REPORT TO THE CISA DIRECTOR

Protecting Critical Infrastructure from Misinformation and Disinformation

Information Sharing Around Foreign Adversary Threats to Elections

September 13, 2022

Introduction:

The Protecting Critical Infrastructure from Misinformation and Disinformation (MDM) Subcommittee submitted a first set of recommendations in June 2022. The recommendations outlined below aim to emphasize and add further detail to key points and provide additional items for consideration.

Findings:

In 2017-2018, in the wake of revelations of persistent social media manipulation by Russia-affiliated organizations such as the Internet Research Agency, there was widespread concern about foreign disinformation operations targeting U.S. audiences — especially in the context of elections. In more recent years, attention has shifted to domestic sources of disinformation, but there are reasons to anticipate that the elections in 2022 and 2024 may again attract significant foreign sources of potential interference. With the U.S. providing significant aid to Ukraine and imposing strong economic sanctions against Russia, the Russian government has every incentive to disrupt the upcoming elections in ways that will exacerbate existing mistrust of the process and potentially cause the kind of chaos that can lead to political violence. China, too, may have an incentive to interfere in the U.S. elections as a response to what they see as provocations regarding Taiwan or to further their narrative that U.S. democracy is chaotic and corrupt. The U.S. federal government, state and local election officials, the courts, social media platforms, traditional media, and other relevant organizations should all prepare for significant information operations, including those enabled by malicious cyber activity (whether successful or merely noisy attempts), from Russia, China, and other adversaries.

If the objective of adversary operations targeting elections is to exacerbate a lack of trust in the process, foreign attacks on U.S. election infrastructure are likely to involve two integrated attack vectors. Similar to a "hack-and-leak" operation, we might term this type of attack a "hybrid cyber-misinformation and disinformation (MDM)" attack. The first vector involves attempting to infiltrate (i.e., hack) that infrastructure to cause damage by changing voter rolls or votes (a traditional cybersecurity threat to a critical function). The second involves information operations to draw attention to infiltration (even if attempted hacks were unsuccessful) or broader information operations designed to undermine trust in the process, thereby undermining the critical function of elections. It is therefore important to prepare for, detect, and respond to these operations holistically — along both their cybersecurity and information dimensions.

Recommendations:

Stemming from these insights, we have the following recommendations outlined below:

- **Share information with state and local election officials.** CISA should work with the Intelligence Community (IC), including the Federal Bureau of Investigation, to ensure that the information needs of election officials around foreign disinformation threats are prioritized. To identify the intelligence requirements of local and state election officials, CISA should work with the Elections Infrastructure Government Coordinating Council (GCC). In particular, the CSAC believes that providing information and assistance to the many local elections officials across the country is critical, not just secretaries of state or election officials at the state level. Considering the fundamental importance of elections, CISA should ensure that intelligence information about adversary activity related to elections is promptly shared with state and local elections officials with as much

detail as possible, including attribution, consistent with protection of sources and methods.

- **Protect the courts.** Given the essential role courts play in ensuring the resolution of disputes about the election process and ensuring the peaceful transfer of power, they, too, may be the target of an intensified campaign to undermine public trust in the legitimacy of their processes. CISA should consider the following two recommendations that:

    - Relevant information around foreign hacking and disinformation attacks are shared with the courts; and
    - The IC includes adversary activity targeting the courts in the collection and analysis priorities related to elections.

Supporting State and Local Elections Officials

September 13, 2022

Introduction:

The MDM Subcommittee submitted a first set of recommendations in June 2022. The recommendations outlined below aim to emphasize and add further detail to key points and provide additional items for consideration.

Findings:

CISA should continue to provide resources for state and local election officials to support their efforts to address misinformation and disinformation (MDM) targeting their jurisdictions. State and local election officials are first-hand sources for information about elections. CISA should support their efforts to effectively communicate accurate information and actively counter inaccurate information about their election materials and processes.

Recommendations:

1. At the highest level, CISA should share up to date "best practices" around how to proactively address and counter MDM based on the most recent research. To help election officials craft their messaging, CISA should provide templates and customizable content that local and state election officials can adapt to their specific needs. A particular need for many local and state election officials is around establishing a website. CISA should provide resources, including templates and grants for technical support — e.g., to create and maintain websites to host election-related resources for their constituents. CISA has a massive audience and communication resources and should leverage both to amplify content — including accurate information about election materials and procedures — from local and state election officials.

2. CISA must ensure that there is a national effort to bring insights together on an ongoing basis, and to share tools, training, and templates. Elections are ultimately local and must be managed locally. That said, some of these disinformation campaigns are likely to use similar tactics, techniques, and messaging aimed at multiple jurisdictions.

3. CISA's role in this whole-of-nation effort to counter adversary information operations around upcoming elections should be consistent with this Subcommittee's earlier recommendations, with a focus on furthering CISA's existing mission. Within the federal government, the intelligence community is likely to have the best insights on foreign adversary activity. CISA's role should be to ensure that those insights are promptly provided to state and local election officials. CISA should also consider unique aspects of foreign information operations when developing tools, templates, and training for those officials.