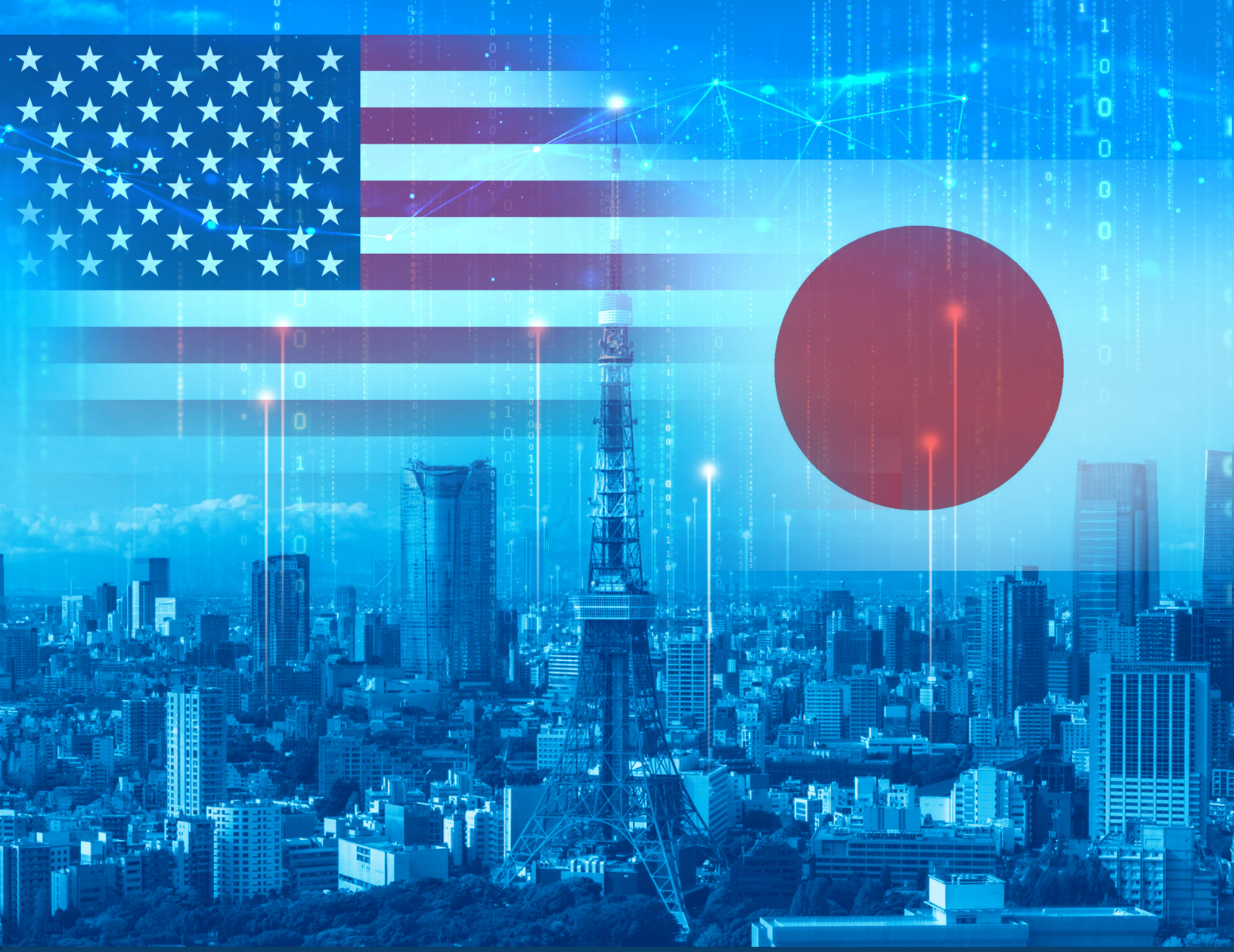

PACIFIC FORUM
INTERNATIONAL

February 2024

US-Japan: Advancing Cybersecurity and Resiliency in the Age of Uncertainty

Mark Bryan Manantan, Editor

Emily Goldman Ph.D. | Mihoko Matsubara | Benjamin Bartlett Ph.D.
Andrew J. Lohn | Mina Takazawa

February 2024

US-Japan: Advancing Cybersecurity and Resiliency in the Age of Uncertainty

Mark Bryan Manantan, Editor

Emily Goldman Ph.D. | Mihoko Matsubara | Benjamin Bartlett Ph.D.
Andrew J. Lohn | Mina Takazawa

PACIFIC FORUM
INTERNATIONAL

About the Pacific Forum

Based in Honolulu, the Pacific Forum 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 cybersecurity and critical technology policy issues, and work to help stimulate cooperative policies through rigorous research, analyses, and dialogue.

Pacific Forum is grateful to the US Embassy in Tokyo for its support to the US-Japan Cyber Forum 2023. We would also like to extend our sincere thanks to Megan Tanaka, Brooke Mizuno, Jesslyn Cheong, Brandt Mabuni, Hanah Park, Munique Tan, Matthew Suh, Kristi Govella, Ph.D., Lami Kim, Ph.D., Crystal Pryor, Ph.D, Akira Igata, Ryo Hinata-Yamaguchi, Ph.D., Hiroki Habuka, Ngor Luong, Carl Baker, and David Santoro, Ph.D.

The Pacific Forum

Web: www.pacforum.org
Facebook: Pacific Forum
Twitter: @PacificForum
Instagram: @pacforum
Podcast: Indo-Pacific Current
Email: pacificforum@pacforum.org

Table of Contents

Executive Summary 7

Introduction and Key Findings 11
Mark Bryan Manantan

Building Collective Cyber Defense and Resilience through Persistence 25
Emily Goldman, Ph.D.

Japan-U.S. Cybersecurity Cooperation to Address Murky Waters in the Indo-Pacific 35
Mihoko Matsubara

U.S. Cyber Diplomacy in Southeast Asia and the Indo-Pacific 43
Benjamin Bartlett, Ph.D.

Artificial Intelligence's Effect on Cyber Security and International Cooperation: Notes for a US-Japan Cyber Forum 51
Andrew J. Lohn

Generative AI's Impact on Cybersecurity and US-Japan Cooperation 59
Mina Takazawa

About the Authors 67

Executive Summary

This report aims to examine the evolving partnership of the US and Japan in cybersecurity amid the unprecedented shifts in the geopolitical environment and the current wave of technological disruptions. Building on the Pacific Forum's previous workshop, "US-Japan Cyber Cooperation: Beyond the Tokyo 2020 Olympics" in 2021, the report addresses the practical dimensions of operationalizing cyber cooperation between Tokyo and Washington DC in three thematic areas: cyber defense, capacity-building, and critical technology.

To obtain cross-cutting perspectives and produce sound and actionable policy insights, the Pacific Forum's Cybersecurity and Critical Technologies program, in partnership with the US Embassy in Tokyo, organized the US-Japan Cyber Forum 2023 in Honolulu, Hawaii that convened key experts and representatives from government, industry, and academia. The closed-door event tackled the following policy challenges: first, identifying the opportunities and challenges of Japan's adoption of active cyber defense and the US cyber strategy of Persistent Engagement; second, establishing trust between the government and the private sector on information-sharing; third, assessing the overlaps and complementarity between the US and Japan in cyber capacity-building to maximize resources that can deliver maximum impact; and finally, adapting to the changing tech landscape in large part due to generative artificial intelligence (AI).

Below are the key recommendations that emerged from the workshop.

Cyber Defense and Resilience

Build converging approaches between Persistent Engagement and active cyber defense to advance collective cyber defense and resilience. Scale up American and Japanese efforts for agile collaboration and continuous pressure against adversarial cyber and cyber-enabled campaigns below the level of armed conflict.

Review and improve existing cyber capacity-building courses to ensure they are fit for the current cyber threat environment. Reduce frictions that harm intelligence-sharing such as sanitizing intelligence to improve intel classification.

Establish a common understanding and approach to addressing cyber threats based on a clear strategy and well-defined set of objectives tailored to mutual interests and availability of resources under specific conditions among states and non-state actors.

