Poll Vaulting: Cyber Threats to Global Elections

By Mandiant

Published: 2024-04-25 · Archived: 2026-04-05 15:10:27 UTC

Written by: Kelli Vanderlee, Jamie Collier

Executive Summary

- The election cybersecurity landscape globally is characterized by a diversity of targets, tactics, and threats. Elections attract threat activity from a variety of threat actors including: state-sponsored actors, cyber criminals, hacktivists, insiders, and information operations as-a-service entities. Mandiant assesses with high confidence that state-sponsored actors pose the most serious cybersecurity risk to elections.
- Operations targeting election-related infrastructure can combine cyber intrusion activity, disruptive and destructive capabilities, and information operations, which include elements of public-facing advertisement and amplification of threat activity claims. Successful targeting does not automatically translate to high impact. Many threat actors have struggled to influence or achieve significant effects, despite their best efforts.
- When we look across the globe we find that the attack surface of an election involves a wide variety of entities beyond voting machines and voter registries. In fact, our observations of past cycles indicate that cyber operations target the major players involved in campaigning, political parties, news and social media more frequently than actual election infrastructure.
- Securing elections requires a comprehensive understanding of many types of threats and tactics, from distributed denial of service (DDoS) to data theft to deepfakes, that are likely to impact elections in 2024. It is vital to understand the variety of relevant threat vectors and how they relate, and to ensure mitigation strategies are in place to address the full scope of potential activity.
- Election organizations should consider steps to harden infrastructure against common attacks, and utilize account security tools such as Google’s Advanced Protection Program to protect high-risk accounts.

Introduction

The 2024 global election cybersecurity landscape is characterized by a diversity of targets, tactics, and threats. An expansive ecosystem of systems, administrators, campaign infrastructure, and public communications venues must be secured against a diverse array of operators and methods. Any election cybersecurity strategy should begin with a survey of the threat landscape to build a more proactive and tailored security posture.

The cybersecurity community must keep pace as more than two billion voters are expected to head to the polls in 2024. With elections in more than an estimated 50 countries, there is an opportunity to dynamically track how

threats to democracy evolve. Understanding how threats are targeting one country will enable us to better anticipate and prepare for upcoming elections globally. At the same time, we must also appreciate the unique context of different countries. Election threats to South Africa, India, and the United States will inevitably differ in some regard. In either case, there is an opportunity for us to prepare with the advantage of intelligence.

The variety of threat actors and intentions exposes election-related targets to a range of cyber threat vectors. In addition to tactics that Mandiant commonly associates with cyber intrusion activity, such as phishing, exploitation of internet-exposed systems, and data theft, election cyber threat activity also seeks to influence public perceptions and voter choices. The tactics to accomplish this public-facing objective often leverage disruptive tactics. This includes web defacements, DDoS attacks, as well as publicizing intrusions and stolen data via leak sites or social media campaigns. Foreign state aligned information operations disseminate content on websites and social media. This is often intended to mislead target populations or encourage social divisions and mistrust in leaders and institutions.

Despite the variety of cybersecurity challenges facing election ecosystems, it is important for the security community to remain level-headed. Information operations and disruptive cyber campaigns thrive when their impacts are built up. This makes objective and data-driven analysis essential. The variety of election cyber threat vectors presents complexity, but also highlights that direct election result interference attempts account for a small proportion of the overall threat landscape.

Diversity of Targets: Protecting the Entire Election Ecosystem

The attack surface of an election involves a range of entities. This includes election systems and infrastructure, election administrators, entities involved in running the election, and organizations involved in political campaigning — including news and media organizations (Figure 1). The ease of targeting and nature of cyber threat activity (cyber espionage, information operations, extortion, etc.) can vary across entities within these categories.

Cyber Threat Activity May Impact a Variety of Election-Related Targets in 2024

Historical Observations Suggest Election Campaigns and Voters Targeted Most Frequently

Figure 1: Cyber Threat Activity May Impact a Variety of Election-Related Targets in 2024; Historical Observations Suggest Election Campaigns and Voters Targeted Most Frequently

Diversity of Tactics: Multiple Threat Vectors at Play

With multiple cyber threat vectors impacting election-related infrastructure, it is vital for defenders to identify the most likely scenarios that could impact them.

Figure 2 depicts our best assessment of the relative likelihood and magnitude of a particular cyber threat tactic being used against the three categories of election-related targets described in Figure 1. The likelihood assessments are based on how frequently we have observed or inferred use of these tactics during past election cycles. Magnitude assessments reflect the average amount of time and effort we estimate organizations expend to recover from events using these tactics as well as the strength of official responses to past incidents.

These assessments consider each tactic in isolation. However, Mandiant suggests that the combination of several tactics in the context of a single event would likely increase the severity of the campaign because we have seen this pattern play out during the most serious cyber threat events targeting elections over the last decade. Hack and leak represents a long-standing example of this in action: sensitive information stolen through a network intrusion boosts the effectiveness of subsequent information operations that can leverage authentic documents to maximize societal disruption.

