CYBLE®

REPORT

U.S. Election Security 2024

Disinformation Is a Far Bigger Threat Than Cybersecurity

Key Takeaways:

- Election security in the U.S. is generally good headed into the November presidential election - in the view of the intelligence community (IC), disinformation is a much bigger concern than security.
- Because of a huge increase in paper ballots, which will comprise greater than 98% of all ballots this year, the election will be auditable, verifiable and reproducible like never before.
- Still, after 8 years of campaign hacks, election denialism and foreign attempts to influence election outcomes, 2024 may be as volatile, if not more so, than 2020 or 2016.
- The intelligence community has deemed Russia, Iran and China to be the three most active nation-state actors trying to influence the election, with varying goals and methods.
- Incidents so far have included a Trump campaign hack, voter database leaks, vulnerabilities in election and polling software, U.S. actions against Russia, and more.
- Social media has played an expectedly outsized role in influence campaigns – with the new addition of AI-generated content and deepfakes – but despite government and social media efforts to curb these disruptive influences, much more needs to be done.
- Cyble data shows significant election chatter on the dark web and in cybercrime forums, around 500,000 posts and records in all in the last 6 months, suggesting that dark web monitoring could be a useful place for monitoring election developments.
- We evaluate election security overall, including recommended processes and security steps.

In early August, some of the world's top hackers descended on a remote corner of the DEF CON conference in Las Vegas with a critical mission: To find security vulnerabilities in some of the voting systems that will be used in the upcoming U.S. presidential elections.

According to the DEF CON Voting Village's organizers, the hackers found enough flaws in the voting machines to fill "multiple pages." The final report hasn't been released yet, and even if it had been, the lengthy process of developing and applying fixes wouldn't be complete until after the election anyway, underscoring the need for a more urgent update process for machines that are critical to the smooth functioning of democracy.

But despite known flaws circulating within 90 days of the hotly contested election between Vice President Kamala Harris and former President Donald Trump, the security of voting machines doesn't seem to be anyone's top concern. Rather, disinformation seems to be the top concern of the U.S. intelligence and cybersecurity officials tasked with overseeing the security of the 2024 election.

In fact, one top election observer in the U.S. – David Becker, executive director and founder of The Center for Election Innovation & Research – sees the DEF CON hacking session as a disinformation risk more than a security risk.

Becker notes that fewer than 2% of all U.S. voters this November will vote on machines without any paper ballot or backup, and those voters reside only in Louisiana (statewide) and a few counties in Texas.

"Everywhere else, there is paper, and there will be more audits than ever," Becker told *The Cyber Express*, a subsidiary of Cyble. "And the chain of physical custody around these machines is as strong as ever, meaning that efforts that do not take physical security of the devices into account, like what happens at DEF CON, are not a realistic depiction of the security around our voting machines. This problem is compounded by DEF CON's use of obsolete machines that are no longer in use, with questionable provenance – often obtained off of eBay and the like.

"The threat of 'hacking' of machines is quite overblown, given the success advocates have had in promoting paper ballots and audits nationwide, along with disconnection from the internet. It is a high risk, low reward endeavor, which, even if attempted, would almost certainly be detected and prosecuted, and the existence of verifiable paper ballots means the election could be reconstructed."

Becker agrees with intelligence and security agencies that the far bigger problem is disinformation – and the DEF CON event will likely add to that problem.

"A far greater risk is that bad actors could attempt through disinformation to make those that supported the losing candidate believe that the machines had been 'hacked,' using rhetoric and language from some of the participants at places like DEF CON," he said. "In fact, Trump's draft 2020 executive order authorizing the military to seize voting machines – which was never signed – quoted extensively from lawsuits brought by some of the participants in DEF CON."

What follows is an in-depth look at the unprecedented threats facing the 2024 U.S. election, in a year in which a quarter of the world's population went to the polls, along with steps to control those risks, some of which are well underway.

Security and Legitimacy Challenges Like No Election Before

In an era of tumultuous presidential elections, the 2024 U.S. election will face security and legitimacy challenges like none before it.

The tumultuous era began with the 2016 Russian hack of a Democratic National Committee (DNC) email server, the contents of which were passed onto WikiLeaks and published by major media outlets, significantly damaging the campaign of Democratic candidate Hillary Clinton – and leading to special counsel Robert Mueller's subsequent investigation into the Trump campaign's ties to Russia.