Improve existing cyber threat intelligence-sharing between the US and Japan through the creation of interoperable security clearance to process contextual, confidential, and sensitive information that cannot be declassified or sanitized.

Enhance US-Japan law enforcement cooperation on ransomware to hold malicious actors accountable and disrupt operations. Improve sharing of actionable intelligence to help ensure business continuity and minimize domino effects in the commercial sector.

Cyber capacity

Establish a US-Japan cyber capacity-building point of contact to improve coordination. Draw personnel from the US Cybersecurity and Infrastructure Security Agency (CISA) and Japan's National center of Incident Readiness and Strategy for Cybersecurity to ease bureaucratic stove piping and improve the clarity of engagements.

Leverage the US and Japan's comparative advantages in supporting digital infrastructure development combined with the promotion of international technical standards to improve interoperability among emerging economies in Southeast Asia and the Pacific.

Institutionalize the US-Southeast Asia cyber capacity-building cooperation through the ASEAN-US Cyber Dialogue and the ASEAN-US Summit. Recalibrate US cyber diplomatic engagements that fit the operational logic of Persistent Engagement and conduct of Hunt Forward Operations.

Generative AI

Expand the current focus of the US-Japan bilateral cooperation on generative AI beyond security per se and consider its wider implications from economic to social aspects.

Urgently lead policy and technical efforts to streamline responsible AI practices across the generative AI development lifecycle among different sectors and players.

Continue to emphasize policy coherence and regulatory interoperability in laying the groundwork for a global governance approach to AI, building on the Hiroshima AI process. Relatedly, utilize UNESCO and OECD foundational frameworks as cross-references to provide useful insights.

Utilize reinforcement learning to apply and scale up autonomous cyber defenses that can be applied in cyber training environments as supplementary to existing cyber table-top exercises or simulations.

Strive for a pragmatic and balanced approach in reaping the rewards of generative AI for defense while still being mindful of its inherent risks and vulnerabilities.

Introduction

Mark Bryan Manantan

After years of repeated requests to step up its cyber defense, Japan has heeded the call. Tokyo's introduction of active cyber defense has received overwhelming attention following the release of the revised National Security Strategy (NSS) alongside the National Defense Strategy and the Defense Build-up Program in December 2022. As Tokyo adopts a pre-emptive stance on its cyber defense, the implications demand further interrogation.

Over the past decade, Japan has faced an existential dilemma over how to best confront the growing cyber threats emanating from state-sponsored hacking groups based in China, Russia, and North Korea. With its lagging capabilities, the Japanese government has faced intense scrutiny over cyber-attacks that often led to public outcry. Tied to the limitations imposed by its pacificist constitution, Japan has wrestled with the challenge of advancing a sophisticated cyber strategy fit for the changing strategic environment.

China has been a major factor in shaping Japan's strategic calculus; however, Russia's unprovoked invasion of Ukraine fast-tracked the NSS' revision process. Through its reorientation towards active cyber defense, the Japanese Self-Defense Force can eliminate the possibility of serious cyberattacks in advance that may cause national security issues. Even if the cyberattack is not

considered as an armed attack, the JSDF must prevent the spread of possible damages. Japan's active cyber defense will demand greater public-private partnerships on information-sharing and incident response, particularly to protect critical infrastructure. There is also an increasing recognition of the need to update Japan's cyber posture against information warfare.

As the NSS seeks to upgrade JSDF's cyber defenses to be on par with its Western counterparts, the goal is for Japan to become well-positioned in monitoring and attributing cyberattacks and launching countermeasures. Japan's move toward active cyber defense points to a stronger trajectory of US-Japan cybersecurity cooperation. The upgrade is indeed vital to bolster the US-Japan's alliance's capacity to adapt and operate in the multidomain environment.

Coping with the drastic changes in the cyber threat environment in large part due to the Ukraine war and strategic competition with China, the US government also released two important documents: the Department of Defense's 2023 Cyber Strategy and the Biden administration's National Cybersecurity Strategy. Reaffirming the concepts of Defending Forward and Persistent Engagement—aiming to disrupt and degrade malicious actors—the US 2023 Cyber Strategy emphasizes "campaigning" that requires a rapid and continuous operational tempo that is still premised on speed, agility, and actions. While the strategy underscores building the cyber capacity and capability of allies and partners like Japan, little information exists on how that will intersect with US cyber diplomatic engagements.

Under the National Cybersecurity Strategy, the Biden administration shifted the onus of ensuring the cybersecurity protection of critical infrastructure from individuals, organizations, and local governments mainly towards the private sector. Reflecting on cyber incidents like the Colonial Pipeline attack, the Biden administration is moving away from self-regulation to mandatory

imposition of cybersecurity rules. This means that the industry is required to invest more into cybersecurity to prioritize both economic and national security interests.

But like all major strategy and policy pronouncements, successful implementation is the true marker of success. Operationalizing concepts like active cyber defense and campaigning or subscribing to national cyber strategy regulatory guidelines requires the mobilization of adequate government resources and the provision of incentive mechanisms. Success will necessitate effective collaboration built on trusted networks and nodes comprising key stakeholders from government, industry, academia, and civil society. At the very core of public-private partnership, trust between the government and the private sector remains the fundamental ingredient to guarantee cooperation and compliance.

Recognizing that cybersecurity is a cross-cutting issue, it is critical to assess how the recent developments in the US and Japan's cyber policies and strategies intersect with their respective cyber diplomatic engagements. Questions also loom surrounding the disruptive effects of generative AI, especially on information warfare given the heightened geopolitical competition with China and Russia.

Going beyond providing key updates on US-Japan cyber cooperation, this report intends to inform the current cyber and tech policy debates within and beyond the US-Japan alliance. The fundamental goal is to dive deeper into the operational merits of recent developments in the US and Japan concerning cyber and critical technologies. The insights generated from this report will provide a deeper understanding to address the myriad of practical issues that complicate the US-Japan cybersecurity cooperation and identify the implications for the broader Indo-Pacific region.

The US–Japan Cyber Forum

Building on the successful outcomes of the US-Japan Cyber Cooperation: Beyond the Tokyo 2020 Olympics workshop, the Pacific Forum has organized the US-Japan Cyber Forum 2023 in Honolulu, Hawaii, held with support from the US Embassy in Tokyo. Oriented around three thematic areas–cyber defense, cyber diplomacy, and critical technology–the closed-door event brought together experts and practitioners to take stock of the sweeping changes in the US and Japan's cyber strategies and policies amid China's increasing technological influence, fraying regional security, and the disruptive effects of generative AI. Adopting a multi-stakeholder approach, the strategic workshop was guided by the following objectives:

Unpack conceptual and often nebulous concepts like active cyber defense and Persistent Engagement and what they mean in practical or concrete terms.

Identify the overlaps and complementarity in capacity-building initiatives to maximize resource allocation and sustain policy attention.

Obtain in-depth perspectives from the private sector to secure initial buy-in, and hopefully, cement trust to ensure open, transparent, and productive collaboration.

Assess the opportunities and challenges of generative AI in the context of US-Japan cybersecurity cooperation.

Key findings of the workshop are outlined in the succeeding pages, accompanied by five policy briefs that further dissect the critical issues in cybersecurity and generative AI that emerged from the workshop. Each policy brief provides actionable policy recommendations for consideration by policymakers.

Setting the stage, Dr. Emily Goldman dove deeper into the conceptual and practical approaches of the US cyber strategy of Persistent Engagement. She demystifies what Persistent Engagement is and what it is not and assesses its potential convergence with Japan's active cyber defense to advance collective resilience through persistence. However, to achieve operational alignment, Dr. Goldman recommends bolstering capacity-building.

Mihoko Matsubara builds on Dr. Goldman's call for collective resilience. She puts forward practical and growing niche areas of cybersecurity collaboration such as ransomware, critical infrastructure protection, and cyber threat intelligence. Drawing key lessons from the Ukraine war, Ms. Matsubara emphasizes the importance of improving interoperability in cyber threat intelligence in the event of any cross-strait contingency. She also explores the benefits of interoperable security clearance between Japan and the US to further improve information-sharing.