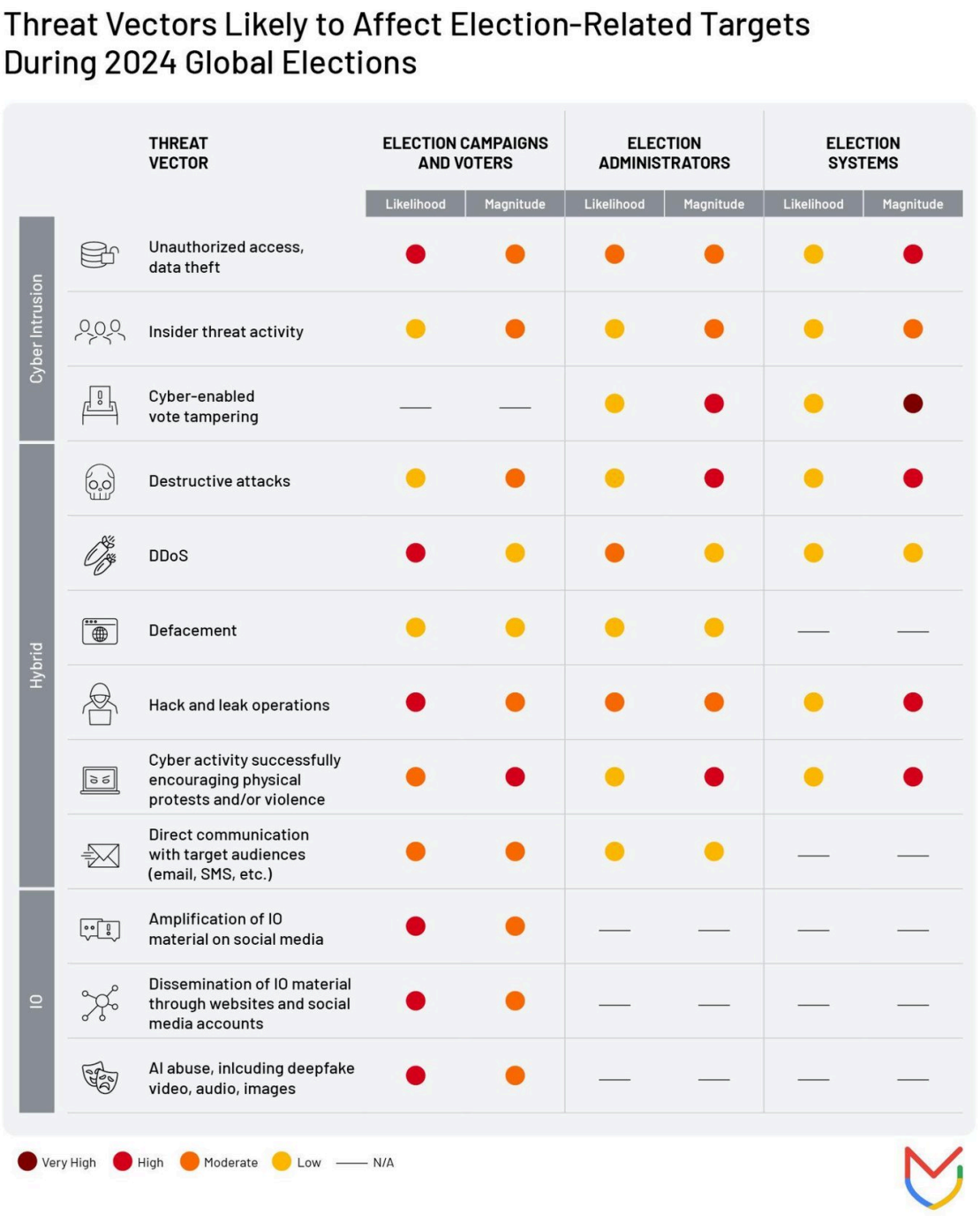


Figure 2: Relevant TTPs for 2024 Global Election-Related Targets

In the most significant cyber incidents targeting elections that Mandiant has tracked, threat actors have deliberately layered multiple tactics in hybrid operations in such a way that the effect of each component magnifies the others.

During the May 2014 Ukrainian presidential election, purported pro-Russian hacktivists CyberBerkut claimed credit for a series of malicious activities against the Ukrainian Central Election Commission (CEC) including a system compromise, destruction of vital data and systems including vote tabulation software, a data leak, a DDoS attack, and an attempted defacement of the CEC website with fake election results. Ukrainian officials suspect that

the operation was not conducted by independent hacktivists, citing the presence of malware on affected systems that is confidently attributed to Russian state attributed cyber espionage operators.

