PACIFIC FORUM

US-Japan Cybersecurity Cooperation:

BEYOND THE TOKYO 2020 OLYMPICS

Edited by:

Mark Bryan Manantan
Crystal Pryor, Ph.D.

PACIFIC FORUM INTERNATIONAL

Based in Honolulu, the Pacific Forum (www.pacforum.org) is a foreign policy research institute focused on the Asia-Pacific Region. Founded in 1975, the Pacific Forum collaborates with a broad network of research institutes from around the Pacific Rim, drawing on Asian perspectives and disseminating project findings and recommendations to global leaders, governments, and members of the public throughout the region. The Forum's programs encompass current and emerging political, security, economic, maritime, and technology policy issues, and works to help stimulate cooperative policies through rigorous research, analyses and dialogues.

PACIFIC FORUM
INTERNATIONAL

US-Japan Cybersecurity Cooperation:

Beyond the Tokyo 2020 Olympics

Edited by
Mark Bryan Manantan
Crystal Pryor, Ph.D.

Acknowledgments

The completion of this Special Edited Volume would have not been possible without the generous contributions of our featured authors, and the active participation and support from all the speakers, advisors, and participants during the US-Japan Virtual Forum on Cybersecurity Cooperation: Beyond the Tokyo 2020 Olympics.

Table of Contents

ABOUT THE AUTHORS 1

INTRODUCTION 3

KEY FINDINGS FROM THE US-JAPAN VIRTUAL FORUM ON CYBERSECURITY COOPERATION: BEYOND THE TOKYO OLYMPICS 2020 6

1. NEXT STEPS FOR US-JAPAN CYBERSECURITY COOPERATION AFTER TOKYO 2020

Mihoko Matsubara 12

2. THREATS & TRENDS IN CRITICAL NATIONAL INFRASTRUCTURE

Gregory Winger, Ph.D. 17

3. STRENGTHENING US-JAPAN COOPERATION ON PROTECTION OF CRITICAL NATIONAL INFRASTRUCTURE

Benjamin Bartlett, Ph.D. 21

4. SEIZING ON US-JAPAN OPPORTUNITIES FOR SUBMARINE CABLE SECURITY

Justin Sherman 25

5. US-JAPAN CYBERSECURITY COOPERATION

Professor Wilhelm Vosse, Ph.D. 29

6. THE CYBER AI NEXUS: IMPLICATIONS FOR THE US-JAPAN CYBERSECURITY ALLIANCE

Mark Bryan Manantan 34

About the Authors

Benjamin Bartlett, Ph.D.
Benjamin Bartlett is an assistant professor in the Department of Political Science at Miami University. He received his Ph.D. in Political Science from the University of California at Berkeley and an M.Sc. in Computer Science from the University of Toronto. His research interests include comparative cybersecurity policy, cybersecurity in East Asia, and international cooperation on cybersecurity capacity building. His most recent publication was a chapter in the Oxford Handbook of Japanese Politics on cybersecurity in Japan.

Mark Bryan Manantan
Mark Bryan Manantan is a resident Lloyd and Lilian Vasey Fellow at the Pacific Forum. His research examines the intersection of International Relations, cybersecurity, and emerging technologies in the context of the US-Japan alliance in the Indo-Pacific, Japan-Australia cyber diplomacy, and China's information warfare and cyber coercion. Concurrently, he is a non-resident fellow at the Center for Southeast Asian Studies at the National Chengchi University in Taiwan. Previously, he was a visiting fellow at the Center for Rule-making Strategies at Tama University in Tokyo, and the East-West Center in Washington D.C., under the US-Japan-Southeast Asia Partnership in a Dynamic Asia Fellowship. Prior to that, he was the recipient of the Japan Foundation's Asia Fellowship 2020 and the Taiwan Research Fellowship in 2019. Aside from conducting policy-relevant research, Mr. Manantan is the founder and strategic director of Bryman media, a social impact communications and consultancy firm based in the Philippines. He obtained his bachelor of arts (*magna cum laude*) in broadcast communication under the Presidential scholarship at the University of the Philippines. A recipient of the Australia Awards Scholarship, he also holds a Master of International Relations (Advanced) with Honours from the Australian National University.

Mihoko Matsubara
Mihoko Matsubara is chief cybersecurity strategist, NTT Corporation, Tokyo, responsible for cybersecurity thought leadership. She previously served at the Japanese Ministry of Defense before her MA at the Johns Hopkins School of Advanced International Studies in Washington DC on Fulbright. Prior to joining NTT, she worked as VP and public sector chief security officer for Asia-Pacific at Palo Alto Networks. She served on Japanese government's cybersecurity R&D policy committee between 2014 and 2018. Mihoko is a prolific writer and has published articles from the Council on Foreign Relations, Lawfare, New America, the RUSI Journal, etc. She published a cybersecurity book from the Shinchosha Publishing Co., Ltd in 2019, which won a JFY 2020 award from the Okawa Foundation for Information and Telecommunications. She has spoken at various engagements internationally such as the NIST Cybersecurity Risk Management Conference 2018 in Baltimore, the RSA Conference 2018 and 2019 in San Francisco, the EU Cyber Forum 2019 in Brussels, and CyCon 2015 and 2019 in Tallinn, Estonia. She is adjunct fellow at the Pacific Forum, Honolulu, and associate fellow at the Henry Jackson Society, London.

Crystal Pryor, Ph.D.
Crystal Pryor is vice president of the Pacific Forum. Before joining Pacific Forum, she held a postdoctoral fellowship in the US-Japan relations program at the Weatherhead Center for International Affairs at Harvard University. Crystal works on nonproliferation in Asia while developing research agendas on technology policy and Women, Peace, and Security. She has researched US-Japan outer space security cooperation, strategic trade control implementation in advanced countries, and Japan's defense industry and arms exports. Crystal received her doctorate in political science from the University of Washington, master's degrees in political science from the University of Washington and the University of Tokyo, and bachelor's degree in international relations with honors from Brown University.

Justin Sherman

Justin Sherman is a nonresident fellow at the Atlantic Council's Cyber Statecraft Initiative. He is also an op-ed contributor at *WIRED* and researches at the Tech, Law, & Security Program at American University Washington College of Law and at *Lawfare*'s Trustworthy Hardware and Software Working Group. His work at the Atlantic Council focuses on the geopolitics, governance, and security of the global internet. Previously, he was a cybersecurity policy fellow at New America, the youngest in the think tank's history, where he wrote reports and commentaries on global internet governance, 5G security, and US-China artificial intelligence relations and worked on New America's Data & Great Power Competition project. He has also worked on cyber and national security issues at the National Security Agency's Laboratory for Analytic Sciences; researched technology transfer and global data policy issues at Duke University's Sanford School of Public Policy; researched technical cybersecurity and data privacy issues at Duke's Computer Science Department; and spent two years as a fellow at Duke Law School's Center on Law & Technology. He co-founded Duke University's nonpartisan initiative Ethical Tech, where he led research, events, and policy education programs on cybersecurity, privacy, and artificial intelligence. He has written numerous articles, including in *The Washington Post*, *The Atlantic*, *Foreign Policy*, *Slate*, *The Diplomat*, *War on the Rocks*, *World Politics Review*, and *Journal of Cyber Policy*, among other popular, policy, and scholarly outlets. He has authored multiple book chapters, spoken before a range of audiences, and provided expert commentary for television and radio including Showtime's "VICE", BBC World Service, National Public Radio, and Public Radio International. He is currently earning his MA in security studies from Georgetown University's School of Foreign Service. He earned his BS in computer science and his BA in political science from Duke University, where he co-wrote two technology policy classes and co-founded the student cyber program.

Professor Wilhelm Vosse, Ph.D.

Wilhelm Vosse is professor of political science and international relations and chair of the department of politics and international studies at the International Christian University (ICU) in Tokyo, Japan. His research interests include Japanese foreign and security policy, especially its cyber diplomacy with new security partners such as NATO and the EU. He has held research positions at Harvard University, Oxford University, and the University of Warwick.

Gregory Winger, Ph.D.

Gregory H. Winger is an Assistant Professor in the Political Science Department at the University of Cincinnati. He specializes in cybersecurity, international security, and US foreign policy. His research examines trust-building processes and in particular, how collaborative activities like defense diplomacy have been used to facilitate cooperation on emerging security issues. Specifically, Dr. Winger has done significant work on how these activities were used to support American alliances in Asia. He is also tracing how similar methods are being used to promote cooperative endeavors in cybersecurity. He has authored several works on these subjects in publications such as *Foreign Affairs, Diplomacy & Statecraft*, and *Armed Forces & Society*. He is the recipient of numerous prestigious awards, including the World Politics and Statecraft Fellowship from the Smith Richardson Foundation and the Leifur Eiriksson Scholarship. He has also held research fellowships with esteemed institutions, including the Center for Small State Studies at the University of Iceland, the Institute for Human Sciences in Vienna, and as a Fulbright Fellow in the Philippines. Dr. Winger received his Ph.D. from Boston University.

Introduction

The Tokyo 2020 Olympics put into sharp focus the increasing significance of cybersecurity to Japan's national security agenda in recent decades. Ahead of the highly anticipated 2020 Olympics and Paralympic Games, Japan's National Intelligence Agency warned the government about an expected influx of state-sponsored hackers targeting critical national and digital infrastructure to disrupt or hijack the historic sporting events. The warning is reminiscent of the 2018 Pyeongchang Winter Olympics held in South Korea, where malware nearly delayed the opening ceremony. In 2018, a recorded cyberattack also compromised 300 computer systems, affecting the internet and television services managed by the International Olympic Committee.

Amid postponement of the 2020 Olympics due to the global pandemic, Japan has remained focused on mitigating malicious cyberattacks, especially with increasing tensions in the region, including US-China geostrategic and geo-economic rivalry and Russia's four-year Olympic ban. Japan continues to ramp up its cyber defenses. Amid the limitations of its pacifist constitution, Japan has made leaps in the adoption of a more defense-oriented posture in cybersecurity. Japan is now an emerging cyber power.

Integral to Japan's overall cybersecurity policy is closer cooperation with the United States. The US-Japan alliance anchors the stability and prosperity of the Indo-Pacific. Enduring regional security therefore relies on the bilateral initiatives undertaken by Tokyo and Washington across all domains, including cyberspace. Although cybersecurity cooperation within the alliance has been robust, the urgency to constantly review, assess, and upgrade facets of cybersecurity engagements — confidence-building measures, and international law and cyber norm promotion — is imperative due to the evolving nature of sophisticated cyberattacks and the disruptive effects of technological advancements.

In light of these recent developments, Pacific Forum hosted a three-day virtual workshop from August 17-19, 2021, titled the *US-Japan Cybersecurity Cooperation Virtual Forum: Beyond the Tokyo Olympics*. The workshop examined the progress, challenges, and prospects for US-Japan cybersecurity cooperation in securing critical national infrastructure (CNI) against the backdrop of the Tokyo 2020/2021 Olympics, COVID-19 pandemic, and ongoing great power competition. The workshop gathered over 70 individuals representing government, industry, academia, and civil society from the Indo-Pacific. The first two days were closed-door, while the final day's proceedings were open to the public. The virtual dialogue featured well-known Japanese and American speakers who tackled key dimensions of cybersecurity cooperation under the US-Japan alliance. In parallel to the virtual discussions, a cybersecurity tabletop exercise was conducted to test and operationalize the concepts and deliberations and formulate actionable and pragmatic policy insights.

To sustain the virtual dialogue's relevance and policy impact, Pacific Forum has compiled this special digital publication with select contributions from the panelists. With the increased attention on state-sponsored cyberattacks, the proliferation of ransomware, and the disruptive effects of emerging technologies, the launch of this special issue comes at an auspicious time. Reflecting on the outcomes of the virtual event, the authors in this volume took a step back to locate gaps in the US-Japan alliance's role in securing cyber stability in the Indo-Pacific region before zooming in on concrete policy recommendations.

This digital publication begins with the Key Findings report that outlines the salient points of the three-day virtual dialogue, including the deliberations during the cybersecurity tabletop exercise. Reflecting on the aftermath of the Olympics, Mihoko Matsubara's "Next steps for US-Japan cybersecurity cooperation after Tokyo 2020" offers insights on the lessons learned and best practices that Japan can apply and sustain with its ongoing collaboration with the US and its partners across Asia and Europe. Dr. Gregory Winger's "Threats and trends in critical national infrastructure" examines the SolarWinds and Colonial pipeline hacks to expose the evolving patterns of malicious behavior on supply chains before calling for a more proactive and persistent type of engagement between the US and Japan.

Focusing on practical collaborative steps that the US and Japan can undertake in protecting their critical national infrastructure, Dr. Benjamin Bartlett's contribution probes into how the alliance can address cyber incidents that fall under the level of an armed attack. He explores what coordinated responses Tokyo and Washington should pursue to confront low-level yet persistent threats like cyber espionage in critical national infrastructure.

Justin Sherman's "Seizing on US-Japan opportunities for submarine cable security" explores the physical dimension of cybersecurity, scrutinizing the strategic issues underpinning undersea cable networks. Mr. Sherman's article emphasizes the importance of regulatory functions and joint capacity building to safeguard submarine cables, which are the connective tissue of US-Japan cyber intelligence-sharing, and more broadly the global internet infrastructure.

Looking ahead, Professor Wilhelm Vosse's piece scans the weaknesses and strengths of Japan's cybersecurity architecture. Although Japan has made impressive strides in its regional and international cyber diplomacy — capacity building, confidence-building measures, and joint training exercises — it needs to review the fundamental elements of its cyber policy. This will entail narrowing the definition of cyberattacks and exploring the notion of what offensive and defensive cyber capabilities look like for Japan given its pacifist constitution amid rising concerns over China, Russia, and North Korea's cyber activities. Finally, Mark Bryan Manantan's "The cyber AI nexus: Implications for the US-Japan cybersecurity alliance" tackles how emerging and dual-use technology like AI is tilting the alliance's cyber cooperation. Mr. Manantan explores the mutual relationship between cyber and AI from normative and technical perspectives to conduct an in-depth analysis of the opportunities, challenges, and prospects for Tokyo and Washington in the age of technological disruption.

As geostrategic competition shifts into the geo-economic and geo-technological spheres, cybersecurity will become even more central. It is our hope that the policy recommendations and insights offered by this digital publication will be applied among policymakers to enable deep reflection on the rapidly changing cyber landscape and consequently upgrade the existing dimensions of cyber cooperation. With current US-China relations hitting a *cul-de-sac*, clandestine and covert operations in the cyber arena will further accelerate — a reality that Tokyo and Washington must confront with both strategic pragmatism and prudence.

Key findings from the US-Japan virtual forum on cybersecurity cooperation: beyond the Tokyo Olympics 2020

Key Findings

As the anchor of stability in the Indo-Pacific region, the US-Japan alliance faces enormous challenges and opportunities to revisit, review, and reinvigorate existing approaches in cybersecurity cooperation. Our two countries face an ever-changing cyber threat environment, especially with the advent of disruptive technologies like artificial intelligence, big data, and cloud computing against the backdrop of deteriorating global internet consensus. The virtual forum aimed to examine the progress, challenges, and prospects for US-Japan cybersecurity cooperation in securing critical national infrastructure (CNI) against the backdrop of the Tokyo 2020 Olympics, COVID-19 pandemic, and ongoing great power competition. Experts convened for two days of closed-door sessions and a cybersecurity tabletop exercise.

Key findings and policy recommendations for future cooperation and next steps for the US-Japan alliance in cybersecurity, especially with regard to securing critical national infrastructure, were then shared by select speakers at a public panel.

