THREAT ANALYSIS

Recorded Future®

By Insikt Group®

December 14, 2023

Aggressive Malign Influence Threatens to Shape US 2024 Elections

Executive Summary

Russia, China, Iran, domestic violent extremists (DVEs), and hacktivist groups will very likely conduct influence operations at varying levels of magnitude and sophistication to shape or disrupt the United States (US) 2024 elections in pursuit of strategic geopolitical goals. The global backdrop of Russia's continued war against Ukraine, Israel's developing conflict with Iran-supported Hamas, China's increasing assertiveness with regard to Taiwan, and the ongoing controversy surrounding content moderation on social media platforms provides a dynamic threat landscape favoring influence actors seeking to aggressively target the 2024 US elections.

Based upon analysis of the influence objectives and tactical to strategic geopolitical goals of Russia, China, Iran, DVEs, and hacktivists, we identified 3 overarching thematic influence trends threatening the 2024 US elections: 1) Increasing polarization and undermining confidence in US democratic institutions; 2) Reducing US domestic support for providing military and financial aid to US allies; and 3) Undermining political candidates projecting unfavorable policies respective to a threat actor's sponsor while promoting candidates projecting favorable policies. Influence operations conducted during the 2024 US elections are forecasted to include historical and innovative influence tactics and techniques, ranging from increased cyber-enabled influence operations to the continued integration of generative artificial intelligence (AI) capabilities.

False and manipulated information propagated by state and non-state influence actors has the potential to influence voter behavior leading into, during, and after the elections and subsequently affect which candidates are elected and their corresponding political stances on a wide range of international and domestic issues. Regardless of an influence actor's ultimate objectives, influence activities related to an election do not need to be successful in order to have a damaging impact on the public's trust in democratic institutions and the integrity of the electoral process. Furthermore, while advanced influence actors will very likely conduct pre-planned strategic influence operations, they will very likely opportunistically leverage official announcements, events, and public statements by prominent US political figures, media personalities, celebrities, and US-based organizations operating at the nexus of controversial political topics in tactical influence operations in pursuit of their objectives.

A continued whole-of-government approach integrated with private industry, including social media organizations, to publicly identify, announce, and refute false information related to the elections will likely reduce the effectiveness of attempted malign influence activities seeking to persuade US voters. Effective prebunking, for example, is one such method to enable the general public to discern credible information and identify deceptive strategies malign influence actors use to potentially influence voting behavior. Additionally, the awareness of government officials, public figures, and business executives regarding false information surrounding the elections, self-assessment of the likelihood of being targeted, and pre-planned playbooks and responses will reduce the risk of false information multiplying across broad audiences and mitigate any potential negative impact on key risk categories. Such risk categories may include but are not limited to personal and organizational brand reputation and competitive disadvantage caused by influence activities such as manufactured misperceptions.

Key Findings

- Russia will almost certainly conduct malign influence to shape or disrupt the 2024 US elections, based on an established precedent of past malign influence in US election cycles, a long-term strategy to favorably reshape US policy toward Russia and erode support for liberal democracies, and a heightened geopolitical motivation to undermine the US in revenge for its support to Ukraine.
- China will very likely conduct malign influence to shape the 2024 US election, although it is unlikely to engage in disruptive activities that may result in a negative impact on its own image worldwide. Recent acceleration of covert influence operations targeting the US government and convergence with Russian narratives likely indicates a stronger appetite for malign influence seeking to shape various upcoming elections internationally, and targeting of the 2024 US elections will almost certainly focus on influencing the future US administration's policy on Taiwan.
- Iranian state-sponsored influence actors will very likely conduct malign influence seeking to shape the 2024 US elections based on Iran's increase in conducting cyber-enabled influence operations, historical efforts to affect the 2018, 2020, and 2022 US elections, and Iran's recent political response to Israel's developing conflict with Iran-supported Hamas.
- Instances of US DVEs physically attacking and threatening election personnel, officials, or infrastructure are very likely. Furthermore, during the past year, DVEs have rebroadcast several state-sponsored malign influence operations that align with their ideological goals and have produced narratives and content that has been cited in foreign malign influence operations — likely creating a feedback loop between DVE and state-sponsored influence operations.
- False information surrounding US-deployed voting technologies and corresponding voting systems manufacturers (VSMs) originating from US domestic sources on alternate media websites and social media platforms will almost certainly increase as the 2024 US elections approach.