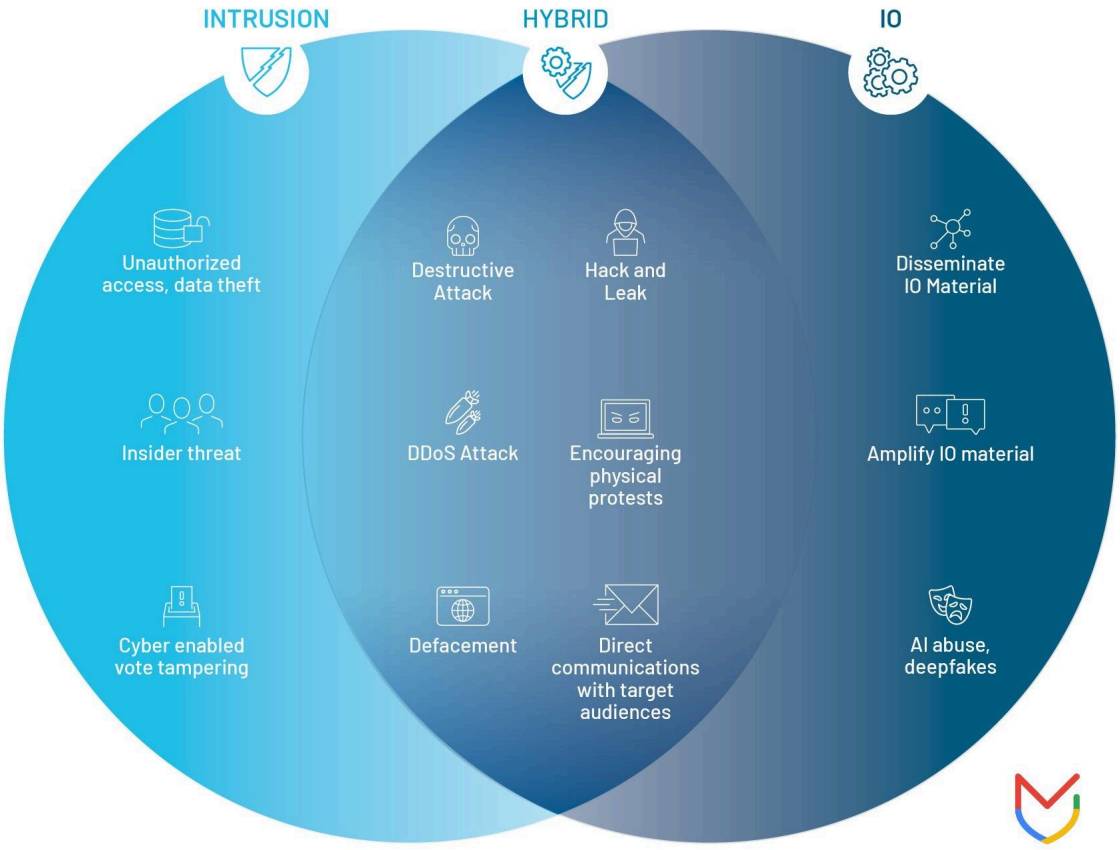


Figure 3: Operations Likely to Combine Traditional Cyber Intrusion and IO Tactics

In 2020, Iranian actors attempted to compromise multiple U.S. state voter registration or information websites. They used stolen voter contact information to send threatening emails and social media direct messages impersonating the “Proud Boys” to intimidate U.S. officials and voters.The operation used a video — also featuring stolen voter data — to publicize a false claim of weaknesses in U.S. election systems (Figure 4). On election day, the actors allegedly attempted to log in to a previously compromised media outlet, likely to use the access to disseminate additional false information. U.S. authorities linked the threat actors to Iranian company Emennet Pasargad, which has contracted with the Iranian government.

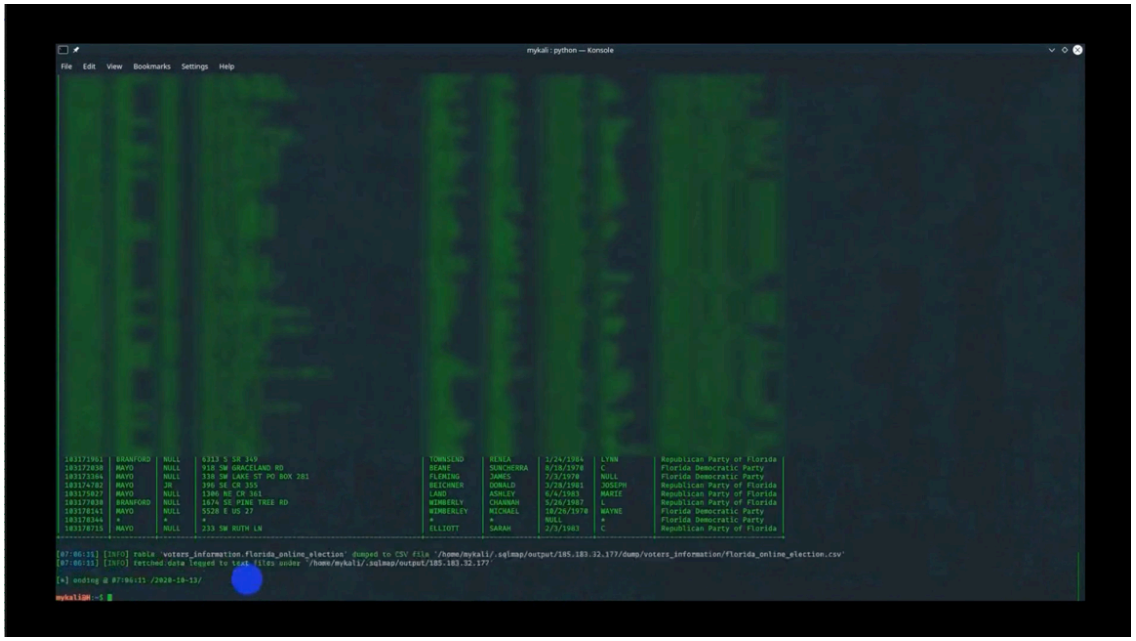
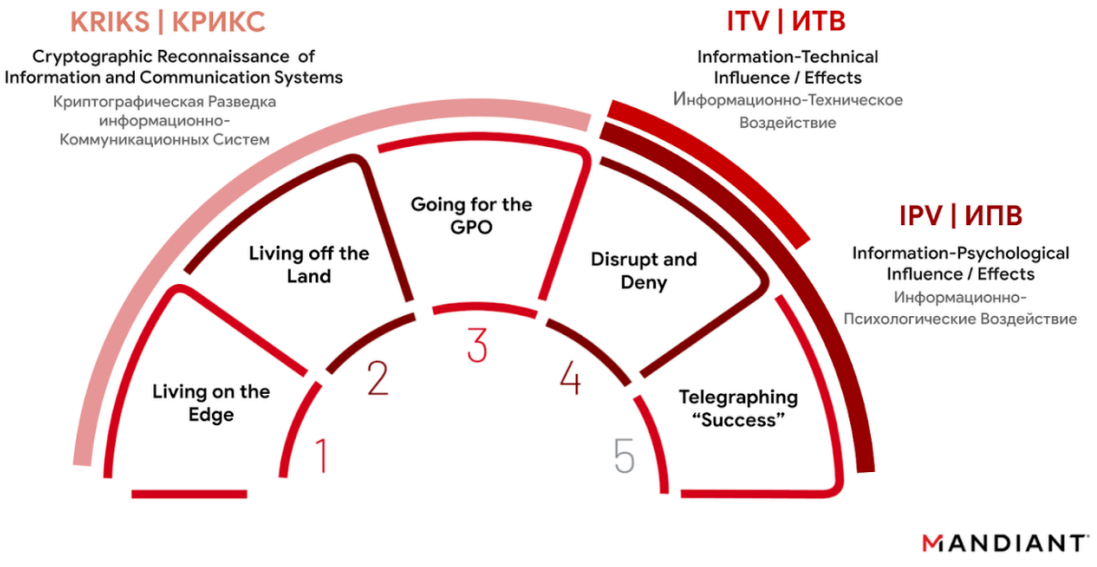


Figure 4: Screenshot from threat actor video

Mandiant has observed similar dynamics of hybrid operations demonstrated frequently during the ongoing Russia-Ukraine conflict.

