[redacted]

NATIONAL INTELLIGENCE COUNCIL

MEMORANDUM

8 October 2024 NICM 2024-25857

[redacted] Foreign Threats to US Elections After Voting Ends in 2024

(U) Key Takeaways

[redacted] ***Scope Note:*** *This assessment responds to a tasking from the Director of National Intelligence to examine the threat of foreign election influence or interference in the US general election from the time the polls close on Election Day (5 November 2024) through Inauguration Day (20 January 2025).*

[redacted] The IC assesses that this year China, Iran, and Russia are better prepared to exploit opportunities to exert influence in the US general election after the polls close on Election Day due to lessons drawn from the 2020 election cycle. We expect these actors to at least conduct information operations denigrating US democracy through Inauguration Day.

- [redacted] These and other foreign actors conducting election operations after voting ends would probably continue to use the same types of tools: information operations, cyber operations, and potentially physical threats or violence. Although we lack information on each actor's threshold for action, we assess their level of activity will likely be shaped by their perception of opportunity, tolerance for risk, and, for those seeking to influence the election toward a particular candidate, how the projected outcome aligns with their preference.

- [redacted] Some foreign actors may conduct activities that seek to disrupt or delay the time-sensitive and tightly sequenced series of processes and events that begin after polls close. Each step, from the tabulation of votes and certification of results to completion of the Electoral College process and inauguration, is potentially susceptible to foreign influence and interference operations in different ways.

[redacted] The IC assesses that foreign actors—particularly China, Iran, and Russia—seeking to influence the US general election will conduct at least information operations after Election Day until the culmination of the process on Inauguration Day. They might also consider stoking unrest and conducting localized cyber operations to disrupt election infrastructure. However, we judge that operations that could affect voting or official counts are less likely because they are more difficult and bring a greater risk of US retaliation. Although we have no reporting as of 1 October about specific foreign plans to target election administration processes after voting ends, foreign actors such as China, Iran, and Russia have previously sought to amplify discord, including after the breach of the US Capitol on 6 January 202 and probably are now better prepared to exploit opportunities after the polls close than in previous cycles.

(U) *This assessment was prepared under the auspices of the National Intelligence Officer (NIO) for Counterintelligence. It was drafted by the National Intelligence Council* [redacted]

Classified By: [redacted] | Derived From: [redacted] | Declassify On: [redacted]

[redacted]

[redacted] Post-Election Day Information Operations Highly Likely

[redacted] Foreign adversaries will almost certainly conduct information operations after voting ends to create uncertainty and undermine the legitimacy of the election process. They probably will be quick to create false narratives or amplify content they think will create confusion and friction about the election process, as they did after the presidential election in 2020, including the breach of the US Capitol. Influence actors will almost certainly post and amplify claims of election irregularities, particularly if the electoral results are c ounter to their preferred outcomes, judging from their pre-election day activity in the present and prior cycles. These activities probably would be designed to undermine faith in US democracy, and could have ramifications for the post-election processes.

- [redacted] This year, Russian influence actors have posted allegations on social media about the possibility of illegal voting, including by undocumented immigrants and deceased individuals, [redacted] In 2020 and 2022, Russian actors identified alleged voter fraud as a "good topic" for influence efforts and promoted claims about irregular voting and the election being stolen. Similarly, in 2020, Iranian cyber actors disseminated a video demonstrating alleged voter fraud.

- [redacted] A foreign actor could use AI-generated materials to amplify doubts about the election's fair conduct, such as false images of election officials taking part in activities to undermine the vote. Russia has generated AI content related to the election across all four mediums we are following—text, images, audio, and video—though the degree to which this content has been released and spread online varies. Iranian actors have used AI to help generate social media posts and write spurious news articles for websites posing as real news sites.

- [redacted] Moscow and Tehran may also see an opportunity to continue pushing content favoring their preferred outcome. For instance, Russian influence actors have pushed negative messaging about Vice President Harris and publicly alleged conspiracy theories about her elevation to the top of the ticket. Iranian cyber actors may try to publish content denigrating former President Trump, [redacted]

[redacted] Foreign Actors Quickly Incorporated Capitol Breach into Information Operations

[redacted] China, Iran, and Russia capitalized on the events of 6 January 2021 to denigrate the US political system, though we have no indication any foreign actor was involved in planning or executing the siege. On 7 January, a Russian official directed Russian media to exploit the US Capitol violence as an opportunity to disparage the United States, and Russian influence actors subsequently posted propaganda on multiple platforms. [redacted] One PRC and various Iranian government officials also cited the attack in narratives characterizing the US as a declining power, including for domestic audiences.