Russia

Russia will almost certainly conduct malign influence seeking to shape or disrupt the 2024 US elections.[1] Russia has demonstrated an established precedent to conduct malign influence against major US elections (2016, 2018, 2020, and 2022) and the elections of multiple European democracies (for example, Estonia, France, Germany, and the United Kingdom [UK]). Russian targeting of Western elections and the processes of liberal democracies can be further traced back to the era of the Soviet Union and the Cold War through Russia's Active Measures (активные мероприятия) doctrine. Russian malign influence extends beyond major election cycles, seeking to shape public opinion, sow discord, and advance Russia's long-term geopolitical objectives.

Furthermore, Russia has greater geopolitical motivations to conduct malign influence during the 2024 US elections than in previous years. Russian malign influence during the 2024 US elections will almost certainly be a form of revenge against the US in response to its continued support of Ukraine and its position as a leader of the diplomatic and economic isolation of Russia. Moreover, the Kremlin is very likely factoring the results of the 2024 US elections into its long-term Ukraine war strategy in the hope that a change in US political leadership will reduce military and financial support to Ukraine and thereby favorably benefit Russia's battlefield prospects and improve its negotiation position. As such, Russian malign influence will very likely seek to erode domestic support for Ukraine and support US political candidates with a more favorable policy stance toward Russia.

Russia's Assessed Influence Objectives

Russia will almost certainly conduct malign influence during the 2024 US elections in support of influence objectives that are aligned with Russia's strategic geopolitical goals. Likely influence objectives and corresponding malign narratives include those described below.

Degrade US domestic support of military and financial aid to Ukraine in support of Russia's war against Ukraine. We previously tracked Kremlin officials and Russian state media suggesting the West was prioritizing Ukraine ahead of the needs of its citizens, with the war directly contributing to the high cost of living and Western economic downturn. Russian sources have further alleged that US aid to Ukraine had been mismanaged, wasted, or illicitly transferred to malign non-state actors via black-market sources, including Hamas.[2] [3] [4] Further, according to Meta's Q2 2023 Adversarial Threat Report, a malign influence network linked to Russia known as Doppelganger, very likely tasked with eroding international support for Ukraine, had expanded to the US, spoofing US mainstream media entities. October 2023 reporting indicates that the Doppelganger network remains highly active; Insikt Group continues to track the network.

[1] Insikt Group defines malign influence as effort undertaken by, at the direction of, on behalf of, or with the substantial support of, a government with the objective of influencing, through overt or covert means: (A) the political, military, economic, or other policies or activities of a sovereign government, including any election within a sovereign nation; or (B) the public opinion within a sovereign nation.
[2] *https://sputnikglobe[.]com/20231009/russia-warned-about-us-weapons-for-ukraine-ending-on-black-market-months-before-bloodbath-in-israel-1114040821.html*
[3] *https://ria[.]ru/20231008/oruzhie-1901335978.html*
[4] *https://ria[.]ru/20231008/izrail-1901282406.html*

Reduce US domestic support of US security commitments to NATO and regional security commitments in Eastern Europe and the Middle East to undermine US global standing, ensure the regional spheres of influence of Russia and its allies, and promote a multipolarity challenge to rules-based international order. Further, the Foundation to Battle Injustice (FBR), a malign influence outlet once financed by the recently deceased Russian oligarch Yevgeny Prigozhin, continues publishing content in English disparaging the NATO alliance and the Ukrainian government.[5]

Exploit socio-political divisions, exacerbate political polarization, and undermine public confidence in the democratic process to damage the US's domestic cohesion and the US's standing internationally, undermining the appeal of liberal democracies worldwide that are viewed as anti-Russian. Russian malign influence in prior US election cycles exploited key wedge issues, including racial equality, American patriotism, gun control, and immigration, to expose US divisions and stoke US domestic tensions. In 2022, Insikt Group and Graphika (2) reported that persistent Internet Research Agency (IRA)-linked malign influence assets attempted to stoke US domestic tensions by provoking allegations of election fraud through inauthentic personas on alternative social media platforms and with a covert website dedicated to "election truth". Aside from publishing negative content associated with NATO and Ukraine, FBR, for example, continues to publish content critical of the US justice system, law enforcement, and political persecution.

Support and promote policies and political candidates that are aligned with Russian interests in direct support of Russia's geopolitical priorities, such as its war against Ukraine and its quest for multipolarity. In previous US election cycles, Russian influence actors reportedly supported 2016 Green Party presidential candidate Jill Stein to draw support away from Hillary Clinton, and in both 2016 and 2020, supported the candidacy of former president Donald Trump. Russian malign influence will very likely support US political candidates with more favorable policy stances aligned with Russian interests discussed above while undermining and denigrating support for candidates with unfavorable positions. Declassified US intelligence reporting in August 2023 indicated that the Russian Federal Security Service (FSB) leveraged independent organizations inside the US, such as Creative Diplomacy, to promote pro-Russian propaganda and groom rising, young socio-political leaders into future pro-Kremlin supporters. In 2024, Russian intelligence services will very likely continue attempting to cultivate emerging American political leaders as assets to slowly shift US policy into alignment with long-term Russian geopolitical goals.