The state of cybersecurity cooperation

The Tokyo 2020-2021 Olympics will be remembered in the modern history of international sporting events as an event like no other. Against the backdrop of a global pandemic, strategic reordering, socio-technological disruptions, and Japan's own brewing domestic opposition to the games, the global sports spectacle took place and redefined resilience in the new normal. Speaking of resilience, cybersecurity was a cornerstone of Japan's hosting and a top priority for ensuring the smooth execution of the games — a resolve that will shape its cyber policy outlook in decades ahead.

After the Summer Games, Japan appears determined to maintain its momentum toward achieving cyber resiliency. Currently, Japan's 2021 cybersecurity strategy is open for public consultation. Through a cursory glance at the 2021 draft, a few major observations come to the fore. First is an increase in the sense of urgency to address Chinese, Russian, and North Korean cyber activities. The propensity of the Japanese government to name and shame specific state actors signals its intent to avoid ambiguity, which is a dramatic shift in its cyber policy. However, the draft remains consistent with the 2018 cyber strategy, with a few developments on data policy. The current draft still does not outline any plans to develop or enhance Japan's offensive cyber capabilities but emphasizes continuing, if not elevating efforts on improving cyber-deterrence. To this end, the US-Japan alliance remains a key plank in Japan's overall cyber policy. The 2021 draft has shown increased government-to-government cooperation on national data security policy, and as such the Japanese Ministry of Defense and the US Department of Defense may be even closer to establishing a more credible data-sharing cooperative framework. As expected, there remain strong expectations for multilateral cooperation with the United Nations and partner countries, like India and Australia, to create a stronger cyber defense to identify and possibly hold attackers accountable.

The Cyber Threat Landscape

The dramatic evolution of the cyber threat landscape over the course of the pandemic — which expanded the conventional classification of critical national infrastructure — combined with the rising influence of non-state actors makes dissecting the many facets of cybersecurity even more necessary, especially under the matrix of US-Japan cooperation.

When deliberating US-Japanese cooperation and critical infrastructure, several considerations emerge. Foremost, what should the channels of coordination between the US and Japan in cybersecurity look like? This question considers the seniority of ministers who should deliberate on cybersecurity matters and the frequency of meetings. Some experts have expressed their preference for more technical, regular meetings. They have also discussed the benefits of greater standard setting and how both allies continue to exchange views in maintaining stability in the cyber domain. The unprecedented impact of COVID-19 has also bred new cybersecurity challenges, especially vulnerabilities related to telework. The pandemic has resulted in individuals spending much more time online, providing malicious actors with greater attack surfaces. Amid the rapid expansion of remote working arrangements, many employees still lack cyber hygiene, and, in some instances, this has led to corporate data being mistakenly uploaded to non-work applications. The emergence of new and more virulent strains of the coronavirus is also a critical consideration for US-Japan cooperation. Hacking operations against pharmaceutical and scientific organizations to steal proprietary information related to vaccine research and development are of utmost concern. Additionally, the proliferation, efficacy, and dangers of ransomware — especially if it contaminates critical infrastructure — are all pressing concerns for the US and Japan.

Ransomware attacks are a particularly pernicious, and growing, cyber threat, with 58% of American and 52% of Japanese companies reporting such incidents between 2020 – 2021. Among those reported, only 24% of ransomware attacks could be stopped before encryption, meaning that three-quarters of attacks were successful. Across industries, manufacturing, health care, and education have the lowest cybersecurity maturity. In healthcare, 86% of health care institutions do not use any email scanning filtering tool, leaving the sector vulnerable to espionage and ransomware. In fact, 48% of US hospitals have had to disconnect their networks in the past six months because of ransomware attacks.

Cybersecurity professionals have also observed a steady growth of supply chain attacks and the emergence of ransomware as a service. Supply chain attacks saw an increase in popularity among state actors, and often target trusted vendors that provide systems and software for target institutions. The growth of ransomware as a service also represents a unique evolution of the technology; it has changed into a form of malicious software that involves gangs of ransomware developers as service providers. As a result, ransomware has become accessible on a massive scale because people using it no longer need to develop it themselves. To deal with this, policymakers need to reshape online conditions to hinder malicious actors and re-engage in the initiative. Here, the importance of US-Japan coordination to start advocating for international norms in relation to ransomware attacks would be paramount.

Submarine cables are an essential conduit connecting cyberspace telecommunication signals with physical land-based stations. Approximately 99% of international traffic, including considerable military communications, passes through undersea cables. Three companies — Subcom, NEC, and Alcatel Submarine Networks, from the US, Japan, and the EU, respectively — control 95% of the cables, however, new Chinese companies are gaining ground. There are several threats to undersea cables. Physically cutting cables is not uncommon; it happens accidentally almost every day, however, malicious actors may also intentionally cut them. This might happen in emergency situations when an adversary is looking to disrupt communications. Government and non-state actors have also been known to tap cables, but optic communications are extremely sensitive and difficult to capture. Current concerns stem from possibly compromised cables, Submarine Line Terminal Equipment (SLTE), and the data transmissions that pass through them. Data capture can be made easier by establishing a connection to SLTEs in a data capturing center. The US remains concerned about China playing out this scenario in Hong Kong.

Data centers are high-value targets among state-sponsored cyber actors. Over 20,000 nation state-attributable cyberattacks have been carried out, with Russia, China, Iran, and North Korea considered the "big four" actors in this domain. These attacks are by nature intelligence operations and rarely target critical infrastructure. In the past year, Indo-Pacific countries have been targeted in about 244 attacks. For Japan, North Korea is the most active perpetrator of these attacks (61%), followed by Russia and China. These attacks usually target government agencies, think tanks, defense institutions, and academics. Interestingly, a higher than average (25%) figure of cyberattacks aimed at Japan has targeted critical infrastructures.

Cybersecurity Tabletop Exercise

The second day of the US-Japan Cybersecurity Conference featured a tabletop exercise (TTX) where participants were presented with a scenario and then broken into three teams: Team Japan, Team USA, and Team IOC. Under time constraints and with limited information, each team was given a set of questions and tasked to formulate the best possible cyber policy recommendations.

In the given scenario, the Japanese Olympic Committee (JOC), as the host nation for the 2020-21 Tokyo Olympics, suffered a major cyberattack. The cyberattack targeted the Games organizers, advisors, logistics services, and sponsors, as well as delivered malware to the executive board members of the JOC. With the cyberattack threatening to overshadow the Closing Ceremony of the Games, Japan is confronted with the difficult choice of protecting its international reputation while navigating the evolving cyber threat landscape and balancing its own interests in lock-step with the US.

Team Japan and Team USA responded to the following questions:

- Identify up to three remediation strategies that your team should undertake within the 24-36 hours following the incident.
- Identify up to three actions that your team wants the other teams TO TAKE.
- Identify up to three actions that your team wants the other teams NOT TO TAKE.
- With a heightened sense of urgency, identify up to three policy recommendations that your team should pursue in close coordination with the other teams — taking into full consideration inherent characteristics such as comparative advantages and political limitations — to address the cyberattack.

Team IOC was presented with the following set of questions:

- Identify up to three remediation strategies that your team should undertake within the 24-36 hours following the incident.
- Identify up to three actions that your team wants Japan TO TAKE.

- Identify up to three actions that your team wants Japan NOT TO TAKE.
- With a heightened sense of urgency, identify up to three policy recommendations that Team IOC should pursue in close coordination with Japan — taking into full consideration the need to successfully close the Olympics and other political and economic limitations – in the aftermath of the cyberattack.

Team USA

Team USA identified attribution, immediate coordination, and ensuring that the attacks have been halted as the three most urgent steps. That being said, the team recognized that before proper attribution could take place due diligence must be conducted. Team USA also acknowledged the weaknesses of Japanese cybersecurity in the past, with concerns over how such failures could impact cooperation. Team USA wanted to ensure Japan was arresting the cyberattacks and that critical information had been secured.

The team sought collaboration between the US and Japan in gathering forensic information on the hack itself. The group also noted that the IOC lacks the ability to retaliate against a cyberattack and would also not consider such a response to be desirable. Team USA also wanted none of the other teams to publicize the attack, but also expressed concern over Japan's historical reticence to engage in attribution until Washington had first taken concrete steps in the process. Finally, in coordination with the other teams, Team USA sought to ensure such attacks would not take place again, implement an after-action response review to see how they could have responded better, and develop an offensive response for future hacking incidents.

Team IOC

In the 24-36 hours following the incident, Team IOC deemed it critical to undertake a baseline risk assessment to establish any ongoing risks to athletes and officials with the sole intent of preventing further harm. The team wanted to clarify whose computer emergency response teams (CERTs) would be tasked with the response to detected cyberattacks and develop backchannels with national computer emergency response teams to allow for notifications on potential cyberattacks during or even between games. The team found it important to share relevant information from the attack between the Olympic Committee and Japanese officials and establish a monitoring process to implement a pre-agreed incident response program. Team IOC wanted Japan to consult with international organizations like Interpol to investigate the incident. It implored Team Japan to sanction any responsible parties under Section 56 of the Olympic Charter and lodge a case before the International Court of Justice. The team asked Japan to avoid publicly attributing the attacks to a state actor until the end of the Olympics. This request was designed to help ensure that the reputation of the IOC endures and assist in the smooth execution of the closing ceremony. Team IOC wanted Team Japan to avoid hacking back, as this would be in contravention of international law and could make the situation worse. Last, Team IOC hoped to work in close coordination with Team USA/Japan to ensure the IOC remained informed as the situation unfolds.

Team Japan

Team Japan sought to arrange immediate coordination between the US and the IOC in the 24-36 hours following the attack. Such coordination would be premised on answering essential questions relating to particular channels of cooperation. It would also make certain that the attack was stopped and begin collecting forensic evidence. Given Japan's recent condemnation of PRC government-affiliated hacking group APT40, the team saw no reason not to follow the same precedent and attribute the group responsible for the cyberattack on the condition that the threat actor was identified and verified with near-perfect certainty.

Team Japan implored the IOC to share all relevant indicators of compromise. Such items could include IP addresses and email addresses affiliated with the attack. This information would be essential to share with the Japanese Olympic Committee, other Olympics sponsor companies, and defense contractors. Team Japan also planned to reach out to the National Cyber Security Centre, United Kingdom, to ask for any additional information they might have on Russian cyberattacks.

More importantly, Team Japan sought consultation with American cybersecurity experts, particularly in the defense and aerospace communities, to see whether they had any additional information on the attack that could be shared with Japanese defense contractors. Team Japan recommended that a public-private partnership (PPP) help streamline information sharing in instances where private companies are hesitant to share details of their cyber vulnerabilities. The team also recommended developing a joint monitoring center in Honolulu where Japanese private sector defense staff and their US counterparts can sit next to one another and monitor cyberattacks. Further, Team Japan recommended inviting relevant components of the Japanese private sector to cybersecurity exercises between the US and Japan. No such structure currently exists, and this could help bolster national security.

As the teams wrap up their respective courses of action, they were presented an additional set of facts.

After a comprehensive technical investigation and close consultation with the Five Eyes community, the US has decided to name and shame China as the perpetrator of the cyberattack against the JOC that reached the MHI-Lockheed Martin joint-development program. According to a Five Eyes report, the Chinese-linked group, APT12 — which has strong ties to the Ministry of State Security — is the primary suspect.

Team Japan, Team US, and Team IOC were asked the following questions:

Does this new information provided change your answers from the first move? If you have changed your answers, please be prepared to explain why in the group presentation.

- Identify up to three remediation strategies that your team should undertake within the 24-36 hours following the incident.
- Identify up to three actions that your team wants the other team(s) TO TAKE.
- Identify up to three actions that your team wants the other team(s) NOT TO TAKE.
- Identify up to three policy recommendations that your team should pursue in close coordination with the other team(s) — taking into full consideration the latest development — to address the cyberattack.

Team USA's desire for speedy attribution and a delay in the publicizing of the attacks was dropped after the team reconvened. The team identified Japanese capitulation to Beijing and the balancing act between attribution and de-escalation as potential areas of concern. The team sought to accommodate Japanese concerns by designating a five-day grace period during which time Team Japan could prepare its own policies and strategies before the public attribution to China would take place. Finally, the team examined the taxonomy of the word "attack" and what the actual implications of its use might mean. The debate between the team primarily centered on the scope and depth of the word "attack" and how its use might affect response formulation.

Team Japan's response to the second set of facts changed little from their initial response. This was especially the case given Japan's new cyber priorities and the central role that naming and attribution plays in this. The group reemphasized the importance of information sharing among allies and organizations, such as the IOC.

Given the IOC's interest in maintaining its apolitical nature, its response between moves did not change significantly. Upon learning that the attack was likely carried out by China, the team proposed the establishment of a specialist tribunal, similar to the World Anti-Doping Agency, that would investigate ongoing and future cyber-related attacks as such incidents have become a growing source of concern in the Olympics over the last decade. The creation of such a body could help the IOC remain apolitical while determining what measures it should take in response to the attack and possible occurrences in the future.

Moving forward

The current issue in the US-Japan alliance in cybersecurity rests on the inherent risks associated with technological disruptions and innovation brought by the Fourth Industrial Revolution. At the same time, malicious actors such as China, Russia, and North Korea are increasingly yet stealthily using offensive capabilities amid a global health crisis. Furthermore, the balkanization of the internet also represents a clear and present danger underpinned by the growing trend of geopolitical tensions being superimposed onto cyberspace.

Strategic latency continues to be a driver of competition as well. Technological changes are a catalyst for increased competition, forcing nation-states to adapt or perish within the cyber realm. Emerging technologies such as artificial intelligence (AI) present both significant opportunities and challenges as a force multiplier of both offensive and defensive capabilities.

Japan is on the frontlines of the geostrategic tech war between the US and China, yet appears unprepared for such a reality. A study published by the International Institute for Strategic Studies titled *Cyber Capabilities and National Power: A Net Assessment* designated Japan in the third tier, ranking its capacity equal to nations such as Indonesia, India, Malaysia, and Vietnam.

While Japan has a strong digital economy, its defensive cyber capabilities are inadequate and its offensive capabilities nonexistent due to limitations imposed by its pacifist constitution. Moreover, its myopic definition of cyberattack continues to hamstring its development in these areas. However, Japan continues to be active in cyber diplomacy. It actively participates in several dialogues with the EU and Australia while engaging with global institutions in the creation of cyber norms. Its provision of foreign aid utilized for technical and policy-centered capacity-building activities and confidence-building measures in Southeast Asia has contributed to maintaining cyber stability in the region.

Although there is cooperation on many levels, the US-Japan partnership should continue to strengthen its atmosphere of mutual trust to improve cross-communication and coordination. This goes hand in hand with upgrading intelligence-sharing mechanisms as the US adopts more offensive posturing in cyberspace with its Persistent Engagement Cyber Strategy. The alliance's lack of clear plans to handle and respond to critical infrastructure attacks is an area in dire need of closer cooperation. To address this, the US and Japan must review their list of what they consider as critical national infrastructure. The segment of the private sector responsible for managing critical national infrastructure should also be encouraged to become even more proactive and open to information-sharing arrangements. Public-private cybersecurity cooperation should not be limited strictly between the US and Japan; other jurisdictions and parties in the EU and ASEAN should be brought in to expand coordination and cooperation.

Along with ongoing efforts to achieve cyber resiliency and exercising prudence in joint public attribution, the US and Japan must sustain the codification of norms and emphasis of international law to mitigate the spiraling security dilemma in the cyber domain. For its part, Japan should seek to increase its defensive cyber capabilities and continue its cyber diplomacy in the Indo-Pacific. This should be reinforced by deepening its cyber threat intelligence sharing with the US but also with increased cooperation with other capable cyber partners like Australia, India, South Korea, and the EU.

