Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure

February 2022

Threat Overview

Malicious actors use influence operations, including tactics like misinformation, disinformation, and malinformation (MDM), to shape public opinion, undermine trust, amplify division, and sow discord. Foreign actors engage in these actions to bias the development of policy and undermine the security of the U.S. and our allies, disrupt markets, and foment unrest. While influence operations have historical precedent, the evolution of technology, communications, and networked systems have created new vectors for exploitation.

A single MDM narrative can seem innocuous, but when promoted consistently, to targeted audiences, and reinforced by peers and individuals with influence, it can have compounding effects. Modern foreign influence operations demonstrate how a strategic and consistent exploitation of divisive issues, and a knowledge of the target audience and who they trust, can increase the potency and impact of an MDM narrative to National Critical Functions (NCFs) and critical infrastructure. Furthermore, current social factors, including heightened polarization and the ongoing global pandemic, increase the risk and potency of influence operations to U.S. critical infrastructure, especially by knowledgeable threat actors.

In recent years, foreign actors have used influence operations to influence U.S. audiences and impact critical functions and services across multiple sectors. Foreign influence operations have been paired with cyber activity to derive content, create confusion, heighten anxieties, and distract from other events. In light of developing Russia-Ukraine geopolitical tensions, the risk of foreign influence operations affecting domestic audiences has increased. Recently observed foreign influence operations abroad demonstrate that foreign governments and related actors have the capability to quickly employ sophisticated influence techniques to target U.S. audiences with the goal to disrupt U.S. critical infrastructure and undermine U.S. interests and authorities.

This CISA Insights product is intended to ensure that critical infrastructure owners and operators are aware of the risks of influence operations leveraging social media and online platforms. Organizations can take steps internally and externally to ensure swift coordination in information sharing, as well as the ability to communicate accurate and trusted information to bolster resilience. CISA encourages leaders at every organization to take proactive steps to assess their risks from information manipulation, increase resilience, and mitigate the impact of potential foreign influence operations.

Assess the Information Environment

- Evaluate the precedent for MDM narratives targeting your sector.
- Learn how and where your stakeholders and customers receive information.
- Map key stakeholders and how you communicate with them. Consider how these channels would allow your organization to identify and respond to MDM activity. Operate on the principle of empowering trusted partners with accurate information.
- Monitor for any changes to online activity related to your organization and sector, such as a sudden increase in tags or followers, a spike in searches, or a high volume of inquiries.

Identify Vulnerabilities

- Identify potential vulnerabilities that could be exploited by MDM. Think about common questions or points of confusion that people have about your sector and operations.

Organizations should establish their own criteria for evaluating the severity of MDM narratives. Examples of indicators could include:

- **High**: Does a narrative significantly threaten to undermine your critical function? What are known examples?
- **Medium**: Does a narrative or incident have the potential to negatively affect your critical function?
- **Low**: What narratives are clearly disprovable, implausible, or pose a limited threat?

Your assessment can inform your information sharing around, and response to, MDM narratives, helping decide whether to respond, and, if so, when. It also can guide which stakeholders you should engage to amplify response efforts.

- Educate staff on securing their personal social media accounts. Encourage all staff members to use multi-factor authentication for social media accounts and review their privacy settings to make sure they know what information about them is visible online.

Cyber Activities and Influence Operations:

Malicious actors can use hacking and other cyber activities as part of influence operations. Hackers assist in surveillance or reconnaissance and provide opportunities for destructive attacks. Hijacking accounts and defacing public facing sites can be used to influence public opinion. Organizations should be aware of cyber risks and take action to reduce the likelihood and impact of a potentially damaging compromise.

- Remind staff to practice smart email hygiene and to be on alert for phishing emails and advise against clicking on suspicious links and/or forwarding questionable information.

Fortify Communication Channels

Build Your Network:

Preparing communication channels and establishing contacts before MDM incidents occur allows you the ability to quickly respond and share information.

- Engage your stakeholders to establish clear communication channels and coordination mechanisms for information sharing.
- Review and update your organization's website to make information as clear, transparent, and accessible as possible.
- Review and update your organization's presence on social media platforms and seek any verification methods that platforms offer for official accounts.
- Review access privileges for company social media accounts. Turn on multi-factor authentication and use complex passwords.

Engage in Proactive Communication

- If your organization has established ways of communicating with its constituents, stakeholders, and/or community, review these practices to identify opportunities for improvement. This may include newsletters, reports, blog posts, events, social media content, podcasts, or other activities.
- Evaluate the reach and engagement of your communication efforts and adjust your strategy as needed.

Communications as a Tool:

Using clear, consistent, and relevant communications that not only responds, but anticipates MDM is an important, effective way to maintain security and build public confidence in your organization.

- Coordinate with other organizations in your sector to amplify and reinforce messaging, with the goal of building a strong network of trusted voices.
- Encourage your communications professionals to maintain contact with key communications outlets.

Develop an Incident Response Plan

- Designate an individual to oversee the MDM incident response process and associated crisis communications.
- Establish roles and responsibilities for MDM response, including but not limited to responding to media inquiries, issuing public statements, communicating with your staff, engaging your previously identified stakeholder network, and in implementing physical security measures.
- Ensure your communication systems are set up to handle incoming questions. Phones, social media accounts, and centralized inboxes should be monitored by multiple people on a rotating schedule to avoid burnout.
- Identify and train staff on reporting procedures to social media companies, government, and/or law enforcement.
- Consider your internal coordination channels and processes for identifying incidents, delineating information sharing and response. Foreign actors can combine influence operations with cyber activities, requiring additional coordination to facilitate a whole-of-organization response.

TRUST Model:

In today's information environment, critical infrastructure owners and operators must play a proactive role in responding to MDM. While each MDM narrative will differ, the TRUST model for incident response can help reduce risk and protect stakeholders.