COLUMBIA UNIVERSITY
Weatherhead East Asian Institute

US-JAPAN CYBER COOPERATION:

Meeting Challenges & Operationalizing Opportunities

2023 December

By Greg Rattray
& Seungmin (Helen) Lee

FOREWORD

Columbia University's Japan Research Program is pleased to publish the following research by Greg Rattray and Seungmin (Helen) Lee on US-Japan cyber cooperation. It provides an important overview of developments in Japanese cybersecurity policy and actions since the adoption of a new National Security Strategy in December 2022 and offers several important recommendations for strengthening Japan's cybersecurity defences and better integrating Japanese and US cybersecurity policies. It emphasizes the importance of Japan developing a strong security clearance system, recruiting more cyber specialists, enhancing its cyber preparedness, and increasing collaboration in cybersecurity with the United States.

The authors wish to thank US Admiral (ret.) Dennis Blair and NTT CEO Shinichi Yokohama for their advice and review of the paper and the Japan Research Program at Columbia University's Weatherhead East Asian Institute and its Director, Gerald Curtis, for support for the publication of this research.

AUTHORS

Greg Rattray is Partner and Co-Founder of Next Peak LLC and the Executive Director of the Cyber Defense Assistance Collaborative (CDAC). Greg previously served as the Global Chief Information Security Officer (CISO) at JPMorgan Chase, founding partner and CEO of Delta Risk LLC, and the Chief Internet Security Advisor to the Internet Corporation for Assigned Names and Numbers (ICANN). Over his career, Greg has worked with various Japanese organizations including JPCERT/CC, the Japan External Trade Organization (JETRO), the IT Promotion Agency (IPA), the National Center for Incident Readiness Strategy and Cybersecurity (NISC), and the Digital Agency. Greg served in the US Air Force as a Colonel until 2007 and was the Director for Cybersecurity in the White House. A thought leader in cyber security, Greg established the concepts of Advanced Persistent Threat and Operational Collaboration. In his capacity as Senior Adjunct Researcher at Columbia University SIPA, Greg initiated the Global Cyber Dialogues including between Columbia and Keio University's Cyber Civilization Research Center (CCRC). Greg has a B.S. degree from the USAF Academy, a M.P.P. from the John F. Kennedy School of Government, Harvard University and a Ph.D. from the Fletcher School of Law and Diplomacy, Tufts University.

Seungmin (Helen) Lee is a Cyber Risk Analyst with Next Peak and a Program Associate with Cyber Defense Assistance Collaborative (CDAC). As a cyber risk analyst, Helen assists with cybersecurity risk and management consulting, and as a program associate at CDAC, she leads the blue force tracker initiative, recording and analyzing international technological defense assistance provided to Ukraine since the onset of the war in 2022. She received her MIA at Columbia University's School of International and Public Affairs in May 2022 and B.A. at Columbia College in May 2021. Helen is fluent in English, Korean, Spanish, Japanese and proficient in Chinese.

INTRODUCTION

With the issuance of its 2022 National Security Strategy (NSS), Japan recognized cybersecurity as an area of priority concern. The process of implementing the NSS activities provides a unique opportunity for increased US-Japan cyber cooperation. Historically, positive diplomatic declarations of collaboration have occurred along with technical coordination within the computer emergency and response team (CERT) community. Yet, limitations exist in operationalizing the partnership at the national security level. Constraints have included the lack of an effective security clearance system extending to the private sector, limited operational cyber capacity of the Japanese government organizations, and less than fully developed public-private partnerships (PPPs). The United States has had competing priorities and until recently, limited ability to invest in a deeper partnership as well. However, we are at an auspicious moment in terms of both opportunities and challenges. By building on existing frameworks of defense cooperation, establishing PPP across the Pacific, and developing joint training and exercise programs, the United States and Japan can deepen operational cyber cooperation.

THE EVOLUTION OF US-JAPAN SECURITY COOPERATION

The post-World War II (WWII) US-Japan security cooperation formally began in 1951 with the US-Japan Mutual Security Treaty, allowing US armed forces to be stationed in Japan. The 1960 revision of the Treaty provided for US bases in Japan and a commitment by the US to defend Japan. The severe limits on the nation's ability to use armed forces imposed by the postwar Japanese Constitution, although they have been relaxed over time, have continued to inhibit the Japanese from fully contributing to security cooperation with the US.