Russia's Malign Influence TTPs

Russia will likely employ a selection of the following tactics, techniques, and procedures (TTPs) in conducting malign influence during the 2024 US elections, based on observed capabilities from past Russian influence operations.

[5] *https://fondfbr[.]ru/en/articles/nato-crimes-en/*

Use of state-owned media: Russian state media, including RT and Sputnik News, commonly covers a multitude of political, social, and economic pain points exclusively with the purpose of disparaging the US. Russian state media produces charged and sensationalist headlines and articles focused on racism, gender inequality, poverty and homelessness, gun violence, drug abuse, and more with the intent of sowing discord and deepening US political divisions.

Leveraging generative AI: Russian state media sources and pro-Russian threat actors have demonstrated creativity in using generative AI for influence purposes and are very likely to continue doing so. For example, in September 2020, RT published a deepfake parody video imagining former US president Donald Trump as an employee at RT if he were to lose the 2020 election.[6] In March 2022, Russia-aligned threat actors successfully defaced several Ukrainian websites with a low-tier deepfake of Ukrainian President Volodymyr Zelensky urging Ukrainians to surrender to Russian forces. Ukrainian media and President Zelensky quickly debunked the deepfake upon publication. In June 2023, RT produced a deepfake video mocking US president Joe Biden, UK prime minister Rishi Sunak, and other Western leaders in their efforts to impose an eleventh sanctions package on Russia.[7]

***Figure 1**: Screenshot of RT's parody video "The 11th Package of Anti-Russian Sanctions Challenge" featuring a deepfake of US president Joe Biden (Source: RT[8])*

Use of covert Russian intelligence-directed news websites, and use of other low-tier news websites: The US government has suspected Russian intelligence services, including the Foreign Intelligence Service (SVR) and the Federal Security Service (FSB), of providing taskings and other direction to multiple online publications, including News Front, South Front, and Strategic Culture Foundation. Russian security services are also suspected of laundering pro-Kremlin malign influence narratives through fringe websites such as The Grayzone and Zero Hedge to obfuscate attribution.

[6] *https://www.rt[.]com/news/501369-donald-trump-rt-deep-fake/*
[7] *https://www.rt[.]com/rt-promo-2022-en/#sanctions*
[8] *https://www.rt[.]com/rt-promo-2022-en/#sanctions*

Inauthentic personas and networks of coordinated inauthentic behavior (CIB): Historically, Prigozhin and his troll farm, the Internet Research Agency (IRA), Lahkta Internet Research, [LIR]), and pseudo-legitimate news organizations the Federal News Agency (RIA FAN) and his Patriot Media Group, were key sources of inauthentic personas and CIB targeting major US elections.[9] Though these entities reportedly shut down after Prigozhin's armed uprising, the once Prigozhin-financed organization FBR — led by Mira Terada since July 2021 and now financed through "private donations from Russian citizens" — remains active as of November 2023.[10] Further, Prigozhin's suspected assassination in August 2023 very likely leaves a leadership vacuum in Russia's global covert influence operations network. Other Kremlin-aligned entities ranging from private firms to Russian intelligence services, and entities connected to Russian state media, have and almost certainly continue to pursue malign influence through inauthentic personas at scale. According to Meta's Q2 2023 analysis of the Doppelganger CIB network, for example, the network was the "largest" and "most aggressively persistent" malign network from Russia observed by Meta since its takedowns of assets attributed to the IRA in 2017 and 2018. Meta's analysis previously attributed Doppelganger to 2 Russian companies, Structura National Technologies and Social Design Agency. Social Design Agency's notable clients include several Russian government ministries as well as multiple local and regional governments inside Russia.[11]

Cyber-enabled influence operations: In 2015 and 2016, Russian cyber threat actors linked to Russian intelligence services, such as APT28 and APT29, conducted targeted intrusions to obtain sensitive information from the Democratic Congressional Campaign Committee (DCCC), the Democratic National Committee (DNC), and the staff of Hillary Clinton's presidential campaign in the hope of harming Clinton's candidacy. As part of hack-and-leak operations, Russian cyber threat actors have planted forgeries containing disinformation alongside authentic documents to damage a political candidacy, create rifts in political movements, or discredit a target.