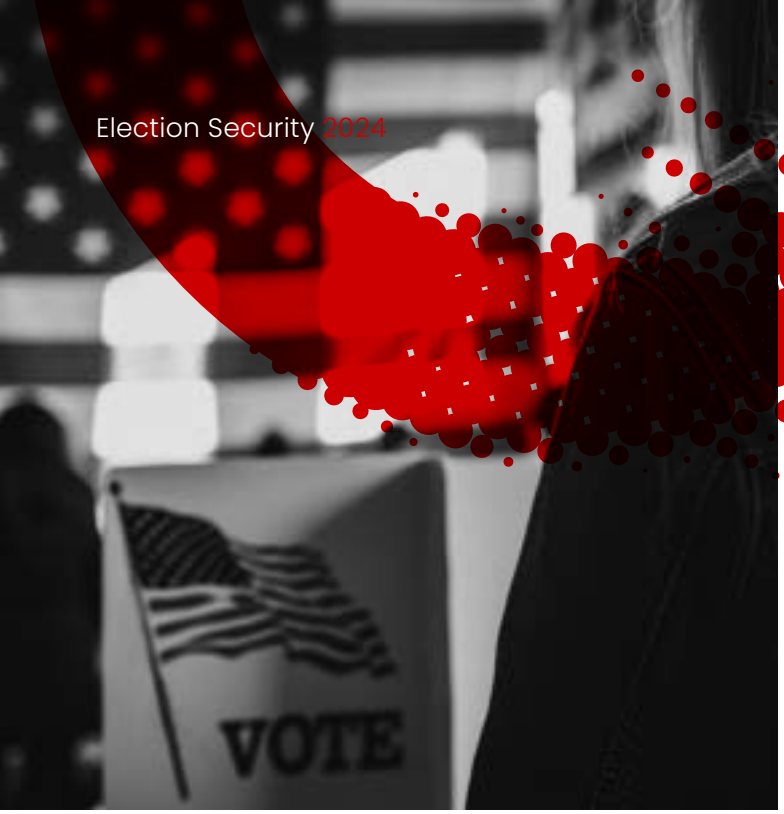
In 2020, after losing his reelection bid to President-elect Joe Biden, Trump falsely claimed the election had been stolen, which culminated in the January 6, 2021 U.S. Capitol riot that resulted in more than 800 convictions and an indictment and second impeachment of Trump himself.

With Trump already suggesting that any result other than him winning in 2024 will be illegitimate, election officials at the state, local and national level face significant pressure to ensure that the election's security and integrity are strong enough to withstand what likely will be scores, if not hundreds, of legal challenges that the GOP has already started, ranging from voter eligibility challenges and voter roll purges to certifying results.

That pressure comes in an election year that has already seen an assassination attempt on Trump, at least one troubling voting software incident, multiple incidents of foreign interference, a robocall campaign intended to suppress Democratic turnout, stolen voter rolls, security weaknesses at a major polling firm, insider threats, doxing of election workers – and a hack of the Trump campaign.

What makes 2024 more challenging than other recent elections, is – in a word – technology. AI makes deepfakes and disinformation campaigns potentially more effective than ever. Adversaries are more skilled and harder to detect. And the influence of social media platforms has changed, with the biggest change being that X (formerly Twitter) – which was once an open platform dedicated to a reasonably open exchange of ideas – has been taken over by the nakedly pro-Trump and pro-Russia partisan Elon Musk.

How a major Western political party like the GOP became a vehicle for disinformation, anti-science and anti-democratic views within just a few years of the campaigns of John McCain and Mitt Romney is beyond the scope of this paper but will certainly occupy historians for a generation or more to come.



Nation-State Threats to U.S. Elections

The U.S. Office of the Director of National Intelligence (DNI) recently named Russia, Iran and China as the three biggest nation-state actors attempting to influence the U.S. election.

The briefing document said the intelligence community (IC) "has not seen any foreign actor seeking to interfere in the 2024 elections. The IC and our partners, however, continue to monitor foreign actors' influence efforts, seeking to uncover any activities that could enable election interference, especially cyber or physical disruptions of election infrastructure."

Manipulating election processes enough to change the outcome would be very difficult, DNI notes: "The interagency election security community assesses that it would be very difficult for a foreign actor to manipulate election processes at a large enough scale to impact the outcome of a federal election without detection by intelligence collection, post-election audits, or physical and cybersecurity monitoring of the decentralized and diverse election infrastructure across the country."

Thus, disinformation and influence remain the intelligence community's biggest concerns.

"Russia, Iran, and China are trying by some measure to exacerbate divisions in U.S. society for their own benefit, and see election periods as moments of vulnerability," the briefing document stated. "These actors most likely judge that amplifying controversial issues and divisive rhetoric can serve their interests by making the United States and its democratic system appear weak and by keeping the U.S. Government distracted with internal issues instead of pushing back on their hostile behavior in other parts of the world."

"We continue to monitor adversaries' efforts to cast doubt on the electoral process or claim that they have interfered in the process when they have not actually done so, a tactic known as 'perception hacking,'" the document said.

