Mapping the Future of US-Japan Cybersecurity Cooperation: Threat Hunting & Active Cyber Defense

Abstract

On November 3, 2023, the US-Japan NEXT Alliance Initiative convened a hybrid bilateral dialogue on the opportunity to enhance Japan-US cyber threat hunting collaboration. It also examined possible strategies for Japan's expanded use of Active Cyber Defense (ACD). Senior Director Jim Schoff welcomed a dozen American and Japanese specialists to the event from both governments, think tanks, and the private sector. Ms. Mihoko Matsubara (Chief Cybersecurity Strategist at NTT) and Mr. Taro Hashimoto (Visiting Fellow from NTT at the Center for Strategic and International Studies) gave opening presentations that touched on positive threat-hunting lessons from Ukraine's experience, as well as opportunities to develop closer ACD cooperation between government and Internet service providers. The group then discussed a range of related topics including cross-sector and multilateral cybersecurity cooperation, enhancing information-sharing infrastructure, and streamlining public-private and interagency relationships to build up shared knowledge more quickly about potential cyber threats. The allies can do more with technical collaboration in addition to sharing actionable cyber threat intelligence to raise defenses to enhance cyber resilience, especially leveraging the speed and global coverage of large private firms. This was the fourth cybersecurity dialogue hosted by the NEXT Alliance Initiative.

Opening Remarks

Ms. Mihoko Matsubara, Chief Cybersecurity Strategist at NTT, kicked off the event with a presentation entitled "Urgent Need for Japan-US Threat Hunting Collaboration." At its core, the presentation covered the efficacy of "threat hunting," citing cyber defenses by Ukraine, and indications that critical infrastructure services are currently under cyberattacks potentially related to future contingencies.

She opened by noting the differences between "red teaming" and "threat hunting." She defined *red teaming* as attacking one's own systems to find vulnerabilities and identify gaps in protection. This differs from *threat hunting* that begins with an assumption there is already an adversary in the system, but system managers are unaware of when, where, or how they were breached. This operation utilizes intelligence to look at the big picture of the threat landscape and then narrows down where threats are most likely.

Matsubara noted that at the end of 2021, in the months leading up to the war in Ukraine, the US Army Cyber Command and industry helped Ukraine with threat hunting according to the *Financial Times*. The joint team found wiper malware in Ukraine's railway network, which could have crippled this piece of critical infrastructure and disrupted Ukraine's ability to evacuate civilians and transfer military assets and vital supplies across the country.[1] Matsubara stressed that as geopolitical tensions in a region increase, it is vitally important to conduct threat hunting operations to manage supply chain risks and ensure a nation's resilience.

In the context of the Indo-Pacific, Matsubara clarified the urgency of conducting such operations in the region. She recalled a July 2023 ransomware attack on the Port of Nagoya that paralyzed cargo shipping for two days. She then cited a *Financial Times* article that said[2], "concerns have been raised at the highest levels in Tokyo over whether the incident was part of an attempt by state actors such as China to test Japan's defenses." Although not confirmed by either government, such

[1] Mehul Srivastava, Madhumita Murgia, and Hannah Murphy, "The secret US mission to bolster Ukraine's cyber defences ahead of Russia's invasion," *Financial Times*, 9 March 2022, https://www.ft.com/content/1fb2f592-4806-42fd-a6d5-735578651471.

[2] Leo Lewis, "Japan's Cyber Security Agency Suffers Months-Long Breach." *Financial Times*, August 29,. 2023, www.ft.com/content/de0042f8-a7ce-4db5-bf7b-aed8ad3a4cfd.

a disruptive cyberattack is concerning to both economic and national security in Japan and the United States.

Matsubara then discussed an ODNI (Office of the Director of National Intelligence) Annual Threat Assessment of the US Intelligence Community from February 2022 that said, "If Beijing feared that a major conflict with the US were imminent, it almost certainly would consider undertaking aggressive cyber operations against US homeland critical infrastructure and military assets worldwide." The ODNI document believes this type of cyberattack aims to impede US decision-making processes and hinder the deployment of forces. Furthermore, she noted that Microsoft had detected the "Volt Typhoon" cyber operation against critical infrastructure in Guam and the United States, and this cyberattack seems to pursue "development of capabilities that could disrupt critical communications infrastructure between the United States and the Asia region during future crises."[3] Although not confirmed by the US Government, a *New York Times* article from July 2023 stated that the government has started threat hunting in the networks of electric power, water, and telecommunication services to support US bases within and outside the country.[4]

Since Japan plays a crucial role in Indo-Pacific security and hosts US bases, Matsubara reminded event participants of the importance in enhancing threat hunting capabilities and actionable threat intelligence, as showcased by the collaboration between Ukraine and the United States prior to the invasion of Russia. She asserted that the US and Japan need to do more with technical collaboration in addition to sharing actionable cyber threat intelligence to raise defenses to enhance cyber resilience.