Fusing cyber diplomacy and cyber defense, Benjamin Bartlett, Ph.D., injects new perspectives to revitalize US cyber diplomatic engagements that are akin to the new strategy of Persistent Engagement. As the US continues to refine its cyber diplomatic toolkit, Dr. Bartlett encourages US policymakers to consult and coordinate with Japan due to the latter's more institutionalized cyber capacity engagements in the region. Undertaking such an approach will assist the US and Japan in investing resources more wisely and cultivating a complementary approach to capacity-building.

Andrew Lohn cautions experts and policymakers on the overstatement and/or misplacement of risks linked to the current boom of generative AI (Gen AI) in cybersecurity. What follows is an elaborate discussion of large language models' cyber effects that include disinformation, malware generation, and hacking. Certainly, AI will amplify the scale and scope of cyber threats,

but AI will also boost cyber defense and resiliency. He suggests reinforcement learning as a technical approach to fortify US-Japan cyber defenses.

Analyzing the regulatory dimension of Gen AI, Mina Takazawa underscores the urgency to develop AI guardrails. As regulations continue to play catch-up with the rapid changes brought by innovation, the US and Japan must lead the application of AI best practices throughout the Gen AI development life cycle. To steer regional and multilateral discussions, Ms. Takazawa urges the US and Japan to complement existing efforts on AI governance in multilateral settings.

Ideally, the workshop's key findings and policy briefs provide useful insights to pave the way for practical collaboration. Although the bilateral relationship continues to endure, Tokyo and Washington are at a crossroads. Japanese and American policymakers are encouraged to reimagine what the alliance should look like in the current era of geopolitical competition and growing influence of global Information and Communications Technology (ICT) companies.

As the US and Japan face mounting pressure to deliver on their promises of achieving a Free and Open Indo-Pacific, their engagements should be coordinated in a strategic fashion to maximize finite resources and utilize their comparative advantages. Certainly, the US can reflect and learn from Japan's sustained engagement in the Indo-Pacific, specifically in Southeast Asia. Considered as the region's most-trusted partner, Japan is well-positioned to buffer against China's growing influence and assertiveness. Japan's subtle diplomacy combined with consistent economic investments, and capacity-building intiiatives in Southeast Asia should inspire the US' calibrated response to reinvigorate its image as the region's security and economic partner of choice.

Despite progress made in the past, now is the moment for Tokyo and Washington D.C., to break free from decades-long path dependence that may have resulted in bureaucratic inertia. Operationalizing resilience at the heart of cyber cooperation requires a comprehensive and balanced approach to cyber defense, cyber diplomacy, and the development of critical technologies. This will enhance and improve coordination and adaptation to possible systemic risks caused by geostrategic and technological factors. Conversely, policymakers must continously evaluate and adjust their engagements for trust and partnership-building among key stakeholders in the public and the private sector. As the US and Japan continue to recalibrate their approaches to cybersecurity cooperation, the policy recommendations provided in this report should turbocharge a more resilient US-Japan alliance based on clear objectives that realize concrete outcomes.

Key Findings

Operationalizing Active Cyber Defense and Persistent Engagement

Operationalizing active cyber defense or Persistent Engagement will require robust information-sharing, particularly in understanding the capabilities of adversaries in exploiting vulnerabilities and/or launching cyberattacks. But to gain a comprehensive picture of the threat landscape, the private sector buy-in is a given, not an option. Given its global access to data, the private sector is invaluable to threat detection and intelligence-sharing.

Defending forward entails actions to disrupt, preclude, or constrain the adversary. Its underlying logic is that if one is still defending within the perimeter, that already equates to strategic loss. Over time, the cumulative effects of strategic losses in cyberspace can be as impactful as loss in conventional kinetic warfare. Therefore, in additon to incident response after an attack, proactively exposing and contesting adversaries' actions must be part of a holistic approach to securing in and through cyberspace.

Legal questions relating to the extent and scope of Persistent Engagement remain especially from the viewpoint of the private sector. From the US government's perspective, cyberattacks should no longer be viewed as incident-specific but as a

continuous pattern of malicious activities that incur cumulative damages in the long run. If there is a clear case that demonstrates present harm and danger, the government must always move in accordance with international law.

Similarly, Japan's active cyber defense has yet to circumvent important legal hurdles from its pacifist constitution that grants protection to the secrecy and privacy to communications. It is also expected that any remit to integrate offensive cyber capabilities in JSDF's toolkit will face political, legal, and normative challenges to becoming operational.

Fundamentally, the prevailing lack of consensus on sovereignty in the cyber domain continues to be a fundamental challenge among US allies and partners, which, consequently, impacts the operational parameters of cybersecurity cooperation. For instance, without a clear and consistent declaratory policy on sovereignty, conducting joint-cyber missions like threat hunting or threat intelligence information-sharing will remain limited.

While foundational challenges relating to sovereignty and international law persist, the US and Japan still have opportunities to improve cyber cooperation in practical areas. Understanding the organizational culture, methodologies, resource constraints, and risk factors between the public and the private sector players is a critical starting point. Establishing a baseline to achieve closer alignment will help reinforce trust and operational efficiency among allies and partners and reduce friction.

With the increasing shift towards multidomain operations, baselining will be very important to identify the add-on value of cyber capabilities. The alignment will facilitate threat information sharing and threat hunting in real-time, especially in the event of a high-impact conflict in the Korean peninsula, the East or South China Seas, and/or Taiwan.

Achieving Synergy in International Cyber Diplomacy Engagements

The US track record in cyber diplomacy is pixelated. This is highly evident with Washington's engagement in Southeast Asia and, to some extent, the Pacific Island countries. After two decades of preoccupation in the Middle East due to the War on Terror, the US has renewed its attention toward Southeast Asia, driven in large part by China's growing influence within the region. Although the US cyber capacity-building has begun to gain momentum, it still lacks formal institutionalization. The US lack of trust among allies outside the Five Eyes also hamstrings its cyber cooperation, especially on information-sharing.

Compared to the US, Japan has more sustained if not elevated cyber capacity engagements in Southeast Asia with regards to cyber capacity-building. In celebration of Japan-ASEAN's 50th anniversary in 2023, joint cyber-capacity building remains a top priority. Japan's approach to China resonates among countries in Southeast Asia. Instead of just frontloading a very hardline anti-China sentiment, it has utilized its limited resources to gain Southeast Asia's trust and confidence through the provision of public goods, investments, and capacity-building.

Providing feasible alternatives to Chinese technologies in critical areas like fifth-generation wireless technology or 5G continues to remain a key challenge for the US and Japan in Southeast Asia. In addition to infrastructural development, the increasing presence of Huawei, Alibaba, Tencent, etc. is also facilitating capacity-building knowledge and tech transfer in the region.

To compete, the US and Japan have been advocating for an Open Radio Access Network. Also worth noting is the expansion of Starlink as a viable choice for Southeast Asia to augment the region's digital connectivity gaps and reduce its reliance on China.

With Japan's reputation as a trusted partner in the region, it would be strategic for Tokyo to take the lead while Washington provides complementary support.

Japan is well-positioned to persuade Southeast Asia on the strategic imperatives of cybersecurity. Here, the US and Japan can build on existing cyber capacity-building initiatives to tackle emerging policy issues in ASEAN like supply chain resilience, data flow, and digital infrastructure like cloud and undersea cables.

Partnerships among close and like-minded allies like South Korea and NATO could also help the provision of digital public goods and cyber capacity-building. The renewal of Japan-South Korea relations offers optimism for greater information-sharing. Relatedly, regional diplomatic platforms like the QUAD continue to support the application of international technical standards and cybersecurity risk-management frameworks.

As American and Japanese policymakers intend to expand the scope and breadth of their cyber diplomatic engagements, prioritization will be key. This will involve greater consultation to avoid duplication of efforts, resulting in careful planning, improved allocation of finite resources, and consistent policy attention.

Expectations of private sector involvement in cyber capacity should be carefully managed. Major Information and Communications Technology firms that have a global presence like Microsoft may be willing to building capacity and promoting norms. However, small and medium enterprises may be less interested due to perceived costs. Providing incentives to improve capacity will help narrow the gap. As part of their corporate social responsibility, large corporations can opt to assist small and medium-sized businesses in establishing cybersecurity guidelines.