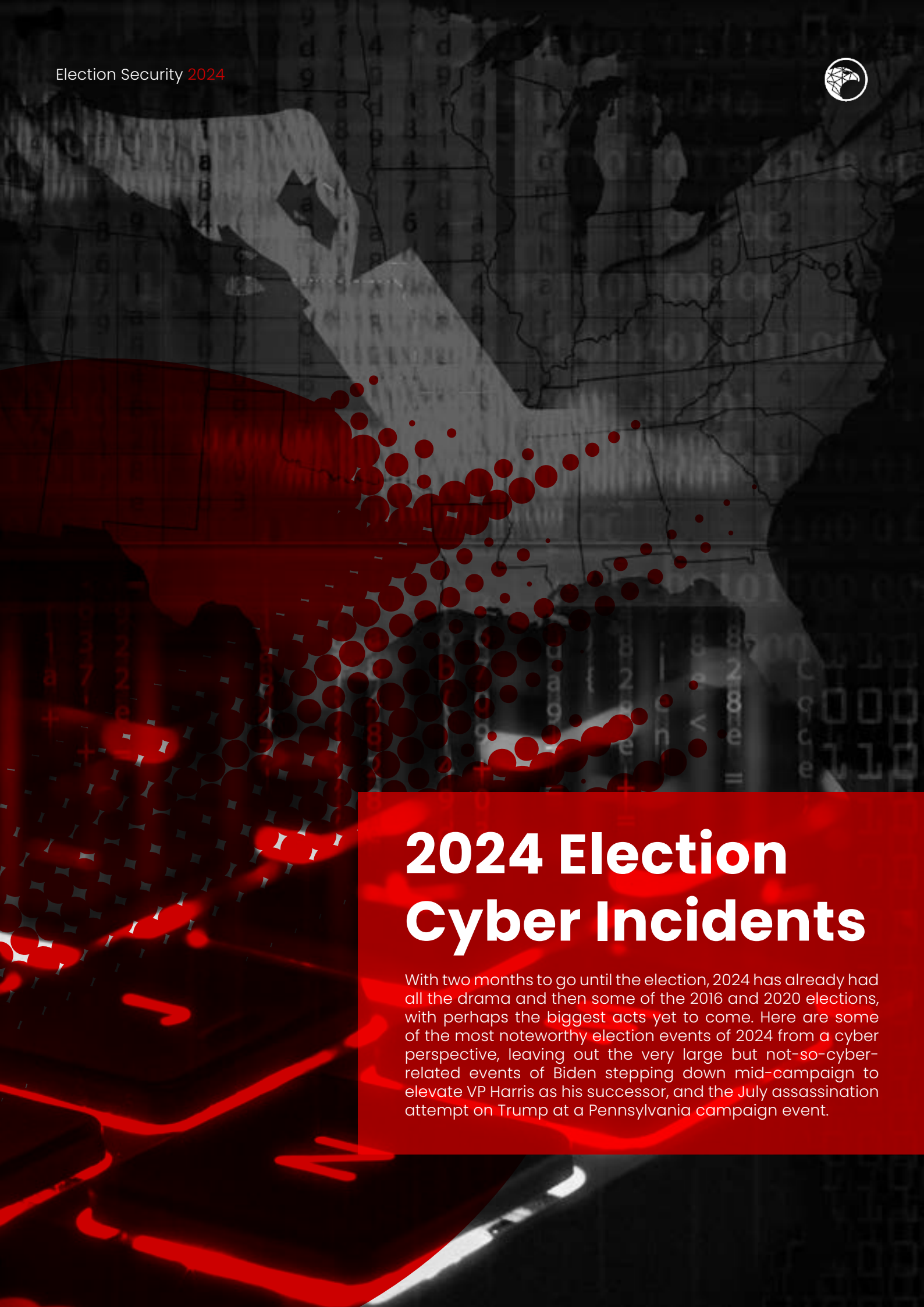
Russia has been most active in its efforts to "amplify divisive rhetoric and influence election outcomes, which is consistent with Moscow's broader foreign policy goals of weakening the United States and undermining Washington's support for Ukraine."

Iran "is making a greater effort than in the past to influence this year's elections, even as its tactics and approaches are similar to prior cycles. Like Russia, Iran has a multi-pronged approach that seeks to stoke discord and undermine confidence in our electoral process. Tehran also has sought cyber access to individuals with direct ties to the presidential campaigns of both political parties while elements have also denigrated the former President."

China, oddly enough, has been more focused on influencing down-ballot races and building relationships with U.S. officials and entities at state and local levels "because it perceives Washington as largely opposed to China. This view likely informs Beijing's greater interest in some non-presidential races."

China's efforts include "focusing on candidates it views as particularly threatening to core PRC security interests."

The DNI has also observed a number of countries "considering activities that, at a minimum, test the boundaries of election influence. Such activities include lobbying political figures to try to curry favor with them in the event they are elected to office."



