HOW DOGE COULD AFFECT U.S.-JAPAN CYBER INTELLIGENCE SHARING, AND WHAT JAPAN CAN DO ABOUT IT

by
Giulia Saccone

Introduction

The U.S. Department of Government Efficiency (DOGE)'s cuts to national cybersecurity in recent months risk compromising situational awareness, incident response and analysis. Combined with the department's controversies, and more broadly, the second Trump administration's negative posture towards globally shared norms, these reductions can seriously erode trust in the U.S.-Japan cyber intelligence-sharing relationship, which relies heavily on the U.S. security umbrella. For Tokyo, this may translate into diminished readiness against evolving cyber threats, increasing vulnerability to advanced persistent threats (APTs) and complicating breach investigations.

The adoption of the Active Cyber Defense (ACD) Bill could not be timelier. However, the rapidly shifting threat landscape requires urgent implementation and intelligence reforms. This would offset the impact of diminished U.S. capabilities, enhance regional collaboration, and transform these challenges into strategic opportunities for diversification and resilience.

U.S.-Japan Cybersecurity Relations

Japan regards its alliance with the U.S. as a key pillar of its defense strategy. In the cyber domain, this cooperation manifests through operational-level integration, information, intelligence sharing, and joint exercises. Over the years, cyber cooperation has gained momentum, as reaffirmed in the 2022 Japan–U.S. summit joint statement. This momentum is ensured by the extension of Article 5 of the US-Japan Security Treaty to cover cyberattacks, and by the efforts of the Working Group on Information Support, the Japan-U.S. cyber dialogue, the Japan-U.S. Cyber Defense Policy Working Group, and the U.S.-Japan IT forum. Additionally, university-level collaboration between the two countries has ensured continuous information exchange and suggestions for best practices

The importance of this alliance for Japan is highlighted in its Defense White Papers which frequently mention cyberattacks on the U.S., particularly those by APT groups that have affected both countries. Intelligence sharing is essential for countering such malicious actors who typically engage in long-term espionage or zero-day attacks, necessitating timely intervention. Japan's reliance on the U.S. is partly rooted in its past cyber defense strategy based on deterrence by denial, and assigns the responsibility of responding to cyberattacks to the partner nation.

Over the years, the Japan-U.S. cyber relationship has evolved beyond bilateral cooperation to broader multilateral partnerships with Indo-Pacific nations and international organizations. This is driven by shared concerns over cyber threats from China, Russia, and the DPRK given their use of third countries as bases for launching cyberattacks and cognitive warfare. Furthermore, tensions in the South China Sea and in the Taiwan Strait have led to an integration of cyber cooperation with other domains. This is exemplified by marine cybersecurity, which focuses on safeguarding vessels against unauthorized data access. Examples of such collaboration include trilateral U.S.-Japan dialogues with ROK and the Philippines.

Cybersecurity Transformation under the Second Trump Mandate

The establishment of DOGE at the start of President Trump's second term has led to significant budget cuts and controversy across the U.S. In the cybersecurity field, experts and government officials have expressed concerns about DOGE practices, including the lack of a formal chain of command and its unauthorized access to all executive branch agencies without congressional oversight. There have also been reports of unauthorized hacking into U.S. government management systems, with consequent violation of various national and foreign data protection frameworks. Sensitive governmental data reportedly stored on unprotected servers had made the DOGE a target for APTs from countries like China, Russia, and North Korea.

Structurally, the U.S. cyber intelligence architecture has been severely disrupted by the dismissal of key personnel. Gen. Timothy Haugh, U.S. Cyber Command's commander and National Security Agency's (NSA) director, was removed without any explanation. This followed the ouster of the NSA Civil Deputy Director Wendy Noble, and the infamous Valentine's Day Massacre, which saw the layoff of more than 130 employees of the Cybersecurity and Infrastructure Security Agency (CISA) reportedly due to their unfitness "for continued employment" and misalignment with "the Agency's current needs". Additionally, in May, the government terminated the heads of six CISA operational and six regional offices, weakening ties between the agency and infrastructure operators. These disruptions are likely to significantly impair situational awareness and responsiveness across the cybersecurity ecosystem.

The targeted nature of the firings have been condemned by 140 cybersecurity professionals as a bullying strategy based on retribution, lacking strategic foresight. These actions were also met with criticism in Japan, with scholars defining DOGE's activity as "going too far". Both the Yomiuri and Asahi Shinbun have reflected a rare tone of disapproval in their coverage.

Implications for Japan

The weakening of U.S. Cyber Command impairs the management and reinforcement of the Department of Defense's (DoD) cyber operations. Simultaneously, the mass firing of CISA contractors and key personnel will affect coordination among the U.S. Computer Emergency Readiness Team (US-CERT), the National Cybersecurity and Communications Integration Center (NCCIC), and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). This could lead to a slowdown in situational awareness, degrading high-level information-sharing with Japan, and stalling the development of best practices to counter cyberattacks. Moreover, DOGE's unauthorized access to DoD personnel data raises significant privacy and security concerns for approximately 25000 Japanese workers employed by U.S. forces in Japan.