For example, DDoS attacks disrupted the websites and some online services of Ukrainian government agencies and financial services organizations shortly before the advancement of Russian troops in February 2022. U.S. and UK officials attributed these DDoS attacks to the Russian Main Intelligence Directorate (GRU). On the same day, Ukrainians also received SMS messages claiming that ATM services were malfunctioning, which were debunked by Ukrainian cyber police as inaccurate. While the DDoS attacks only caused short-term technical disruption to online banking services, the overarching aim of the campaign was to undermine public trust in the integrity of the Ukrainian financial services industry and provoke panic in the run-up to a physical conflict.

In fact, the blending of cyber and information operations is an essential pillar of Russia's strategy. This is reflected in its information confrontation doctrine that combines reconnaissance, disruptive technical effects, and psychological operations (Figure 5). This approach plays out in the wiper operations conducted by the GRU in Ukraine. Here, Russian threat actors steal data from targeted systems, deploy wiper malware, and then telegraph the success of their operations by calling attention to the disruption and providing evidence of a compromise with the stolen materials via Telegram channels.



Russia's approach to wiper operations in Ukraine highlights the importance of understanding threats from an adversary's perspective. By understanding the doctrine and cyber strategy of state threats, we can better understand how they might seek to target election-related processes.

Diversity of Threat Actors: More Players in the Game

Elections attract cyber threat activity from nearly every variety of threat actor that Mandiant tracks in terms of motivation, capability and intent. Mandiant assesses with high confidence that state-sponsored cyber threat actors pose the most serious risk to elections, particularly when these operations can combine state level resourcing with traditional cyber intrusion activity, disruptive and destructive capabilities, and information operations and hacktivist style tactics, elements of public-facing advertisement and amplification of threat activity claims.

- **State-sponsored actors**: Government organizations, contractors, and others working on behalf of governments are the most persistent threat to elections. Military and security services are regularly tasked with cyber espionage intelligence collection against election related targets, with information operations and election interference increasingly becoming standard practice. State media services also have a role in information operations. Operations by these actors often benefit from long planning cycles, significant resources, and specific expertise. Based on previously observed activity taking place in the runup to elections, these operations are conducted for a variety of purposes, although rarely in an attempt to directly impact the process of voting and the tabulation of results.

- **Cybercrime**: Financially motivated actors may affect elections despite no specific interest in the elections themselves. Ransomware and extortion operations target victims simply for their ability to pay. It is common for cyber criminals to offer compromised data or access for sale on underground forums, including from election-related organizations. The plentitude of election related organizations and systems significantly increases the likelihood of a related criminal event.

- **Hacktivists**: Ideologically or politically motivated independent actors have carried out attacks on election related targets on several occasions. This activity is often sporadic, linked to foreign conflicts or domestic

controversies, and typically causes only superficial impacts, such as the temporary disruption of election related websites.

- **Insider threats**: Insider threats have become a concern for election officials given the privileged access they hold. Some are malicious insiders such as employees looking to steal data or sabotage the organization. Others are unintentional insiders such as employees who make mistakes or fall victim to phishing attacks.
- **Information operations as-a-service**: Mandiant and open sources have documented PR firms using deceptive information operations tactics during elections to promote messaging that supports or criticizes candidates or issues. These tactics include coordinated inauthentic social media advocacy, comment brigading, and operating sock puppet accounts. Mandiant tracks several prominent examples, such as the HaiEnergy and Doppelganger campaigns, that we suspect or have confirmed conduct this activity on behalf of nation states.

HaiEnergy Exploits U.S. News Outlets via Newswire Services and Stage In-Person Protests

Mandiant believes the pro-People's Republic of China (PRC) HaiEnergy IO campaign is linked to Shanghai Haixun Technology Co., Ltd (上海海讯社科技有限公司), a Chinese PR firm. HaiEnergy used two self-described “press release” services—"Times Newswire" and "World Newswire" —and dozens of subdomains of legitimate U.S.-based news outlets to disseminate campaign materials that appear to come from trustworthy sources. The content is then further amplified by additional inauthentic news sites and associated social media accounts. Mandiant assessed the news sites to be inauthentic because although they presented themselves to be independent news organizations operating in a variety of countries and languages, they were all hosted on infrastructure owned by Haixun, they used the same Chinese-language HTML template, and they frequently included links to, or republished identical content from, other websites in the network.

Promoted articles praise the PRC and criticize U.S. foreign policy, politicians, and highlight domestic issues, such as ethnic tension or gender inequality. Mandiant observed HaiEnergy promote articles critical of Taiwanese President Lai Ching-te (candidate at the time of this observed activity), describing him as lacking political acumen and the Democratic Progressive Party (DPP) as plagued by internal conflicts and a series of scandals. HaiEnergy assets also promoted narratives positively portraying electoral changes implemented by the PRC in Hong Kong ahead of the district council election.