The nexus of cybersecurity and AI present both challenges and prospects in the US-Japan alliance. Based on their Joint-High Level Committee on Science and Technology held in 2019, the two nations have designated quantum science and AI as critical future industries. However, there continues to be a wide margin in terms of AI maturity and a dearth of governance in sharing credible data which creates shortcomings in the development, design, testing, and deployment of AI-infused capabilities.

To remedy this, the US-Japan alliance should create a cyber-AI focus group to bridge capacity failures and streamline risk management approaches to enable AI systems resilient to emerging threats like adversarial AI. The alliance should develop an accreditation system to ensure that third-party, and commercial vendors operate within a clearly delineated standard of quality control and due diligence. In the long term, the US-Japan alliance must focus on strengthening the fundamental technical basis for AI development that is transparent and inclusive to better understand diverging systems espoused by China and Russia. This would ensure that the human component is kept within the AI development loop, to minimize ambiguity biases, and inhibit escalation.

1. Next steps for US-Japan cybersecurity cooperation after Tokyo 2020

By Mihoko Matsubara

Japan successfully completed the Tokyo 2020 Olympic Games on August 8 without any major disruptions caused by cyberattacks.[1] This article examines anticipated cyber threats to the games, public-private partnerships, new developments by the police and the Ministry of Defense (MOD) and Self-Defense Forces (SDF), and their implications for the future Japan-US cybersecurity cooperation.

Potential cyber threats to Tokyo 2020

The anticipated cyberattacks against Tokyo 2020 were believed to be intended to achieve financial gains, damage Japan's reputation and trust and disrupt operations.[2] For example, a cyberattack on the PyeongChang 2018 Winter Olympics Games crushed their servers and Wi-Fi, causing some people to be unable to print out their tickets for events.[3] These types of disruptive hacks must be prevented.

Leading up to Tokyo 2020, ransomware had proven to pose an enormous risk, following the cyberattacks on the Colonial Pipeline, global meat processing firm JBS, and US-based IT company Kaseya between May and July 2021. Ransomware attacks increased by 64% year over year as of August 2021, compared to 2020.[4] Nobuhiro Endo, chairperson to the Japanese Supply Chain Cybersecurity Consortium (SC3), issued an open letter to member companies and their business executives on July 7, 2021 — two weeks prior to the opening ceremony of Tokyo 2020.[5] The SC3 was established in November 2020 to bring in both large and small-sized companies and trade associations to enhance cybersecurity capabilities across supply chains.[6]

Endo's letter aimed to remind Japanese business leaders, including Tokyo 2020 sponsors and critical infrastructure companies, that previous Olympic and Paralympic Games had been targeted by cyberattacks. He urged them to ensure that their cyber defenses were in place in order to protect Tokyo 2020 and Japan from cyber espionage and disruptive cyberattacks such as distributed denial of service (DDoS) and ransomware attacks; and cybercrimes using fake applications or phishing sites to steal money and personal information.

Cybersecurity success factors

Fortunately, the Tokyo 2020 Olympic Games did not experience any major disruptions caused by cyberattacks from July to early August 2021. Japan, however, still experienced some financially motivated cybercrimes. Following the resurgence of COVID-19 cases, the Organizing Committee decided to bar in-person spectators. Akamai, a global content delivery network, streamed a record-breaking 500 million hours from Tokyo during the Olympic Games, which is more than double the 234 million hours of video streamed from the Rio Olympic Games in 2016.[7] Cyber criminals made multiple phishing websites claiming to broadcast the torch relay and opening ceremony, however, no disruption by any cyberattack to the Tokyo 2020 operations has been reported to the Japanese government as of today.[8] Now, it is time to apply the success story and share lessons learned with the future hosts of the 2024 and 2028 Olympic Games in Paris and Los Angeles, such as pandemic risk management and critical infrastructure protection.

Japan had an advantage in organizing the Olympic Games because it had previously hosted several major international events, such as the G20 Osaka Summit and the 2019 Rugby World Cup. These events served as milestones to enhance Japanese national cybersecurity capabilities and launch public-private partnerships. The 2015 Cybersecurity Strategy expressed Japan's strong will to take advantage of the 2019 Rugby World Cup as a test of the Tokyo 2020 Computer Security Incident Response Team (CSIRT) and

[1] 2021. "*Daikibo saiba higai nashi Gorin heimaku de Kajiyama keisansho.*" *Sankei Shimbun*.https://www.sankei.com/article/20210810-K7FYBVI2ZFOZ5HG2PLFN5FW37Q/.

[2] Saka, Akira. 2020. "Sekai teki spotsu ibento wo meguru saiba kyoi no jokyo to taio." *Olympic and Paralympic Organising Committee*. https://special.nikkeibp.co.jp/atclh/NXT/21/techmedia0129/#kicyo.

[3] Ng, Alfred and Daniel Van Boom. 2018. "Winter Olympics cyberattack designed to cause chaos." *CNET*.https://www.cnet.com/tech/services-and-software/winter-olympics-pyeongchang-cyberattack-hack-internet-wifi/.

[4] 2021. "Barracuda threat report reveals evolving ransomware attack patterns." *Barracuda Networks*. https://www.barracuda.com/news/article/832.

[5] Endo, Nobuhiro. 2021. "Tokyo 2020 Orinpikku Pararinpikku kyogi taikai ni mukete – SC3 kaiin kigyo soshiki no keieisha heno saiba sekyuriti taisaku ni kansuru messeji." https://www.ipa.go.jp/files/000092539.pdf.

[6] METI, 2020. "Sapurai chein saiba sekyuriti konsoshiamu (SC3) ga setsuritsu saremasu" *METI*.https://www.meti.go.jp/press/2020/10/20201030011/20201030011.html.

[7] Murakami, Sakura, Ju-min Park and Antoni Slodkowski. 2021. "Olympics host city Tokyo bans spectators amid COVID-19 emergency." *Reuters*.https://www.reuters.com/world/asia-pacific/japan-set-declare-state-emergency-tokyo-area-through-aug-22-minister-2021-07-08/; Greig, Jonathan. 2012. "Tokyo Olympic streaming numbers double figures from Rio 2016: Akamai." *ZDNet*.https://www.zdnet.com/article/tokyo-olympic-streaming-numbers-double-figures-from-rio-2016-akamai/.

[8] Dotate, Souichi. 2021. "*Supotsu chukei saito jitsu ha nisemono fisshingu sagi ni chui*." *Asahi Shimbun*.https://www.asahi.com/articles/ASP7J764YP7JUTIL056.html;Okamoto, Katsuyuki. 2021. "*Tokyo orinpikku kaikai chokuzen nise no hoso yotei peji kara burauza tsuchi supamu he yudo suru kogeki wo kakunin*." *TrendMicro Security Blog*. https://blog.trendmicro.co.jp/archives/28308. NHK, "Kato kanbo chokan 'Tokyo gorin para kikanchu saiba kogeki kakunin sarezu' [Chief Cabinet Secretary Kato said that the government had seen no cyberattack to disrupt the operation of the Tokyo 2020 Olympic and Paralympic Games]," September 27, 2021, https://www3.nhk.or.jp/news/html/20210927/k10013278331000.html.

operationalize collaboration between key stakeholders such as the government, sponsors, the Organizing Committee, and critical infrastructure companies.[9]

The COVID-19 pandemic cast a long shadow over the operations of Tokyo 2020, forcing the games to be postponed for one year. Japan has been under an unprecedented amount of pressure to ensure both cyber and physical security for the games but also to minimize the risk of COVID-19 infections among operators and visitors.

Remote work by Tokyo 2020 stakeholders also created a new challenge to secure their home IT environment. During the declaration of a state of emergency between April and May 2020, over 90% of the Tokyo 2020 Organizing Committee members had to work from home.[10] The National center of Incident readiness and Strategy for Cybersecurity (NISC) had listed potential cyber risks to Tokyo 2020 and some 300 Japanese critical infrastructure companies, assessing risks multiple times before the pandemic. Yet, the growing reliance on remote workers had the NISC recreate the risk list and carry out risk assessment again.[11]

The success of Tokyo 2020's cyber defense should be attributed to proactive prevention by real-time monitoring and cyber threat intelligence sharing, said Dr. Brian Gant, assistant professor of cybersecurity at Maryville University.[12] Tokyo 2020's Security Operation Center analysts adopted user and entity behavior analytics (UEBA) to detect potential cyber threats. Tokyo 2020 also worked with the intelligence community from the UK that hosted London 2012 and the US that will host Los Angeles 2028. Companies from Japan, Israel, and Taiwan also contributed to Tokyo 2020's cybersecurity.[13]

Public-private partnerships

The cybersecurity of any Olympic and Paralympic Games entails multi-layered, public-private partnerships since the event is a global platform to showcase innovation, political leaders' meetings, and various types of sports competitions. These partnerships emphasize the development of cybersecurity talent and sharing of cyber threat intelligence and cybersecurity best practices.

The Cabinet Secretariat, an office to support the Japanese Cabinet's missions, ran the Security Response Coordination Center and shared Tokyo 2020-related security information — regarding cyberattacks, natural disasters, and terrorism — with 350 organizations from March to September 2021. The members included the central and local municipal governments in Tokyo, the Organizing Committee, and critical infrastructure and cybersecurity companies. The coordination center conducted at least five security exercises before the Olympic Games.[14]

NTT, NEC, and Hitachi created the Cross-Sector Forum to educate, hire, retain, and train cybersecurity professionals in collaboration with academia and the government in June 2015, aiming to close the gap of the cybersecurity professional shortage before Tokyo 2020.[15] As of October 2020, the forum has 43 member companies.[16]

Since talent development requires the definition of cybersecurity professionals and their missions and skillsets, the Cross-Sector Forum has been publishing documents to protect critical infrastructure based on the National Institute of Standards and Technology (NIST)'s Cybersecurity Framework. Since 25% of forum members are Tokyo 2020 sponsors and all forum members have global business presence, the forum chose a global framework as a common language to defend different critical infrastructures and share its expertise with the world.[17]

The forum has also been serving as a focal point of an academia-industry-government collaboration to strengthen Japan's cybersecurity capabilities. The Japa-

[9] Matsubara, Mihoko. 2021. "Tokyo 2020 and Japan's Ongoing Cybersecurity Efforts." *Institut français des relations internationales' Asie Visions*. No. 119. https://www.ifri.org/sites/default/files/atoms/files/matsubara_mochinaga_japan_cybersecurity_strategy_2021.pdf.; and NISC. 2015. "*Saiba sekyuriti senryaku*." https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku.pdf.

[10] Saito, Yusuke. 2021. "Gorin soshiki i `rimoto de junbi susumanu` kaimaku made 200 nichi." *Asahi Shimbun*.https://www.asahi.com/articles/ASP143TBMP14UTIL004.html.

[11] 2021. "*Saiba kogeki joho wo 350 soshiki de kyoyu Tokyo gorin para he taisei kyoka*." *Sankei Shimbun*.https://www.sankei.com/article/20210707-NTDMIID54FLQDHKFJBYZHFA64A/?outputType=theme_tokyo2020.; and TrendMicro. 2020. "*Tokyo 2020 taikai wo shien suru Naikaku Saiba Sekyuriti Senta (NISC) to ha*."https://www.trendmicro.com/ja_jp/about/trendpark/nisc-interview-202003-29-01.html.

[12] Gant, Brian. 2021. "The Tokyo Olympics are a cybersecurity success story." *Security Magazine*.https://www.securitymagazine.com/articles/95880-the-tokyo-olympics-are-a-cybersecurity-success-story.

[13] Ibid

[14] 2021. "*Gorin anzen kakuho he chosei senta tero saiba kogeki ni taio – seifu*." *JiJi*. " https://www.jiji.com/jc/article?k=2021032401311&g=pol.; 2020. "The support of the National center of Incident Readiness and Strategy for Cybersecurity (NISC) to Tokyo 2020." *TrendMicro.;* 2021. "350 organizations share information on cyberattacks to prepare for the Tokyo 2020 Olympic and Paralympic Games and strengthen cybersecurity." *Sankei Shimbun*.

[15] 2018. "Success Story: Japanese Cross-Sector Forum." *National Institute of Standards and Technology*.https://www.nist.gov/cyberframework/success-stories/japanese-cross-sector-forum.

[16] Cyber Risk Intelligence Center – Cross Sector Forum website, https://cyber-risk.or.jp/.

[17] Matsubara, Mihoko. 2019. "Japanese Cross-Sector Industry Forum Is Shaping Cybersecurity Talent Development Strategy." *New America*. https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/japanese-cross-sector-industry-forum-shaping-cybersecurity-talent-development-strategy/.

nese government has been bringing in forum members to cybersecurity policy meetings to include industry voices in national strategies, such as the 2017 Cybersecurity Talent Development Program.[18] Some member companies sponsor cybersecurity courses at multiple universities.[19]

Japanese law enforcement and public attribution

Japan's National Police Agency (NPA) and the SDF contributed to Tokyo 2020's cybersecurity as well. The National Police Agency sent 59,900 police officers from all over Japan to the Olympic Games for physical and cybersecurity.[20] The Tokyo Metropolitan Police Department established the Cyber Incident Response Center in March 2020 and started monitoring and analyzing any potential cyberattacks on Tokyo 2020 in June 2021. The Tokyo Police sent liaison officers to the Tokyo Metropolitan Government and Organizing Committee to share information on cybersecurity.[21]

The police have also increased their capabilities to collect and analyze cyber threat intelligence. While this is not directly related to Tokyo 2020, during a press conference in April 2021, Commissioner General Mitsuhiro Matsumoto of the National Police Agency attributed this new push to a cyber espionage campaign attempted between 2016 and 2017 against 200 Japanese organizations and carried out by the Chinese army's PLA Unit 61419 and a Chinese hacker group called Tick. It was a groundbreaking statement by the Japanese government and the first public accusation of China. The NPA sent the case to the Prosecutor's Office.[22]

The Cybersecurity Strategy 2021 draft released in July 2021 — Japan updates its national cybersecurity strategy every three years — expresses Japan's strong commitment to enhance its cyber threat intelligence and attribution capabilities to hold culprits accountable by taking any effective measures such as diplomatic, economic, legal, and political actions. The draft referred to the public attribution by the NPA, stating that Japan will continue to crack down on cyber attackers.[23]

In June 2021, the NPA announced the creation of the Cyber Bureau in April 2022, which will respond to large scale cyberattacks, including state-sponsored ones. The agency will also launch a team of 200 cybercrime investigators recruited from nationwide police departments to support the bureau by March 2023. Since the end of World War II, criminal investigations have been done at a prefectural level except for the Imperial Guard Headquarters. This national integration of criminal investigation capabilities will facilitate the NPA's response to cyberattacks that impact multiple prefectures. This new bureau will also partner with foreign law enforcement agencies, such as the Federal Bureau of Investigation.[24]

The Ministry of Defense and Self-Defense Forces

Upon the request of the Organizing Committee, the SDF mobilized 8,500 members to maintain security around the venues and assist flag-raising ceremonies.[25] Some of the members were involved in cybersecurity operations.[26] This was not the first time that the SDF worked with industry to defend critical infrastructure.

Previously operating in an observational capacity, in April 2021, the MOD and SDF participated in a cyber exercise named Locked Shields which is hosted annually by the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) in Tallin, Estonia. Japan is not a NATO member, but decided to join the NATO CCD COE in 2018.[27]

[18] 2017. "*Saiba sekyuriti jinzai ikusei puroguramu*." Cybersecurity Strategic HQ. https://www.nisc.go.jp/active/kihon/pdf/jinzai2017.pdf.