Weaponizing the perception of interference as influence: During the 2022 US election cycle, pro-Russian hacktivist personas, such as Killnet and Cyber Army of Russia Reborn, claimed responsibility for targeting US and state government websites, in addition to the Democratic Party's official website. Though these campaigns had a negligible impact on government operations and the US election process, the attacks and the publicity that followed were themselves elements of Russian influence operations aimed at creating the impression that Russia was successfully interfering in US elections and that the US failed to ensure the integrity of its election systems. Attempted interference, therefore, does not need to be successful to have a damaging impact on the trust of democratic institutions and the integrity of the electoral process. We expect Russia to amplify news or discovery of attempted intrusions into election systems and political organizations in order to further erode public confidence in the integrity of the vote.

[9] Meta defines coordinated inauthentic behavior (CIB) as "coordinated efforts to manipulate public debate for a strategic goal where fake accounts are central to the operation".
[10] *https://fondfbr[.]ru/en/english/*
[11] *https://sp-agency[.]ru/clients/*

China

China will very likely conduct malign influence seeking to shape the 2024 US elections. China has repeatedly demonstrated its capability and will to conduct malign influence operations targeting elections and referendums. While varied in intensity and scale, examples include the 2018 Taiwan municipal elections, the 2020 Taiwanese elections, the 2021 Canadian elections, the 2022 US midterms, the 2023 Canadian by-elections, and the 2023 Australian Indigenous Voice referendum. China has also demonstrated its intent to conduct large-scale covert influence operations in pursuit of other geopolitical priorities, including targeting US allies (such as the UK and Australia), private companies, and critics of the Chinese Communist Party (CCP) (including NGOs and exiled dissidents).

Furthermore, China's influence efforts targeting Taiwan and the US will likely increase, given that the CCP considers Taiwan "the core of [China's] core interests" and recent major developments in cross-strait relations. These developments include former Speaker of the US House of Representatives Nancy Pelosi's watershed visit to Taiwan in August 2022, followed by Taiwan President Tsai Ing-Wen's stopover in the US in April 2023, and finally, Taiwan vice president William Lai's visit to the US coupled with the approval of the first transfer of US military equipment to Taiwan in August 2023. Additionally, China is very likely aiming to "be ready by 2027" for a potential invasion of Taiwan in case the CCP decides an invasion is necessary at that time or at a later date. Notably, 2027 falls within the next US administration's mandate. These developments support the assessment that China will very likely conduct malign influence during the 2024 US elections, likely with the Taiwan issue in mind.

China's Assessed Influence Objectives

China will very likely conduct malign influence during the 2024 US elections in support of influence objectives that are aligned with China's strategic geopolitical goals. Likely influence objectives and corresponding malign narratives are described below.

Weakening US domestic support for foreign military aid to Taiwan in support of China's geopolitical goal to preserve what it views as its sovereignty and territorial integrity. Influence narratives will likely draw comparisons to other regions benefiting from US military aid, such as Ukraine — Chinese state media has already referred to Taiwan as a potential "second Ukraine". Covert networks hijacking the Hawaii wildfires in August 2023 also attempted to blame the US government for spending disproportionately on the US military rather than disaster relief.

Shaping the next administration by targeting CCP critics and unfriendly political leaders, specifically political leaders demonstrating support for adversaries of the CCP, such as Taiwan and Uyghur dissidents. This is likely in support of China's geopolitical objectives to defend its global reputation and pursue its interests by promoting China-friendly political leaders in foreign governments. Recent examples include covert influence operations targeting Nancy Pelosi and Tsai Ing-Wen during Pelosi's visit to Taiwan in August 2022 and Liz Truss in September 2022 (who condemned China's response to Pelosi's visit). In August 2023, the Canadian government also reported on a coordinated campaign on

WeChat targeting Canadian member of Parliament Michael Chong in May 2023, almost certainly as a result of the politician's longstanding criticism of the CCP's treatment of Uyghurs. China has also been accused of conducting intelligence operations aiming to groom China-friendly candidates in the US, EU, Canada, and the UK.

Sowing division and highlighting failures of the US democratic process by exploiting wedge issues in US politics, such as gun control and racial discrimination, in support of China's broader narrative war on democracy. For example, a February 2023 statement by the Ministry of Foreign Affairs (MFA) titled "Gun Violence in the United States: Truth and Facts" points to "how the U.S. political system is designed and operates" as the "root cause" for the domestic divide on gun control. Recent Chinese malign influence undermining democratic processes includes attempted voter suppression by covert networks during the 2022 US midterm elections.