Significantly, Mandiant uncovered evidence that HaiEnergy financed at least two small, staged in-person protests in Washington, D.C., a marked escalation in tactics leveraged by pro-PRC actors. Both protests, which occurred around June and September 2022, were documented via video and subsequently used as source material to support narratives published by HaiEnergy assets and infrastructure (Figure 6).

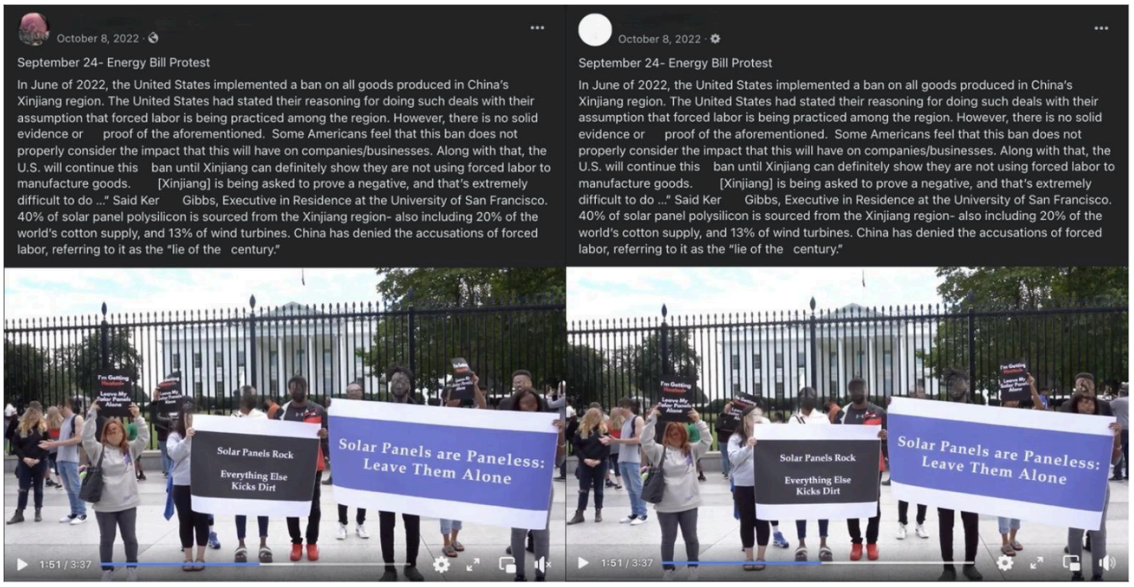


Figure 6: HaiEnergy Accounts Promote Identical Text from Times Newswire Article and Video of Protest in Washington, D.C.

State-Aligned Activity

State-sponsored cyber threat actors target election-related infrastructure for a variety of reasons, although rarely in an attempt to directly impact the result of an election or disrupt voting. Direct interference in elections comes with significant risk of retaliation and escalation leading to most states constraining their activity. Activity against election-related targets is therefore often intended to achieve other objectives, including:

- Apply pressure on another government around a specific issue or as an attempt to influence foreign policy outcomes.
- Retaliation for previous disputes between the two countries.
- Amplify issues and causes in a foreign country that coincide with a government's own national interests.

Mandiant compiled a list of state-aligned cyber threat actors and personas we assess to be likely to target election-related organizations in 2024 (Figure 7). In addition to threat actors focused on intrusion activity, we have also included groups that are involved in cyber threat activity targeting broad public audiences, such as hack and leak and information operations. This is because these public-facing campaigns often serve complementary objectives to more covert intrusion activity, and in some cases are coordinated.

To assess the likelihood of activity, Mandiant considered how likely different threat actors are to target election-related entities and the sort of activity they conduct. This list is based on groups that have been observed targeting government, civil society, media, or technology organizations.

This list should not be viewed as comprehensive; it is possible that additional known actors or previously unobserved groups will also engage in cyber threat activity related to 2024 elections. However, it could represent a useful guide for prioritizing defensive strategies and hunt missions.

State-Aligned Cyber Threat Actors and Personas Likely to Target 2024 Global Elections

Figure 7: Relevant actors for 2024 global elections threat modeling

Russia

Mandiant assesses with high confidence that Russian state-sponsored cyber threat activity poses the greatest risk to elections in regions that Russia closely monitors, such as the U.S., the UK, and the EU. Multiple Russian groups have targeted past elections in the U.S., France, and Ukraine, and these groups have continued to demonstrate the capability and intent to target elections both directly and indirectly. However, we do not know how Russia's operational tempo in Ukraine will impact any decision and resources available to target elections in 2024.

APT44 (aka Sandworm Team) • *Intrusion* • *Hybrid* • *IO*	GRU-linked APT44 (aka Sandworm Team) has conducted several of the most impactful hybrid cyber threat operations combining cyber espionage with hack-and-leak and other influence operations related to elections in the U.S., Ukraine, France, and Georgia over the past 10 years. Mandiant previously assessed that hacktivist personas XakNet Team and CyberArmyofRussia_Reborn have collaborated with the GRU's network attacks to create second-order psychological effects during the ongoing conflict in Ukraine. Moreover, Solntsepek has notably been the primary vehicle used to claim responsibility for cyber attacks and to leak stolen documents from operations linked to APT44 in 2023.
UNC4057 (aka COLDRIVER) • *Intrusion* • *Hybrid* • *IO*	UNC4057 conducts cyber espionage and information operations in support of Russian national interests. Mandiant observations suggest that this group has primarily focused on Ukraine and NATO countries since Russia's 2022 invasion. However, Mandiant believes that UNC4057 poses a risk to election-related organizations because information UNC4057 stole from victim mailboxes has reportedly been used in a hack-and-leak operation seeking to exacerbate Brexit-related political divisions in UK politics in 2022 (Figure 8). Notably, the style of the leak site was reminiscent of the 2016 DCLeaks campaign in the U.S. attributed to APT28.
KillNet and Other Pro-Russia Hacktivists • *Hybrid*	Mandiant is tracking multiple self-proclaimed hacktivist groups primarily conducting DDoS attacks and leaking compromised data in support of Russian interests. These groups claim to have targeted organizations spanning the government, financial services, telecommunications, transportation, and energy sectors in Europe, North America, and Asia; however, target selection and messaging suggests that the activity is primarily focused on the conflict in Ukraine. Relevant groups include KillNet, Anonymous Sudan, NoName057(16), JokerDNR/DPR, Beregini, FRwL_Team (aka "From Russia with Love"), and Moldova Leaks.
NAEBC and Other Pro-	Since October 2020, the inauthentic media organization called the Newsroom for American and European Based Citizens (NAEBC) has persistently attempted to