2024 Election Cyber Incidents

With two months to go until the election, 2024 has already had all the drama and then some of the 2016 and 2020 elections, with perhaps the biggest acts yet to come. Here are some of the most noteworthy election events of 2024 from a cyber perspective, leaving out the very large but not-so-cyber-related events of Biden stepping down mid-campaign to elevate VP Harris as his successor, and the July assassination attempt on Trump at a Pennsylvania campaign event.

Trump campaign hacked: In August, the Trump campaign was hacked by Iran-linked threat actor group APT42, also known as Charming Kitten, an attack that led to a subsequent warning from U.S. intelligence agencies about Iranian attempts to influence the election. The hackers sent documents from the campaign – reportedly including a 271-page assessment of vice presidential candidate JD Vance's potential weaknesses – to major media outlets, but unlike 2016, media outlets declined to publish the information.

New Hampshire election code security: While upgrading their voter registration database, New Hampshire officials discovered some disturbing oddities. The Connecticut-based contractor. WSD Digital, had offshored part of the work, giving unknown coders outside the U.S. access to the software. The state hired a forensic firm to investigate, which led to the discovery of a misconfigured connection that led to servers in Russia and the use of open-source code overseen by a Russian computer engineer convicted of manslaughter. A coder also programmed the Ukrainian national anthem into the database. The problems were caught and fixed but show that software supply chain risks can threaten election security too.

U.S. response to Russian influence efforts: In early September, the U.S. announced a multi-agency response to Russian influence efforts. U.S. officials alleged that an unnamed Tennessee company was paid $10 million by Russia Today for English-language videos on social media spreading Russian views on immigration, inflation and other issues, and officials also took aim at general Russian disinformation efforts. The U.S. actions included two indictments in absentia, the seizure of 32 domains, visa restrictions on 10 individuals and two entities, and a reward of up to $10 million for information on RaHDit (Russian Angry Hackers Did It).

ChatGPT shuts down Iranian operation: OpenAI announced in August that it had shut down accounts linked to an Iranian influence operation that was using the large language AI model to generate social media content on the U.S. election and other issues, highlighting the new role AI tools and LLMs are playing in disinformation campaigns.

Gallup XSS vulnerability: Researchers identified critical cross-site scripting (XSS) vulnerabilities in the website of leading polling company Gallup, which could have led to application and data takeover, potentially corrupting polling results. The incident highlights the public good that ethical hacking can do.

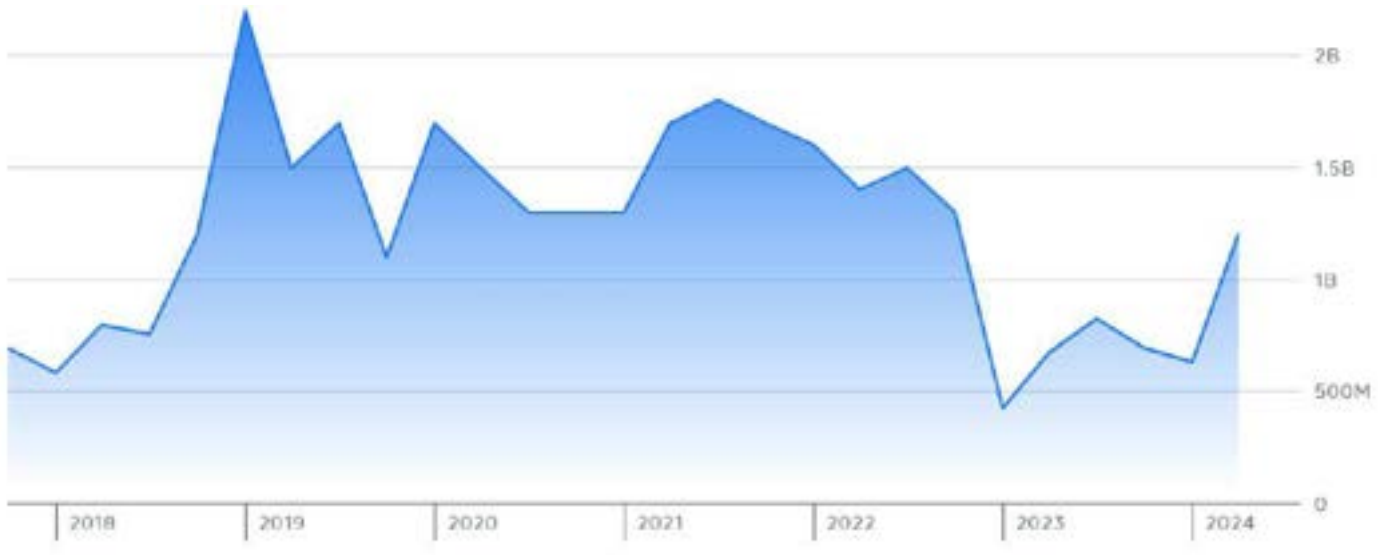
Biden robocall case: A telecom company agreed to pay a $1 million fine as part of an FTC settlement for using a deepfake voice clone of President Biden in an effort to suppress New Hampshire primary turnout, in yet another example of the election-related dangers of AI technology.