Prioritization will also involve putting in place adequate resources in anticipation of future crises. Lessons learned from Russia's invasion of Ukraine showed that pursuing proactive rather than reactive measures carry immense benefits in the event of full-blown cyber warfare. Adopting such an anticipatory approach allowed Ukrainians to harden cyber defenses and fortify information-sharing in a timely and strategic fashion even prior to Russia's invasion.

Considering the volatility of the geostrategic environment, the US and Japan's strategic planning should begin to consider possible hotspots where cyber warfare could erupt. This can include Taiwan, China, Singapore, Guam, Hawaii, Indonesia, the Philippines, Southeast Asia, the Baltics, and Latin America.

Unpacking the Implications of Generative AI on Cybersecurity

Generative AI (Gen AI) will usher in new forms of vulnerabilities like malware and social engineering tactics as well as the proliferation of deepfakes. Such breakthroughs have the potential to erode trust among societies. Strategic competitors can leverage Gen AI to conduct surveillance and use deepfakes for disinformation campaigns.

Apart from driving innovation, states are also competing with the private sector in setting AI guardrails. Silicon Valley-based companies like Microsoft, Google, Apple, Meta, and Amazon are actively integrating and exploring generative AI in their respective business models while also setting the global agenda on AI governance. In such a dynamic, advancing innovation while establishing regulatory coherence will be a major challenge. It raises a host of issues from interoperability to security that will shape the development of AI-enabled technologies, with military and non-military applications.

In addition to developing advanced data-driven analytics and machine-learning models, semiconductors are taking center stage in the current Gen AI race. NVIDIA and Taiwan Semiconductor Company are investing heavily in research and development and setting up factories in the US, Asia, and Europe to develop the next generation of AI chips. While they could benefit from the subsidies from the CHIPS and Science Act, semiconductor companies have yet to find a feasible solution to buffer the impact of the US and Japan's evolving export control regulations.

With the current Gen AI boom, job displacement will be a critical issue for the US and Japan. To remain competitive, there is an urgent need to review and revise educational curriculums fit for the digital economic era. As Gen AI paves the way toward general-purpose AI, social science will be critical in redefining human-machine interaction. Rather than focusing on narrow skill sets skewed toward Science, Technology, Engineering, and Mathematics, arts and humanities will play an important role in producing a well-rounded workforce and professionals that are analytical and adaptative but also creative.

Building Collective Cyber Defense and Resilience through Persistence

Emily Goldman, Ph.D.

Cyber Realities and Strategic Convergence

Most malign state-sponsored cyber behavior consists of non-violent operations below the level of armed conflict. When translated into coherent campaigns, their potential and purpose is to gain or sustain a strategic advantage or to erode an opponent's sources and instruments of national power. In some cases, this activity performs double duty by helping to set conditions for a state or coalition to prevail in a future militarized crisis or armed conflict.

Such operations and campaigns have shaped the evolving US strategic approach to this cyberspace reality. In 2018, spurred by past strategic losses, a series of policy and legal changes empowered US cyber military forces to operate with greater latitude and push back against cyberspace aggression below armed conflict. Between 2018 and 2022, experience gained through operating in day-to-day competition matured the US thought and practice, and these ideas gained traction in the US and abroad. The run-up to Russia's invasion of Ukraine in late 2021 continued

maturing US thought, and practice based on the insight that successful contingency operations begin with cyber campaigning in competition.

Throughout this evolution, the role of allies and partners has proven to be essential. The challenge for the US and its democratic allies and partners now is to bring their tools, insights, and experience to bear in a coordinated and collective fashion that thwarts the strategically impactful activity of rival states below armed conflict and that sets conditions to deter and prevail should a crisis or armed conflict arise. Collective efforts require a healthy appreciation for distinct state approaches, shaped as they naturally are by domestic politics, national legal systems, cultural attitudes, geopolitical situations, and interpretations of international law. These differences exist within a common reality: cyberspace is an interconnected and contested strategic environment, which allows continuous exploitation of vulnerabilities for cumulative advantage. This common context is fostering a convergence in perspective between the US and its partners—however incrementally—toward operating proactively and persistently.[1]

Origins and Evolution of the US Approach

The technologies of global networked computing and ubiquitous access that underpin the cyber strategic environment create a structural interconnectedness that places friends and foes in a condition of constant contact.[2] Cyberspace is at once micro-vulnerable (or inherently vulnerable to exploitation) and macro-resilient (or systemically stable). Together these qualities of cyberspace allow aggressive regimes and actors to continuously exploit opportunities made available through interconnectedness. There is always some entity somewhere seeking to exploit cyber vulnerabilities to gain advantage. Cumulatively those gains can rise to a level that is strategically consequential. All this

activity occurs without the threat or use of kinetic capabilities. Cyberspace enables winning without coercing or fighting.

The US policy community recognized how cyberspace campaigns below armed conflict were cumulatively leading to strategic losses for the nation. That realization has increased with time. Theft of intellectual property at scale has degraded competitive advantage and economic power. Theft of military R&D and (more recently) supply chain disruption and manipulation threaten US military advantage. Cyber-enabled information and influence operations eroded US political influence by undermining social cohesion and alliance solidarity, delegitimizing democratic institutions, and casting doubt on election outcomes.

A doctrine of self-restraint, coupled with the threat to respond once attacked (e.g., deterrence) was not working. Most adversary activity ensued unchallenged because discrete incidents rarely rise to a level that warrants a timely response. As a result, adversaries are further emboldened to operate with near-impunity, reaping the cumulative gains of their cyber aggression.

The US approach to cyberspace is shaped by domestic politics and operational experience. 2018 was a watershed year. The US Department of Defense published its Defend Forward strategy.[3] Commander ADM Mike Rogers signed the US Cyber Command Vision, Achieve and Maintain Cyberspace Superiority, introducing the concept of Persistent Engagement.[4] The 2019 National Defense Authorization Act defined operations in cyberspace as a traditional military activity exempt from the approval and oversight procedures applicable to covert actions. Finally, a new Presidential policy delegated more authorities to DOD for cyberspace operations. A new operational approach for military cyberspace forces coupled with the legal authorities and political guidance to implement that approach was in place.

Both Defend Forward and Persistent Engagement aligned security efforts to the nature of the cyberspace strategic environment by complementing the deterrence of significant cyberattacks with persistence and resilience in the face of cyberspace campaigns short of armed conflict. Persistent Engagement addresses the mismatch between threat and response with a set of principles and operating concepts that guide how US Cyber Command employs its forces in competition, crisis, and armed conflict. Persistent Engagement emphasizes competing with adversaries now, continuously, and proactively; enabling domestic and foreign partners; and acting in and through cyberspace to seize and maintain initiative across the competition continuum.

At its core, Persistent Engagement means continuously seeking initiative to set the conditions of security and the terms of competition in one's favor; anticipating what vulnerabilities competitors plan to exploit and how they may do so; and adapting before they can be weaponized or exploited, rather than reacting to what has occurred. Rather than waiting for something to happen, the Command is always operating outside the United States to identify adversary tools, hackers, infrastructure, and malware. A key element in this approach is sharing information, tradecraft, signatures, and indicators with the private sector to scale cybersecurity efforts.

Persistent Engagement also broadens the aperture from wartime planning and execution to include confronting continuous, widespread adversary cyberspace campaigns calibrated to remain below the level of armed conflict, yet which cumulatively result in strategic gains. The purpose is not to deter malicious cyber activity (because in cyberspace there is a structural imperative to act), but to render the opponent unable to succeed.

As military cyberspace forces began operating with greater latitude, insights from operational experience suggested the Command was on the right track with its pivot from a "response" force to a "persistence" force. New ideas were first put to the test as part of the USG's efforts to protect the 2018 midterm elections from Russian interference and influence. These operations showed that the US could defend elections and disrupt cyber activities aimed at interfering with them without causing escalation to armed conflict. Operations included cyber effects disrupting Russian actors' use of cyber capabilities to undermine the elections. For the first time, defensive cyber teams were sent abroad (with host country permission) to hunt for adversary activity on foreign networks that could harm the US homeland. By going where adversaries were operating, cyber teams discovered new activity, alerted foreign partners and helped secure their networks, and shared information directly with industry so they could develop mitigations.

