SECURING ELECTION INFRASTRUCTURE AGAINST THE TACTICS OF FOREIGN MALIGN INFLUENCE OPERATIONS

WHAT ARE FOREIGN MALIGN INFLUENCE OPERATIONS?

Foreign malign influence operations refer to hostile efforts by or on behalf of foreign governments to shape U.S. policies, decisions, and discourse. These operations may occur overtly or covertly, taking many forms and using a variety of tactics and techniques to accomplish their goals. Foreign malign influence operations are not new; however, technology developments have enabled actors to conduct operations while more effectively hiding their identities. To help critical infrastructure stakeholders increase the resilience of the elections process to foreign malign influence operations, CISA publishes materials, such as this guide, to explain the tactics used by these operations, such as the potential for malicious use of generative artificial intelligence (AI) tools. Generative AI tools enable or support large-scale creation of more realistic fake videos, images, audio, and text for foreign malign influence operations. Several of the tactics outlined below can be powered by generative AI tools to increase the scale of foreign malign influence operations.[i] In addition, the tactics covered below can also be utilized by domestic actors to spread disinformation.

THE USUAL SUSPECTS

According to the Office of the Director of National Intelligence, the People's Republic of China (PRC), the Russian Federation, and the Islamic Republic of Iran continue to be the primary nation-state actors leveraging influence operations exploiting perceived sociopolitical divisions to undermine confidence in U.S. democratic institutions and shaping public perception toward their interests.[ii] These actors employ a variety of methods to conduct foreign malign influence operations, such as using networks of fake online accounts to pose as Americans; enlisting real people to wittingly or unwittingly promote their narratives; and using proxies to launder their influence narratives through an array of overt and covert proxy websites, individuals, and organizations that appear independent. These operations often attempt to exacerbate existing social divides, amplify polarization, push narratives that fit into the nation-state's objectives, and increasingly, experiment with generative AI to enable their efforts.[iii] Since at least 2016, we have seen foreign malign influence campaigns specifically promote messaging that undermines public confidence in the security and integrity of the American elections process and exacerbate partisan tensions.

The Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and Office of the Director of National Intelligence (ODNI) produced this guide to highlight tactics used by foreign malign influence operations that seek to disrupt American life and the critical infrastructure that underlies it. The publication of informational materials about this issue are intended for public awareness, and are not intended to restrict, diminish, or demean any person's right to hold, express, or publish any opinion or belief, including opinions or beliefs that align with those of a foreign malign influence actor, are expressed by a foreign influence malign influence actor, or dissent from the majority. CISA, FBI, and ODNI respect the First Amendment rights of all U.S. persons and publications.

FOREIGN MALIGN INFLUENCE TACTICS EXPLAINED

The following tactics are frequently part of a foreign malign influence campaign, including some we have seen used to target the American elections process in recent election cycles. While some tactics can be used in isolation, they are often used in a coordinated manner to advance a strategic influence goal. Each foreign actor uses influence operations in unique ways. Their efforts can use a mixture of overt and covert methods to spread information, engage with key groups, or sow division. One consistent technique is the creation of a range of inauthentic social media personas, from spam-like profile accounts to deeply developed personas. These personas are sometimes intended to infiltrate targeted online communities and develop their own following. Additionally, foreign malign influence agents engage real people with the goal of having them echo foreign malign influence messaging, essentially co-opting their already established online megaphone, while hiding the foreign origin of the influence message. Many of these tactics are not new, but generative AI tools have made it much easier and cheaper to generate and spread convincing foreign malign influence content.

Disguising Proxy Media

A goal of foreign nation-state actors is to portray “proxy” media entities as established and trustworthy outlets to the population they are targeting and to use those sites to distribute their influence messaging. Proxy media outlets often portray themselves as independent, but actually have ties to foreign nation-state actors.[iv] Foreign malign influence actors seek to make proxy media sources blend in with real media sources to increase the chance that target populations will believe their message.

Highlighted Examples

- Researchers recently uncovered Russian Federation-linked proxy news sites masquerading as U.S. local news outlets, with titles like “D.C. Weekly” and “New York News Daily.” These sites mixed actual news reports with Russian disinformation, such as a fake recording of a U.S. State Department official discussing a shift in U.S. foreign policy away from supporting Ukrainian opposition to supporting Putin’s regime according to reporting from the New York Times in March 2024. [v]
- Other tactics to hide proxy media include “typo squatting,” a method recently observed in Russian Federation influence networks, where a URL (website name) for a proxy website is one or a few characters away from the actual well known media website name according to Facebook.[vi]
- Finally, pro-PRC influence actors have used AI-generated news anchors to make influence content look like real news content.[vii]

Voice Cloning of Public Figures

Voice cloning tools allow foreign nation-state actors to create a fake recording of a public official or figure to falsely attribute statements to them. While these fakes can sometimes be detected, recent advances in generative AI make such recordings more believable and harder to detect.