Voter database leaks: Voter database leaks, scrapes and hacks have been numerous this year. Illinois and Virginia were two states experiencing incidents, while the RansomHub ransomware group claimed responsibility for a data exfiltration attack on the Jefferson County, Kentucky Clerk's Office that also stole information on voting machines. While much voter registration information is public, it could still be used for influence campaigns, not to mention more basic cyberattacks like phishing and identity theft.

Social Media Controls and Controversies

Not surprisingly, much of the disinformation campaigns have played out on social media, where bot farms and deepfakes have been used to spread disinformation and dissension using posts, videos, memes and AI-generated fakes.

Social media companies like X and Meta routinely publish transparency reports, in part for compliance reasons. X reports more than 500,000 enforcement actions taken between October 2023 and March 2024, while Meta reports taking down more than 1 billion fake accounts in the second quarter of 2024, a number that's been rising steadily since the start of 2023 (see charts below).



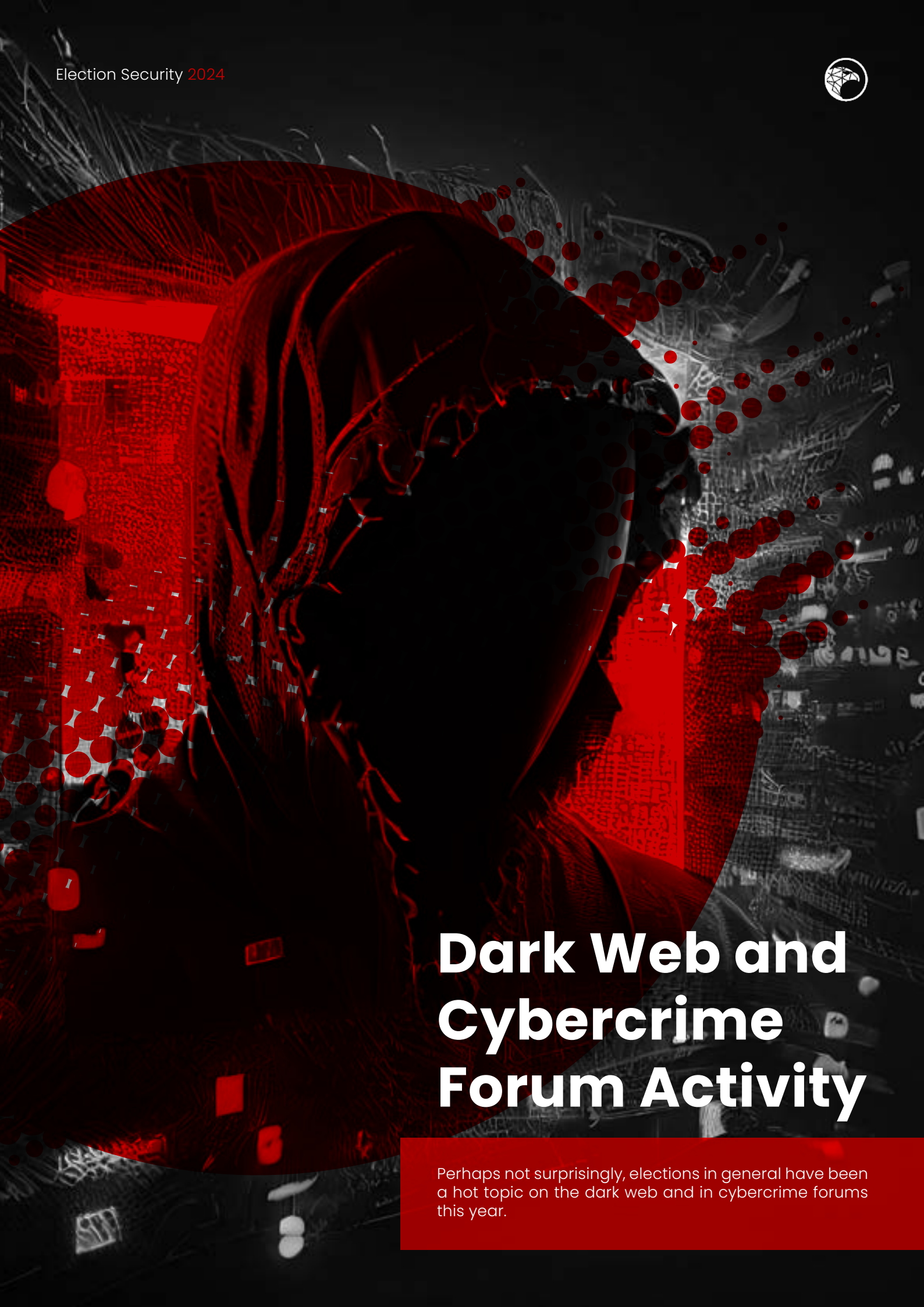
Facebook fake account takedowns by quarter (source: Meta)