Mr. Taro Hashimoto, Visiting Fellow (from NTT) at the Japan Chair of the Center for Strategic and International Studies (CSIS) gave a presentation entitled "Japan's Active Cyber Defense – From Industry Perspective." He explained the overall Active Cyber Defense (ACD) concept in general, how it is implemented, and in what ways ACD differs and improves upon traditional cybersecurity systems. He noted that while there is no common definition for ACD, generally it is

[3] Microsoft, "Volt Typhoon targets US critical infrastructure with living-off-the-land techniques," May 24, 2023, https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/.

[4] Sanger, David E., and Julian E. Barnes. "U.S. Hunts Chinese Malware That Could Disrupt American Military Operations." *The New York Times*, The New York Times, July 29, 2023, www.nytimes.com/2023/07/29/us/politics/china-malware-us-military-bases-taiwan.html.

any kind of proactive operation on a spectrum between passive and offensive cyber defense. However, he underscored that the textbook definition is less important than understanding what Japan is trying to do based on its new National Security Strategy (NSS), which includes a heavy emphasis on cyber defenses focusing on ACD. Hashimoto used a slide to summarize what will change with the introduction of ACD specified in the NSS and in what ways it would best be implemented.

Japan's ACD at a glance (with some assumptions)

	Now	Future with ACD
Who	Government (NISC, NPA, JSDF, etc.)	Government (**New cyber organization** and others) in stronger cooperation with **private sector**
What	Government system	Government system and **critical infrastructure**
When	When cyberattacks are conducted as part of armed attack	When potential serious cyberattacks or their signs are identified, even if they **don't amount to an armed attack**
How	Reactively defend	**Proactively defend** – eliminate threats in advance and prevent the spread of damage

Necessary measures to implement ACD:

(a) **Enhance public and private partnership**

(b) **Detect attacker infrastructure using information provided by ISPs**

(c) **Authorize government to operate against attacker infrastructure**

Hashimoto's presentation was guided by points (a) (b) and (c) described in the NSS, as summarized at the bottom of the above slide. He emphasized (a) as the most important and foundational for national cybersecurity, noting that it would intend to enhance especially government's cyber capabilities, authorities, and resources, which will lead to driving bidirectional and operational public-private collaboration. He added that for proactive cyber operations with international public-private partners, speed is the key. He noted that industry is generally able to act quickly when it comes to security operations with its technical expertise, and it can add speed to public-private cooperation. It can also provide threat/incident information with global coverage as a front-line resource. He emphasized that the most effective way to mitigate potential damage is to mount a strong defense that can be executed proactively at speed before attacks expand.

Hashimoto outlined some areas of potential improvement for the Japanese government, noting that it needs more technical experts and coordinators working with various partners domestically and

internationally. He mentioned some of the positive steps the government is taking recently, such as the Self-Defense Forces (SDF) and National Police Agency (NPA) expanding their cyber capabilities, as well as a new cyber organization being prepared based on the NSS. He also noted that this could be another area where industry could contribute in different ways, including exchanging human resources and providing training.

Hashimoto noted that Japan should consider a wide range of proactive operations with the goal of defending against attacks. He added that while offensive capabilities like (c) may be effective in some cases, having it alone would not necessarily be a perfect solution. He suggested a combined approach of vulnerability handling, information sharing, advisory, attribution, filtering, disrupting operations, and other tools as the most effective way for Japan to realize ACD and be truly proactive at speed against potential attacks. Hashimoto asserted that discussion regarding Japan's ACD is ongoing, and that further moves from the government will likely be seen in the coming months.

Discussion Summary

In the discussion segment, participants focused on public-private sector partnership strategy and the tactics that could promote greater cross-sector, cross-border, and interagency cooperation.