Subsequent "hunt forward" missions matured doctrine in unanticipated ways. Initiated in support of the broad, interagency effort to defend elections against foreign interference and influence, these intelligence-driven, partner-requested operations illuminated what malicious cyber actors are doing globally. Insights shared with domestic and foreign partners to harden infrastructure increased operational costs for adversaries by exposing their activities and tools—taking time, money, and access away from them. These missions have grown in importance and impact – enabling new cybersecurity partnerships, increasing infrastructure resiliency, and gaining new insights. When cyber forces hunt forward on partner networks at home and abroad, tip industry, publicize malign activity, and expose malware, they preclude options, reduce attack vectors, and deny terrain to malicious actors. They also assure allies and partners; build and strengthen partnerships; and bolster defense of critical US, allied and partner networks.

Operations in support of US national security objectives in Ukraine have advanced understanding of the role of cyberspace capabilities in crisis and conflict. Successful contingency operations begin with persistent engagement--or in the language of the US 2022 National Defense Strategy, "campaigning"--in competition.[5] Campaigning generates insights, opportunities, and options to constrain adversary freedom of maneuver and deny them leverage in crisis and conflict. Experience also revealed the power of information exposure and the vital need to secure partner networks for intelligence sharing before a crisis. Campaigning now and continuously in and through cyberspace can thus reduce strategic loss in competition and set conditions to deter and prevail in crisis and conflict.

Experience is further helping the Command articulate the value proposition of cyberspace operational activities. Conventional military assessment methodology evaluates success and failure in terms of whether cyber operations produce independent decisive results in conflict, as a substitute for kinetic effects. Operations and activities in support of US government goals in the Russia-Ukraine conflict, however, revealed how the value of cyberspace activities and operations is more usefully understood in terms of cumulative impact on the adversary and enduring advantage for the US and its coalition partners. Impact need not be immediate. Time is a critical variable and cyber activities and operations can be a corrosive accelerant through cumulative impact over time. In the context of an adversary pursuing an attrition doctrine, persistent erosion of trust, efficiency, and capability matters. Linked through campaigning, even small changes can have an amplified impact on who holds the initiative.

Military cyber operations and campaigns typically also include a range of activities that enable interagency partner objectives and activities and advance broader strategic goals of the nation. For instance, they enable demarches, amplify sanctions, inform Rewards for Justice (a US Department of

State program that offers rewards for information that protects American lives and furthers US national security objectives), and facilitate indictments and arrests. The default assessment of cyber value in terms of independent decisive strategic outcomes in conflict is deceptive because it equates strategic decisiveness and strategic utility. Cyber operations and campaigns may not be independently strategically decisive in conflict, but they have strategic utility when they contribute directly or indirectly to outcomes. Treating cyber capabilities as independent from (or as substitute for) conventional capabilities in conflict and crisis may be intellectually interesting but operationally and strategically immaterial. Cyber strategic utility rests in proactive use in competition to stabilize and advance interests, while simultaneously setting conditions for management of potential crisis or conflict in the future.

US–Japan Partnership Opportunities

Working with allies and partners is a key element in US defense, military, and cyber strategies. The Department of Defense recognizes that the United States' global network of allies and partners represents a foundational advantage in the cyber domain that must be protected and reinforced.[6] States have different methodologies, risk appetites, legal interpretations, approval processes, and timelines. These can complicate collective efforts if not recognized and accounted for. An attainable goal is to achieve complementary proactive strategies aligned with states' opportunities and constraints. This means focusing first on where there is overlap and alignment. For the US and Japan, there appears to be a common understanding of the cyber strategic environment and the adoption of a persistent, campaigning mindset.

Japan's National Security Strategy (December 2022) and National Defense Strategy (December 16, 2022) independently endorsed "active cyber defense" to eliminate "in advance the possibility of serious cyberattacks that may cause national security

concerns…". Active cyber defense calls for closer collaboration with the private sector to share information and detect malicious behavior. Implementation requires legislative changes to expand authorities and capabilities to detect, penetrate, and then disrupt or neutralize malicious activity in advance—to include the authority to "penetrate and neutralize attacker's servers and others in advance to the extent possible."[7] Under current laws, such measures may be triggered only after an emergency or military attack. Under active defense, the roles and missions of the military establishment would expand, although whether that aligns with the US Defend Forward strategy remains to be seen. Active cyber defense represents a shift toward a more proactive and anticipatory approach to the realities of cyberspace.[8] As such, it aligns with the underlying logic of Persistent Engagement.[9]

The US and Japan can build upon their converging approaches to advance collective cyber defense and resilience through persistence. Adapting the roles and missions of military cyber forces allows both states to scale up their whole of nation efforts for agile collaboration and continuous pressure against adversary cyber and cyber-enabled campaigns below armed conflict.

Several avenues for further development seem promising. First, "cybersecurity foundations" development focuses on capacity building to better secure, operate, and defend networks. Second, securing networks for information and intelligence sharing is critical to enable common defense and interoperability. These efforts must precede crisis and conflict to fortify mission partner environments and set the conditions for successful contingency operations. They are prerequisites for "cyberspace operations" development with its focus on combined cyber campaigns. Finally, steps that reduce obstacles to partnership should be pursued wherever possible, such as sanitizing intelligence and lowering classifications to enable sharing.

Above all, proactively looking for and contesting threats requires trust and common understanding within and across governments, societies, and states. The wider embrace of Persistent Engagement-like approaches, tailored to respective interests, conditions, and authorities of states is a positive step toward increasing the scale, initiative, and strategic coherence needed to compete against an ambitious well-resourced adversary with a clear strategy and well-defined end-state.

The views expressed in this article are those of the author and do not reflect official positions of the Department of Defense or any U.S. government entity.

[1] Richard J. Harknett, Michael P. Fischerkeller, Emily O. Goldman, "U.K. National Cyber Force, Responsible Cyber Power, and Cyber Persistence Theory" (April 5, 2023), https://www.lawfaremedia.org/article/uk-national-cyber-force-responsible-cyber-power-and-cyber-persistence-theory; Alexander Martin, "NATO's Christian-Marc Lifländer on how the alliance can take a 'proactive' cyber stance," The Record (July 10, 2023), https://therecord.media/christian-marc-liflander-on-nato-cyber-defense.
[2] Michael P. Fischerkeller, Emily O. Goldman and Richard J. Harknett, Cyber Persistence Theory: Redefining National Security in Cyberspace (Oxford University Press, 2022).
[3] Department of Defense Cyber Strategy Summary (2018), https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.
[4] Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command (2018) https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf.
[5] National Defense Strategy of the United States of America (2022) https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF
[6] Fact Sheet: 2023 DoD Cyber Strategy, https://media.defense.gov/2023/May/26/2003231006/-1/-1/1/2023-DOD-CYBER-STRATEGY-FACT-SHEET.PDF
[7] National Security Strategy of Japan (December 2022), provisional translation, pp. 23-24.
[8] https://asia.nikkei.com/Politics/Japan-to-upgrade-cyber-defense-allowing-preemptive-measures; https://www.dragonflyintelligence.com/news/japan-shift-to-a-more-offensive-cyber-posture-in-2023/; Tokuchi Hideshi, "Japan's New National Security Strategy and Contribution to a Networked Regional Security Architecture," CSIS (June 23, 2023), https://www.csis.org/analysis/japans-new-national-security-strategy-and-contribution-networked-regional-security.
[9] Under US doctrine, Persistent Engagement is more than active cyber defense in terms of its traditional use in DOD and IT circles. Active cyber defense in the US is limited to activity on one's own networks, and directly managing contested areas. Persistent Engagement rests on initiative and the anticipatory setting and resetting of conditions across the entire digital space.