[19] Matsubara, Mihoko. 2019. "Japanese Cross-Sector Industry Forum Is Shaping Cybersecurity Talent Development Strategy." *New America*. https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/japanese-cross-sector-industry-forum-shaping-cybersecurity-talent-development-strategy/.

[20] *Sankei Shimbun* newspaper, "*Gorin para keibi, Mukankyaku demo shijo saidai kibo 6 man nin saiba kogeki no kenen mo* [The security of the Tokyo 2020 Olympic and Paralympic Games still require the record number of 60,000 police officers despite no spectators and there is still a concern over cyberattacks]," July 16, 2021, https://www.sankei.com/article/20210716-WARMLB653BI6VNN2RFEC7PEFDU/?outputType=theme_tokyo2020.

[21] 2021. "*Irei no gorin, keibi honkakuka mukankyaku demo kako saidai kibo – zenkoku keisatsu ichigan de genkai taisei*." *Jiji*. https://www.jiji.com/jc/article?k=2021071900872&g=soc.

[22] 2021. "*Kokka Kouan Iinkai Iincho kisha kaiken yoshi*" *National Public Safety Commission*. https://www.npsc.go.jp/pressconf_2021/04_22.htm.;Sakaguchi, Yuichi. 2021. "Japan lashes out against alleged Chinese military cyberattacks – Tokyo goes on offensive, names Beijing as culprit for first time ever." *Nikkei Asia*.https://asia.nikkei.com/Business/Technology/Japan-lashes-out-against-alleged-Chinese-military-cyberattacks.

[23] 2021. "*Jiki saiba sekyuriti (an) ni tsuite*." https://www.nisc.go.jp/conference/cs/dai30/pdf/30shiryou01.pdf, 11-12, 29-30.

[24] 2021. "Japanese police to launch team to fight state-sponsored cyberattacks." *Kyodo News*.https://www.japantimes.co.jp/news/2021/06/24/national/crime-legal/police-cybercrime-team/.

[25] 2021. "Tokyo Olympics' 10,000-spectator cap to be reviewed due to COVID rise." *Kyodo News*. https://english.kyodonews.net/news/2021/07/8e3b1c9fa01b-breaking-news-olympic-5-party-meeting-on-spectator-cap-could-be-held-july-8.html.

[26] 2021. "*Tokyo 2020 Orinpikku Pararinpikku Kyogi Taikai ni okeru Boeisho Jieitai no torikumi ni tsuite*." *MOD*. https://www.mod.go.jp/j/press/news/2021/07/02a.pdf.

[27] 2018. "Japan to Join the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn." NATO CCD COE. https://ccdcoe.org/news/2018/japan-to-join-the-nato-cooperative-cyber-defence-centre-of-excellence-in-tallinn/.

The MOD had sent an official as an observer in 2015, 2016, and 2019[28] making this the ministry's first official participation.[29] Despite Locked Shields 2020 being cancelled due to the COVID-19 pandemic,[30] more than 2,000 people from 30 countries joined the exercise virtually.[31]

The MOD and SDF teamed up with US Indo-Pacific Command, NISC, Japanese Ministry of Internal Affairs and Communications, Information-Technology Promotion Agency, Japan Computer Emergency Response Team Coordination Center (JPCERT/CC), and critical infrastructure companies to participate in Locked Shields 2021. This structure has two significant meanings.

First, the team underscores the strong alliance between Japan and the United States in the Indo-Pacific region. Since the NATO CCD COE is located in Estonia, the US had the option of sending their troops stationed in Europe. Instead, the US decided to send members from the Indo-Pacific and partner with Japan. This allowed the two allies to prepare for potential cyberattacks and share cyber threat intelligence with industry in a timely manner.

Second, the bilateral, cross-sectoral collaboration provided a golden opportunity to test US and Japanese capabilities to respond to cyberattacks on the financial services sector, mobile networks, and water supplies.[32] Scenarios that threaten national security include not only cyberattacks against military IT networks but also against critical infrastructure that supports national security such as communications, energy, or electricity, as the ransomware attack on Colonial Pipeline showcased in May 2021.

Next steps for future US-Japan cybersecurity cooperation

After Tokyo was selected to host the 2020 Olympic and Paralympic Games in September 2013, Japan ramped up its cybersecurity efforts to forge cybersecurity talent and public-private partnerships and enhance cyber threat intelligence capabilities. The eight years of preparation resulted in the prevention of significant disruption to the Tokyo 2020 Olympic Games.

Now, it is time for the Japanese government and the industry to start sharing lessons learned from its success with Paris 2024 and Los Angeles 2028. The Tokyo 2020 experiences, Locked Shields 2021, and Japan's new Cybersecurity Strategy will allow Japan to work together with US counterparts to respond to cyberattacks and share information on cyberattacks and attackers. It will help the allies hold culprits accountable and contribute to better Indo-Pacific cybersecurity.

[28] Wing Aviation Press, "Boeisho NATO no saiba enshu ni hatsu seishiki sanka [the Japanese Ministry of Defense is officially participating in a NATO cyber exercise for the first time]," April 14, 2021, https://www.jwing.net/news/37407.

[29] 2021. "*NATO Saiba Boei Kyoryoku Senta ni yoru saiba boei enshu `Locked Shields 2021` heno sanka ni tsuite*." https://www.mod.go.jp/j/press/news/2021/04/13b.pdf.; 2021. "*Reiwa 3 nen ban Boei Hakusho*." https://www.mod.go.jp/j/publication/wp/wp2021/pdf/R03030303.pdf.

[30] NATO CCD COE, "General Notice on Cancellation of Events," March 12, 2020, https://ccdcoe.org/news/2020/general-notice-on-cancellation-of-events/.

[31] 2021. "EDA participates in 'Locked Shields' cyber defence exercise." *European Defense Agency*. https://eda.europa.eu/news-and-events/news/2021/04/13/eda-participates-in-locked-shields-cyber-defence-exercise.

[32] Vavra, Shannon. 2012. "NATO tests its hand defending against blended cyber-disinformation attacks." *CyberScoop*. https://www.cyberscoop.com/nato-blended-cyber-disinformation-defense-locked-shields-article-v/.

2. Threats & trends in critical national infrastructure

By Gregory Winger, Ph.D.

Introduction

In the months preceding the 2020 Tokyo Olympics, the world witnessed an unprecedented wave of major cyber incidents. These attacks ran the gamut of "cyber doom" scenarios with ransomware attacks crippling critical infrastructure to massive breaches of core government systems. Major attacks occurred on a nearly weekly basis and left governments and businesses alike reeling in their wake.[1]

The dramatic escalation in size, scope and frequency of major cyber incidents is neither an illusion nor an accident, but the result of larger behavioral changes by malicious actors. Specifically, the growth of supply chain attacks and ransomware as a service have altered the cyber threat landscape by making the mass-targeting of systems a preferred method for attackers. As both Japan and the United States respond to this spree of attacks, understanding the evolving nature of this malicious behavior is essential to responding effectively. While the steps taken by the Biden administration following the cyberattacks on Colonial Pipeline and SolarWinds to promote national cybersecurity are essential measures, international coordination and persistent engagement with allies, like Japan, are necessary to make sustained progress towards achieving cybersecurity.

Is the cyber sky falling?

In 2012, then-Secretary of Defense Leon Panetta warned the world of the potential hazards lurking within the digital domain. He cautioned that the true danger in cyberspace stemmed not from crime or harassment, but from a cyberattack "as destructive as the terrorist attack on 9/11," that "could virtually paralyze the nation."[2] Panetta was not the first prophet of this cyber doom, but his speech served as a clarion call for the potential dangers of cyber insecurity and the threat they posed to powerful nation-states.[3]

While there has not yet been a single massive cyberattack on the scale Panetta feared, there has been a proliferation in attacks that nevertheless have had the cumulative effect of disrupting societies and undermining national security.[4] This has been particularly evident over the past year, as a series of major cyber incidents have underscored the precarious state of global cybersecurity. In December 2020, it was discovered that SolarWinds' popular Orion software had been compromised, leading to one of the largest breaches of US government networks in history. This attack was soon followed by revelations of other vulnerabilities in popular software including Microsoft Exchange and Kaseya's virtual systems administrator.

There has also been a dramatic spike in ransomware attacks. From 2019 to 2020, global ransomware attacks increased by 62%.[5] In 2021, ransomware attacks are expected to lead to over US $20 billion in costs, a monumental escalation from the US $325 million that these attacks claimed in 2015.[6] More disconcerting has been the growth of attacks targeting critical infrastructure. In 2021, major energy suppliers, food production facilities, and ports have all been crippled as a result of ransomware attacks and, perhaps most worrying, in the past six months nearly half of US hospitals reported having to disconnect their networks as a result of ransomware attacks.[7]

Bad guys behaving badly

The escalating number of major cyber incidents is being driven by behavioral changes amongst malicious actors rather than any shift in capabilities or sophistication. Specifically, what has emerged in recent months are behavioral patterns that prioritize mass attacks that strike at a large number of systems rather than more focused operations aimed at a few select targets. In particular, the current rash of attacks reflects the growth of supply chain attacks and ransomware as a service.

Supply chain attacks have become an increasingly popular attack vector, especially amongst state actors.[8] It marks an evolution in how attackers strike at their ultimate target. Instead of directly attacking institutions,

[1] Stieb, Matt. 2021. "What's Driving the Surge in Ransomware Attacks." *New York Magazine*.; "Age of the cyber-attack: US struggles to curb rise of digital destabilization." *The Guardian*. [https://www.theguardian.com/technology/2021/jun/14/age-of-the-cyber-attack-us-digital-destabilization]

[2] Panetta, Leon. 2012. "Remarks on Cybersecurity to the Business Executives for National Security." *US Department of Defense*. www.hsdl.org/?abstract&did=724128.

[3] Lawson, Sean. 2013. "Beyond cyber-doom: Assessing the limits of hypothetical scenarios in the framing of cyber-threats." *Journal of Information Technology & Politics* 10, no. 1: 86-103; Lawson, Sean T. *Cybersecurity Discourse in the United States: Cyber-Doom Rhetoric and Beyond*. Routledge, 2019.

[4] Harknett, Richard J., and Max Smeets. 2020. "Cyber campaigns and strategic outcomes." *Journal of Strategic Studies*: 1-34.

[5] Blaine, Geoff. 2021. "Tipping Point: SonicWall Exposes Soaring Threat Levels, Historic Power Shifts In New Report." *SonicWall Blog*. https://www.sonicwall.com/2021-cyber-threat-report/.

[6] Jeffery, Lynsey and Ramachandran Vignesh. 2021. "Why ransomware attacks are on the rise — and what can be done to stop them." *PBS*. https://www.pbs.org/newshour/nation/why-ransomware-attacks-are-on-the-rise-and-what-can-be-done-to-stop-them.

[7] Muncaster, Phil. "Half of US Hospitals Shut Down Networks Due to Ransomware." *Info Security Magazine*. https://www.infosecurity-magazine.com/news/half-us-hospitals-shut-networks/.

[8] Greenberg, Andy. 2021. "Hacker Lexicon: What is a Supply Chain Attack?" *Wired*. https://www.wired.com/story/hacker-lexicon-what-is-a-supply-chain-attack/.

like a government agency or company, attackers instead target the vendors who supply key systems and services to the target. Once the vendor is compromised, the attacker can then leverage the existing relationship between the vendor and the target agency to subvert a target's defenses and breach their systems. For example, a malicious actor can piggyback on a vendor's automatic update system to clandestinely install malware on every computer that runs that system, including their primary targets. However, because the updates with the malware are pushed out to every customer who operates the vendor's program, it leads to a large number of organizations potentially being attacked.

The SolarWinds attack is emblematic of this pattern. Rather than individually targeting US government agencies, Russia instead targeted SolarWinds who provides IT management software. By compromising SolarWinds' update system, Russia was able to clandestinely install malware on systems of SolarWinds' customers who installed the update. It is estimated that up to 18,000 users could have had the malware installed via this method. This included a large swath of US government agencies including the Departments of Treasury, Justice, Energy, Homeland Security, and Defense.[9]

Ransomware as a service follows a similar pattern of behavioral changes resulting in a historically common attack method becoming increasingly dangerous. Ransomware has existed since the 1980s and is one of the most common forms of cyberattack. However, ransomware as a service is a shift in how ransomware creators utilize their malware. Instead of simply using the ransomware themselves, professional ransomware gangs instead partner with outside criminal organizations and allow these affiliated groups to use their ransomware in exchange for a percentage of the proceeds.[10] The result has been an explosion of technologically unsophisticated actors, like organized crime, now being able to conduct ransomware attacks on a mass scale.

This increase in ransomware users has underpinned the targeting of critical infrastructure. Because the overwhelming majority of ransomware victims pay, the practice is a lucrative enterprise for criminals and the essential nature of critical infrastructure makes it an inviting target since it allows attackers to easily extort large sums from victims. The Colonial Pipeline and JBS food processing attacks are both examples of this trend with the attacks reportedly yielding ransoms of US $5 and US $11 million respectively.[11]

A persistent response to cyber insecurity

The Biden administration has taken several key steps to redress the current state of cyber insecurity. For state actors, like Russia and China, the US has continued to "name and shame" them as a mechanism for dispelling the anonymity of the cyber domain and holding them responsible for their actions.[12] In response to the SolarWinds hack, the Biden administration expelled Russian diplomats and issued sanctions against Russian entities involved in cyber operations. Additionally, after the Microsoft Exchange attack, the US took the unprecedented step of issuing a joint statement with its allies to condemn China's dangerous behavior.

Following the Colonial Pipeline attack, President Biden also issued an executive order dedicated to improving national cybersecurity.[13] The order marks one of the most extensive measures to date to improve national cybersecurity and includes measures to improve government cybersecurity, create a Cyber Safety Review Board, and remove barriers to information sharing about cyber threats.[14] The order's section detailing steps to improve software supply chain security through new standards, oversight and enforcement was particularly important. This section outlines the creation of guidelines for government software suppliers and constitutes one of the US government's first attempts to wield its considerable power as a consumer to improve cybersecurity by furthering best practices in secure software development.

Biden's executive order is an important and necessary step to redress the current spate of cyberattacks. But it is not

[9] Temple-Raston, Dina. 2021. "A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack." *National Public Radio*. https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack; Sanger, David, Nicole Perlroth and Eric Schmitt. 2021. "Scope of Russian Hacking Becomes Clear: Multiple US Agencies Were Hit." *The New York Times;* Lin, Herb. 2020. "Reflections on the SolarWinds Breach." *LawfareBlog*.

[10] Crowd Strike. 2021. "Ransomware as a Service (RaaS) Explained." https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas./

[11] Richardson, Ronny, and Max M. North. 2017. "Ransomware: Evolution, mitigation and prevention." *International Management Review* 13, no. 1.

[12] O'Connor, Tom. 2021. "After confronting Russia, Biden Accuses China of Running Cyber Criminal Ops." *Newsweek*; Marks, Joseph. 2021. "The US and Allies are taking a stand against Chinese hacking." *The Washington Post*.

[13] Biden, Joe. 2021. "Executive Order on Improving the Nation's Cybersecurity." *The White House*.https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[14] Chesney, Robert, and Trey Herr. 2021. "Everything You Need to Know About the New Executive Order on Cybersecurity." *LawFare*.https://www.lawfareblog.com/everything-you-need-know-about-new-executive-order-cybersecurity.

enough. Cybersecurity is a constantly evolving domain and requires persistence to sustain progress towards a digitally secure world. As the US embraces persistent engagement as its guiding doctrine in cyberspace, the US-Japan alliance will be essential to effectively navigating this digital domain and seizing the advantage from malicious actors.[15] Notably, with the United States developing guidelines for software suppliers, it is important that allies like Japan be included in this process. By combining efforts, the implementation of Biden's executive order represents an important opportunity to leverage the US-Japan alliance as a "norm entrepreneur" and establish best practices in software development as international standards.[16] Such measures will not resolve the current state of cyber insecurity but will significantly complicate the operations of malicious actors and deny them easy victories.