Highlighted Examples

- During the Slovak Republic’s 2023 elections, a fake recording of a political party leader discussing vote rigging spread widely just two days before voters went to the polls.

Cyber-Enabled Information Operations

Nation-state adversaries use information operations and cyber intrusions hand-in-hand to further foreign malign influence goals. For example, foreign adversaries can conduct "hack and leak" operations or find sensitive internal documents by compromising a target organization's IT systems, then publish those documents as salacious "leaks" to damage the organization or individual's reputation.

Highlighted Examples

- The Islamic Republic of Iran has engaged in aggressive cyber-enabled influence operations against Israel and its allies in recent months aimed at sowing internal discord within the Israeli population and undercutting Israeli domestic confidence in the Israeli government. Iranian cyber threat actors have compromised a variety of IT systems tied to the State of Israel, publicizing the compromises using their influence accounts that are often disguised as domestic Israeli activists. The Islamic Republic of Iran has used information operations to hide their involvement in the cyber intrusions, to exaggerate their significance, and to make it seem they are the product of internal dissent.

- Foreign nation-state actors often attempt to compromise sensitive IT systems to steal personal information that could be used for malign influence operations. For example, the Russian Federation compromised the email account of a former British official and stole classified documents, then leaked the documents ahead of the British elections in 2019.

Manufacturing False Evidence of an Alleged Security Incident

Foreign nation-state actors can create and spread false "proof" of cyber or physical incidents, to include creating fake cybercriminal personas to spread fake "hacked" documents or false reports. While these reports may eventually be proven to be fake, the initial alarm created may not entirely dissipate. Often original disinformation spreads farther than follow-up efforts to provide correct or clarifying information.

Highlighted Examples

- Pro-PRC influence actors spread many fabricated political documents, some allegedly "hacked" from Taiwanese government systems, to try to influence Taiwan's 2024 elections. Ahead of the vote, Pro-PRC influence accounts published falsified political documents ranging from DNA tests to fake "hacked" Taiwanese military documents. Fake documents provide fodder for influence accounts and proxy media to push foreign malign influence messaging.[viii]
- Foreign actors can also generate and amplify fake images of alleged security incidents to incite alarm. In May 2023, a false image of an explosion at the Pentagon presumed to be AI-generated caused the U.S. stock market to briefly dip and was amplified by Russian Federation state media, demonstrating the desire of foreign adversaries to stoke alarm according to reporting from NPR.[ix]

Paid Influence

To spread influence messaging further and hide their hand in originating it, foreign nation-state actors will pay influential people and organizations, who are often unaware of the requestor's foreign origin, to push their messaging. Foreign malign influence actors utilize established internet entities, such as online influencers with an existing follower base, to push content aligned to the nation-state's influence goals, often hiding the true source of their messaging.

Highlighted Examples

- The PRC has used Western social media production companies to distribute pro-PRC influence content to Western video platforms on issues that could impact their strategic objectives, such as countering accusations of PRC's human rights abuses in Xinjiang. These companies' services enable PRC influence content, often produced for domestic Chinese consumption, to spread among global audiences without disclosure that the content was produced by the PRC.[x]
- Additionally, Russian Federation influence activities have long used public relations (PR) firms both in and outside of Russia to spread influence messaging.[xi] Recently, the U.S. State Department revealed Russian influence actors paid a PR firm to create content aligned with Russian influence messaging for editorial staff at local media outlets in Latin America.[xii]

Leveraging Social Media Platforms

Foreign malign influence actors may leverage certain social media platforms to intensify belief in a foreign malign influence narrative among specific user groups. Foreign malign influence operators may seek to take advantage of alternative platforms with less stringent content moderation policies and fewer controls to detect and remove inauthentic content and accounts than other social media platforms.