Art. 15.1.c: TIUC Terms of Service and Rules Restricted Reach Labels - 21/10/23 to 31/3/24			
Policy	Auto-Enforced	Manually Enforced	**Total**
Abuse & Harassment		21,853	**21,853**
Hateful Conduct	437,410	38,298	**475,708**
Violent Speech		5,359	**5,359**
Total	**437,410**	**65,510**	**502,920**

X enforcement actions Oct. 2023-March 2024 (source: X)

While election-related disinformation may be only a small part of those actions, judging from the ease with which actors can set up bot farms on X and Musk's aversion to moderation, fake accounts and influence campaigns are likely a much bigger problem on X than acknowledged. By comparison, Meta appears to be doing a better job at battling election misinformation, including designating more than 700 hate groups globally.

Other platforms have also had disinformation issues. YouTube was a target of recent U.S. actions against Russian campaigns, and fears that TikTok could be misused by China to spread misinformation has been central to U.S. demands that ByteCentral, TikTok's Chinese owner, divest from TikTok by January 19 or face a ban.



Dark Web and Cybercrime Forum Activity

Perhaps not surprisingly, elections in general have been a hot topic on the dark web and in cybercrime forums this year.

Data from Cyble Vision, Cyble's AI-powered threat intelligence platform, turned up more than 500,000 posts and records – a number that continues to grow as the election grows nearer – in "elections" searches covering the last six months, suggesting significant election activity across the dark web.

Cyble data queries found:

Data exposures: 285,585 records
Ransomware leaks: 12,463
Exposed endpoints: 1,608 (3 months of data)
Compromised files: 264,296
Tor links: 37,082
Cybercrime forum mentions: 426
Dark web marketplaces: 763
Telegram mentions: 15,669
Discord: 873

The records include many exposed voter and election worker records, not just in the U.S. but also globally.

Cyble researchers also found a lot of dark web chatter surrounding the U.S. election. While the data didn't turn up anything explicitly violent, a number of posts suggest the possibility that responses to the election could become increasingly volatile as the results become known.

Here are excerpts from two Telegram posts as examples:

"The legal and psychological landscape are very different in 2024 vs 2020. This will be the first election in American history where the majority of the People know our elections are being rigged. All the elements for a perfect storm are in place."

"We have an entity that prints, mails, receives, scans and stores our ballots that does not have to comply with FOIA requests, has little to no oversight and has more control than our County. A company paid for by THE TAX PAYERS."

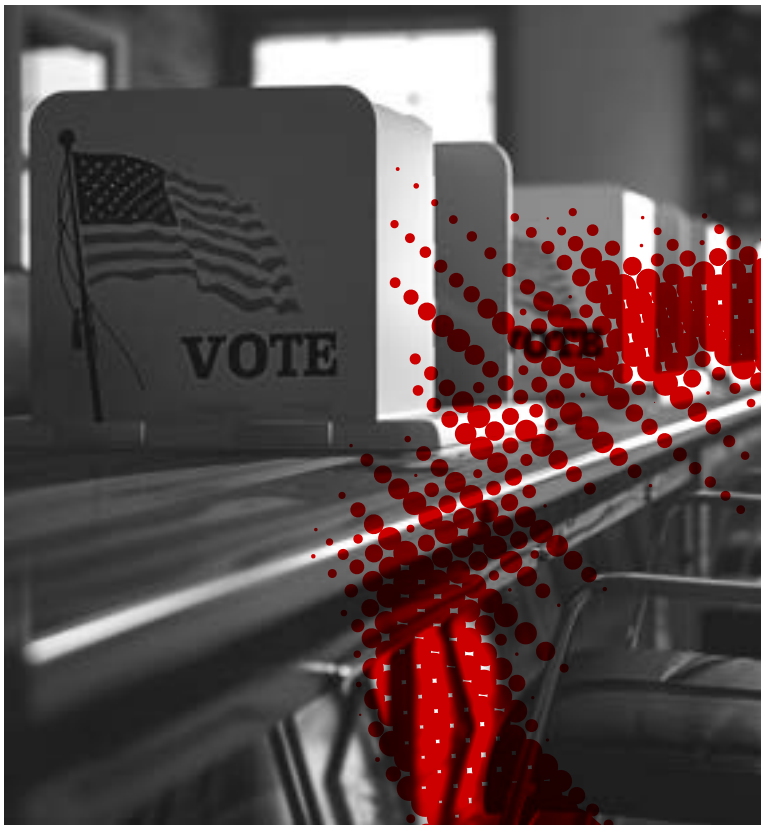
Kaustubh Medhe, Cyble's Vice President of Research and Threat Intelligence, said Cyble's work confirms what U.S. intelligence officials have said – that the election is secure, and any incidents are more likely to be used to cast doubt on the legitimacy of the election.