An American participant emphasized speed as the key in cyber operations. He said that for the successful execution of any strategy, leadership and workforce development is critical to private sector and government cooperation. Another participant said it is attribution that takes the longest, yet the most immediately helpful are the indicators of compromised networks and certain technical information, which only private sector companies could provide. They continued by saying that while they noticed a maturation of the threat hunting process, our governments should now resource critical infrastructure companies to conduct hunts with the expectation that they would share information back and across the sector.

An American participant noted that Volt Typhoon revealed a lack of US-Japan information sharing until just before the public announcement, and he wondered how to address this if information sharing is so critical. A Japanese participant said she believed an intelligence-sharing framework and info-sharing infrastructure for cybersecurity is needed between the allied nations. Others

suggested that Japan's planned reform of its National Center of Incident Readiness and Strategy for Cybersecurity (NISC) should be a good nexus point for the allies, if sufficiently empowered for information security. A third participant said the private sector would be able to help support such a mechanism, as it could generate reports on incidents that do not have the same threshold for secrecy that government intelligence reports must go through before release. She said that a difficult part of conducting cyber operations is addressing actionable info and contextualizing priorities. Sharing of incidents and indicators of compromise can currently be done with greater efficiency, but knitting the pieces together with context will take longer to develop.

An American participant concurred, saying that sorting out live fluid incidents and identifying priorities for government is a key role the private sector could play. Another participant added that an important part is pulling together the tactics, techniques, and procedures (TTPs) that different companies and governments utilize, which could help with the attribution process. She continued by noting the example of MITRE ATT&CK, a globally accessible knowledge base of adversary tactics and techniques based on real-world observations,[5] which pulls together all the TTPs that companies and governments find together and contributes to attribution as the TTPs identify patterns in the approaches of bad actors through this crowd source database. The database helps to identify these pieces and thus allows companies to familiarize themselves with those TTPs when threat hunting, in addition to sharing who else has seen similar actions by bad actors.

An American participant added another example of a public-private partnership that has good potential (called InfraGard with over 80,000 individual members), involving the FBI and the private critical infrastructure sector. He thought that a modified version of InfraGard could be developed to provide an important interface between the government and private sector companies for cross-border information sharing.

An American participant, asking about gray-zone conflicts, wanted to understand gradations of authorities within Japanese industry and asked if companies possessed the authorities to threat hunt within their own networks. The participant was particularly curious about Internet Service Providers (ISPs), and whether they had the authority to do what needed to be done. A Japanese

[5] "Mitre ATT&CK®." *MITRE ATT&CK®*, attack.mitre.org/. Accessed 4 Dec. 2023.

participant responded that ISPs' network operations are generally restricted strictly by law to protect the secrecy of communications, but some operations are permitted if they are considered as legitimate businesses for them or necessary operations to protect their own network. This can be a matter of legal interpretation which needs to be discussed among a panel of experts and include the government.

Another Japanese participant added that if private companies (including critical infrastructure companies) want to do red teaming or threat hunting, they can, but what the three new Japanese national security documents allow for is the Ministry of Defense (MOD) and SDF to help protect industry assets from cyber threats. The Japanese Defense Buildup Plan occurring in this decade will improve SDF and MOD threat hunting capabilities. The participant also noted that if the MOD cannot directly help with threat hunting operations, they are not prohibited from helping with important tests through other contractors. The participant underscored the ideal state would be for the government, SDF, and industry to steadily improve their collaboration and information sharing.

NEXT Steps

Senior Director Schoff closed the event by thanking the participants for the lively dialogue, good discussion examples, and for their insightful comments. He planned to continue the discussion in another iteration of the series, perhaps through a lens of cooperation with Taiwan on threat hunting. The goal of the NEXT Alliance Initiative is to build on the important takeaways of the cyber advisory committee events to begin building its "Alliance Mapping Tool" before the end of the fiscal year in March of 2024.

---

*The **US-Japan NEXT Alliance Initiative** is a forum for bilateral dialogue, networking, and the development of joint recommendations involving a wide range of policy and technical specialists (in and out of government) to stimulate new alliance connections across foreign, security, and technology policy areas. Established by Sasakawa Peace Foundation USA with support from the Nippon Foundation, the goal is to help improve the alliance and how it serves shared interests, preparing it for emerging challenges within an increasingly complex and dynamic geostrategic environment. Launched in 2021, the Initiative includes two overlapping lines of effort: 1) Foreign & Security Policy, and 2) Technology & Innovation Connections. The Initiative is led by Sr. Director Jim Schoff.*