Highlighted Examples

- Russian influence operators use Telegram, a foreign-based messaging platform with less stringent moderation policies, to spread overt and covert influence messaging to audiences abroad. Russian Federation-linked Telegram channels enable a wide variety of Russian influence activity, from reposting Russian Federation state media articles to using fake personas to justify Russian Federation invasion of Ukraine.[xiii] Russian Federation actors have also leveraged less stringent social media platforms to spread divisive political narratives in the U.S.[xiv]

MITIGATIONS: HOW TO PREPARE FOR AND RESPOND TO FOREIGN MALIGN INFLUENCE OPERATIONS TARGETING ELECTION INFRASTRUCTURE

Election officials have faced the threat of foreign malign influence operations and disinformation targeting election infrastructure for multiple election cycles. Election officials and other election infrastructure stakeholders can take steps in advance of an incident to help mitigate the impacts on election operations and maintain public confidence in the security and integrity of the American democratic process. The following steps will help election infrastructure stakeholders prepare for and respond to efforts by foreign adversaries to undermine our elections process.

Communicate Early and Promote Transparency Around the Elections Process

- Foreign adversaries often use the same or similar narratives across their campaigns. To get ahead of these nefarious efforts, develop ways to educate the public about the elections process and proactively debunk or "prebunk" (that is, proactively warn about future influence operations) potential foreign malign influence narratives related to your elections process.
- In both traditional and social media communication activities, direct audiences to official websites and trusted sources of information. If you have not already, sign up for a .gov website domain to easily signal your status as an official government organization.
- Train staff on standard procedures for responding to suspected AI-generated media and understand the mechanisms for notifying members of your organization about this activity. Include these types of incidents in your incident response plans.
- Establish relationships with local media and community leaders; build a team of trusted voices to amplify accurate information proactively and in the event of an incident.

Secure Your Systems, Your Accounts, and Your Public-Facing Content

- For public officials, consider making personal social media accounts private so malicious actors have less access to your image or voice.
- Harden personal and organizational social media accounts by implementing changes such as applying the strongest security and privacy controls possible, deactivating or deleting profiles no longer in use, and removing personally identifiable information from organizational social media profiles.
- Establish and enforce strong cybersecurity protocols, like email authentication security protocols and Multifactor Authentication (MFA) for all accounts.
- With respect to your public-facing content, consider utilizing non-repudiation and authentication techniques, such as watermarks, to mark your content as verifiably originating from you and to be able to point out when an altered version of your content lacks your unique digital watermark. Talk to vendors about adopting provenance and authentication measures for election-related records.

Educate Your Stakeholders and Staff

- Create opportunities for voters in your jurisdiction to learn about the elections process and better understand the actions being taken to ensure its security and integrity.
- Encourage voters to verify the sources of articles, papers, and other resources before sharing them.
- Educate employees on potential for AI-based impersonation and use "safe words" for authentication.
- Educate organization leadership on how their personal and professional social media presence may be targeted to spread foreign malign influence content.

FOREIGN MALIGN INFLUENCE TACTICS AT A GLANCE

The following table provides a summary of the above highlighted foreign malign influence tactics and examples.

TACTIC	EXAMPLE
DISGUISING PROXY MEDIA Foreign malign influence actors disguise proxy media used to spread content as established media, by impersonating established outlets and local news sources.	*PRC actors used AI news anchors for fictitious media outlets to spread pro-PRC content.* [xv]
VOICE CLONING PUBLIC FIGURES A fabricated recording of a public official is used to mislead the public or a targeted individual.	*Voice clones of a political party leader were disseminated in the Slovak Republic two days before the election as reported by Wired magazine in October 2023.* [xvi]
CYBER-ENABLED INFORMATION OPERATIONS Foreign adversaries compromise IT systems of prominent organizations to find and leak damaging private information.	*Russian Federation actors hacked and leaked US-UK trade documents prior to Britain's 2019 election according to Reuters.* [xvii]
MANUFACTURING FALSE EVIDENCE OF SECURITY INCIDENT A false report of a physical or cybersecurity incident is spread.	*Pro-PRC actors distributed fake leaked Taiwanese government documents before the Taiwanese elections.* [xviii]
PAID INFLUENCE Foreign malign influence actors launder messaging by covertly paying online influencers, hiring PR firms, or employing journalists to spread disinformation.	*The PRC use influencers to push foreign malign influence content about Xinjiang on Western social media.* [xix]
LEVERAGING SOCIAL MEDIA PLATFORMS Foreign nation-state actors leverage social media platforms to spread influence narratives in specific communities.	*Russian Federation actors leveraged social media platforms with less stringent content-moderation policies to spread divisive political narratives in the U.S.* [xx]

ADDITIONAL TACTICS AT A GLANCE

The table below provides a supplemental list of commonly used foreign malign influence tactics that were not discussed above. Combined with the above tactics, the supplemental list provides a more comprehensive overview of common foreign malign influence tactics. For more information on these additional tactics, see CISA's 2022 publication.[xxi]

