assessment-2024_508C_V6_13Sep23.pdf
[123] https://www.counterextremism.com/blog/reactions-trump-assassination-attempt-extreme-right-telegram-channels
[124] https://www.justice.gov/opa/pr/maryland-woman-and-florida-man-charged-federally-conspiring-destroy-energy-facilities
[125] https://thesoufancenter.org/intelbrief-2023-february-10/
[126] https://www.eisac.com/portal/s/article/E-ISAC-Monthly-Report-February-2024
[127] https://www.eisac.com/portal/s/article/E-ISAC-Monthly-Report-April-2024
[128] https://www.iso-ne.com/about/key-stats/maps-and-diagrams/#system-diagram
[129] https://atlas.eia.gov/apps/all-energy-infrastructure-and-resources/explore

[130] https://www.cfr.org/news-releases/there-risk-extremist-violence-around-2024-us-presidential-election-warns-new-cfr
[131] https://www.cisa.gov/sites/default/files/2024-09/Physical-Security-Checklist-for-Election-Offices-508.pdf
[132] https://www.cisa.gov/sites/default/files/2023-09/Preparing%20for%20and%20Mitigating%20Foreign%20Influence%20Operations%20Targeting%20Critical%20Infrastructure.pdf