The evolution of geopolitics, particularly tensions with China, has accelerated change in the Japanese national security perspective. Friction between China and Japan over the East China Sea and the Senkaku Islands/Diaoyu flared in 2010, increasing Japan's worries of Chinese expansionism. In 2012, those concerns heightened as China sharply increased its presence in the East China Sea in response to the Japanese government acquiring three of the five uninhabited Senkaku Islands from their private Japanese owners. Concerns about China and North Korea led to Japan's 2015 historic interpretation of its constitution, allowing participation in collective defense operations with the United States in certain limited situations. Furthermore, the Quadrilateral Security Dialogue (Quad)—a group of Indo-Pacific democracies including Australia, Japan, India, and the United States—was revitalized in 2017, in large part to provide a counterbalance to China.

The US and Japanese governments and technical communities have historically coordinated on cyber security. The CERT/Coordinating Center (CC) at Carnegie Mellon University's Software Engineering Institute, the US CERT in the Department of Homeland Security (DHS), and Japan's JPCERT/CC have been close collaborators for over two decades. Japan has joined Western efforts to enhance an open and secure global cyberspace by supporting the Budapest Convention on Cybercrime and the United Nation's norms of responsible state behaviour in cyberspace. The 2011 US-Japan Security Consultative committee's joint statement included cyberspace as an area of mutual interest as well as the establishment of bilateral strategic policy dialogue on cybersecurity for effective cooperation in promoting the resilience of critical infrastructure, information security, and space systems. In recent years, the United States and Japan have sustained a bilateral cybersecurity dialogue, generally calling for continued cooperation but with limited operational collaboration.

CURRENT SECURITY CONTEXT IN JAPAN

The rise of China over the past 20 years coupled with its increasing aggressive diplomatic, military, and economic policies have produced a major reframing of how Japan views its national security. China has been intruding into Japanese airspace around the Senkaku Islands. In 2021, the Japan Air Self-Defense Force reacted 722 times against Chinese aircrafts' overflight into Japanese airspace, and 652 of those incidents occurred in the airspace over the Senkaku Islands. Additionally, in November 2022, the Japanese Ministry of Defense (MoD) announced that China's People's Liberation Army Navy (PLAN) intruded into Japanese waters five times since October 2021, setting a record high.

Along with the Senkaku Islands issue, Japan is increasingly concerned about potential Chinese aggression in the Taiwan Strait. In April 2021, then Japanese Prime Minister Yoshihide Suga and US President Joe Biden released a joint statement highlighting the mutual interest of both countries in peace and stability across the Taiwan Strait. This declaration was the first time since 1969 in which Japan and the United States mentioned Taiwan in a joint statement. According to an Asahi Shimbun's survey in May 2023, some 80% of Japanese are worried that a Taiwan Strait conflict between the United States and China would involve Japan.

North Korea, long a security concern, has evolved into a multi-faceted threat for Japan. Over the past decade, North Korea's nuclear and ballistic missile programs have accelerated. The 2023 annual "Defense of Japan" white paper stated that "North Korea's military activities pose[d] an even more grave and imminent threat to Japan's national security than ever

before," with an unprecedently high frequency in missile testing and the development of long-range cruise missiles. North Korean cybercrime is also of concern for the Japanese as North Korean hackers use stolen cryptocurrency to fund the country's weapons programs.

Although defense cooperation with Japan has been hindered by unresolved historical issues, recent mutual security concerns between Japan and South Korea over China and North Korea have created incentives for both countries to seek a normalization of relations and a resumption of defense cooperation. In March 2023, a bilateral summit between South Korean and Japanese leaders took place for the first time in over a decade. In 2023 South Korean President Yoon Suk Yeol, Japanese Prime Minister Fumio Kishida, and US President Joe Biden held a historic meeting at Camp David. The three leaders agreed to annual multi-domain military exercises as well as deeper information sharing on North Korean missile and cyber activities.

CURRENT STATE OF CYBER AFFAIRS

Along with the recent changes to Japan's overall national security posture, its approach to cyber defense as a national security concern has also dramatically shifted. A growing recognition of the significance of national security-related cyber breaches as well as the limitations of Japanese national and enterprise cyber programs exist. Chief Cabinet Secretary Hirokazu Matsuno publicly stated in July 2023 after the Nagoya Port cyberattack: "It is increasingly important to improve the defense and resilience of the information systems of Japan's infrastructure." The chart from Nikkei Asia provides an example of increasing media coverage as well as increasing detected cyberattacks in Japan.