Japan-U.S. Cybersecurity Cooperation to Address Murky Waters in the Indo-Pacific

Mihoko Matsubara

Cybersecurity cooperation has become more important than ever in Japan and the United States from the perspective of economic and national security. The two allies share concerns over cyber espionage and sabotage. Cyber espionage sometimes can be a precursor to destruction or disruption to steal information. As the world has become more reliant on information and communication technologies (ICTs), cybersecurity is now crucial not only for economic prosperity but also for international security. Japan and the US have shown strong resolve to fortify their cybersecurity cooperation with key initiatives on the horizon—ransomware, critical infrastructure protection, and cyber threat intelligence—to cope with the changing cyber threat landscape.

Ransomware Initiative

The ransomware attack on Colonial Pipeline in May 2021 was a wake-up call to policymakers that a financially motivated criminal group can disrupt economic or national security with a supply chain attack on a single organization. The U.S. major energy firm ended up suspending its fuel supplies for six days[10].

In July 2023, the Port of Nagoya—the largest cargo throughput in Japan—was hit with a ransomware attack, that interrupted its shipping operations for almost two days. The incident also forced Toyota Motor to stop its shipments of auto parts at four distribution centers for one day.[11] Despite this, the Port of Nagoya quickly restored its data and restarted its business operations in only two days. This is a major feat considering that the average downtime of ransomware attacks is 25 days.[12] Nevertheless, the increasing frequency of such cyberattacks further stressed the importance of cyber resilience in ensuring business continuity and minimizing domino effects given the high interdependence in the commercial sector.

In response to the alarming disruptions caused by major cyberattacks, the U.S. government convened virtually the Counter Ransomware Initiative meeting involving 30 allies and like-minded countries including Japan in October 2021.[13] From October 2022 to November 2022, the group met in person to tackle collective resilience and disrupt ransomware operations.[14]

Japan has already started to contribute to this international effort by sharing actionable intelligence. In May 2023, the U.S. Department of Justice highlighted the Japanese National Police Agency's valuable assistance that led to the two indictments of Mikhail Pavlovich Matveev, a Russian national, who conducted ransomware attacks against critical infrastructure in the United States.[15] While the detailed nature of cooperation was not provided due in large part to maintaining the confidentiality of future criminal investigation and intelligence collection, this indictment

showcases the importance of closer Japan-U.S. law-enforcement cooperation on ransomware to hold perpetrators accountable and disrupt their operations.

Critical Infrastructure Protection

The resiliency and protection of critical infrastructure are essential for security and stability, in the Indo-Pacific region, especially given the rising attention to a potential crisis in the Taiwan Strait.[16] Recent cyber threats may point to an ever-increasing likelihood of a cross-strait contingency.

In May 2023, Microsoft warned that since mid-2021, "a state-sponsored actor based in China" had been targeting "critical infrastructure organizations in Guam and elsewhere in the United States," particularly communications and utility. The global ICT firm suspects that the end goal of the cyber espionage campaign is likely to "disrupt critical communications infrastructure between the United States and Asia region during future crises."[17] Obviously, as a major U.S. air base and port, Guam will play an important role in the US military operations during a potential Taiwan crisis.[18] As of July 2023, the U.S. government is reportedly involved in threat-hunting operations for China-made malware within its networks of communications, electric power, and water supplies to support military bases within and outside the United States. It is believed that the malware could delay the deployments of the U.S. Forces in the case of contingency.[19]

Threat-hunting operations are designed to proactively look for potential breaches and delete adversary's foothold in networks, minimize cyberattack damages, and beef up organizational resilience. But governments cannot do it alone. International public-private partnerships are vital to effectively search and counter an adversary's virtual footsteps in critical infrastructure networks based on shared cyber threat intelligence. Japan and the United States have been sharing cyber threat intelligence and

cybersecurity best practices to protect critical infrastructure sectors such as electricity[20], finance[21], and information technology.[22]

Recent developments in Japan's cyber policy landscape might further increase its current scope of collaboration with the United States. In December 2022, Japan released the National Defense Strategy, declaring that the Ministry of Defense and Self-Defense Forces (SDF) would begin to "support cybersecurity entities other than the SDF" by JFY 2027,[23] despite not being the mandate of the SDF Law. The new Defense Buildup Program will also support the SDF's potential pursuit of capabilities to conduct threat hunting.[24]

In addition, interoperable security clearance is key to further enhancing cyber threat intelligence-sharing efforts because some intelligence can be obtained only by the government and certain intelligence such as context information cannot be declassified or sanitized. If implemented, this will benefit the existing arrangements between the Japanese and US governments and critical infrastructure companies. In June 2023, Japanese Economic Security Minister Sanae Takaichi expressed her interest in submitting a bill to expand security clearance that is similar to the US and European systems to advance economic security in 2024.[25]

Without the interoperable security clearance, it would be challenging for Japan, the United States, and partner countries to fuse different intelligence feeds, obtain a clearer shared picture of the cyber threat landscape, and minimize potential damages in a timely manner. Understandably, it takes time and resources to establish a security clearance system that spans governing mechanisms, technology, and sensitive compartmented information facilities (SCIFs) to collect, analyze, process, and disseminate intelligence feeds.

Cyber threat-intelligence-sharing

In parallel with establishing the security clearance system, Japan would need to create a platform to quickly share cyber threat intelligence among the community of cyber defenders who do not necessarily hold a security clearance. Japan may consider lessons learned from the U.S. Cybersecurity and Infrastructure Security Agency's Shields Up campaign website. Launched a few days prior to Russia's invasion of Ukraine in February 2022, the online portal issues warnings to industry leaders as well as critical infrastructure defenders regarding the latest cyber threats and mitigation measures.[26]

Should the Japanese government create a similar resource, it will bring valuable insights to government policymakers and industry representatives in Japan, the United States, as well as like-minded countries. Strategically, the information shared and obtained may help improve coordination given the high stakes of contingency in the region. Operationally, the online platform will be also essential to ensure the continued provision of cyber intelligence feeds in a timely fashion.[27]

Conclusion

Evidently, Japan and the United States have made concrete progress in cybersecurity cooperation over the past year with international efforts like Counter Ransomware Initiative. However, the two allies must now shift their focus towards a potential regional crisis. Collective resilience will become even more important. With the Japanese National Security Strategy allowing for threat hunting in critical infrastructure, Japan, and the United States will be able to pursue more. An expanded cyber threat intelligence arrangement can also be the next step to process unclassified and classified information to mitigate threat collaboration, especially as companies are increasingly under cyberattack.

[10] Mary Louise Kelly, Jason Fuller, and Justine Kenin, "The Colonial Pipeline CEO Explains The Decision To Pay Hackers A $4.4 Million Ransom," NPR, June 3, 2021, https://www.npr.org/2021/06/03/1003020300/colonial-pipeline-ceo-explains-the-decision-to-pay-hackers-4-4-million-ransom.
[11] Apurva Venkat, "Japan's Nagoya port resumes operations after ransomware attack," CSO Online, July 6, 2023, https://www.csoonline.com/article/644765/japans-nagoya-port-resumes-operations-after-ransomware-attack.html.
[12] Coveware, "Uber Verdict Raises New Risks for Ransom Payments," October 26, 2022, https://www.coveware.com/blog/2022/10/26/q3-2022-quarterly-report.
[13] The White House, "Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting October 2021," October 14, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/.
[14] The White House, "International Counter Ransomware Initiative 2022 Joint Statement," November 1, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/international-counter-ransomware-initiative-2022-joint-statement/.
[15] U.S. Department of Justice, "Press Release: Russian National Charged with Ransomware Attacks Against Critical Infrastructure," May 16, 2023, https://www.justice.gov/opa/pr/russian-national-charged-ransomware-attacks-against-critical-infrastructure.
[16] Alex Willemyns, "CIA director: China readying for Taiwan invasion by 2027," Radio Free Asia, February 3, 2023, https://www.rfa.org/english/news/china/cia-taiwan-invasion-02032023160341.html.
[17] Microsoft, "Volt Typhoon targets US critical infrastructure with living-off-the-land techniques," May 24, 2023, https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/.
[18] David E. Sanger, "Chinese Malware Hits Systems on Guam. Is Taiwan the Real Target?," The New York Times, May 24, 2023, https://www.nytimes.com/2023/05/24/us/politics/china-guam-malware-cyber-microsoft.html.
[19] David E. Sanger and Juliane E. Barnes, "U.S. hunts Chinese malware amid military disruption fears," The New York Times, July 29, 2023, https://www.nytimes.com/2023/07/29/us/politics/china-malware-us-military-bases-taiwan.html.
[20] EE-ISAC, "Trilateral Memorandum of Understanding | JE-ISAC, US-ISAC, EE-ISAC," October 17, 2018, https://www.ee-isac.eu/trilateral-memorandum-of-understanding-between-japan-u-s-and-european-energy-isac/. ISAC stands for Information Sharing and Analysis Center, referring to critical infrastructure sector-driven cooperation to share cyber threat intelligence and best practices.