[redacted] We assess foreign actors are positioned to use cyber operations and espionage to sow doubt about the integrity of the election and collect data, judging from cyber actors' prior activities. In particular, actors might seek to disrupt or alter public-facing state government and news websites to promote confusion about election results; claim they have interfered in the election, even if false, to undermine trust in the election; and acquire publicly available voter registration data and nonpublic information on local election officials, which they can leverage in future cyber or influence operations.

- [redacted] For instance, in 2022, pro-Russia, Main Intelligence Directorate (GRU)-connected cyber actors known as the Cyber Army of Russia Reborn conducted a distributed denial-of-service (DDoS) attack against a public-facing US state election office website, rendering it periodically inaccessible throughout Election Day.

- [redacted] As of August 2023, Islamic Revolutionary Guard Corps (IRGC) [redacted] actors were aware of unspecified information on US voters in 27 unnamed states available for download on a leak website, which, if acquired, could be used to target voters with disinformation—as in 2020, when Iranian cyber actors used data on more than 100,000 voters for its operation impersonating the Proud Boys. As of February, IRGC [redacted] cyber actors had accessed a network domain associated with a US state government's division of elections and probably obtained data on voter registration and on whether or not some of the registered individuals voted, [redacted]

[redacted] Foreign Actors' Goals Likely To Persist in Post-Election Period[a]

[redacted] Even after the polls close on Election Day, China, Iran, and Russia are likely to continue efforts to undermine US democracy, stoke societal unrest, and position their preferred candidates.

- [redacted] Russia seeks to denigrate American democracy and undermine confidence in the election. [redacted]

- [redacted] We assess Iran is trying to encourage societal discord, stoke violence, and undermine trust in the US democratic process, regardless of who wins the election. [redacted]

- [redacted] We assess China seeks to denigrate American democracy, but without fueling the perception that it seeks to influence or interfere in the US presidential election. China may be more willing to meddle in certain Congressional races.

[redacted] Potential for Physical Threats and Cyberattacks After Election Day

[redacted] Foreign actors also have the capacity to stoke protests, take violent actions, and conduct cyberattacks against some election infrastructure, and probably will decide whether to use such tactics based on their perception of the election outcome and domestic US reaction. In general, we expect foreign actors will be more likely to consider these tactics if they perceive they will resonate with the domestic population and they can maintain plausible deniability; we are closely monitoring for indications of a shift toward these actions.

[redacted] **Physical Threats and Violence**. Iran and Russia are probably willing to at least consider tactics that could foment or contribute to violent protests, and may threaten, or amplify threats of, physical violence in the post-Election Day timeframe. [redacted] efforts by Iran to assassinate former President

[a] [redacted] For more information about adversaries' efforts, please see NICA-2024-23931 [redacted]

Trump and other former US officials, which are likely to persist after voting ends, regardless of the projected outcome. [redacted]

- [redacted] Foreign adversaries that have demonstrated a willingness to encourage participation in non-election-related, First Amendment-protected protests may extend this practice to any potential violent protests in the post-election period to further widen domestic divides. In January, a GRU unit sought to recruit a probably unwitting US person to organize protests in the United States. In May and June, Iran's Ministry of Intelligence and Security (MOIS) encouraged a US person via social media, including by offering to send money for travel, to attend a pro-Palestinian protest in Washington, DC.

- [redacted] Iran could use cyber-enabled influence operations that lead to physical threats, including doxing and leaking of sensitive information. In mid-December 2020, IRGC [redacted] cyber actors were almost certainly responsible for the creation of a website containing death threats against US election officials, [redacted] The Iranian actors also published personally identifiable information about US federal and state officials to try to incite violence.

[redacted] **Cyberattacks Against Election Infrastructure**. We assess that some US adversaries—at a minimum China, Iran, and Russia or Russian-affiliated actors—have the technical capability to access some US election-related networks and systems. That said, we assess foreign actors will probably refrain from disruptive attacks that seek to alter vote counts because they almost certainly would not be able to tangibly impact the outcome of the federal election without detection; such activity would carry a risk of retaliation, and there is no indication they attempted such attacks during the past two election cycles.

- [redacted] Separately, in February, Killnet 2.0, a pro-Russia cyber group, announced its intent to interfere with the 2024 US election—though it did not specify how—before deleting the post.

- [redacted] In addition, nonstate foreign actors, such as hacktivists, cybercriminals, and terrorists, may have lower thresholds for cyber or physical attacks. We cannot, for example, rule out the possibility of an inadvertent attack in which an effort to procure ransom payments from a victim unexpectedly crashes systems needed for election activities, or a situation in which a software or security update goes awry.