Undermining the Biden administration's legitimacy by highlighting domestic and foreign policy failures, in support of China's geopolitical goal to challenge a US-led "unipolar" world as well as its security and economic interests. Influence efforts will also likely focus on the administration's failure to act on wedge issues mentioned above as a means to erode support for the incumbent administration during the 2024 elections. A recent Empire Dragon influence operation identified by Insikt Group in October 2023 found the network spreading narratives highlighting the Biden administration's failure to curb homelessness and the opioid crisis in cities like San Francisco and Los Angeles. Chinese media have also highlighted the Israel-Hamas conflict as a recent foreign policy failure undermining the US's "unipolar push".

Throughout this process, China will likely seek to target both English speakers as well as Chinese-speaking diaspora communities located in the US, the latter of which are likely being targeted to divide diaspora communities from host countries. China will also likely continue secondary influence objectives, such as promoting itself as a legitimate superpower, in line with its objectives to move "toward the world's center stage".

China's Malign Influence TTPs

China will likely employ a selection of the following TTPs in conducting malign influence during the 2024 US elections, based on observed capabilities from past Chinese influence operations.

Coordinated Overt Sources: Content disseminated directly from official CCP sources is coordinated with secondary sources, such as diplomatic social media accounts and state-owned media. Insikt Group has observed instances of this tactic being used to target the US government. On February 9, 2023, the MFA released a statement titled "Drug Abuse in the United States", blaming the US government for failing to "raise public awareness of the harm of narcotic drugs". The statement was amplified on the same day and at regular intervals for the following weeks by state-owned media outlets and Chinese diplomatic social media accounts, effectively extending the content's presence on social media until the end of February 2023.

Covert Networks Supporting Overt Sources: Covert networks like Empire Dragon directly amplify narratives pushed by the Chinese government. For example, Chinese state media's permanent recycling of the Snowden and Shadow Broker leaks and public attribution of cyberattacks on Chinese infrastructure to the US National Security Agency led to a flooding of Western social media platforms by inauthentic Empire Dragon accounts, further extending the reach of Chinese state media outside of the mainland.

Covert Networks Conducting Large-Scale Operations: Covert networks like Empire Dragon (very likely overlapping with Spamouflage Dragon and DRAGONBRIDGE) have conducted some of the "largest ever" covert influence operations observed by social media platforms in recent years. In addition to observing CIB over hundreds of sources in over 20 languages, Insikt Group has also noted a pivot from long-standing strategic influence operations to shorter, high-volume, tactical operations in response to world events and publications of reports by CCP critics. Furthermore, Chinese covert influence operations have begun employing narratives converging with Russian influence operations, such as blaming the US for the Nordstream pipeline sabotage and funding biolabs in Ukraine.

Iran

Iran will very likely conduct malign influence seeking to shape the 2024 US elections. Iran has demonstrated its intent to conduct malign influence against the 2024 US elections based on historically observed influence activity specifically targeting US elections, as well as a recent increase in demonstrating the operational capability to conduct cyber-enabled influence operations. During the 2018, 2020, and 2022 US elections, Iran conducted a variety of influence operations targeting US voters. Additionally, since June 2022, there has been an observed increase in Iranian state-sponsored cyber-enabled influence operations.

Furthermore, recent geopolitical events and Iran's domestic affairs support the assessment that Iran will very likely conduct malign influence against the 2024 US elections. Geopolitically, these events include increased US military support to Israel after the August 7, 2023, attack by Hamas and the recent pause by the US and Qatar on transferring $6 billion dollars to Iran, which was part of a previously negotiated prisoner exchange. Domestically, Iran continues to allege the US and other Western countries incited mass protests that occurred within Iran following the death of Mahsa Amini in September 2022. These geopolitical and domestic events, combined with Iran's continuation of its ongoing "Soft War" (نرم جنگ), focused on shielding the Islamic Republic from external cultural, political, and societal influences, increases the likelihood Iran will conduct malign influence operations against the 2024 US elections.[12]

Iran's Assessed Influence Objectives

Iran will very likely conduct malign influence during the 2024 US elections in support of influence objectives that are aligned with Iran's strategic geopolitical goals. Likely influence objectives and corresponding malign narratives are described below.