[21] Financial ISAC, "Cooperation with FS-ISAC," Accessed August 8, 2023, https://www.f-isac.jp/cooperation/index_e.html.
[22] Scott Algeier, "IT-ISAC Formalizes Operational Partnership with ICT-ISAC Japan," November 12, 2019, IT-ISAC, https://www.it-isac.org/post/it-isac-formalizes-operational-partnership-with-ict-isac-japan.
[23] Ministry of Defense, "National Defense Strategy," December 16, 2022, https://www.mod.go.jp/j/policy/agenda/guideline/strategy/pdf/strategy_en.pdf, p. 26.
[24] Ministry of Defense, "Defense Buildup Program," December 16, 2022, https://www.mod.go.jp/j/policy/agenda/guideline/plan/pdf/program_en.pdf, p. 11.
[25] Erika Kobayashi, "Japan plans security clearances similar to U.S. and Europe," Nikkei Asia, June 7, 2023, https://asia.nikkei.com/Politics/Defense/Japan-plans-security-clearances-similar-to-U.S.-and-Europe.
[26] Cybersecurity and Infrastructure Security Agency, "Shields Up!," Accessed August 7, 2023, https://www.cisa.gov/shields-up.
[27] Email interview with David Beabout on August 7, 2023.

U.S. Cyber Diplomacy in Southeast Asia and the Indo-Pacific

Benjamin Bartlett, Ph.D.

As of now, the U.S. has played a relatively minor role in providing cybersecurity capacity-building assistance to Southeast Asia. Major efforts to provide capacity-building assistance to the region, outside of more globally-focused capacity-building projects, began under the Trump administration and have been continued and built upon by the Biden administration. These efforts appear to be part of a wider strategy to engage with Southeast Asia to counter Chinese influence in the region. However, cooperative efforts on cybersecurity between the U.S. and Southeast Asia are not yet strongly institutionalized, and it is unclear whether a new administration will continue to build on the Biden administration's efforts. Also, Japan already plays a major role in providing cybersecurity capacity-building assistance to the region, it may be better for the U.S. to focus on areas where it can provide a unique contribution or that clearly align with its new "Persistent Engagement" cyber strategy.

Gaining Momentum: US–ASEAN Cyber Cooperation

The first major project the U.S. sponsored in SoutheastAsia began in 2016 in cooperation with Singapore. The Singapore-United States Third Country Training Program (TCTP) Cybersecurity Workshops have occurred at least five times since then, covering topics such as the development of cybersecurity strategies, incident management frameworks, public outreach campaigns, and responsible state behavior in cyberspace.[28] The two countries also jointly enacted the U.S.-Singapore Cybersecurity Assistance Program in 2019, which provided ASEAN member-states with industry perspectives on how to raise the capability and maturity of their Computer Emergency Response Teams (CERTs).[29] Singapore has been a major partner for the U.S. when it comes to cybersecurity: In 2021 the two countries signed three Memoranda of Understanding (MoUs) about enhancing cybersecurity cooperation, building on an earlier MoU that had been signed in 2016.[30]

Other projects in Southeast Asia funded by the U.S. include the 2018-2022 Malware Mitigation Assistance program, run by the George C. Marshall European Center for Security Studies, which educated participants from Indonesia, the Philippines, Thailand, and Malaysia about North Korean illicit cyber activities[31]; the United States Trade and Development Agency helped Thailand comply with international standards for data protection and cybersecurity, which ran in 2021[32]; another project is Building Cyber Hygiene Capacity in Thailand, the Philippines, and Indonesia, a program run by the Cybersecurity and Infrastructure Security Agency in 2023 which invited participants from multiple sectors to learn about various cybersecurity-related issues.[33] The U.S. has also instituted joint programs with Japan and the EU, such as the 2018 Japan and U.S. Joint Training for Industrial Control Systems Cybersecurity[34] and the Japan-U.S.-EU Industrial Control Systems Cybersecurity Week for the Indo-Pacific Region.[35]

Although cooperation between the U.S. and Southeast Asia on cybersecurity capacity-building is still not heavily institutionalized, leaders of the U.S. and ASEAN member-states did release a Statement on Cybersecurity Cooperation at the Sixth ASEAN-U.S. Summit in November 2018. In this statement, they agreed to cooperate to maintain a secure information technology (IT) environment and capacity-building. They also reaffirmed the applicability of international law to cyberspace[36] and established the ASEAN-U.S. Cyber Dialogue in 2019. The Dialogue has occurred three times, covering topics such as 5G technologies, the applicability of international laws and cyber norms, and the potential for regional cooperation including cybersecurity capacity-building.[37,38]

Increased cooperation between the U.S. and Southeast Asian countries on cybersecurity has coincided with a rising sentiment within Washington, D.C. that the U.S. needs to do more to counter an increasingly assertive China, as exemplified by the elevation of the U.S.-ASEAN relationship to Comprehensive Strategic Partnership by the Biden administration in 2022.[39] However, it remains to be seen if future US administrations will continue to invest in deeper cooperation with Southeast Asia.

A major factor potentially hindering U.S. cybersecurity cooperation among potential and current partners in Southeast Asia and the wider Indo-Pacific (except for Australia) is a reluctance on the part of the U.S. to share information on cyber threats and cyber incidents. This is largely because the U.S. is worried that its partners would leak the shared information, which in the worst case scenario could reveal U.S. sources and its methodologies among its adversaries.[40] But despite the potential risk of leakage, the US should still find ways to share information. This include sanitizing information in a manner that makes the revelation of sources and methods less likely. Additionally, the US must also provide clear guidelines among partners and allies to protect the shared information.

The China Factor in the US–Japan Cybersecurity Cooperation

Along with cybersecurity cooperation, the U.S. is also trying to limit the influence and spread of Chinese technology in Southeast Asia and the wider Indo-Pacific through initiatives such as the Digital Silk Road. To this end, it has been cooperating with its ally and partner Japan. For example, in April 2021, the two countries announced the U.S.-Japan Competitiveness and Resilience (CoRe) Partnership.[41] Under this partnership, the U.S. and Japan have agreed to cooperate on a number of issues related to digital technologies, such as promoting Open Radio Access Network (RAN) for cellular networks, which allows for interoperability between cellular equipment from different vendors. One major advantage the Chinese supplier Huawei has is that it can provide equipment and services across the entire 5G protocol stack; by making sure that the equipment of different vendors is interoperable, it is easier for non-Chinese firms to compete.[42]

The U.S. and Japan agreed to develop and promote international technical standards both bilaterally and through the Quad. International technical standards can influence which products will have better opportunities in the international market. It also impacts interoperability between different countries' products and services and can create international ethical and normative conventions. For these reasons, China has been working hard to establish more influence over international technical standards-setting in recent years.[43]

The U.S. and Japan also agreed to support quality infrastructure development in the Indo-Pacific, which will give them opportunities to promote their favored IT infrastructure technologies. One way that Japan has competed with China when it comes to infrastructure in Southeast Asia is by focusing

on "quality".[44] Given U.S. dominance in areas such as cloud computing, there are real opportunities for it to do likewise. However, quality is not the only factor that matters. One other issue is price: China offers generous financing for its technologies. The U.S. is increasingly willing to take steps to counter this by providing loans of its own.[45] The second, more difficult, challenge is that Chinese technologies are often employed as surveillance tools which the U.S. and Japan, for normative and ethical reasons, are unwilling to offer.[46] Unfortunately, surveillance technologies are appealing to a number of Southeast Asian governments.

