Written Testimony

of

Iranga Kahangama

Assistant Secretary for Cyber, Infrastructure, Risk, and Resilience

Office of Strategy, Policy, and Plans

U.S. Department of Homeland Security

and

Mona Harrington

Assistant Director, National Risk Management Center

Cybersecurity and Infrastructure Security Agency

U.S. Department of Homeland Security

Before

Subcommittee on Oversight, Investigations, and Accountability

Committee on Homeland Security

United States House of Representatives

Official Title: “Censorship Laundering Part II: Preventing the Department of Homeland Security’s Silencing of Dissent”

December 13, 2023

**Introduction:**

Chairman Bishop, Ranking Member Ivey, and members of the subcommittee, we appreciate the opportunity to appear before you today to discuss the Department of Homeland Security's (DHS or the Department) efforts to counter the impacts of foreign influence operations and disinformation impacting homeland security.

First and foremost, at the core of the Department's mission is a commitment to safeguard the American people, our homeland, and our values. We are committed to carrying out this mission in a manner that protects the privacy, civil rights, and civil liberties, including the freedom of speech, of all Americans. These rights are fundamental to our freedom and to who we are as a nation. The Department works every day to ensure that all our activities are carried out in a manner that protects these values.

In its Homeland Threat Assessment for 2024, the Department's Intelligence Enterprise assesses Russia, China, and Iran likely see the upcoming election season in 2024 as an opportunity to conduct overt and covert influence campaigns aimed at shaping favorable U.S. policy outcomes and undermining U.S. stability, and they will likely ramp up these efforts in advance of the election. These adversarial states are likely to use generative artificial intelligence (AI) enabled technologies to improve the quality, scope, and scale of their influence operations targeting U.S. audiences.

Further, nation-state adversaries likely will continue to conduct influence operations aimed at undermining trust in government institutions, our social cohesion, and democratic processes. The proliferation and accessibility of emergent cyber and AI tools probably will help these actors bolster their malign information campaigns by enabling the creation of low-cost, synthetic text-, image-, and audio-based content with higher quality. Russia, China, and Iran continue to develop the most sophisticated malign influence campaigns online. Many of the tactics these adversaries use to influence U.S. audiences will likely be used in the lead-up to the 2024 election.

This risk is not new. In its 2023 Annual Threat Assessment, the U.S. Intelligence Community noted that China largely concentrates its U.S.-focused influence efforts on shaping U.S. policy and the U.S. public's perception of the People's Republic of China (PRC) in a positive direction but has shown a willingness to meddle in select election races that involved perceived anti-PRC politicians. For example, Beijing's growing efforts to actively exploit perceived U.S. societal divisions using its online personas move it closer to Moscow's playbook for influence operations.

Russia presents one of the most serious foreign influence threats to the United States because it uses its intelligence services, proxies, and wide-ranging influence tools to try to sow discord inside the United States. Moscow views U.S. elections as opportunities for malign influence as part of its larger foreign policy strategy. Moscow has conducted influence operations against U.S. elections for decades, including as recently as the U.S. midterm elections in 2022. Russia's influence actors have adapted their efforts to increasingly hide their hand, laundering their preferred messaging through a vast ecosystem of Russian proxy websites, individuals, and organizations that appear to be independent sources.

**Election Infrastructure Mission:**

In 2017, the Secretary of Homeland Security established election infrastructure as a critical infrastructure subsector. To manage risks to the nation's election infrastructure on behalf of the Department, the Cybersecurity and Infrastructure Security Agency (CISA) works collaboratively with state and local governments, election officials, federal partners, and private sector partners. The collaboration includes working in a nonpartisan, voluntary manner with state and local election officials, who are the trusted and expert voices within their communities, to hold secure elections in their jurisdictions and to equip the American public with accurate information about the conduct and security of elections.

CISA provides publicly available resources on election security for both the public and election officials in its efforts to protect America's election infrastructure against new and evolving threats. For example, CISA recently publicly released the No Downtime in Elections Guide to Mitigating Risks of Denial of Service. Moreover, CISA has partnered with the Federal Bureau of Investigation to publish election security-related Public Service Advisories; and CISA has compiled a toolkit of free services and tools intended to help state and local government officials, election officials, and vendors enhance the cybersecurity and cyber resilience of U.S. election infrastructure.

CISA also provides numerous voluntary and no-cost election security services, such as cybersecurity assessments, cyber threat hunting, cyber incident response, training, and exercises to state and local government officials and private sector election infrastructure partners. In addition, CISA reduces risk to U.S. critical infrastructure by building resilience to foreign influence operations and disinformation intended to impact critical infrastructure.

Through these efforts, DHS helps the American people understand the scope and scale of activities targeting election infrastructure and enables them to take action to mitigate associated risks. The Department's efforts include an emphasis on transparency with respect to sharing accurate information about election infrastructure security, as well as increasing awareness about the threat posed by foreign influence operations and disinformation.

**Foreign Influence Operations and Disinformation:**

DHS is charged with safeguarding the United States against threats to its security. In recent years, many of those threats have been exacerbated by disinformation. As part of its mission, DHS has worked across multiple administrations to address and mitigate different forms of disinformation that threaten the authorized missions of the Department. Countering disinformation that threatens the homeland and providing the public with accurate information in response are critical to fulfilling DHS's congressionally-mandated missions. DHS efforts are limited to combating disinformation that threatens the homeland and homeland security missions, such as border security, emergency response, and infrastructure security. Examples of such efforts include working to combat human smuggling, protecting critical infrastructure, and responding to malign foreign influence efforts.

CISA’s work on foreign influence operations and disinformation targeting election infrastructure is of limited scope and focuses predominantly on its impact to public confidence in election infrastructure security. Out of CISA’s $2.9 billion budget, less than 0.07% is spent on these efforts. CISA’s work has been transparent, briefed to Congress many times, and is available to the public on its website at cisa.gov.

In support of these efforts, CISA has developed voluntary resources to help individuals identify and mitigate the threats of foreign influence and disinformation operations. Recently, CISA has released guides that highlight tactics, such as manipulating content service providers or defacing public websites, used by foreign actors engaged in disinformation campaigns that seek to negatively impact U.S. critical infrastructure and disrupt American life. Such public products help Americans understand how automated programs like social media bots simulate human behavior on social media platforms and how foreign malign actors use them to spread false or misleading information, shut down opposition, and elevate their own platforms for further manipulation.

Additionally, CISA provides context to common disinformation narratives and themes that relate to the security of election infrastructure through our Election Security Rumor vs. Reality website. Lastly, CISA seeks to combat foreign disinformation by amplifying accurate election security-related information shared by state and local officials with the public.

## Conclusion:

DHS is committed to continuing to build resilience to foreign influence operations and disinformation, in close coordination with our interagency partners. In these efforts, DHS will continue operating within our authority and in accordance with all legal requirements, and with respect for the Constitutional rights and civil liberties of all Americans.

Thank you again for the opportunity to appear before you today, and we look forward to continuing to work closely with you to keep our homeland safe and secure.