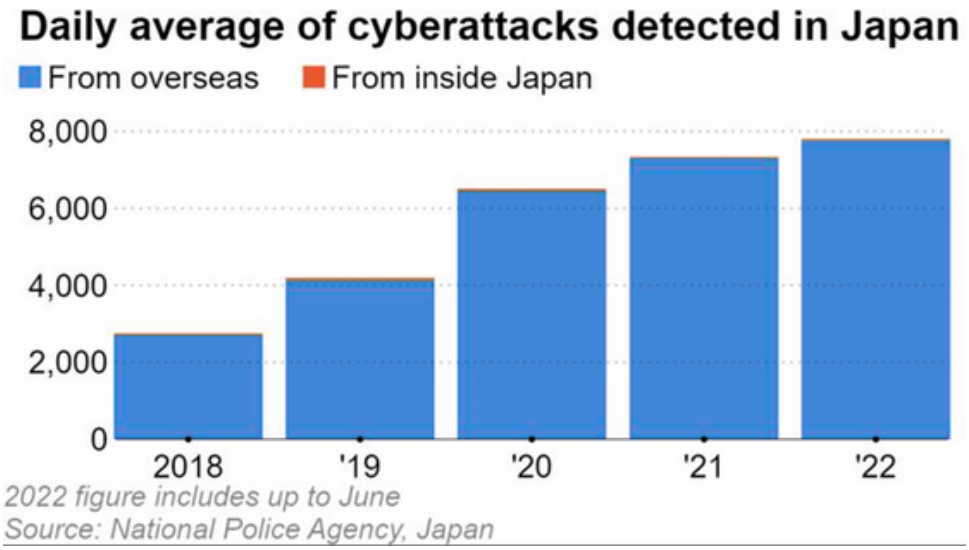

*Chart Source: *Cyberattacks on Japan soar as hackers target vulnerabilities – Nikkei Asia*

According to Japan's National Police Agency (NPA), there were about 7,800 cyberattack cases in Japan from foreign nations in the first half of 2022, which was double the number of cases in 2019. There also was a surge in cyberattacks against Japanese companies and government offices from March 2023 up to the May 2023 Group of Seven summit hosted in Japan. Targets in these attacks included the West Japan Railway, Tokyo Electric Power Company Holdings, local governments of Osaka, Aichi, Kumamoto, and Nara, as well as the Cabinet Office's public relations' websites. Since 2017 Japan has lost $720 million worth of cryptocurrency to hackers affiliated with North Korea, which makes up 30% of such losses worldwide; Japan is the nation with the biggest cryptocurrency losses to North Korean hackers. The number of ransomware attacks also increased by 57% between 2021 and 2022. Appendix A provides a listing of notable cyber incidents in Japan since May 2020.

Increase in cyberattacks contributed to the public dialogue about the need to meet Japan's cyber challenges. Public and private exchanges have increased between US and Japanese leaders seeking to understand and help improve Japanese capabilities, including the Multilateral Cyber Action Committee (MCAC).[1] In November 2022, Yomiuri Shinbun published an article calling for Japan to have a cyber security command post directing active cyber defense. In the article, US Admiral (ret.) Dennis Blair, the former US Director of National Intelligence and Commander of USPACOM, was quoted as describing Japan's cyber efforts as 'minor league' at a meeting of Japan's Liberal Democratic Party (LDP) security subcommittee in an effort to prompt recognition of the serious national uplift Japan needs to undertake. Over the past year, broad acknowledgment of the need to evolve the Japanese cybersecurity posture and strategy has occurred within the political and governmental leadership.

The 2022 National Security Strategy (NSS) strongly reflected these concerns. The NSS, also influenced by the hybrid war in Ukraine, stated the need for a much stronger national cybersecurity program that includes deeper PPPs and a nationally directed capability to perform active cyber defense. Furthermore, the 2022 NSS called for the government to strengthen its ability to analyze and aggregate the situation on disinformation, use of artificial intelligence (AI) to enhance monitoring of the information space, and restructure the Cabinet's National Center for Incident Readiness and Strategy for Cybersecurity (NISC) to coordinate cybersecurity policies with Japan's Self-Defense Force's (JSDF) and the police's cyber units. The MoD plans to train 4,000 cyber "warriors" and 16,000 JSDF personnel in cybersecurity in five years. Over the next five years, Japan also plans to spend $58 billion for cybersecurity and space defense.