TACTIC	EXAMPLE
CULTIVATE FAKE OR MISLEADING PERSONAS AND WEBSITES Foreign malign influence actors create networks of fake personas and websites to increase the believability of their message with their target audience.	*A network of fake accounts developed by the PRC recently pretended to be U.S. military families against Taiwan.*[xxii]
"ASTROTURFING" AND FLOODING THE INFORMATION ENVIRONMENT Foreign malign influence actors post overwhelming amounts of content with similar messaging to manufacture the perception of widespread support.	*A network of pro-PRC fake accounts called for protests of a rare-earth mineral processing facility in Texas.*[xxiii]
EXPLOIT INFORMATION GAPS Foreign malign influence actors fill data voids with influence content.	*PRC officials and media exploited data voids to spread conspiracy theories about a U.S. army research facility.*[xxiv]
MANIPULATE UNSUSPECTING ACTORS Foreign nation-state actors deceive prominent individuals into unintentionally amplifying their influence materials.	*Russian Federation-aligned actors manipulated celebrities' Cameo videos to spread disinformation according to CNN.*[xxv]
SPREAD TARGETED CONTENT To gain insider status with targeted online communities, foreign nation state actors produce tailored content likely to resonate.	*Pro-PRC disinformation network spread tailored content to U.S. audiences.*[xxvi]

[i] https://www.cisa.gov/resources-tools/resources/risk-focus-generative-ai-and-2024-election-cycle

[ii] https://www.dni.gov/files/ODNI/documents/assessments/NIC-Declassified-ICA-Foreign-Threats-to-the-2022-US-Elections-Dec2023.pdf

[iii] https://www.dni.gov/files/ODNI/documents/assessments/NIC-Declassified-ICA-Foreign-Threats-to-the-2022-US-Elections-Dec2023.pdf

[iv] https://www.state.gov/russias-pillars-of-disinformation-and-propaganda-report/

[v] https://www.nytimes.com/2024/03/07/business/media/russia-us-news-sites.html

[vi] https://about.fb.com/news/2023/05/metas-adversarial-threat-report-first-quarter-2023/

[vii] https://graphika.com/reports/deepfake-it-till-you-make-it

[viii] https://www.aspistrategist.org.au/as-taiwan-voted-beijing-spammed-ai-avatars-faked-paternity-tests-and-leaked-fake-documents/

[ix] https://www.npr.org/2023/05/22/1177590231/fake-viral-images-of-an-explosion-at-the-pentagon-were-probably-created-by-ai

[x] https://www.aspi.org.au/report/frontier-influencers

[xi] https://about.fb.com/news/2022/12/metas-2022-coordinated-inauthentic-behavior-enforcements/

[xii] https://www.state.gov/the-kremlins-efforts-to-covertly-spread-disinformation-in-latin-america/

[xiii] https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/russian-threat-actors-dig-in-prepare-to-seize-on-war-fatigue

[xiv] https://cyber.fsi.stanford.edu/io/publication/bad-reputation; https://www.dni.gov/files/ODNI/documents/assessments/NIC-Declassified-ICA-Foreign-Threats-to-the-2022-US-Elections-Dec2023.pdf

[xv] https://graphika.com/reports/deepfake-it-till-you-make-it

[xvi] https://www.wired.com/story/slovakias-election-deepfakes-show-ai-is-a-danger-to-democracy/

[xvii] https://www.reuters.com/article/us-britain-russia-hack-exclusive-idUSKCN24Z1V4/

[xviii] https://www.aspistrategist.org.au/as-taiwan-voted-beijing-spammed-ai-avatars-faked-paternity-tests-and-leaked-fake-documents/

[xix] https://www.aspi.org.au/report/frontier-influencers

[xx] https://cyber.fsi.stanford.edu/io/publication/bad-reputation

[xxi] https://www.cisa.gov/sites/default/files/publications/tactics-of-disinformation_508.pdf

[xxii] https://transparency.fb.com/sr/Q4-2023-Adversarial-threat-report

[xxiii] https://www.mandiant.com/resources/blog/dragonbridge-targets-rare-earths-mining-companies

[xxiv] https://securingdemocracy.gmfus.org/data-void-china-covid-disinformation/

[xxv] https://edition.cnn.com/2023/12/07/tech/cameo-celebrity-russia-propaganda-video/index.html

[xxvi] https://www.mandiant.com/resources/blog/pro-prc-influence-campaign-expands-dozens-social-media-platforms-websites-and-forums