"Underground commentary on the election appears largely aimed at amplifying any perceived anomaly as 'proof' that the election is 'rigged.' We expect this rhetoric to intensify as the election gets closer, with language increasingly suggesting violence if the outcome doesn't go as desired," said Medhe.

"In our investigation, a detailed search on our dark web and threat intelligence platform did not find any credible evidence of tools or techniques that have been designed or actively deployed that are capable of ballot rigging. We concur with CISA and the FBI that it is extremely unlikely that an election outcome could be altered by a malicious party, but that any perceived anomaly or issue will be used to cast doubt on the legitimacy of the election.

"We anticipate that the coming months will be a trying time for election security, with widespread disinformation campaigns on social media, additional spear phishing and attempted breaches of candidates' campaign infrastructure, and an election infrastructure that will receive intense scrutiny, including the potential for physical intrusion attempts on election offices and DDoS attacks on election websites. It is important to understand that none of these threats can disrupt voting or prevent votes from being counted."

In 2022, for example, Russian hackers targeted state government websites in Colorado, Kentucky and Mississippi a month before the midterm elections, but the sites recovered quickly, with no negative effect on the election.



What Does Good Election Security Look Like?

So what does good election security look like? A lot like regular security, but with additional physical, chain of custody and provenance controls required to ensure confidence in results and to protect election workers. Paper ballots, audits and physical custody are critically important for election integrity and backup measures.

CISA recommends some basic system security controls and best practices, such as:

- Multi-factor authentication
- Strong email security, including DMARC, filtering and employee training
- A secure website, including a .gov domain and DDoS protection
- Secure encrypted backups
- A vulnerability and patch management program
- Strong physical security of offices and election equipment

CISA also offers free cyber and physical security assessments for election offices, among other services, including the Albert Managed Intrusion Detection System offered in partnership with the Center for Internet Security (CIS). The Elections Infrastructure Information Sharing and Analysis Center (EI-SAC) is another free resource for election offices, offering free endpoint security services and malicious domain blocking.

Election workers have faced a number of threats in recent years that need to be addressed in addition to election security. Doxing is one prominent threat, and swatting is another. At the same time, in this hyper-partisan and suspicious era, election offices need to keep an eye on potential insider threats too.

Conclusion: Election Security is on The Ballot Too

Oddly, election security is on the ballot too this fall, as some troubling initiatives in the GOP's Project 2025 playbook would weaken both election security and cybersecurity, risking turning future elections into a chaotic nightmare of foreign influence.

But at least through the November 2024 election, the U.S. election infrastructure appears secure enough to weather any attacks while producing verifiably accurate results. The challenge facing intelligence and security officials will be to minimize foreign influence that could sway those results, as potentially occurred in 2016.

Longer term, the role of social media and AI in disinformation must continue to receive scrutiny, and hopefully adequate controls that do not unduly repress free speech.

Lastly, cybersecurity researchers and media should consider how hackable a vulnerability is rather than hyping every newly discovered vulnerability. More restrained reporting in the case of the DEF CON voting machine hacks and other potentially divisive issues would lower their potential to fan the flames of disinformation. Alternatively, the consumers of such research should skeptically apply their own thought and judgment. After all, democracy is what's fundamentally at stake here.

Sources and further reading:

https://www.politico.com/news/2024/08/12/hackers-vulnerabilities-voting-machines-elections-00173668

https://www.nbcnews.com/politics/2024-election/democrats-grow-concerned-republicans-are-planting-seeds-legal-suits-ov-rcna168961

https://www.politico.com/news/2024/09/01/us-election-software-national-security-threats-00176615

https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2024/3981-joint-odni-fbi-and-cisa-statement-on-iranian-election-influence-efforts

https://www.dni.gov/files/FMIC/documents/ODNI-Election-Security-Update-20240906.pdf

https://www.justice.gov/opa/pr/two-rt-employees-indicted-covertly-funding-and-directing-us-company-published-thousands

https://home.treasury.gov/news/press-releases/jy2559

https://www.state.gov/u-s-department-of-state-takes-actions-to-counter-russian-influence-and-interference-in-u-s-elections/

https://www.justice.gov/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence

https://openai.com/index/disrupting-a-covert-iranian-influence-operation/

https://checkmarx.com/blog/critical-xss-vulnerabilities-identified-on-gallup-com/