However, the most important step to overcoming national security challenges in cyberspace is psychological, not policy-based. As proven by the recent wave of attacks, the behavioral patterns of malicious actors are constantly changing. Consequently, cybersecurity must be thought of as a process dedicated to developing the institutions, mechanisms, and procedures to respond to future challenges rather than just meeting the current crisis. Within the framework of the US-Japan alliance, this means incorporating cybersecurity into every level of the strategic dialogue and developing collaborative mechanisms to support joint actions in the cyber domain. This includes expanding information sharing on threats and vulnerabilities as well as bilateral exercises to practice effective responses to major cyber incidents.[17]

The current, tenuous state of global cybersecurity is the by-product of malicious actors utilizing mass-targeted attacks to achieve their objectives. As the US and Japan both respond to this evolving threat, it is important to not limit the response to defeating the current crisis. Through coordination on cyber standards, cooperation, and persistence, it is possible to seize the initiative in the cyber arena and achieve meaningful gains towards a cyber secure world.

[15] Fischerkeller, Michael andRichard Harknett. 2021. "Initiative Persistence as the Central Approach for US Cyber Strategy." *Kybernao* 1. https://www.artsci.uc.edu/content/dam/refresh/artsandsciences-62/departments/political-science/ccsp/pdf_downloadableflyers/Kybernao_PaperSeries_Issue1_Final.pdf.

[16] Glen, Carol M. 2021. "Norm Entrepreneurship in Global Cybersecurity." *Politics & Policy*; Hurel, Louise Marie and Luisa Cruz Lobato. 2018. "Unpacking cyber norms: private companies as norm entrepreneurs." *Journal of Cyber Policy* 3, no. 1: 61-76; Adamson, Liisi. 2019. "Let Them Roar: Small States as Cyber Norm Entrepreneurs." *European Foreign Affairs Review*. 24, no. 2.

[17] Chernenko, Elena, Oleg Demidov, and Fyodor Lukyanov. 2018. "Increasing international cooperation in cybersecurity and adapting cyber norms." *Council on Foreign Relations*.

3. Strengthening US-Japan cooperation on protection of critical national infrastructure

By Benjamin Bartlett, Ph.D.

Introduction

From state actors to ransomware, threats to critical national infrastructure (CNI) are increasing every day. Given the risks to their national security and economies, this is a vital area for US-Japan cooperation. Based on discussions held over three days at the Pacific Forum's US-Japan Virtual Forum on Cybersecurity Cooperation, this article discusses current channels for cybersecurity cooperation between the US and Japan, ways those channels can be strengthened, and concrete policy steps the two countries can take to better cooperate on protecting CNI.

Channels for cybersecurity coordination

There are a number of existing channels of coordination between the US and Japan. The primary one is the Japan-US Cyber Dialogue, which has been held annually since 2013 and is led by the Japanese Ministry of Foreign Affairs (MOFA) and the US State Department, and includes representatives from a variety of agencies from both countries. The dialogues cover a wide range of topics related to cybersecurity cooperation, including the exchange of threat information, comparing national strategies, cooperating on the protection of critical national infrastructure (CNI), and national security cooperation.[1,2,3]

There is also the MOD-DOD Cyber Defense Policy Working Group, which deals with the military aspects of cybersecurity and held its first meeting in 2014. Japan's Deputy Director of the Bureau of Defense Policy acts as chair, with members joining from the Bureau of Defense Policy, the Operational Planning Bureau, and the Joint Staff Office. Members from the US include the Assistant Secretary of Defense for East Asia, the Joint Chiefs of Staff, US Indo-Pacific Command, and US forces in Japan. The group discusses issues such as information exchange and cooperation on the training and development of human resources and other areas of cooperation.[4,5]

There are also channels that focus more on the economic aspects of cybersecurity. The Japan-US Policy Cooperation Dialogue on the Internet Economy is the primary channel and touches on a number of issues related to the digital economy, including cybersecurity. Recent topics include securing information and communications technology (ICT), including 5G networks, Internet-of-Things (IoT) devices, and supply chain vulnerabilities. Participants include the US Deputy Secretary of State for Cyber and International Communications and Information Policy and representatives from the State Department, the Commerce Department, the National Telecommunications and Information Administration, and the Federal Communications Commission (FCC). From Japan, participants include the Director-General of the Ministry of Internal Affairs and Communications's Global Strategy Bureau and officials from several relevant agencies. Importantly, it includes not only government officials, but also representatives from private sector organizations such as Keidanren, the American Chamber of Commerce in Japan, and the US Chamber of Commerce. These organizations also participate in a working group under the umbrella of this dialogue.[6]

Steps to strengthen channels of cooperation

One major theme that was raised multiple times at the Pacific Forum event was the need to strengthen communication and trust, both between the two governments and between the governments and their nations' respective private sectors. There are steps that could be taken to strengthen the channels for cooperation between the two countries that would help with these issues.

Currently much of the discussion between the two countries on CNI takes place within the Japan-US Cyber Dialogue. This has some advantages, including the fact that the government organizations primarily responsible for protecting the cybersecurity of critical infrastructure (NISC and DHS) are included, and the focus is specifically on cybersecurity. On the other hand, the private sector is not represented, which is a problem given that in both countries, CNI is primarily located within the private sector. One beneficial step that the US and Japan could take would be to create a channel including representatives from CNI firms, such as a working group. Given the rapidity with which circumstances can change and the importance of the issue, it would be helpful for this workshop to meet at least several times a year.

A second way to strengthen these channels would be

[1] 2019. "The 7th Japan-US Cyber Dialogue." *Ministry of Foreign Affairs of Japan.* https://www.mofa.go.jp/press/release/press4e_002646.html
[2] 2019. "The Seventh US-Japan Cyber Dialogue." *US Department of State.* https://2017-2021.state.gov/the-seventh-u-s-japan-cyber-dialogue/
[3] Soesanto, Stefan. 2020. "Japan's National Cybersecurity and Defense Posture: Policy and Organizations." *ETH Zurich.*
[4] Ibid.
[5] 2018. "防衛省・自衛隊：日米サイバー防衛政策ワーキンググループ（CDPWG）第６回会合について." Translated to "About the 6th Meeting of the United States-Japan Cyber Defense Policy Working Group." *Ministry of Defense of Japan.* https://warp.da.ndl.go.jp/info:ndljp/pid/11623291/www.mod.go.jp/j/press/news/2018/09/21e.html.
[6] 2019. "Joint Statement on the 10th US-Japan Policy Cooperation Dialogue on the Internet Economy." Ministry of Economy, Trade and Industry. https://www.meti.go.jp/press/2019/10/20191018005/20191018006-2.pdf.

to engage in personnel exchanges, in particular between agencies other than MOD/DOD; for example, between NISC and CISA. This would help in the coordination of policy by having someone from the other government "in the room" when decisions were being made.[7] Second, it would help to build personal relationships between the two governments and create clear points of contact. Third, it would help the US and Japan to move their cooperation beyond the more narrow framework of the US-Japan Alliance. The alliance plays a very important role in cybersecurity cooperation but for many cybersecurity-related issues, including the protection of CNI, there needs to be more cooperation and coordination among a variety of government agencies on both sides.

Steps to strengthen cooperation on CNI

There are are also a number of concrete policy steps that the US and Japan could take in order to strengthen their cooperation on protecting CNI, many of which were raised during the three-day event held by the Pacific Forum. To begin, there are steps that could be taken to strengthen government-to-government cooperation. First, it would be helpful for the US and Japan to put a plan in place for dealing with threats to CNI that fall short of an armed attack. The US and Japan have made it clear that in the case of a cyber attack that rises to the level of an armed attack, Japan would be able to use its Self-Defense Forces in response and the US would assist Japan under the terms of the alliance. However, it is not clear how the two would respond in the case of a cyber operation that falls short of this level. For example, how can the two coordinate on a response to the mere presence of a state-sponsored actor in the CNI? This is important because a coordinated response by the two countries is likely to have a stronger effect than unilateral action.

Second, both sides need to continue to address obstacles to the sharing of classified information. While it has been controversial in Japan, the US has welcomed the Japanese 2013 Specially Designated Secrets Act (SDS), which among other things strengthened penalties for leaking sensitive information. This was reassuring after a series of breaches in Japan in the 2000s.[8] There are reports, however, that the US continues to be reluctant to share intelligence with Japan until Japan develops a better system for protecting classified information.[9] Having greater access to US intelligence on cyber threats would help Japan to engage in proactive defense, but at least as importantly, it would make it easier for the two to coordinate on attribution. Japan may be more reluctant to join the US in making attribution if it cannot see the intelligence upon which said attribution was based. Thus it would be helpful to both sides to find ways to make the sharing of classified or sensitive information easier.

There are also steps that could be taken to improve cooperation between CNI firms in both countries, as well as between these firms and the two governments. One participant in the three-day event mentioned that US and Japanese Information Sharing and Analysis Centers (ISACs), private-sector organizations supporting information sharing about cyber threats for various critical infrastructure sectors, were already sharing information with each other. This is an important step, since the threats faced within a given sector will be similar in the US and Japan and firms from each country can learn from each other. The two governments should work to support these efforts and to share information about cyber threats with the ISACs as well with each other and encourage cooperation with ISACs from other friendly countries.

Another idea that was raised by a participant was to invite CNI operators to participate in joint exercises along with participants from the US and Japanese governments. This would help to build trust and relationships between the private and public sector, and would also provide opportunities to practice coordinated responses to cyber events. This would be an important step in developing a better joint response to cyber threats against CNI.

Along with these actions, the US and Japan should work to build cooperation beyond the bilateral framework. Already we are seeing activity along these lines within the framework of the Quadrilateral Security Dialogue, a strategic dialogue between the US, Japan, India, and Australia. Japan has also been working to improve cybersecurity cooperation with European states as well as other regional actors, such as Vietnam. Given the similar threats to CNI globally, there are obvious benefits to bringing in other actors where possible, though in some areas this is limited by, for example, concerns about sharing intelligence. Increased US-Japan-South Korea cybersecurity cooperation

[7] The difficulty of coming up with coordinated policy without someone from the other government in the room was highlighted by the tabletop exercise put on by the Pacific Forum. Without having an easy way to get input from one's partner early on in decision-making, there ends up being a lot of back-and-forth and extra work coordinating.

[8] Fishlock, Nicholas. 2019. "The Development of Japan's Intelligence Policy in the 21st Century."*Institute for Security & Development Policy*. https://www.isdp.eu/publication/development-of-japans-intelligence-policy/.

[9] Levy, James L., Douglas E. Schoff, and Joshua Rake. 2021. "A High-Tech Alliance: Challenges and Opportunities for US-Japan Science and Technology Collaboration." *Carnegie Endowment for International Peace*. https://carnegieendowment.org/2021/07/29/high-tech-alliance-challenges-and-opportunities-for-US-japan-science-and-technology-collaboration-pub-85012.

would be helpful as well, particularly given that Japan and South Korea face similar regional threats, though no doubt such efforts will face similar challenges as have efforts to improve intelligence cooperation.[10]

Finally, the US and Japan could work together to promote the advancement of cybersecurity capacity within developing countries. We have seen through such events as natural disasters in Southeast Asia that with modern global supply chains, the US and Japan are vulnerable not only to disruptions of their own critical infrastructure but to disruptions of CNI elsewhere in the world. Increasing cybersecurity capacity in the developing world is critical to reducing these supply chain risks. The US and Japan have made efforts in this regard, such as through the US-Japan Cybersecurity Joint Training with ASEAN Member States, which focused on building cybersecurity-related human resources in ASEAN member states with a particular focus on CNI.[11] These efforts should be built upon and strengthened.

The US and Japan have already taken important steps to improve cooperation on protecting the cybersecurity of critical national infrastructure. By building upon these efforts and expanding cooperation to other friendly countries, they can continue to reduce the risks cyber threats to CNI pose to their national security and economies.

[10] Botto, Kathryn. 2020. "Overcoming Obstacles to Trilateral US-ROK-Japan Interoperability." *Carnegie Endowment for International Peace*. https://carnegieendowment.org/2020/03/18/overcoming-obstacles-to-trilateral-US-rok-japan-interoperability-pub-81236.
[11] 2018. "US-Japan Cybersecurity Joint Training with ASEAN Member States Held." Ministry of Economy, Trade and Industry. https://www.meti.go.jp/english/press/2018/0914_001.html.

4. Seizing on US-Japan opportunities for submarine cable security

By Justin Sherman

Submarine cables — metal tubes filled with fiber optic lines, laid across the ocean floor — are deployed in the hundreds worldwide. These cables haul internet traffic between continents and are vital to the function of the global internet.

Yet submarine cables are under increased threat as risks to their security and resiliency grow. Authoritarian governments, especially China and Russia, are exerting more control over internet infrastructure in order to reshape it in their favor. More cable owners are using remote network management systems for cables, linking cable systems to the internet in ways that increase operational security risks while the data flowing through the cables grows in volume and sensitivity each year. The United States and Japan have an opportunity to invest in the security and resilience of submarine cables that underpin the global internet.

The cables powering the global internet

As of December 2020, there are hundreds of submarine cables deployed around the world, collectively controlled by 383 entities spread across the world — state-owned firms, privately owned firms, and international consortia.[1] If an internet user in California accesses a website in Berlin or a businessperson in Tokyo emails a client in Sydney, it is highly likely that the data travels over these cables laid across the ocean floor.

Eighty submarine cables presently touch the US mainland and 25 cables touch Japan,[2] many of which directly connect the two countries. The Trans-Pacific Express Cable System, deployed in August 2008, runs almost 18,000 kilometers and links Nedonna Beach in the US to Maruyama in Japan, as well as cities in China, South Korea, and Taiwan.[3] The Japan-US Cable Network, deployed in September 2001, extends over 22,600 kilometers and connects three cities in Japan with three cities in the US.[4] More recently, the New Cross Pacific Cable System was deployed in May 2018 and links Pacific City, US with Maruyama, Japan, as well as cities in China, Taiwan, and South Korea.[5]

International collaboration is vital to submarine cable planning, construction, and maintenance. Laying cables is a logistically complex and financially expensive process, with newer and longer cables often costing hundreds of millions of US dollars. The process of laying cables involves multiple companies to produce the fiber within a cable, lay the cable along the ocean floor, and maintain the landing stations along the shorelines. Hence collaborations not just between US and Japanese firms, but those from countries all over the world are necessary. There are emerging risks to submarine cables, however, that are making this international collaboration a point of geopolitical contention.

Risks to the internet infrastructure

There are three trends that are increasing the risks to the security and resiliency of submarine cables.

First, more authoritarian governments, especially in China and Russia, are exerting control over internet companies within their borders to reshape the global internet in their favor. This spans everything from building cables that encourage data to move through new midpoints for potential espionage, to capacity building and cable investment projects that can generate profits for businesses and connect new markets to the internet, but could also be vectors for increasing economic and technological dominance.

Second, more cable owners are using remotely controlled, internet-connected systems to manage cable networks. By linking their cable systems to the internet using software with poor security, they are increasing the vulnerability of submarine cables to hacking.