Initiatives in the Diet, Cabinet, ministries, and agencies are already underway to operationalize the NSS objectives. The LDP's 2023 Digital Policy Recommendations for Enhancing Security[2] recommends establishing an information sharing system with the private sector and implementing joint public-private exercises. The document also supports the strengthening of the nation's digital infrastructure under the new Digital Agency. The document recommends monitoring cyber developments and establishing international exercises such as a Japan-Australia joint exercise resembling Locked Shields 2023.

Japan has also been making clear its desire to strengthen cybersecurity cooperation with the United States. This desire is explicitly mentioned in the new US-Japan alliance framework outlined in the NSS. Japanese government officials are increasingly engaging US cyber leaders to learn about the takeaways from the war in Ukraine and to seek more US support and advocacy for a Japanese cyber effort.[3] Japan has been supporting Ukraine through the Japan International Cooperation Agency. Japan is also looking to increase its cooperation with the Five Eyes intelligence sharing network and is pushing to expand the framework of Five Eyes beyond the English-speaking democracies.

The United States has reciprocated the interest in US-Japan cyber cooperation as well. Since fall 2020, senior US national security advisors have been warning Japan of Chinese state hackers infiltrating Japanese defense networks. In November 2021, Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger discussed next steps for deeper cyber defense collaboration with Japan. In December 2022, US National Cyber Director Chris Inglis visited Japan to share the US government's upcoming national cybersecurity strategy seeking to enhance synergies between the two national cyber strategies. The Biden Administration's 2022 Indo-Pacific Strategy also highlighted the need to strengthen strategic partnerships in the region, especially in cyberspace.

The bilateral and mutual interest in US-Japan cyber cooperation led to the Joint Statement of 2023 US-Japan Security Committee ("2+2") which agreed to collaborate on countering increasingly sophisticated and persistent cyber threats. Japan's Ministry of Economy, Trade and Industry and the DHS signed a Memorandum of Cooperation on cybersecurity in early January 2023 to increase operational collaboration, enhance security of industrial control systems, deepen capacity building for the Indo-Pacific Region, and establish an ongoing dialogue. A strong step in the right direction was the September 2023 Joint Cybersecurity Advisory from US Cybersecurity and Infrastructure Security Agency (CISA), US National Security Agency, US Federal Bureau of Investigation (FBI), Japan's NPA, and Japan's NISC

regarding Chinese cyber activity targeting government, industrial, technology, media, electronics, telecommunication, and defense industrial base sectors. The growing collaboration also extends to engaging with the Japanese private sector. Recently, NTT Corporation—the largest Japanese and fourth largest global telecommunications company—joined the DHS's Joint Cyber Defense Collaborative (JCDC), setting a precedent for trans-Pacific PPP that needs to extend to more companies.

Multilaterally, the focus of US-Japan cooperation is also shifting towards cybersecurity. The Quad has called for increased cooperation on cybersecurity, deployment of secure 5G technology, and multilateral research on AI. The 2022 Quad Leaders' Tokyo Summit launched a Critical and Emerging Technologies Working Group which included cooperation on interoperability and telecommunications cybersecurity, improved software, and coordination of cyber security standards for managed service providers. The 2023 Quad Leaders' Joint Statement reaffirmed the nations' commitment to a more secure cyberspace and launched the first Quad Cyber Challenge, an initiative to promote cyber awareness and empower Indo-Pacific participants to protect themselves in the cyberspace.

CHALLENGES FOR THE US-JAPAN CYBER COOPERATION

Despite growing Japanese cybersecurity awareness and mutual interest in a US-Japan cyber cooperation, challenges for US-Japan cooperation remain for both nations. For Japan, legal restrictions on operations outside of the country and constraints imposed by the Constitution's Article 9 continue to have significant resonance with the public and the media. Calls for constitutional change as well as increases in the defense budget continue to face resistance. Japan's legacy of lacking underinvestment in cybersecurity inhibits the ability to pursue other types of security collaboration due to worries about loss of sensitive information and technology. The International Institute for Strategic Studies' 2021 report titled "Cyber Capabilities and National Power" classified Japan in the lowest tier, tier 3. The small size of its cyber force, limited funding for cyber defense, current lack of an established national cybersecurity program and leadership, and the shortage of cybersecurity expertise are also limitations to deeper cyber cooperation. Finally, the limited depth and breadth of PPPs in cybersecurity and critical infrastructure protection constrain the ability to conduct operational collaboration with all the necessary stakeholders.