At the political level, incipient signs of distrust in Japan can be perceived from the above-mentioned newspaper articles. Trust is a key factor for intelligence sharing and joint exercises; it underpins situational awareness, and determines the degree of disclosure and clearance access. The removal of NSA and Cyber Command key personnel together with the DOGE's poor cyber hygiene practices may diminish the trust of Japanese stakeholders involved in cyber and ICT dialogues as well as CERT coordination.

Furthermore, the open letters of concern from U.S cybersecurity professionals against the current administration have negatively impacted the United States' international credibility. This may deter Japan from engaging in future intelligence-sharing activities and joint cyber exercises, thereby affecting confidence-building measures, one of the core pillars of Japan's cyber diplomacy.

Time to Test Japan's Active Cyber Defense (ACD)

Japan's cyber defense based on deterrence by denial has increasingly been viewed as a barrier to decisive action against cyberattacks, as recognized also in the 2021 National Cybersecurity Strategy of Japan. The document called for the adoption of ACD to enable real-time threat disruption. In April 2025, the ACD bill passed successfully in the Lower House, with full implementation expected by 2027.

The legislation aims to improve coordination between private stakeholders, CERTs, Information Sharing Analysis Centers (ISACs) and the National Center of Incident Readiness and Strategy for Cybersecurity (NISC). At the practical level, it allows Japan to carry out AI-assisted offensive tactics to impede cyberattacks through deception technology, improving responsiveness and information sharing. These techniques also help isolate and analyze the threat while reducing incident response times.

While the ACD bill addresses cyberattack responsiveness, Japan still lacks a national cyber intelligence system. By creating a national cyber intelligence apparatus with an ISAC coordination center under the Prime Minister's office, Japan can improve cyber intelligence sharing among both internal and external actors. Moreover, Japan has proposed legislation to broaden the range of information that can be labeled as classified to improve intelligence sharing. Expanding the categories of confidentiality degree could establish a clearer hierarchy of information sharing with other governments.

Enhancing Relations with Third Parties

During the first Trump administration, Japan was prompted to diversify its strategic alliances beyond the U.S., particularly by strengthening engagement with ASEAN to counteract China's influence. In this context, cyber diplomacy has emerged as a useful instrument to mitigate the uncertainties of possible conflicts arising from cyberspace. It involves confidence-building measures (CBMs) that serve both as a deterrent and as a means to enhance predictability, transparency and crisis management.

Japan has proven the effectiveness of this approach through its cyber diplomacy, based on promoting the rule of law in cyberspace, CBM measures, and cyber capacity building initiatives with like-minded partners. Examples include the 2020 collective digital defense exercise involving more than 20 countries, and the establishment of the ASEAN-Japan Cybersecurity Capacity Building Center in 2018.

Japan should now strengthen these partnerships by leveraging its improved cyber capabilities. Cyber diplomacy should become Japan's first tool for improving situational awareness until the ACD is fully implemented. This could also enhance Japan's perception as a norm entrepreneur, especially when it comes to ASEAN, where a partnership focused on cyber capacity building, with an emphasis on marine cyber security, can function as a deterrence method.

Moreover, promoting regional CBMs, upgrading existing bilateral intelligence sharing agreements, and creating new ones with Five Eyes and Quad members can help provide a preliminary framework for collective cyber intelligence sharing among like-minded partners in the Indo-Pacific. In turn, this could lead to the development of customary practices and norms for countering cyberthreats, including joint attribution declarations and unified pressure on liable actors in international fora.

Conclusion

The largescale DOGE layoffs are leading to a weakening of the U.S. cyber intelligence system. This administrative upheaval conducted in less than 100 days into the second Trump administration is eroding operational effectiveness. In response, Japan must move with similar urgency to acquire sufficient cyber capabilities and set up cyber intelligence institutions to offset the vulnerabilities created by the weakening of the U.S. cyber defense apparatus. While the ACD already provides the grounds for greater resilience against cyberattacks, its implementation has to be accelerated and paired with the institution of a state-level cyber intelligence body. Together, these initiatives would position Japan to sustain and expand its cyber diplomacy efforts, especially with Indo-Pacific actors. By employing bilateral agreements as bases for collective ones, and CBMs for enhancing predictability and transparency, Japan can facilitate better crisis management. This would not only boost regional cyber intelligence flows but contribute to a stable regional order in the Indo-Pacific.

Giulia Saccone is an intern at the ISDP's Stockholm Center for South Asian and Indo-Pacific Affairs and member of the cybersecurity team at the International Team for the Study of Security Studies. She holds a bachelor's degree in Japanese Language and Culture from Ca' Foscari University of Venice, and an MSc in Asian Studies from Lund University.