Russia IO • *IO*	influence U.S. audiences on issues related to U.S. politics and elections. In addition, Mandiant is tracking a variety of other pro-Russia IO campaigns, including RUsponder, Cyber Front Z, Secondary Infektion, and Doppelganger. Belarusian-linked Ghostwriter also frequently promotes pro-Russia narratives. Recent activity from these campaigns has been primarily focused on the war in Ukraine.
APT28 • *Intrusion* • *Hybrid* • *IO*	In 2016, GRU-linked APT28 compromised U.S. Democratic Party organization targets as well as the personal account of the Democratic presidential candidate's campaign chairman and orchestrated a leak campaign ahead of the 2016 U.S. Presidential election. Leaked materials were amplified using the "DC Leaks" persona.
UNC2589 and "Free Civilian" • *Intrusion* • *Hybrid* • *IO*	Mandiant assesses that UNC2589 conducted intelligence collection and destructive attacks against Ukrainian targets ahead of the 2022 Russian invasion, as well as defacements of Ukrainian government websites in 2022 and 2023, claiming credit under false hacktivist persona "Free Civilian." This cluster is worth monitoring for its potential to threaten global election related organizations and history of conducting destructive attacks combined with hacktivist style tactics.
UNC5101 • *Intrusion* • *Hybrid* • *IO*	In addition to traditional cyber espionage against political targets in Europe, Palestinian Territories, and the United States, Mandiant has seen UNC5101 conduct information operations using spoofed Ukrainian government domains and letterhead to disseminate false narratives directly to inboxes of Ukrainian government employees. Ahead of Russia's September 2023 elections, Mandiant also observed this actor register domains referring to jailed Russian opposition politician Alexei Navalny and his "smart voting" application used to promote candidates with the best odds of defeating those backed by the Kremlin and the United Russia Party. Ahead of Russia's March 2024 presidential election, Mandiant identified UNC5101 domain registrations and a likely associated IO campaign attempting to deceive Russian opposition voters about the timing of a protest.
APT29 • *Intrusion*	Mandiant tracks frequent APT29 campaigns targeting diplomatic organizations globally, particularly in Europe and NATO member states. In the past 12 months, Mandiant has observed APT29 targeting technology companies and IT service providers in the United States and Europe, which is a potential risk to elections as APT29 has demonstrated a pattern of targeting these types of organizations to facilitate third party compromises of government and policy organizations. According to open sources, APT29 compromised the Democratic National Committee (DNC) ahead of the 2016 U.S. election.

Figure 8: UNC4057 leak website attempting to inflame public debate around Brexit

Iran

Mandiant assesses with moderate confidence that the risk of Iranian cyber espionage and cyber-enabled influence campaigns will rise as elections approach in key nations of interest to the Islamic Republic, such as counterparts in the currently stalled nuclear negotiations, and countries offering support to Israel during current fighting in Gaza. Past Iranian activity targeting elections has primarily focused on the U.S., and has involved intrusion activity as well as online narrative promotion, claimed data leaks, and attempted voter intimidation. However, observations suggest that Iranian cyber threat groups are currently focused on domestic surveillance, the Gaza conflict, and Iranian opposition organization People's Mojahedin of Iran (MEK), potentially reducing the likelihood of large-scale attempts to interfere with global elections in 2024.

APT42 • *Intrusion*	Throughout 2023, Mandiant identified domains spoofing U.S. media organizations and think tanks that exhibit similarities to APT42 infrastructure naming and registration patterns for credential harvesting operations. The Iranian APT group TAG tracks as CALANQUE - which has significant overlaps with APT42 - was behind publicly reported attempts in 2020 to compromise email accounts belonging to U.S. presidential campaign staff. Microsoft reported similar activity.

UNC2448 • *Intrusion* • *Hybrid*	In 2022, the U.S. indicted threat actors it accused of conducting ransomware operations in the United States, United Kingdom, Israel, and elsewhere. Joint reporting from U.S., UK, Canadian, and Australian officials and U.S. sanctions linked the indicted individuals to the Islamic Revolutionary Guard Corps (IRGC) and highlighted that they also pursue a cyber espionage mission. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) disclosed that an Iranian threat actor Mandiant tracks as UNC2448 exploited the Log4Shell vulnerability (CVE-2021-44228) to compromise a Federal Civilian Executive Branch (FECB) organization in 2022.
UNC757 • *Intrusion* • *Hybrid*	In September 2020, CISA disclosed that UNC757 targeted U.S. federal agencies, exploiting VPN vulnerabilities and installing web shells. Mandiant tracked similar activity through late 2019 and early 2020. In April 2023, the head of U.S. Cyber Command's Cyber National Mission Force, disclosed that UNC757 had successfully gained access to a U.S. city website used to report election results during the 2020 election. This access could have been used to stage a defacement reporting false election results, though reporting indicates that Cyber Command removed the attackers' access before any additional activity took place.
Pro-Iran Hacktivist Personas • *Hybrid* • *IO*	Mandiant is tracking several threat actor personas that claim to be conducting hacktivist or cyber criminal operations, such as hack-and-leak activity or ostensible ransomware encryption resulting in data destruction. Mandiant notes that messaging and target selection for these personas often aligns with Iranian strategic interests. According to U.S. officials, many of the most significant pro-Iran disruptive or hack-and-leak incidents from the past several years can be linked back to Iranian company Emennet Pasargad, which TAG tracks as MARNANBRIDGE, including efforts to disrupt the 2020 U.S. election, as previously described. In November 2022, open sources reported that an additional persona, "Al-Toufan," defaced Bahraini government websites ahead of the nation's general elections.