For the United States, competing priorities limit the State Department and interagency resources available to deepen operational collaboration with Japan despite highly positive joint statements. The United States limits its technology and intelligence sharing with Japan due to concerns over Japan's lagging cybersecurity systems and lack of a security clearance system that includes private sector companies and researchers. Additionally, a major capability gap exists between the US and Japanese cyber systems. The United States issued its first National Strategy to Secure Cyberspace in 2003. In the last two decades, the Department of Defense (DoD), intelligence community, DHS, FBI, and other government agencies have built-up their capabilities. Major efforts to increase cyber security of vital companies and operational nodes within key critical infrastructure sectors have occurred. The US cybersecurity industry's global leadership has continued to grow, driven in part by the dominance of US-based tech platforms. In comparison, Japan only formed its NISC in 2015 and lacks a strong national program and investment in cybersecurity across both government and much of the private sector. In the military sphere, the United States established Cyber Command (CYBERCOM) in 2010. As of 2019, CYBERCOM had 133 teams and 6,200 personnel and continues to grow. Japan created its military cyber unit—the Cyber Defense group—in 2014, and as of 2022, contains a little more than 500 personnel. Further, Japan lacks programs and well-trained, experienced personnel in cyber threat intelligence and "hunting" operations to find adversarial activity.

RECOMMENDATIONS FOR COOPERATION

Despite the challenges, Japan and the United States can build on existing programs and learn from experience over the past twenty years to ensure deeper collaboration that improves both nations' national security. The growing Chinese and North Korean threats make deeper collaboration essential. Such activities should leverage existing US-Japan security forums and processes for military-to-military collaboration as much as possible. Our recommendations for deepening US-Japan cyber cooperation follow below.

1) INTRODUCE A SECURITY CLEARANCE SYSTEM IN JAPAN

As noted, the United States limits its technology and intelligence sharing with Japan due to the lack of an information classification and a security clearance system. The United States expanded its approach to providing national security information and clearances after 9/11. The United States can help provide guidance on the parameters for a Japanese security clearance system that would mitigate concerns over sharing sensitive information and technology as well as potentially

allow collaboration on how to implement procedures and train personnel. The Japanese Diet is actively considering how to provide implementation guidance for the government's information classification and security clearance system and is seeking ways to allow for Japanese industry participation in sensitive technological research and development. In the meantime, the United States and Japan can expand on pre-existing high-level information sharing and cooperation agreements such as the agreement that allows for Japan, the United States, and Australia to share submarine technology, beginning to overcome the concern that previously existed in this area.[4]

2) COMMITTED PLANNING AND ROADMAP TO DEEPEN US-JAPAN CYBER COOPERATION

The United States and Japan should maintain a high-level steering committee with key governmental and private sector leaders to establish a long-term roadmap and accountability for progress on US-Japan cyber cooperation focused on strengthening operational capabilities and joint planning and exercises along with the private sector. A small, standing joint steering committee focused on cyber collaboration planning within the US-Japan Security Consultative Committee structure could facilitate quarterly meetings to ensure coordination of the agenda and input from working groups. This steering committee should include private sector leaders. Working groups should meet monthly to discuss progress on key operational collaboration projects such as those outlined below and actively address key issues blocking progress in a timely fashion.

3) OPERATIONAL COLLABORATION ON PLANNING, TRAINING, AND EXERCISING

While ongoing dialogue is necessary for deeper cooperation, talks must move beyond and operationalize actions. Joint US-Japanese assessment, planning, training, exercise, and resiliency programs should be executed with a focus on understanding the vulnerability of critical infrastructure that would support military operations and bases in Japan if a Taiwan Strait Crisis were to escalate. These activities should be on-going and inclusive of a broad spectrum of key public and private organizations. Joint operational collaboration will also help develop doctrine and concepts of operations for Japan's active cyber defense activities in coordination with the United States. Further, the two countries should establish joint cyber ranges to establish a broader joint training and evaluation program, such as military activities between cyber organizations to improve full spectrum operations.[5] The range environments will facilitate broader training and exercise programs that include key critical infrastructure companies for detection and eradication of advanced persistent threats to economic and national security. Such

range environments could include both those focused on military and classified operations as well as those designed to enhance the cyber defense posture and personnel of non-national security agencies and critical infrastructure operators.