Third, the volume and sensitivity of data flowing across undersea cables is rapidly rising. As this occurs, governments have greater incentive to spy on cables and position themselves to control cable chokepoints, and malicious non-state actors may have greater incentive to monitor cable data or disrupt cable operation altogether.[6]

Disruptions to these cables are so harmful — to the flow of internet traffic, to free speech, to economic and national security — because they are central to the global internet. If a cable is physically damaged, data must be rerouted along other paths, which slows the overall flow of data. Cable repair is thus an economic and security issue, as delays in fixing damage from a ship collision or underwater earthquake mean delays in restoring full

[1] Sherman, Justin. 2021. "Cyber Defense Across the Ocean Floor: The Geopolitics of Submarine Cable Security." *Atlantic Council*. https://www.atlanticcouncil.org/in-depth-research-reports/report/cyber-defense-across-the-ocean-floor-the-geopolitics-of-submarine-cable-security/.

[2] 2021. "Submarine Cable Map." https://www.submarinecablemap.com/.

[3] 2021. "Trans-Pacific Express (TPE) Cable System." *Submarine Cable Map*. https://www.submarinecablemap.com/submarine-cable/trans-pacific-express-tpe-cable-system.

[4] 2021. "Japan-US Cable Network." *Submarine Cable Map*. https://www.submarinecablemap.com/submarine-cable/japan-u-s-cable-network-jus.

[5] 2021. "New Cross Pacific (NCP) Cable System." *Submarine Cable Map*. https://www.submarinecablemap.com/submarine-cable/new-cross-pacific-ncp-cable-system.

[6] Sherman, Justin. 2021. "Cyber Defense Across the Ocean Floor: The Geopolitics of Submarine Cable Security." *Atlantic Council*.

internet connectivity to a region. There is also a national security concern that a terrorist organization could destroy a cable or hold a cable landing station physically hostage, or that adversaries might damage cables in a military conflict. For all the abstract verbiage around the "cloud" and other technologies, the internet still depends on physical infrastructure that can be seized, damaged, degraded, or destroyed.

Investing in cables is a way for internet and telecommunications companies as well as governments to make money — delivering faster internet speeds to new markets, and licensing the use of bandwidth on the cable. But governments may also invest in cables to shape the internet's physical layout. By investing in faster cables in select places, states can encourage global internet traffic to flow through particular midpoints for interception and could also enable the build up of a connected country's technological and economic dependence. American policymakers have raised these precise concerns around cable projects that would link the US to China, alleging that Beijing could tap into a Chinese-side landing point for espionage.[7] Japanese policymakers have expressed similar concerns that growing Chinese investment in submarine cables may heighten security risks to the nation.[8]

Many of the Chinese investments in the global submarine cable network are controlled by the Chinese government — spanning state-owned telecoms, like China Telecom, China Unicom, and China Mobile to state-controlled firms like CITIC Telecom International.[9] Beijing's investment decisions influence the internet's changing physical shape and also heighten the risk that it may attempt to use that influence for espionage and other purposes.

These risks are specifically high for the US and Japan since the Chinese government partly owns many of the undersea cables linking the two countries. The aforementioned Trans-Pacific Express Cable System is collectively owned by private companies AT&T and Verizon in the US, Chunghwa Telecom in Taiwan, KT in South Korea, and NTT in Japan — as well as China Telecom and China Unicom, both of which are owned by the Chinese government.[10] China Mobile, China Telecom, and China Unicom are co-owners of the New Cross Pacific Cable System.[11] China Telecom and China Unicom are also co-owners of the Japan-US Cable Network. Broadly, these Chinese state-owned telecoms play an active role in cable investments in the Asia-Pacific.[12]

Forging US-Japan submarine cable security

For years, liberal-democratic governments took a relatively hands-off approach to the internet because of the general belief that the internet was inherently democratizing when left untouched.[13] However, there is now growing recognition across those states — the US and Japan included — that issues with privacy, cybersecurity, and internet provider and internet platform behavior demand greater regulation.[14] While there is no consensus, even within individual democracies, on how to regulate the internet, the need for regulation is clear.[15] In October 2020, Kazuyuki Furuya, the head of Japan's Fair Trade Commission, said the commission will be investigating market abuses by internet and technology companies.[16] In January 2021, the Japanese parliament passed a new law regulating the market behavior of large technology

[7] Department of Justice Office of Public Affairs. 2020. "Team Telecom Recommends that the FCC Deny Pacific Light Cable Network System's Hong Kong Undersea Cable Connection to the United States." *The US* Department of *Justice*. https://www.justice.gov/opa/pr/team-telecom-recommends-fcc-deny-pacific-light-cable-network-system-s-hong-kong-undersea.

[8] 2020. "Japan's government to counter China's submarine cable presence." *The San Francisco Chronicle*. https://www.sfchronicle.com/news/article/Japan-s-government-to-counter-China-s-submarine-14958953.php.

[9] Sherman, Justin. 2021. "Cyber Defense Across the Ocean Floor: The Geopolitics of Submarine Cable Security.." *Atlantic Council*.

[10] 2021. "Trans-Pacific Express (TPE) Cable System." *Submarine Cable Map*.https://www.submarinecablemap.com/submarine-cable/trans-pacific-express-tpe-cable-system.

[11] 2021. "New Cross Pacific (NCP) Cable System." *Submarine Cable Map*. https://www.submarinecablemap.com/submarine-cable/new-cross-pacific-ncp-cable-system.

[12] 2021. "How China Telecom is Connecting Countries Across Asia with the APG Line." *China Telecom.*. https://www.ctamericas.com/china-telecom-connecting-countries-across-apg/.

[13] Morgus, Robert and Justin Sherman. 2018. "The Idealized Internet vs. Internet Realities (Version 1.0): Analytical Framework for Assessing the Freedom, Openness, Interoperability, Security, and Resiliency of the Global Internet.*"New America*. https://www.newamerica.org/cybersecurity-initiative/reports/idealized-internet-vs-internet-realities/; Morozov, Evgeny. 2011. "The Net Delusion: The Dark Side of Internet Freedom.*" PublicAffairs*.

[14] Sherman, Justin. 2019. "How Much Cyber Sovereignty Is Too Much Cyber Sovereignty?" *Council on Foreign Relations*. https://www.cfr.org/blog/how-much-cyber-sovereignty-too-much-cyber-sovereignty.

[15] Chander, Anupam and Haochen Sun. 2021. "While it does not exclusively cover liberal democracies." *Georgetown University Law School*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3904949.

[16] Kihara, Leika and Takahiko Wada. 2020. "Japan to join forces with US, Europe in regulating Big Tech firms: antitrust watchdog head." *Reuters*. https://www.reuters.com/article/us-japan-economy-ftc/japan-to-join-forces-with-u-s-europe-in-regulating-big-tech-firms-antitrust-watchdog-head-idUSKBN2740DZ.

platforms.[17] The US executive branch and legislature have placed a similar focus on technology regulation, even as bills in the US Congress have stalled.

There is considerable political and strategic momentum for the US and Japan to better secure submarine cables as part of this regulatory wave and there are several key strategies identified to accomplish this goal. Of many possible action items to pursue, a few merit priority.

First, the US and Japan should review current intelligence-sharing mechanisms on threats to undersea cables. While there is little documented evidence of governments damaging submarine cables, it is quite possible that in a conflict scenario a government could seize, degrade, or disrupt submarine cable infrastructure. This would impair the flow of global internet traffic and undermine the sharing of civilian, business, and government and military communications. The US and Japan should ensure they are adequately sharing intelligence on these kinds of threats to the global internet infrastructure, especially as national security analysts in the US raise these concerns *vis-à-vis* China and Russia.[18]

Diplomats in Washington and Tokyo should also advance conversations, and potentially conduct joint studies, on how their governments can better integrate submarine cables into overseas capacity-building programs. The Chinese government is notably accelerating its investment in the global submarine cable network, including as part of its multi-billion-dollar Belt and Road Initiative.[19] While there are undoubtedly many commercial drivers behind this work, there is also the risk that the Chinese government could leverage its undersea cables for espionage and other malicious activities. American and Japanese policymakers should examine how they can support the submarine cable network's maintenance and expansion in ways that uphold an open and secure internet.

Aside from risks from authoritarian states, there are also many places around the world — such as throughout the Asia-Pacific — where companies are building cables and linking them to poorly secured systems. This exposes cable management systems to hacking. The US and Japan should therefore examine ways to support the development of cybersecurity standards for international cable projects, particularly where countries may lack the capacity to do so themselves. The Japanese company NEC is one of the world's largest builders of undersea cables[20] and provides the Japanese government with another opportunity to help incentivize better security for cable infrastructure.

Finally, the US has begun establishing the Cable Ship Security Program, an initiative for government supported, fast repair of cables relevant to national security.[21] Two privately owned, government-approved ships will be placed on standby, with funding from the US government, to repair damaged undersea cables whose operation is judged relevant to the national security of the US. While this is a program unique to the US, the Japanese government could explore developing a similar initiative to ensure that any Japan-linked cables are quickly repaired in the event of damage.

Looking forward

The private sector has long played a large role in the global undersea cable network for many reasons. Perhaps most significantly, this has enabled the development of global internet connectivity without democratic states controlling telecommunications companies' projects or playing too large a role in their internet infrastructure. International collaboration between companies and state-owned firms likewise has many benefits, such as covering the enormous costs and management of the complex logistics of inter-country and inter-continental internet connectivity. Nonetheless, the risks to submarine cable security and resilience are accelerating. The US and Japan's global political influence, economic power, and ability to incentivize telecoms within their borders present a key opportunity to use this leverage to promote cable security and resilience.

[17] 2021. "Japan's new law regulating tech giants' commerce platforms takes effect." *Japan Times*. https://www.japantimes.co.jp/news/2021/02/01/business/tech/tech-giant-law-takes-effect/.

[18] Birnbaum, Michael. 2017. "Russian submarines are prowling around vital undersea cables. It's making NATO nervous." *The Washington Post*. https://www.washingtonpost.com/world/europe/russian-submarines-are-prowling-around-vital-undersea-cables-its-making-nato-nervous/2017/12/22/d4c1f3da-e5d0-11e7-927a-e72eac1e73b6_story.html.

[19] Kelkar, Keshav. 2018. "From silk threads to fiber optics: The rise of China's digital silk road." *Observer Research Foundation*. https://www.orfonline.org/expert-speak/43102-from-silk-threads-to-fiber-optics-the-rise-of-chinas-digital-silk-road/.

[20] Chanthadavong, Aimee. 2020. "NEC appointed to build Asia Pacific submarine cable." *ZDNet*. https://www.zdnet.com/article/nec-appointed-to-build-asia-pacific-submarine-cable/.

[21] 2021. "Request for Applications To Be Considered for Enrollment in the Cable Security Fleet." *The Federal Register*. https://www.federalregister.gov/documents/2021/01/05/2020-29159/request-for-applications-to-be-considered-for-enrollment-in-the-cable-security-fleet.

5. US-Japan cybersecurity cooperation

By Professor Wilhelm Vosse, Ph.D.

Introduction

In the last decade, major Japanese companies, government ministries, the National Diet, military manufacturers and even the Self-Defense Forces (SDF) have been the target of cyberattacks. In response, Japan has begun to harden its IT infrastructure, releasing several cybersecurity strategies and intensifying its cooperation with like-minded countries and its sole security ally, the United States. Japan has become a major cyber-diplomatic actor and a core partner for improving cyber capacity and confidence-building measures and, as a result, was able to prevent a major cyber attack before or during the Tokyo Olympics and Paralympics.

Despite these positive developments, Japan continues to suffer from some major weaknesses which could become more obvious in the case of a major coordinated and persistent attack against core Japanese infrastructure. This paper highlights some of these strengths and weaknesses, before making some policy suggestions.

Strength of Japan's cybersecurity policy

Cyber diplomacy

Japan is one of the most active players in cyber diplomacy on a bilateral as well as a multilateral level. Apart from the US-Japan Cybersecurity Dialogue, it has built similar dialogues with almost a dozen other countries and associations, such as the European Union, Germany, France, Estonia, the United Kingdom, Australia, India, Israel, and ASEAN. In recent years, it has deepened its partnerships with NATO and its NATO Cooperative Cyber Defense Center of Excellence. In terms of multilateral cooperation, Japan has long played an active role in the United Nations Group of Governmental Experts (UNGGE) and, since its inception, the United Nations Open-Ended Working Group (OEWG).

The core pillars of Japan's cyber diplomacy are the promotion of the rule of law in cyberspace, the development of confidence-building measures and cooperation on capacity building. In 2018, Japan's then-Foreign Minister Taro Kono stressed that Japan is using "cyber diplomacy to realize a free, fair, and secure cyberspace," in which "existing international law should be applied."[1] A central way to achieve this is to strengthen international rules and norms in various fora, including the United Nations.

Cyber capacity building

Capacity building is one of the core policy elements of Japan's cybersecurity strategy and its broader cyber diplomacy efforts.[2] The core components are (1) capacity building, (2) international cooperation in the sharing of expertise and the coordination of policies, and (3) incident response. Japan also encourages companies and other stakeholders to contribute to the security of cyberspace at home and in other countries based on measures that were developed in the 2016 *Basic Strategy on Cybersecurity Capacity Building for Developing Countries*. The document laid out a list of policy objectives specifically targeting the improvement of cybersecurity capacities in developing countries, fighting cybercrime, and sharing an understanding and awareness of confidence-building measures.[3]

Japan's regional focus is on ASEAN member states, where its capacity-building initiatives are promoted through the ASEAN-Japan Information Security Policy Meeting, the ASEAN-Japan Ministerial Policy Meeting on Cybersecurity Cooperation JASPER Project (Japan-ASEAN Security Partnership), and by cooperating with Asian Cyber Incident Response Teams (CSIRTs) under the TSUBAME Project. Moreover, the ASEAN-Japan Ministerial Meeting (AMMTC+Japan) and the Senior Officials Meeting on Transnational Crime (SOMTC+Japan) are central to the dialogue among senior government officials from ASEAN countries and Japan.[4]

The latest and most concrete Japanese initiative in capacity building is the launch of the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC), which opened in Bangkok, Thailand, in September 2018. The core objectives are improving the skills of security-related agencies in 10 ASEAN countries, the development of a standardized Incident Reporting Framework across the region and the establishment of ASEAN Computer Emergency Response Team (ASEAN-CERT).[5]

On a practical level, over the last decade Japan's National Center of Incident Readiness and Strategy for

[1] Kono, Taro. 2018. "Speech by H.E. Taro Kono, Minister for Foreign Affairs of Japan at the Closing Session on the First Day of the 18th Doha Forum.". https://www.mofa.go.jp/me_a/me2/page4e_000959.html.

[2] National Center of Incident Readiness and Strategy for Cybersecurity. 2018. "Cybersecurity Strategy." https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf.

[3] 2016. "Saibāsekyuriti bun'ya ni okeru kaihatsutojōkoku ni taisuru nōryoku kōchiku shien." Translated to "Basic Policy to Support Cybersecurity Capacity-Building in Developing Countries." *National Center of Incident Readiness and Strategy for Cybersecurity*. http://www.nisc.go.jp/conference/cs/dai10/pdf/10shiryou09.pdf.

[4] Information Security Policy Council Japan. 2013. "International Strategy on Cybersecurity Cooperation: J-Initiative for Cybersecurity." https://www.nisc.go.jp/eng/pdf/InternationalStrategyonCybersecurityCooperation_e.pdf

[5] Bhunia, Priyankar. 2018. "ASEAN-Japan Cybersecurity Capacity Building Centre to Be Launched in Thailand in June 2018." *OpenGov Asia*. https://www.opengovasia.com/asean-japan-cybersecurity-capacity-building-centre-to-be-launched-in-thailand-in-june-2018/.