[12] *https://www.sid[.]ir/fa/journal/ViewPaper.aspx?ID=463413*

Decrease US citizens' approval of providing Israel with US military and financial aid in support of Iran's geopolitical goal to strengthen its relationships with neighbors and allies to offset the West. Example malign narratives may include themes such as alleging that politicians who support Israel are complicit in alleged war crimes and that providing support to Israel is akin to supporting the oppression of Palestinians.[13] [14]

Increase US domestic social polarization in support of Iran's geopolitical goal to preserve, advance, and export its own Islamic revolutionary belief system. Example malign narratives may include themes such as "The US is on the brink of a civil war", "There is a growing divide between the American population", and "The US is on the decline as a world power".[15] As an example, the graphic below was originally published on the authoritative state-run website *khamenei[.]ir* with the title "evidence of America's decline on the eve of the new world order" and later posted on mainstream social media.[16]

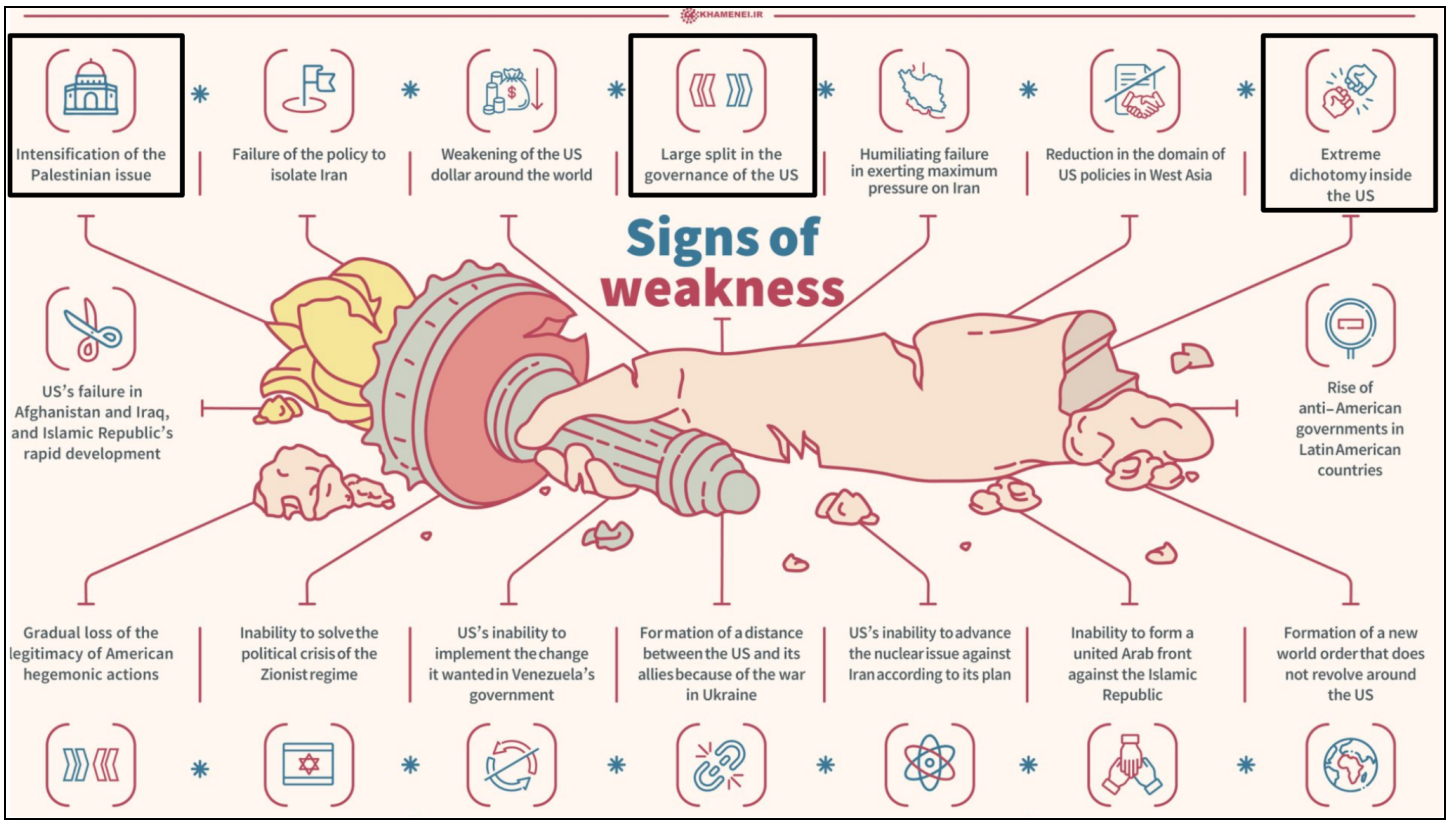

***Figure 2**: Screenshot of social media account @Khamenei_m post with superimposed black boxes highlighting overlapping themes with Iran's likely influence objectives during the 2024 US presidential election (Source: Social Media, khamenei[.]ir[17])*

[13] *https://english.khamenei[.]ir/news/10221/Definite-accomplice*
[14] *https://english.khamenei[.]ir/news/10228/Gaza-is-about-the-oppression-of-the-Palestinians-and-their-power*
[15] *https://www.presstv[.]ir/Detail/2023/08/17/709074/Indictment-Series-*
[16] *https://farsi.khamenei[.]ir/photo-print?id=53914*
[17] *https://farsi.khamenei[.]ir/photo-print?id=53914*

Iran's Malign Influence TTPs

Iran will likely employ a combination of the following TTPs in conducting malign influence during the 2024 US elections, based on observed capabilities associated with previously executed Iran state-sponsored influence operations and currently assessed motivations based on recent geopolitical and domestic events.