4) STRENGTHENING JAPANESE CAPABILITIES FOR THREAT IDENTIFICATION AND ERADICATION

The 2022 NSS directly called for the establishment of active cyber defense capabilities which is generally conceived of as a spectrum of possible activities. Subsequently, a productive discussion regarding the composition of a Japanese active cyber defense program and potential fruitful initial steps has emerged. Japan should focus on stronger cyber threat intelligence capabilities to effectively identify the presence and tactics of on-going adversarial cyber campaigns in collaboration with US government, other allies, and private sector companies. Such focused intelligence could serve as the basis for the establishment of "threat hunting" teams capable of operating on Japanese government and critical infrastructure networks to search for and help eradicate adversarial activity. Proper authorities will need to be in place, and growing such capabilities at scale will require focused organizational structures and talent. US government and companies can provide productive approaches to hunt operations and train operators in the Japanese public and private sectors, especially if joint range environments are in place.

5) STRENGTHEN CROSS-PACIFIC PUBLIC PRIVATE PARTNERSHIPS

There are various ways that the United States, Japan, and their allies can strengthen the essential role of the private sector in operational collaboration. Japan has world class technology talent and organizations with deep information technology and networking expertise. The United States should continue to engage Japan with lessons from over two decades of experience seeking to build effective PPPs. A successful example is Japan's adoption of the Finance-ISAC model into its own Financials-ISAC Japan (F-ISAC JP). The United States established Information Sharing and Analysis Centers (ISACs) in 1998 in order to create industry-specific organizations, to gather and share cyber threat information to critical infrastructures, and to facilitate data sharing between public and private sector groups. Japan created F-ISAC JP in 2018, and it has become a respected cyber threat sharing and analysis hub for Japan. The United States can help Japan establish operational approaches and learn stakeholder management to focus on deeper collaboration that addresses national cybersecurity concerns such as the Analysis and Resilience Center for Systemic Risk and CISA's JCDC.

The Japanese government must allow for bidirectional information sharing between the public

and private sector and should consider mechanisms for visualization, rapid information dissemination, and prioritization or triaging of cyber incidents. The Australian Signals Directorate's Australian Cyber Security Centre Partnership (ACSC) Partnership Program provides a good example. The ACSC Program includes cybersecurity experts from government, industry, academia, and research space who come together to increase situational awareness, technical expertise, and insights as well as collaborate on threats and opportunities.

Japan and the United States should also pursue bilateral PPP coordination and exercises that engage the private and public sector of both nations. Public-private information sharing will help engage the private sector when cyber risks to supply chains and geopolitical crises arise. Joint US and Japan exercises with the private sector that leverage the JCDC—a bridge that has been started by NTT—can develop mutual understanding of challenges and scenarios to drive training, development of response capabilities, and opportunities for collaboration. The two governments should encourage multinational companies with strong presence in both countries, such as Toyota and Mastercard, to actively engage in PPP. The learnings from these exercises should help create a joint national response process to future cyber conflicts involving both countries. Japan is showing increasing interest in the US Cyber Defense Assistance Collaborative (CDAC), a group of leading cybersecurity companies that are providing operational cyber defense to Ukraine since the 2022 Russian invasion. Japan has already begun attempting the creation of its own J-CDAC, [6] and Japanese companies can participate in the US CDAC as well.

CONCLUSION

The United States and Japan have established a strong security collaboration since WWII. Recent geopolitical tensions resulting from aggressive Chinese actions around the Senkaku Islands and in the Taiwan Strait as well as North Korea's increasing military activity and cybercrime make imperative even deeper US-Japan cooperation. The high number of cyberattacks have contributed to Japan's realization of cybersecurity as a key national security concern and of the limitations of its current cyber defenses. Japan's 2022 NSS reflects a focus on improving cybersecurity capabilities and a new framework for the US-Japan alliance. Both the United States and Japan are eager for deeper cyber cooperation as reflected by recent bilateral and multilateral declarations and efforts.