Cybersecurity (NISC) has organized workshops with incidence response organizations in Brunei, Cambodia and Indonesia to improve their cyber-incident response and to better protect their information infrastructure by holding joint cybersecurity exercises. The Japanese government has also begun including cyber capacity building as an element of its traditionally strong development assistance (ODA). A recent example is the technical cooperation project, Capacity Building in Policy Formation for Enhancement of Measures to Ensure Cybersecurity in ASEAN Region, launched in early 2020 by Japan's International Cooperation Agency (JICA).[6]

Confidence-building measures

One objective of Japan's capacity building is to improve public confidence and trust in information technology through intergovernmental cooperation on setting norms and regulations in cyberspace. Its 2018 cybersecurity strategy highlights the importance of strengthening confidence among states in order to prevent the "occurrence of unforeseen circumstances and deterioration of the situation caused by cyberattacks" and an unintentional increase of tensions. Japan aims to build "international communication channels, increase transparency, and deepen policy dialogues in bilateral and multilateral consultations as central components."[7]

As with capacity building, the corresponding confidence-building measures are heavily focused on ASEAN and the ASEAN Regional Forum (ARF). For example, between 2017 and 2019, the Cabinet Office and MOFA held several bilateral consultations within the ARF framework to share policies on threat awareness and cybersecurity strategies as a means to build trust. These also helped to establish an inter-sessional meeting on cybersecurity and the ARF expert meeting in order to improve the predictability of responses and activities of these countries.[8]

Joint training exercises

In order to streamline and improve coordination between different actors after a cyber attack, joint training exercises are a central tool. Over the last few years, NISC has increasingly participated in joint cyber exercises with the United States and, since it joined the NATO Cooperative Cyber Defense Center of Excellence (CCDCOE) as a full member in December 2019, also with other NATO members. At that time, Japan's Defense Ministry admitted that it had little experience in international cyber exercises and that multilateral exercises would enable it to better prepare for actual operations.[9] Since then, Japan has participated in the NATO Cyber Defense Exercise, Cyber Coalition 2019 in December 2019 in Estonia, and in August 2020 joined ten other countries including the United States and several European NATO members, Australia and Israel in another NATO cyber exercise.[10] In April 2021, a team from the Japanese Ministry of Defense and the JPCERT/CC participated in the NATO CCDCOE Locked Shields 2021 cyber exercise.[11]

As these exercises are normally based on real world scenarios and run over a few days, the Japanese participants not only improve their cyber defense capabilities and learn from the methods and tools of emergency response teams in partner countries, but they can also help both sides to exchange information and apply tools in case of a major cyberattack. These exercises could potentially function as an equalizer and strengthen Japan's cyber defense capabilities, however, their effectiveness also depends on the political will in Tokyo, which has only just begun to shift.

Weaknesses of Japan's cybersecurity policy

Framing of cyberattacks

One weakness of Japan's approach to cybersecurity is that cyberattacks are only considered crimes (cybercrime), even when the attack is conducted by a foreign agent and is targeting major infrastructure. A number of cyberattacks, including those against major entities like Mitsubishi Heavy Industries, the National Diet of Japan, the Japan Pension Service and even the Ministry of Foreign Affairs and the Ministry of Defense, all triggered investigations by the National Police Agency (NPA). If the attack

[6] Okano-Heijmans, Maaike and Wilhelm Vosse. 2021. "Promoting Open and Inclusive Connectivity: The Case for Digital Development Cooperation." *Research in Globalization*. https://doi.org/10.1016/j.resglo.2021.100061.

[7] "Cybersecurity Strategy." National Center of Incident Readiness and Strategy for Cybersecurity.

[8] 2018. "ARF Inter-Sessional Meeting on Security of and in the Use of Information and Communication Technologies (ICTs) and 1st ARF-ISM on ICTs Security." *Ministry of Foreign Affairs of Japan*. https://www.mofa.go.jp/press/release/press4e_002011.html.

[9] 2019. "Japan joins NATO cybersecurity drills to counter Chinese hackers." *Nikkei Asian Review*. https://asia.nikkei.com/Politics/International-relations/Japan-joins-NATO-cybersecurity-drills-to-counter-Chinese-hackers.

[10] 2019. "Natō saibā bōei enshū 'saibā koarishon 2019' e no sanka ni tsuite." Translated to "Participation in NATO cyber defense exercise 'Cyber Coordination 2019.'" *Ministry of Defense of Japan*. https://www.mod.go.jp/j/press/news/2019/index.html; The Yomiuri Shimbun, 2020. "Japan Orchestrating 1st Joint Cyber Drill with US" *The Japan News*.

[11] Japan Ministry of Defense. 2021. "Participate in International Cyber Exercise.", April 2021. https://www.mod.go.jp/en/article/2021/04/5fd96950ea91fddb91d84033407c1f9b16d95378.html;
Mochinaga, Dai. "JPCERT/CC Participated in the Locked Shields 2021." JPCERT/CC Eyes, April 2021. https://blogs.jpcert.or.jp/en/2021/05/locked-shields-2021.html.

originated from outside Japan, the Japanese police will try to cooperate with police forces in those countries and the Japanese government will ask foreign government or intelligence services for their cooperation, in some cases taking advantage of the Convention on Cybercrime or the Criminal Assistance Convention with the United States, and the International Criminal Police Organization (ICPO). However, in the end it is only treated as a criminal offense and not an attack against the Japanese state.

Because individuals in state-sponsored cyberattacks can rarely be identified without the help of the country from which the attack originates, a domestic investigation does not serve as a deterrent for foreign-based perpetrators. Japan should revise the narrow definition of cyberattacks and strengthen the subsequent government response.

Public attribution

Japan has traditionally been very careful in publicly responding to or attributing cyberattacks, specifically when Japanese institutions had not directly been targeted or when Russia was involved. For example, after the cyber attack against Estonia in 2007, Japan did not join the United States in publicly attributing it to Russia. Even after the Sony Picture hack, which indirectly involved a Japanese company, the Japanese response was quite muted. In a press conference on December 22, 2014, Chief Cabinet Secretary Suga only confirmed the attribution of North Korea in the Sony Pictures Entertainment attack, but did not independently accuse North Korea.[12] In recent years, we have seen some initial changes. After the WannaCry and NotPetya attacks in 2017 and the cyber attack against Georgia in 2019, Japan joined the public attribution from the United States, the EU and the UK, albeit with somewhat weaker statements.[13]

One reason for Japan's timidness in public attribution is its concern to get into the firing line of possible counter attacks by the accused countries. This weakens the message from countries otherwise in favor of strengthening international cyber norms. The other reason is Japan's underdeveloped cyber intelligence capabilities compared to Five-Eyes nations,[14] which could allow Japan to independently verify the accusations. One way out of this dilemma might be better cyber intelligence exchange between the United States and Japan. However, without Japan developing independent capabilities which could assist NATO and US cyber intelligence, this might not happen in the near future.

Weak offensive cyber capabilities

In his attempt to define and categorize different types of cyber defense activities, Robert Dewar distinguished three modes of cyber defense, namely (1) active cyber defense (ACD), (2) resilient cyber defense (RCD), and (3) fortified cyber defense (FCD).[15] In the last 10 years, Japan's preference has been strongly for resilient cyber defense. For the US and the UK, active cyber defense includes the penetration of their adversaries' ICT systems and developing cyber tools such as viruses to harm their information security infrastructure. Japan's cybersecurity strategy uses a much narrower definition. Under the banner "Realization of a society where people can live safely and with peace of mind," Japan's cybersecurity strategy (2018) limits "active cyber defense" to (1) measures and efforts to protect society, (2) the protection of critical infrastructure in the public and private sectors, and (3) strengthening the security of government agencies. However, it also demands that Japan develop active cyber defense capabilities in cooperation with cyber-related enterprises, including preventive measures against threats allowing Japan to act in advance of a possible attack. The strategy specifically mentions capabilities to prevent cybercrime and cyberattacks by sharing and utilizing relevant information, and using technologies to induce attacks by collecting information on attackers or measures against botnets.[16] However, it does not explain in more detail what technologies and methods might be developed or used by Japan. In 2019, there were reports that the SDF was working on ways to fight back against cyberattacks and the Ministry of Defense (MOD) announced that it was considering developing a computer virus which could be used as a defensive measure against cyberattacks by 2020. While this malware would be able to "break into computer systems" it was predominantly meant to be a deterrent and not an offensive cyber capability.[17]

Japan's new National Defense Program Guidelines for 2019 and beyond goes a bit further by demanding Japan strengthen its "cross-domain operations" in the

[12] 2014. "Press Conference by the Chief Cabinet Secretary. " *Prime Minister of Japan and His Cabinet.* https://japan.kantei.go.jp/tyoukanpress/201412/22_a.html.

[13] 2017. "The US Statement on North Korea's Cyberattacks (Statement by Press Secretary Norio Maruyama)." *Ministry of Foreign Affairs of Japan.* December 20, 2017. https://www.mofa.go.jp/press/release/press4e_001850.html.

[14] A group of five countries which exchanges intelligence. They are Australia, Canada, New Zealand, the United Kingdom, and the United States.

[15] Dewar, Robert. 2017. "Active Cyber Defense." *Risk and Resilience Team Center for Security Studies.* https://doi.org/10.13140/RG.2.2.19236.17287.

[16] "Cybersecurity Strategy." National Center of Incident Readiness and Strategy for Cybersecurity.

[17] The Yomiuri Shimbun, 2018. "SDF May Get Ability to Fight Back Against Cyber-Attacks." *The Japan News.* http://the-japan-news.com/news/article/0004414829; 2019. "In First, Japan to Develop Computer Virus to Defend Against Cyberattacks." *The Japan Times.*

space, cyber and electromagnetic domains, and to improve capabilities for monitoring SDF command and communications systems. Among other things, it demands the SDF strengthen its cyber defense capabilities including its ability to "disrupt, during attack against Japan, opponent's use of cyberspace for the attack,"[18] by strengthening the SDF's command, control, communications and information (4CI) capabilities.[19]

In August 2021, Defense Minister Nobuo Kishi reiterated that cyber deterrence is a central capability which is going to be enhanced in order to protect Japan's security interests from cyber-attacks and as an element of the US-Japan alliance. However, this would mostly be limited to defending the MOD network, and detecting, investigating and analyzing cyberattacks in order to identify and hold attackers accountable.[20]

Others stressed that offensive cyber operations have not been widely discussed in public by the Japanese government and that the preferences outlined so far are predominantly aimed at deterrence by denial, and not at deterrence by punishment.[21] For these and other reasons, Japan is widely perceived as being behind other countries in developing and potentially deploying such tools or weapons. Recent comparative surveys on cyber power, like those from the International Institute for Security Studies (IISS), came to the conclusion that Japan's independent cyber-security capabilities were not strong because it had no offensive capabilities, relying instead on cooperation with the United States.[22] However, the 2020 IISS report *Cyber Capabilities and National Power* gave Japan's cyber power a mid-ranked position because of its strong commercial capabilities and influence in the setting of international norms.[23]

Overall, Japan's preference for non-militarist values and lack of public support for more active cyber defense means that Japan, while continuing to strengthen its resilience against cyberattacks, will refrain from using any capabilities which could potentially be perceived as offensive, even by countries like China or Russia.

Policy Recommendations

Japan's risk aversion does not send clear signals to foreign adversaries. One challenge for both sides is Japan's "defensive defense" policy and its constitutional constraints. Since 2013, the US-Japan Cyber Defense Policy Working Group (CDPWG) has aimed at producing a better understanding of Japan's constraints and its preference for upholding international law. The second issue for Japan is its staff shortage in the MOD Cyber Defense Unit, which is also a concern for the United States.[24]

The April 2019 US-Japan Security Consultative Committee stressed "space, cyberspace, and the electromagnetic spectrum as priority areas to better prepare the Alliance for cross-domain operations" and agreed to enhance their cooperation in "deterrence and response capabilities." The most consequential development is the decision to extend the defense guarantee of Article 5 of the US-Japan Security Treaty to cyberattacks, even though as for any other security threat, the decision to invoke Article 5 would be made on a case-by-case basis.[25]

Given the above-mentioned strengths and constraints, the following policy recommendations would take advantage of the strengths and weaknesses of both the United States and Japan. First, by closer cooperation in cyber capacity building with a focus on less cyber-mature countries in the Indo-Pacific. Japan is already working with European countries, Singapore and Australia. Second, deepening cyber intelligence cooperation would allow Japan to join international, coordinated public attributions with stronger-worded statements and possible actions. Third, improved coordination of supply-side security of IT equipment, joint investment in digital infrastructure in developing countries, and lowering the dependency on a small number of IT hardware manufacturers could benefit not only the United States and Japan, but also economic partner countries in the region. And finally, through cybersecurity cooperation beyond the QUAD with European countries based on a lessons-learned approach, Japan would benefit from the specific experience and strength of a larger number of like-minded countries.

[18] 2018. "National Defense Program Guidelines for FY 2019 and Beyond." Ministry of Defense of Japan.https://www.cas.go.jp/jp/siryou/pdf/2019boueikeikaku_e.pdf

[19] Ibid.

[20] 2021. "Minutes of the House of Councilors: Foreign and Defense Committee." House of Councilors of Japan. https://kokkai.ndl.go.jp/#/detail?minId=120413950X01620210603&current=2.

[21] Matsubara, Mihoko. 2018. "How Japan's Pacifist Constitution Shapes Its Approach to Cyberspace." *Council on Foreign Relations*.https://www.cfr.org/blog/how-japans-pacifist-constitution-shapes-its-approach-cyberspace.

[22] 2021. "Cyber Capabilities and National Power: A Net Assessment." International Institute for Strategic Studies.

[23] Julia Voo et al., 2020. "National Cyber Power Index 2020."

[24] 2015. "Joint Statement of the US-Japan Cyber Defense Policy Working Group." *Ministry of Defense of Japan*.https://www.mod.go.jp/j/press/news/2015/05/30a_1.pdf.

[25] 2019. "Joint Statement of the Security Consultative Committee." https://www.mofa.go.jp/mofaj/files/000470738.pdf.

6. The cyber AI nexus: Implications for the US-Japan cybersecurity alliance

By Mark Bryan Manantan

The pulsating beat of the Fourth Industrial Revolution has set the tempo for the new era of strategic competition. The ground is shifting among nation-states, forcing them to adapt and innovate to compete in the new multi-domain environment. With the exponential increase in digital data and more sophisticated computing power, the artificial intelligence (AI) race is on.[1] The renewed interest in advancing AI is expected to precipitate existing security dilemmas in contested spaces like the cyber realm. As a dual-use technology, AI presents both opportunities and challenges for cybersecurity, either as a force multiplier of offensive and defensive cyber operations or as a threat vector itself in the form of adversarial AI.[2] Although the full extent of AI's actual and operational feasibility across military capabilities remains to be explored, its application in cybersecurity has demonstrated improved prospects that could generate further insights. Cybersecurity and AI have a mutually reinforcing relationship. As Whyte and Stevens contend, "you cannot talk about AI without cyberspace. Cyberspace is the fundamental architecture upon which AI technologies or systems are built upon [and] they depend on it."[3] Due to their mutual relationship, AI and cybersecurity could be resilient and vulnerable all at the same time. AI functions are not independent from the technical parameters and normative structures or conflicts that shape behavior in the cyber domain.[4]

As AI-based applications present new challenges and opportunities in the field of cybersecurity, this article aims to examine the implications of their so-called integration, commonly referred to as the "cyber AI nexus" in the context of the US-Japan alliance. While there have been ongoing discussions on improving coordination and synchronization of AI-based military applications *writ-large* in the alliance, an in-depth analysis on the potential impact of cyber AI is still underexplored. To this end, this paper will assess the opportunities, challenges and the prospects of the cyber AI nexus in the context of the US-Japan alliance and its implications for regional security.