Pro-Iran IO • *IO*	Mandiant tracks a number of notable pro-Iran influence campaigns (e.g., Liberty Front Press (LFP), Roaming Mayfly, and Endless Mayfly), and Mandiant has observed these campaigns target audiences globally and leverage wide-ranging TTPs. Influence infrastructure used in operations attributed to these campaigns most frequently relied on Arabic-language assets and targeted countries within Iran's sphere of influence. Mandiant has observed pro-Iran influence campaigns impersonating voters and officials and promoting partisan content during past U.S. elections, though we also note the use of websites and networks of social media accounts focused on the UK, India, and Indonesia used to promote narratives in line with Iranian interests. Recurring themes promoted by these campaigns amplify both anti-U.S. and anti-Israel narratives.

China

Mandiant expects PRC state-sponsored intrusions to focus on election-related targets for intelligence collection while pro-PRC influence operations generally praise China and undermine its adversaries. Mandiant has seen pro-China information operations campaigns carry out election-related activity in the U.S., Taiwan, and Hong Kong. These campaigns used AI-generated imagery and video content, and used increasingly nuanced tactics, such as posing as legitimate organizations or real individuals, to target and engage authentic users with some success. A segment of their activity appears to have increased audience engagement in the form of comments, likes, and/or shares from seemingly authentic accounts. As of the time of writing, Mandiant has not observed Chinese state-sponsored actors combine intrusion activity with information operations, though we have observed pro-PRC actors using falsified allegedly leaked materials to drive campaigns.

Observed Activity Surrounding the January 2024 Taiwanese Election

- **Cyber Espionage:** Mandiant observed TEMP.Hex and other PRC cyber espionage actors target Taiwanese organizations in the education, technology, government, and telecommunications sectors in the weeks leading up to and following Taiwan’s January 2024 election. In late summer, TAG tracked multiple PRC APT phishing campaigns targeting members of all three political parties, the TPP, the DPP, and the KMT. More broadly, TAG noted a substantial increase in Chinese cyber espionage targeting of Taiwan in 2023 compared to 2022.
- **Information Operations:** In the days surrounding the 2024 Taiwan presidential election held on Jan. 13, 2024, Mandiant observed an influx of pro-PRC information operations (IO) activity promoting a wide variety of narratives pertaining to the election. Mandiant identified three notable operations that leveraged seeded content and/or purportedly leaked information to promote narratives containing ad hominem attacks against outgoing President Tsai Ing-wen and President-elect Lai Ching-te. Allegedly leaked materials included a dubious DNA report purportedly providing evidence supporting the narrative that Lai has an illegitimate child and documents and audio recordings cited in a video as purported evidence supporting the claim that Lai had worked as a government informant, spying on DPP officials. We have not independently validated the authenticity of the allegedly leaked information; however, multiple sources,

including official statements and credible media reports, indicate that the various alleged "leaked" information is likely false.

TEMP.Hex • *Intrusion*	Prolific TEMP.Hex activity targeting governments, think tanks, and foreign affairs organizations across Asia, Europe, North America, Oceania, the Middle East, and Africa likely seeks intelligence to support China's political and economic interests. In August 2023, Mandiant identified a likely TEMP.Hex phishing operation using a Taiwanese presidential-themed lure to deliver a malicious Microsoft Windows Installer (MSI) file that, when executed, delivered the SOGU.SEC backdoor. In March 2023, Mandiant identified suspected TEMP.Hex phishing activity using lure documents named "Myan-Russia" and "General election" to deliver BROWNSPARK to targets in Southeast Asia. It is possible that the election-themed lures were referencing proposed plans to hold elections in Myanmar for the first time in decades.
APT41 • *Intrusion*	APT41 conducted large-scale vulnerability exploitation and scanning activity that compromised U.S. government organizations ahead of the 2020 and 2022 U.S. election cycles.
APT31 • *Intrusion*	In March 2024, the UK disclosed that APT31 "almost certainly" conducted reconnaissance against email accounts of UK parliamentarians in 2021. The U.S. DOJ likewise described APT31 activity targeting politicians. UK officials also announced that unspecified PRC threat actors compromised the UK electoral commission from 2021 to 2022, likely exfiltrating Electoral Register and email data. Proofpoint described phishing activity targeting U.S.-based journalists focused on politics and national security throughout 2021 and 2022, often posing as journalists to conduct this activity. Mandiant tracks the group referenced in the report as APT31. In 2021, Finnish officials indicated that APT31 targeted its parliament in 2020. Google TAG reported that APT31 targeted U.S. President Biden's campaign staff during the 2020 U.S. election. In the March 2024 indictment, the U.S. DOJ confirms that APT31 targeted election campaign staff from both major parties in 2020.
APT40 • *Intrusion*	New Zealand announced in March 2024 that APT40 compromised its Parliamentary Counsel Office and Parliamentary Services in 2021. Mandiant assesses with high confidence that APT40 compromised the website of Cambodia's National Election Commission in mid-2018 based on the use of AIRBREAK malware, overlaps with previously identified infrastructure, and consistent targeting. Cambodia's July 2018 elections likely served as the major driver for this campaign as Cambodia supports