However, challenges for a deeper cyber cooperation remain. These include Japan's legislative restrictions, lack of a security clearance system, and limited national cyber capabilities. The United States also continues to have competing priorities in committing to US-Japan cyber cooperation. This paper proposes recommendations to move forward, namely, to improve the

Japanese capabilities for threat identification and eradication; and pursue a joint approach to PPP with major private sector players. The geopolitics of the next decade in East Asia will rapidly create increasing cyber challenges for the United States and Japan. The time for both nations to move forward together is now.

APPENDIX A: NOTABLE CYBER INCIDENTS IN JAPAN SINCE MAY 2020

DATE	TARGET	DESCRIPTION
May 7, 2020	Nippon Telegraph & Telephone (NTT)	Hackers breached several layers of IT infrastructure, reached an internal Active Directory, and stole 621 customers' data.
Jun 2020	Honda Motor Co 7267.T	Ekans ransomware attack affected computer server access, mail usage, and internal system usage leading to a global halt in operations.
Jun 21, 2020	Various countries and organizations including Japan and the Japanese Ministry of Finance	North Korea's Lazarus Group sent COVID-19-themed phishing emails to 5 million businesses and individuals across 6 countries and claimed to have 1.1 million individual's email IDs.
Jun 2020–Oct 2020	Japan's construction, manufacturing, and government organizations	Chinese hackers' 11 ransomware attacks including one using the Pulse Secure flaw.
Oct 2020	South Korea, US, and Japan	North Korean government-linked hacker group Kimsuky conducted intelligence-gathering intrusions against targets in Japan.
Nov 2020	Capcom	Ragnar Locker ransomware used to compromise devices, steal 1TB of sensitive data and 350,000 confidential documents, and demand a $11 million ransom in return for not publishing the data and offering a decryption tool.

May 24, 2021	Japanese agencies	Breached via Fujitsu's ProjectWEB information sharing tool and stole customer data including 76,000 email addresses.
Jul 1, 2021	Kawasaki Kisen Kaisha ("K" Line)	Overseas subsidiary systems' computers breached for the second time in months.
Jul 23, 2021–Sep 5, 2021	Tokyo Olympics and Paralympics	450 million cyberattack attempts on the official website and organizing committee's system.
May 21, 2020–Aug 18, 2021	Japanese beauty e-trailer Acro	Third-party data breach of more than 100,000 payment cards across two of Acro's four websites.
Jun 22, 2021–Nov 3, 2021	Panasonic	Network infiltration and data breach occurred.
Mar 1, 2022	Toyota Motor	Cyberattack on a supplier on ground led to the halt of 14 factories and the suspension of 13,000 vehicles' outputs.
Mar 13, 2022	Morinaga	Unauthorized access to the servers by a third party led to the leak of 1,648,922 customers' personal data.
June 2022	Japanese political establishments	Chinese-speaking advanced persistent threat (APT) actor MirrorFace's spear-phishing campaign Operation LiberalFace using backdoor LODEINFO to deliver malware.
Sep 7, 2022	Japanese companies and government ministries	Japanese companies and government ministries

Jul 6, 2023	Nagoya Port	Russian-based cybercrime organization Lockbit executed a ransomware attack that affected 15,000 containers and related businesses.

ENDNOTES

[1] The MCAC involved global cyber leaders seeking to characterize and make recommendation regarding cyber risks. Its principal report is titled "Implications for Cybersecurity in Western-Chinese Technology Decoupling" and was published by CSIS in March 2022. The MCAC continues a focused dialogue and visits between US and Japanese leaders including Admiral Dennis Blair and one of the paper's authors, Greg Rattray.

[2] "Digital Policy Recommendations for Enhancing Security," Liberal Democratic Party of Japan, Headquarters of the Promotion of Digital Society, Project Team for Digital Security, April 19, 2023.

[3] Insight from Greg Rattray's meetings with Japanese officials in February and June 2023.

[4] In the 1980's, the Soviet government procured sensitive information on submarine technology from Japanese company Toshiba, inciting US concern of sensitive information leakage from Japan.

[5] Full spectrum operations refer to a combination of offensive, defensive, and stability operations overseas or on US soil.

[6] Insights from Greg Rattray's trip to Japan in June 2023. The Japanese have informed both former and current US national cybersecurity leaders about their J-CDAC intent.


COLUMBIA UNIVERSITY
Weatherhead East Asian Institute