Drivers of cooperation

Established architecture of bilateral and multilateral cybersecurity cooperation

There is no question about the highly intricate web of initiatives and channels of cybersecurity cooperation between the US and Japan that cuts across different venues, sectors, and stakeholders. Under their bilateral governmental meetings, the US and Japan have established networks such as the US-Japan Cyber Dialogue led by the Ministry of Foreign Affairs and the Department of State as well as the US-Japan Policy Cooperation Dialogue on the Internet Economy chaired by the Ministry of Internal Affairs and Communications and the US Economic Bureau of State. The US and Japan are also active in key multilateral frameworks that promote international law and cyber norms such as the UN Group of Governmental Experts, the North Atlantic Treaty Organization, and the Association of Southeast Asian Nations (ASEAN).[5] On defense cooperation, the revised *2015 Guidelines for Japan-US Defense Cooperation* envisages the overall cybersecurity coordination between the US' Department of Defense (DOD) and Japan's Ministry of Defense (MOD).[6] The revised guidelines, which include a chapter on outer space and cyberspace, is significant as it emphasizes a reconfiguration of the US-Japan alliance on crucial dimensions such as network vulnerabilities and interoperability, information-sharing and deterrence.

Growing convergence on AI

As mentioned, the *2015 Guidelines for Japan-US Defense Cooperation* laid the groundwork for expanded defense cooperation between the US and Japan. With China's aggressive investments in core technologies, the US and Japan anticipate a dramatic change in the dynamics of the operational environment. With the growing integration of multi-domain capabilities, the successful development and deployment of future military capabilities will be highly contingent on cybersecurity and more so on AI's multiplier effects.

The articulation of policy initiatives centered on seizing AI-based military applications' challenges and opportunities is rapidly gaining traction in the alliance. For instance, during the Joint-High Level Committee on

[1] Cave, Stephen and Sean S. OhEigeartaigh. 2018. "An AI Race for Strategic Advantage." *AIES*. https://dl.acm.org/doi/pdf/10.1145/3278721.3278780.
[2] Taddeo, Mariarosaria, Tom McCutcheon, and Luciano Floridi. 2019. "Trusting artificial intelligence in cybersecurity is a double-edged sword." *Nature*. 557-560. https://doi.org/10.1038/s42256-019-0109-1.
[3] Mavrona, Katerina. 2021. "The AI-cyber nexus: mending defenses, recasting threats." *Science Media Hub*. https://sciencemediahub.eu/2021/07/07/the-ai-cyber-nexus-mending-defences-recasting-threats/.
[4] Ibid.
[5] Wells II, Linton, Motohiro Tsuchiya, and Riley Repko. 2017. "Improving Cybersecurity Cooperation between the Governments of the United States and Japan." *Sasakawa Peace Foundation*. https://spfusa.org/wp-content/uploads/2017/02/Improved-Cybersecurity-cooperation.pdf.
[6] Ibid.

Science and Technology held in 2019, the US and Japan vowed to advance AI and quantum science and technology as two critical future industries.[7] Exploring other avenues for collaboration was also raised through Japan's Moonshot Research and Development Program. In 2020, the US Joint-Artificial Intelligence Committee (JAIC) also held the first-ever AI Partnership for Defense (PFD) that enlisted military and defense forces from 13 nations, including Japan. The two-day dialogue focused on "AI ethical principles for defense, including defining principles and best practices for implementing principles into the AI delivery pipeline."[8] By convening like-minded partners, the PFD endeavored to devise "frameworks and new tools for international data-sharing, cooperative development, and strengthened interoperability."[9]

The China factor

The combination of China's civil-military fusion, science and technology aspirations, ambitious industrial policies, and aggressive foreign policy are all catalytic in bringing the US and Japan's defense, security, and foreign policy priorities into lockstep alignment. At the first US-Japan summit under the Biden-Suga administrations, the two leaders asserted to cooperate across all domains. In their joint statement, Japan will bolster its national defense capabilities for the alliance and the stability of the entire Indo-Pacific. For its part, the US vowed to defend Japan using its full range of capabilities to bolster the umbrella of extended deterrence. Together, both countries will "enhance deterrence and response abilities in line with the increasingly challenging security environment to deepen defense cooperation across all domains, including cyber and space."[10]

In the same vein, deepening collaboration on emerging technologies like AI has also been highlighted as one of the critical areas to advance competitiveness and spur digital connectivity in the region. *Pro-forma* statements aside, the recent summit did not fall short in projecting strength against China. The outcome of the Biden-Suga summit is expected to further boost Japan's defense spending which has already seen a dramatic spike since the Abe administration. For the US, the need for a more sophisticated and targeted approach to push back against Beijing is also imperative to avoid further raising the tension and alienating other partners in the region.

Potential roadblocks to cooperation

Although there seems to be a close alignment between the US and Japan to move forward on cyber AI, a few significant roadblocks persist that may hinder the successful fruition of their cooperation. These realities are not unique to the two countries. However, they still require deeper examination to translate the integration of AI and cybersecurity from mere aspirations to successful use-case applications and operationalization. This section will zero in on the critical areas where crucial gaps, diverging attitudes, and varying priorities between the US and Japan might impede cooperation in cyber AI.

Divergence in cybersecurity outlook and capacity

The *2018 US National Cybersecurity Strategy* lays down the fundamental principles of the US Persistent Engagement Cyber Strategy, putting it on a more offensive stance. Under the banner of a "defend forward imperative," the US Cyber Command will now operate seamlessly and ubiquitously, anytime and everywhere.[11] Despite Japan's notable rise as a cyber power, with increased investments in cyber defenses, and proactive participation on public attribution, it might still be reluctant to fully support the US Persistent Engagement Cyber strategy.[12] Under its pacifist constitution, Japan can only push its cyber strategy towards the seams of cyber defense. Moreover, the Persistent Engagement Cyber Strategy also raises international legal and ethical questions on what constitutes "legitimate cyber operations" in light of possible and unintended adverse effects it may generate within and beyond the networks of Japan.[13]

Wide-margin on AI-maturity

Over the past few years, Japan has made significant

[7] Nurkin, Tate and Ryo Hinata-Yamaguchi. 2020. "Emerging Technologies and the Future of US-Japan Defense Collaboration." *The Atlantic Council*. https://www.atlanticcouncil.org/wp-content/uploads/2020/04/Emerging-Technologies-and-the-Future-of-US-Japan-Defense-Collaboration.pdf.

[8] JAIC Public Affairs. 2020. "JAIC Facilitates First-Ever International AI Dialogue for Defense." *JAIC*. https://www.ai.mil/news_09_16_20-jaic_facilitates_first-ever_international_ai_dialogue_for_defense_.html#:~:text=By%3A%20JAIC%20Public%20Affairs%20%7C%20SEP,defense%20forces%20from%2013%20nations.

[9] Ibid.

[10] 2021."US- Japan Joint Leaders' Statement: 'US – Japan Global Partnership for a New Era." *The White House*.https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/16/u-s-japan-joint-leaders-statement-u-s-japan-global-partnership-for-a-new-era/.

[11] Manantan, Mark. 2021. "The Missing Pieces of the US Cyber Strategy of Persistent Engagement." *The Diplomat*. https://thediplomat.com/2021/04/the-missing-pieces-of-the-us-cyber-strategy-of-persistent-engagement/.

[12] Manantan, Mark. 2021. "Advancing Cyber Diplomacy in the Asia Pacific: Japan and Australia." *Australian Journal of International Affairs. https://www.tandfonline.com/doi/abs/10.1080/10357718.2021.1926423?journalCode=caji20*

[13] Manantan, Mark. 2021. "The Missing Pieces of the US Cyber Strategy of Persistent Engagement."

leaps to advance its footprint in the ongoing global AI race. Japan has been ranked as the world's number one supplier of industrial robots and holds the third spot after the US and China when it comes to AI research and development investments. Similarly, Toshiba Japan is trailing behind IBM and Microsoft based on existing AI patents. Although Japan's investment in AI for commercial applications is accelerating, it still does not have a concrete AI strategy dedicated to defense and security. Compared to the US, Japan's foray into AI application in the military and defense sector is still very much embryonic.

Similar to all major issues relating to the broader context of US-Japan defense capability development, cyber AI could present similar challenges from varying priorities on operational concepts and capability requirements to technology development.[14] But unlike conventional defense technology and military capabilities, the general-purpose nature of AI and cybersecurity presents a unique set of challenges because the bulk of AI development occurs in the commercial sector. The reliance of the defense and military sector on the private sector has real implications for the defense procurement and acquisition process as AI-enabled tools and platforms must undergo reconfigurations before becoming fully functional for defense and military deployment.

Lack or absence of governance structure on AI-ready data.

AI relies on the continuous feed of trusted streams of data. Thus, ensuring the "integrity of data" is essential to building and training reliable AI over time. The US DOD has pointed out it will work only with trusted tech vendors, and this mandate extends to close allies like Japan. This development raises the urgency to establish a shared framework in the alliance to streamline data collection, storage, data preparation, algorithmic training, and application development.[15]

As the role of AI gains momentum in multi-domain operations, the need for reliable data and the protection of AI systems against cyberattacks are all vital towards its successful deployment. In this regard, the secured collection, storage, management, and training of data — which AI and machine learning systems rely on — is crucial and will demand collaboration with trusted private companies, data scientists, and engineers. Such a reality can trigger new challenges on how Japan's MOD can establish or participate in a credible data-sharing framework with the US through trusted third parties. Without a robust infrastructure in place, the alliance cannot be in lockstep towards maximizing information-sharing and analyzing cyber-related threats, and joint-development of AI military applications in multi-domain competition.

Charting the next steps in US-Japan cyber cooperation

The US-Japan alliance serves as the fundamental organizing framework that outlines the underlying motivations upon which the two countries advance their interests and achieve strategic advantage in the evolving technological competition. The previous sections probed the commonalities and asymmetries that may hinder cooperation in the emerging field of cyber AI. Although unsurprising, the distinctions are significant when viewed against the rapid developments made by China and Russia on AI military applications and their increasingly sophisticated cyber capabilities. These rivals provide compelling reasons why the US and Japan should step up their defense-oriented collaboration and cooperation to bridge the existing gaps, identify overlaps, leverage comparative advantages, and anticipate future disruptive effects of cyber AI. This step should take place under the matrix of improved alliance coordination and management. In that case, the paper outlines the following recommendations:

Establishing a cyber AI-focused experts' group built around the current cyber cooperation

The varying outlook of the US and Japan on cybersecurity and AI maturity, strategy, and technological capabilities might constrain the integration of AI-infused cyber capabilities. These distinctions will have a real world impact on developing, disseminating, and testing cyber AI use-cases on US-Japan joint operations, mandating a possible realignment of operational concepts. To remedy this, the existing and relevant levers of cybersecurity cooperation between the US and Japan must prioritize reducing barriers and creating new frameworks that integrate mutually supportive capabilities like AI and cybersecurity. Setting up a joint-technical working group built around the current cyber defense cooperation will allow deeper coordination regarding the on-the-ground implications of cyber AI. Such a step is necessary to find feasible grounds for collaboration and reinforcement between the US and

[14] Rubinstein, Gregg. 2019. "Japan's Future Fighter Program and the US-Japan Alliance: Collaboration or Collision." *Carnegie Endowment for International Peace*. https://carnegieendowment.org/2019/05/22/japan-s-future-fighter-program-and-US-japan-alliance-collaboration-or-collision-pub-79179.

[15] Stanton, Charlotte, Vivien Lung, Nancy (Hanzhuo) Zhang, Minori Ito, Steve Weber, and Katherine Charlet. 2019. "What the Machine Learning Value Chain Means for Geopolitics." *Carnegie Endowment for International Peace*. https://carnegieendowment.org/2019/08/05/what-machine-learning-value-chain-means-for-geopolitics-pub-79631.

Japan, especially as the former goes on the offensive with its Persistent Engagement Strategy.

With Japan's internalization of the defend forward imperative from an operational viewpoint and its impact on legitimate cyber operations, it can better contribute to executing the overall Persistent Engagement Strategy. An improved normative and functional understanding between the US and Japan will tilt the alliance towards a more harmonized approach, facilitating the reassessment of existing markers — indicators of compromise, intrusion detections, malware signatures, and social engineering tricks — and engagements in the context of joint operations, intelligence sharing and capacity building.

Streamlining risk management approach of cyber AI development

As the US and Japan move toward establishing a framework for sharing AI-ready data, the concept of "security by design" will be integral to managing risks.[16] Adopting the 'security by design' approach will help ensure that the training models become more resilient against adversarial AI attacks, model subversion or data poisoning.[17] It provides early warning detection, protection, and remediation of potential vulnerabilities. Mapping out risks at the earliest stage in data collection can ensure the integrity of datasets and as the design process progresses, the robustness of the training models is monitored and guarded. Conversely, third-party and commercial vendors involved in the development or training of AI models must also undergo certification and accreditation to maintain high-quality control standards and due diligence. Such processes will help enforce appropriate security and risk protocols from the research, development, production, acquisition, and delivery to the operations of AI-enabled cybersecurity architecture.

Advancing regional and global consensus on AI standard-setting

The US and Japan are founding members of the Global Partnership on AI built around the Organization for Economic Cooperation and Development Principles on AI.[18] But rather than just building a political coalition of highly-advanced economies or "like-minded states," the process should attempt to genuinely foster inclusivity and transparency to effectively build a fundamental blueprint of AI development. In doing so, the inevitability of divergent systems from countries like China and Russia can be better understood because a fundamental framework exists.

Conclusion

The hype underpinning AI should not overshadow the practical challenges that cybersecurity continues to face. AI can surely automate tasks and augment human resource constraints to produce actionable threat intelligence, for instance. But still intrinsic in the so-called blackbox of cyber AI is maintaining the human in the loop. A hybrid model that leverages the technical advantage of AI/machine learning in cybersecurity combined with human reason and intuition that considers political and social factors would be the better solution to minimize ambiguity, misperception, bias, and even escalation. In addition to pursuing cyber norms and international law which aims to foster responsible state behavior in cyberspace, the US and Japan must seize the opportunity of championing an inclusive international blueprint on AI development to ameliorate the balkanization of the internet that could further exacerbate the ongoing cyber instability.

[16] 2016. "Secure Hardware and Software: Security by Design Working Group 6 – Final Report: Best Practices Recommendations for Hardware and Software Critical to the Security of the Core Communications Network." *Communications Security, Reliability and Interoperability Council.* https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG6_FINAL_%20wAppendix_0316.pdf.

[17] Babuta, Alexander, Marion Oswald, and Ardi Janjeva. 2020. "Artificial Intelligence and UK National Security." *The Royal United Services Institute*. https://rusi.org/explore-our-research/publications/occasional-papers/artificial-intelligence-and-uk-national-security-policy-considerations; Taddeo, Mariarosaria, Tom McCutcheon, and Luciano Floridi. 2019. "Trusting artificial intelligence in cybersecurity is a double-edged sword." *Nature*. 557-560. https://doi.org/10.1038/s42256-019-0109-1.

[18] 2020. "Joint Statement From the Founding Members of the Global Partnership on Artificial Intelligence." US Department of State. https://www.state.gov/joint-statement-from-founding-members-of-the-global-partnership-on-artificial-intelligence/

PACIFIC FORUM
INTERNATIONAL