[redacted] Adversaries Could Target Various Post-Election Day Process Vulnerabilities

[redacted] Foreign adversaries are likely to perceive varying opportunities to undermine each stage of the post-voting process. This period also has a sequence of deadlines that, if missed, could disrupt the normal process and have cascading and varied effects on later stages of the process.

[redacted] **Tabulation and Unofficial Reporting**. Official vote tabulation is highly secure, but adversaries might exploit the period of uncertainty before results are finalized to spread disinformation about the counting process and use cyber operations to reinforce the credibility of those narratives.

- [redacted] Foreign actors almost certainly will see the period between polls closing and the certification of official results as an opening to generate disinformation about election integrity. Complexities and variations across states—including voter demographics, how states process and count ballots, and when states start releasing unofficial results—create uncertainties that foreign actors almost certainly will see as fertile ground to exacerbate confusion. We assess they would most likely concentrate on states and races consistently identified as too close to call, although media coverage about how close the election is shaping up to be might lead them to cast a wider net and include some states and races on which there is less focus.

- [redacted] Foreign actors mostly likely judge that cyberattacks against public-facing websites—such as pro-Russian cyber actors' DDoS attack in 2022—or claims of hacking election infrastructure will resonate or increase doubt during this period and could undermine confidence in the accuracy of the election outcome. If they can gain access, foreign actors could also deface these websites by posting fake, unofficial results that, despite not impacting the security or integrity of the process, would amplify claims of election irregularities. Delaying announcements of outcomes for even a short period, for example, would underscore messaging about electoral chaos.

- [redacted] Some actors may use generative AI or other tools to post fake elections results or create voice or video to report unofficial results, even though they will be debunked by official results. Voice cloning or cutting into livestreams with AI-manipulated content would amplify concerns about the tabulation process.

(U) Vote Casting Resilient Against Manipulation Attempts

[redacted] Foreign actors almost certainly would not be able to manipulate official vote tallies and results on a large scale. Vote casting machines in polling stations are by standard practice not connected to the Internet or to each other, and most methods for exploiting them require physical access. Physical security measures prevent unauthorized access and provide evidence of tampering if it does occur. The overwhelming majority of registered American voters—estimated at more than 97 percent in this election—live in jurisdictions where the voting systems produce a paper record that voters can verify and provide a paper audit trail. Since at least January 2017, when election infrastructure was designated critical infrastructure, the Federal Government has seen no evidence that a foreign actor has impacted voter data integrity, the ability to vote, the tabulation of votes, or the timely transmission of election results.

[redacted] **Certification and the Electoral College Process**. Foreign actors may perceive a window of opportunity to push disinformation or foment or amplify protests and physical threats during the period between certification and the joint session of Congress to count electoral votes on 6 January. This process involves various activities at the state and local levels to certify election results and conduct the Electoral College process. The most critical dates in this time period include: the deadline for issuing Certificates of Ascertainment on 11 December; the meeting of electors to vote in each state and the District of Columbia on 17 December; and when Congress convenes in a joint session to count the electoral votes on 6 January.

- [redacted] Foreign actors creating or amplifying narratives questioning the legitimacy of the election results or the voting process could try messaging to increase popular pressure on state or local officials not to certify results and challenge states' ability to meet the deadline for signing the Certificates of Ascertainment on 11 December,

[redacted] Adversaries' messaging campaigns also may also seek to amplify any protests that could interfere with the certification process.

- [redacted] Foreign-driven or -amplified violent protests, violence, or physical threats to election workers or state and local officials could challenge state and local officials' ability to conduct elements of the certification and Electoral College process, particularly if they prevent necessary physical access to facilities or venues. Some states require the certification of election results or the meeting of electors for the Electoral College to be in-person or at a specific point of time and do not have laws that allow for variation in the procedure, such as by switching to a virtual forum, which adds to the risk of a disruption.

[redacted] **After 6 January to Inauguration**. Adversaries' efforts to disrupt the peaceful transfer of power probably would hinge on information operations introduced in earlier phases of the process that succeeded in fomenting or amplifying lingering protests or physical threats to the inauguration ceremony itself. If protests persist in this period, foreign actors are likely to further capitalize on the opportunity to denigrate the US political system and fan protests—as they did in the 2020 election cycle—[redacted]

[redacted]

[redacted] A multipronged approach that includes direct warnings to adversaries, public messaging to Americans that prebunks or debunks false narratives, and proactive communication between local officials and law enforcement has the best chance of thwarting foreign influence efforts after the election. US adversaries' longstanding interest in undermining American democracy suggests it will be difficult to dissuade them from engaging during the post-election period.

- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]