Use of state-owned media: Iran continues to utilize overt media outlets such as Press TV to publish content amplifying US political wedge issues. For example, in September 2023, Press TV published a series of episodes titled "Indictment series!" that focuses on former US president Donald Trump's ongoing legal procedures while simultaneously weaving in themes about "national civil war", "secession", and the "huge divide that has occurred across average Americans".[18]

Cyber-enabled deception operations: Throughout 2023 there has been an increase of operations attributed to Iran that generally involve an unknown group announcing and taking responsibility for an alleged cyberattack on social media; upon further investigation, the allegations that this cyberattack took place are later proven false. These deception operations, which almost certainly seek to exaggerate the psychological effects of a nonexistent cyberattack, will almost certainly provide a low-cost opportunity for Iran to conduct malign influence activities during the 2024 US elections.

Use of CIB networks to amplify influential content: Historically demonstrated TTPs observed during the 2016, 2020, and 2022 US elections include the use of CIB networks on social media, spreading both truthful information and disinformation via non-attributable news outlets with corresponding amplification networks on social media, and deceptive online engagement utilizing social engineering to impersonate or misattribute identity to ultimately deceive or incite conflict among US target audiences. Since June 2022, Iran has increasingly conducted cyber-enabled influence operations involving similar TTPs, layering offensive computer network operations with influence operations to achieve psychological effects.

Domestic Violent Extremists

DVEs very likely pose a physical risk to election personnel, officials, and infrastructure in advance of and during the 2024 US elections.[19] Based on DVE activities during previous US election cycles, it is very likely that there will be instances of DVE threat actors motivated by a variety of personal and political grievances — but especially those motivated by partisan animus — physically attacking, approaching, threatening, harassing, and conducting doxxing and swatting campaigns against election personnel, and to a lesser degree, against election infrastructure and facilities. The likely objectives of these activities are coercing the US election system towards their favored political outcome(s) through

[18] *https://www.presstv[.]ir/Detail/2023/08/17/709074/Indictment-Series-*

[19] The US Intelligence Community defines a domestic violent extremist as "an individual based and operating primarily in the United States without direction or inspiration from a foreign terrorist group or other foreign power and who seeks to further political or social goals wholly or in part through unlawful acts of force or violence. This assessment does not evaluate the actions of individuals engaged solely in activities protected by the First Amendment or other rights secured by the Constitution of the United States".

violence (or the threat thereof) and, more generally, sowing public distrust in the US election system and the US government.

DVEs will almost certainly continue rebroadcasting state-sponsored malign influence operations during the 2024 US elections that align with their ideological goals, likely magnifying their reach and credibility in segments of the US population. For instance, during the past year, DVE sources have promoted claims and content about salient political controversies — natural disasters, the Russia-Ukraine and Israel-Hamas conflicts, and US foreign aid programs — that Insikt Group has attributed to Russian, Chinese, Iranian, and other influence operations. In certain instances, state-sponsored actors have harvested DVE reactions to political events in the US and used them as evidence for their influence operations. This dynamic will likely apply to election mis- and disinformation, creating a feedback loop between specific state-sponsored and DVE efforts to undermine the 2024 US elections.

Based on previous election cycles, the following indicators and scenarios also likely heighten the risk of DVE violence and influence operations during the 2024 US elections:

- "Swing states", states and jurisdictions with highly contested elections, and jurisdictions with local or state ballot measures on controversial social and political issues (such as abortion, gun control, or LGBTQ+ issues) are more likely to face risks from DVEs. DVE groups on opposing sides of these issues are likely to demonstrate and counter-demonstrate outside of election facilities, which can escalate into violence and disruptions of election operations.
- Local and state-level election officials and other personnel are more likely to face threats and harassment from DVEs than their national-level counterparts. Compounding the threat, they often lack personal protection resources, mechanisms for reporting threats, and knowledge about personal and operational security.
- Extended election processes — including real or perceived delays in vote counting, recounts, reviews, audits, contested elections, or the refusal of a losing candidate to concede — are likely to increase DVE targeting of election infrastructure and personnel. These dynamics will also likely increase DVE influence campaigns centered around allegations of inefficiencies, fraud, and illegitimacy in the US electoral process.