	Beijing in South China Sea disputes and construction of the Belt and Road Initiative (BRI).
UNC3658 • *Intrusion*	From March to May 2022, Mandiant identified multiple examples of election-themed lure material leveraged against the Philippine Government ahead of its May elections, including "Risk Factors on National and Local Elections 2022.docx" and "CSAFP'S_GUIDANCE_RE_NATIONAL_AND_LOCAL_ELECTION_2022_NLE .docx." The timing of this activity, which took place prior to the May 2022 general election in the Philippines, may indicate specific interest in election-related information. It is also possible that the threat actors sought to take advantage of general interest in the election to support other collection objectives.
UNC4713 • *Intrusion*	UNC4713 targeted attendees of the 2023 G7 summit in Hiroshima with spear phishing messages. The campaign used a compromised Indonesian Ministry of Foreign Affairs G20 account to send the phishing messages. Recipients included individuals from Australia, Canada, India, Italy, Singapore, and the UK. While this targeting is not election specific, it represents recent interest and capacity to target government organizations in a number of countries holding elections in 2024.
Pro-PRC Influence Campaign (DRAGONBRIDGE) • *IO*	In addition to a regular cadence of DRAGONBRIDGE pro-PRC IO activity promoting diverse narratives regarding global politics, news events, and issues concerning the domestic and foreign affairs of various countries and regions, Mandiant has observed narrative promotion specifically targeting 2024 elections in Taiwan (Figure 9) and the U.S.
Pro-PRC IO Campaign (HaiEnergy) • *IO*	Pro-PRC IO campaign HaiEnergy-promoted articles frequently criticize U.S. foreign policy, U.S. politicians, and highlight purported examples of domestic friction, such as ethnic or gender inequality. Content also praises PRC policies. In December 2023, Mandiant observed HaiEnergy promote articles critical of Taiwanese Presidential candidate Lai, describing him as lacking political acumen and the DPP as plagued by internal conflicts and a series of scandals. HaiEnergy assets also promoted narratives positively portraying electoral changes implemented by the PRC in Hong Kong ahead of the district council election in December 2023.
Pro-PRC influence campaign (Fictitious Brands)	Mandiant identified a pro-PRC IO campaign that we assess with high confidence is promoting content pertaining to the U.S., Tibet, and India in support of the PRC. This campaign consists primarily of clusters of X (formerly Twitter) accounts that pose as independent media outlets, research institutions, or social organizations that

• *IO*	we judge to be fictitious brands, and an amplifier network. The U.S.-focused accounts posted ideologically inconsistent partisan content copied from other users, including posts attempting to initiate “follow trains”, boost follower counts, and foster engagement. The "U News" fictitious brand account reposted a TikTok video showing a "deepfake" of U.S. actor Morgan Freeman criticizing U.S. President Joe Biden.

Figure 9: Sample Posts by DRAGONBRIDGE Accounts Targeting the 2024 Taiwan Presidential Election with Chinese-Language Posts Attempting to Discourage Taiwanese Citizens from Voting for the DPP

North Korea

Prior to the April 10, 2024 election, **Mandiant forecast that Democratic People’s Republic of Korea (DPRK) government-affiliated actors** would conduct campaigns to collect relevant intelligence from South Korean government organizations, political parties, and technology and manufacturing firms around the 2024 South Korean legislative election. In early 2024, Mandiant tracked operations associated with several North Korean threat groups targeting South Korean civil society and nonprofits, media entities, and other organizations.

APT43 • *Intrusion*	Prior to the March 2022 South Korean presidential election, Mandiant identified samples of GOLDDRAGON.POWERSHELL that we attribute to APT43. This activity appears to be consistent with South Korean media reporting describing an increase in North Korean cyber threat activity targeting security, defense, and diplomacy experts in February 2022. Similarly, Mandiant uncovered a spear-phishing campaign targeting South Korea-based media organizations, Korean webmail portals, and international non-governmental organizations (NGOs) promoting democracy from late March to early April 2020, immediately preceding the April 2020 South Korean legislative election.

Conclusion

Impacts to elections are not a foregone conclusion. Many of the aforementioned actors have struggled to influence or achieve significant effects, despite their best efforts. Wary and experienced defenders and populations are harder targets and without the element of surprise adversaries will be at a disadvantage.

Within Google, we are blending different perspectives on the threat landscape across TAG, Mandiant, VirusTotal, Google Cloud, and Trust & Safety. And we're sharing information about intelligence, insights, and the action we're taking with the security community and broader public through a variety of fora, such as our Google Safety Engineering Centers, Mandiant reporting, and the quarterly TAG Bulletin on the coordinated influence operation campaigns that Google disrupts.

Additional tools and resources

For mitigation and hardening recommendations, please review the following:

- How to Understand and Action Mandiant's Intelligence on Information Operations blog post
- Proactive Preparation and Hardening to Protect Against Destructive Attacks white paper
- Linux Endpoint Hardening to Protect Against Malware and Destructive Attacks white paper
- Distributed Denial of Service (DDoS) Protection Recommendations white paper

Google offers a suite of free of cost tools to help protect high-risk users from the most pervasive digital attacks, to which politicians, journalists, and campaigns are often most vulnerable. Examples include protecting accounts from targeted attacks with Advanced Protection Program and safeguarding campaign websites from DDoS attacks with Project Shield. Review these linked blog posts for more specifics on how Google is supporting the U.S., Indian, and EU elections this year.

Posted in

- Threat Intelligence
- Security & Identity