https://www.cisa.gov/topics/election-security

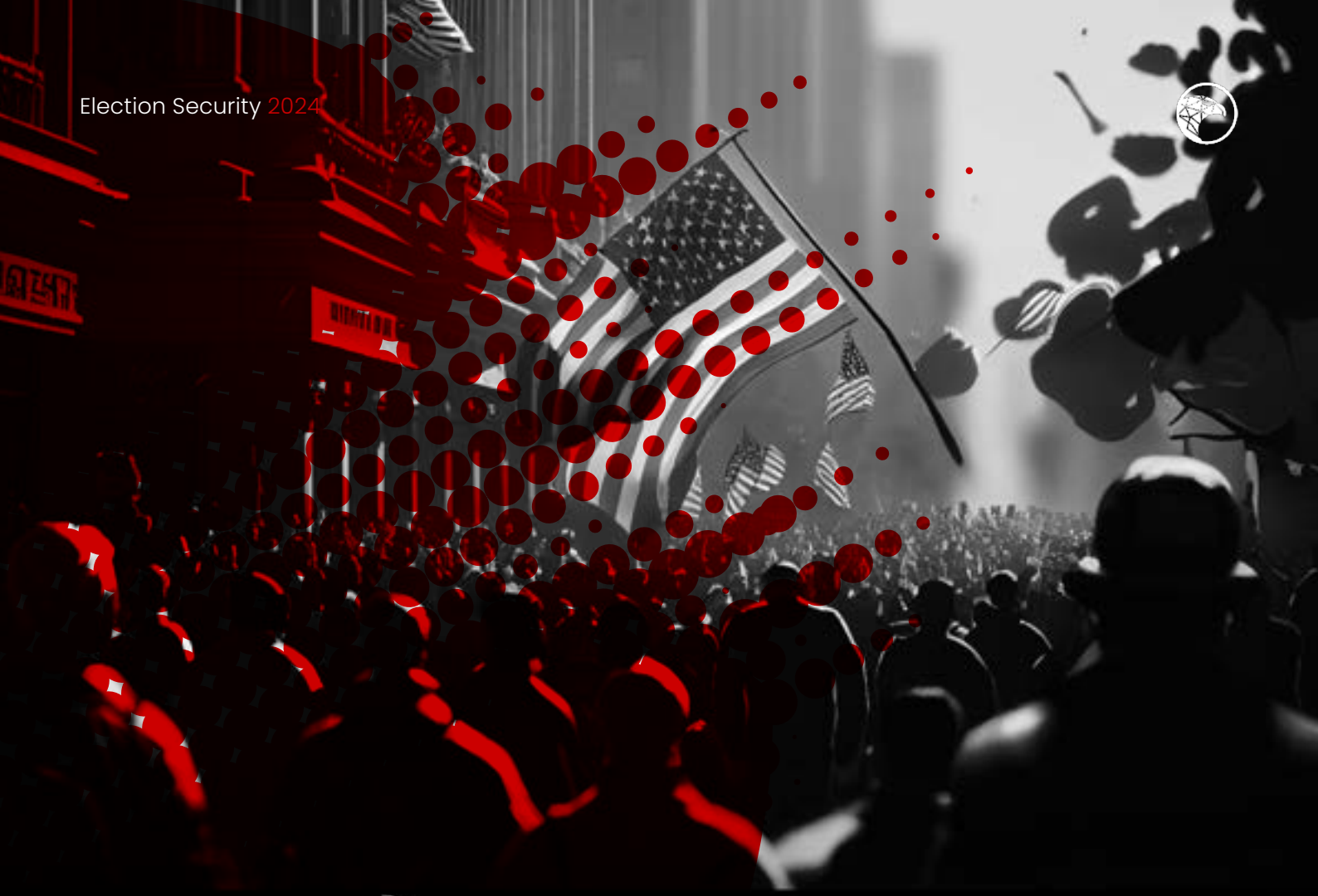
https://www.cisa.gov/topics/election-security/protect2024

https://www.dhs.gov/topics/election-security

https://www.ic3.gov/Media/News/2024/240628.pdf

https://www.cisecurity.org/insights/spotlight/ei-isac-cybersecurity-spotlight-doxing

https://www.cisa.gov/sites/default/files/2024-09/Readiness-and-Resilience-Checklist-for-Election-Offices-508.pdf



About Cyble

Cyble Inc. is a cybersecurity company specializing in dark web monitoring and threat intelligence services. Cyble leverages proprietary AI-based technology to help enterprises, federal bodies, and individuals stay ahead of cybercriminals. The company is known for its expertise in tracking cyber threats, data breaches, and other malicious activities.

See Cyble in Action

11175 Cicero Drive Suite, 100 Alpharetta GA 30022, US. | contact@cyble.com | +1 888 673 2067