Voting Technology (Voting Machines)

Mis- and disinformation targeting US-deployed voting technologies and corresponding VSMs will almost certainly increase as the 2024 US elections approach. News organizations and cybersecurity professionals will very likely continue to report legitimate concerns surrounding the security of US voting technology, which will provide malign influence actors a dynamic opportunity to amplify and exploit such content in support of malign narratives.[20] Concurrently, the implementation of the US Election Assistance Commission's (EAC) updated certification guidelines for voting machines, titled Voluntary Voting System Guidelines (VVSG) 2.0, took place on November 15, 2023. Under VVSG 2.0, voting systems currently certified under the previous VVSG 1.0 "will remain federally certified after

[20] *https://www.rt[.]com/news/574968-fox-dominion-lawsuit-settlement/*

November 15, 2023, and jurisdictions can continue using and purchasing those systems consistent with state or territorial laws and regulations". However, the National Association of State Election Directors (NASED) expressed concerns surrounding the implementation of VVSG 2.0 one year prior to a presidential election and the potential for the emergence of inaccurate claims about the eligibility of certain voting equipment that will be used during the 2024 US elections (specifically, the possibility of false allegations spreading that claim specific equipment cannot be used during the 2024 US elections under the pretext of mischaracterizing VVSG 2.0 and VVSG 1.0).

Separately, in April 2023, Fox Corporation and Fox News Network reached a settlement to pay $787.5 million to Dominion Voting Systems as the result of a defamation lawsuit that claimed Fox News projected false information about Dominion Voting Systems during the 2020 US presidential election. Similarly, Smartmatic continues its own defamation lawsuit with the same allegations against Fox Corporation and Fox News Network. The level of false information Insikt Group observed during the 2022 US midterm elections, the continuation of lawsuits, and concerns around false information related to the implementation of new certification guidelines suggest that well-known VSMs such as Dominion Voting Systems, Smartmatic, and Election Systems & Software will almost certainly face increased levels of false information surrounding electronic voting systems, voting machines, and various EAC-approved software and hardware leading into the 2024 US elections.

Consistent with narratives observed during the 2022 US midterm elections, throughout 2023, false information surrounding voting machines has originated primarily from US domestic sources on alternate media websites and social media platforms. Dynamic events continue to provide opportunities for the amplification of narratives related to the security of voting machines, exemplified by a September 17, 2023, post on *patriots[.]win* alleging that "the [MGM Resorts International] casino hack confirms electronic voting machines are susceptible to hacking and manipulation". Other historically consistent narratives persist, such as claims that "voting machines are vulnerable to vote switching". An emerging narrative centers around reports alleging states will not complete updates to their voting technology, such as installing new software and hardware, prior to the 2024 US elections. This emerging narrative, combined with the official update to certification guidelines for voting machines scheduled for later this year, presents ample opportunities for malign actors to spread false information about voting technology.

In addition to the spread of false information about voting technology, hacktivist and cybercriminal threat actors seeking opportunistic targets very likely pose increased risks to US election infrastructure, such as voter registration databases, as well as amplifying true or false narratives claiming cyberattacks on election infrastructure. According to Recorded Future® Intelligence Cloud data, on October 10, 2023, "pwncoder", a member of the low-tier BreachForums 2, claimed to be selling a database containing 600,000 voter records obtained from "DC Board of Elections". According to the threat actor, the database contains voter IDs, registration dates, the last 4 digits of Social Security numbers (SSNs), driver's license numbers, full names, phone numbers, dates of birth, email and physical addresses, and other information. Although such claims remain unconfirmed, events like this, whether legitimate or not, increase the risk of triggering or amplifying mis- and disinformation narratives surrounding the security and integrity of US election technological infrastructure.

Outlook

Russia, China, Iran, DVEs, and hacktivist groups will very likely conduct influence operations taking advantage of an evolving geopolitical threat landscape to aggressively target the 2024 US elections. False and manipulated information propagated by state and non-state influence actors has the potential to influence voter behavior leading into, during, and after the elections and subsequently affect which candidates are elected and their corresponding political stances on a wide range of international and domestic issues. A continued whole-of-government approach integrated with private industry, including social media organizations, to publicly identify, announce, and refute false or manipulated information related to the elections will likely reduce the effectiveness of attempted malign influence activities seeking to persuade US voters.

Recorded Future®

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,700 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence. Learn more at recordedfuture.com.