When it comes to countering Chinese influence and building cybersecurity capacity in Southeast Asia, the U.S. and Japan could benefit from stronger coordination. One difficulty is that IT- and cyber-diplomacy are not entirely coordinated within each country. Both have bureaucratic organizations pursuing their own IT- and cyber-diplomacy-related projects. It would be helpful to have a single organization in charge of coordinating these efforts in each government, which could then serve as a point of contact for the other organizations. For cybersecurity specifically, the obvious organizations are the Cybersecurity and Infrastructure Security Agency (CISA) in the U.S. and the National center of Incident readiness and Strategy for Cybersecurity (NISC)[47] in Japan.

Future Areas of Cooperation

Of course, before the two countries can successfully cooperate on cyber capacity-building assistance and other forms of cyber diplomacy in Southeast Asia or the wider Indo-Pacific, a key question that needs to be resolved is how large a role the U.S. should play, particularly given that Japan is already heavily active in the region. At the very least it would be helpful for the U.S. to figure out in what areas it could offer additional value on top of Japan's efforts.

More importantly, given the U.S. turn toward a strategy of "Persistent Engagement", where the goal is to anticipate your adversaries and make them react to you, it is an open question whether these efforts, which are partly reactive and focused on responding to Chinese actions and influence, are the best use of American resources. This is not to say that the U.S. should eschew cyber cooperation or cyber diplomacy, but instead it may be better to adjust the form of cooperation that fits its new overall strategy. As a starting point, it may want to explore introducing the concept of Hunt Forward Operations among its trusted allies in the region.

[28] Cybil, "Singapore-United States Third Country Training Programme (TCTP) Cybersecurity Workshops - Cybil Portal," February 22, 2021, https://web.archive.org/web/20230803154534/https://cybilportal.org/projects/singapore-united-states-third-country-training-programme-tctp-cybersecurity-workshops/.
[29] Cybil, "US-SG Cybersecurity Technical Assistance Programme - Cybil Portal," December 2, 2020, https://web.archive.org/web/20230803175522/https://cybilportal.org/projects/us-sg-cybersecurity-technical-assistance-programme/.
[30] Aqil Haziq Mahmud, "More Cybersecurity Cooperation between Singapore, US in Public, Defence and Financial Sectors," Channel News Asia, August 23, 2021, https://web.archive.org/web/20230804142738/https://www.channelnewsasia.com/singapore/singapore-us-mou-cybersecurity-cooperation-public-defence-finance-2130121.

[31] Cybil, "Malware Mitigation Assistance - Cybil Portal," October 21, 2021, https://web.archive.org/web/20230803174833/https://cybilportal.org/projects/malware-mitigation-assistance/.
[32] U.S. Trade and Development Agency, "Thailand Cybersecurity and Data Protection Standards Workshop," January 26, 2021, https://web.archive.org/web/20230803175148/https://ustda.gov/wp-content/uploads/STCP-Thailand-Cyber-Security-Workshop-Flyer.pdf.
[33] Jamila Baraka, "CISA - Building Cyber Hygiene Capacity in Thailand, the Philippines and Indonesia | CISA," April 21, 2023, https://web.archive.org/web/20230803180053/https://www.cisa.gov/news-events/news/cisa-building-cyber-hygiene-capacity-thailand-philippines-and-indonesia.
[34] Cybil, "Japan & US Joint Training for Industrial Control Systems Cybersecurity - Cybil Portal," June 15, 2020, https://web.archive.org/web/20230803180623/https://cybilportal.org/projects/japan-us-joint-training-for-industrial-control-systems-cybersecurity/.
[35] Ministry of Economy, Trade and Industry, "'JP-US-EU Industrial Control Systems Cybersecurity Week for the Indo-Pacific Region' Was Held," October 31, 2022, https://warp.da.ndl.go.jp/info:ndljp/pid/12362322/www.meti.go.jp/english/press/2022/1031_001.html.
[36] Governments of the Member States of ASEAN and Government of the United States of America, "ASEAN-United States Leaders' Statement on Cybersecurity Cooperation," November 7, 2018, https://web.archive.org/web/20230803181029/https://asean.org/wp-content/uploads/2018/11/ASEAN-US-Leaders-Statement-on-Cybersecurity-Cooperation-Final.pdf.
[37] Prashanth Parameswaran, "What's Behind the New US-ASEAN Cyber Dialogue?," The Diplomat, October 4, 2019, https://web.archive.org/web/20230803184859/https://thediplomat.com/2019/10/whats-behind-the-new-us-asean-cyber-dialogue/.
[38] Government of the United States of America and Government of Indonesia, "Co-Chairs' Statement on the Third ASEAN-U.S. Cyber Policy Dialogue," United States Department of State (blog), February 3, 2023, https://web.archive.org/web/20230803185822/https://www.state.gov/co-chairs-statement-on-the-third-asean-u-s-cyber-policy-dialogue/.
[39] The White House, "FACT SHEET: President Biden and ASEAN Leaders Launch the U.S.-ASEAN Comprehensive Strategic Partnership," The White House, November 12, 2022, https://web.archive.org/web/20230609054019/https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/12/fact-sheet-president-biden-and-asean-leaders-launch-the-u-s-asean-comprehensive-strategic-partnership/.
[40] Based on conversations with government officials.
[41] The White House, "Fact Sheet: U.S.-Japan Competitiveness and Resilience (CoRe) Partnership | The White House," April 16, 2021, https://web.archive.org/web/20230720185825/https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/16/fact-sheet-u-s-japan-competitiveness-and-resilience-core-partnership/.
[42] David Sacks, "China's Huawei Is Winning the 5G Race. Here's What the United States Should Do To Respond | Council on Foreign Relations," March 29, 2021, https://web.archive.org/web/20230803191950/https://www.cfr.org/blog/china-huawei-5g.
[43] Robert D. Hormats, "Who Will Set Standards for 21st Century Technologies — the US or

China?," Text, The Hill (blog), June 3, 2021, https://web.archive.org/web/20230804150949/https://thehill.com/opinion/technology/556047-who-will-set-standards-for-21st-century-technologies-the-us-or-china/.

[44] Sophie Jackman, "Japan Pushing 'quality' Aid to Counter China's Clout in ASEAN," Japan Today, September 12, 2016, https://web.archive.org/web/20160912163507/https://www.japantoday.com/category/politics/view/japan-pushing-quality-aid-to-counter-chinas-clout-in-asean.

[45] Stu Woo, "U.S. to Offer Loans to Lure Developing Countries Away From Chinese Telecom Gear," Wall Street Journal, October 18, 2020, sec. Tech, https://web.archive.org/web/20230510203906/https://www.wsj.com/articles/u-s-to-offer-loans-to-lure-developing-countries-away-from-chinese-telecom-gear-11603036800.

[46] Bulelani Jili, "China's Surveillance Ecosystem and the Global Spread of Its Tools," Atlantic Council (blog), October 17, 2022, https://web.archive.org/web/20230803193105/https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/chinese-surveillance-ecosystem-and-the-global-spread-of-its-tools/.

[47] There is currently a discussion within Japan about possibly replacing NISC with another organization, in which case this organization would be the appropriate one.

Artificial Intelligence's Effect on Cyber Security and International Cooperation: Notes for a US–Japan Cyber Forum

Andrew J. Lohn

Like most countries, the US and Japan are grappling with the increasing scope and scale of cyberattacks. Adding to this challenge is how AI is simultaneously changing the cyber threat environment. In these tumultuous conditions, analysts can easily overstate or misplace risks but equally, there are also many that are worth attending to. Some risks are not overstated, and others foretell a shifting cyber threat landscape that is not necessarily more or less risky but is different in kind, scale, or speed. On the defensive side, some AI technologies may be less valuable than many hope while others are more promising. This article recounts and contextualizes some of the work that the CyberAI project has done on these topics as part of the Center for Security and Emerging Technology.

Disinformation, Phishing, and Scams

Disinformation is now commonly included among cyber effects, and the CyberAI project has been studying it since our inception in 2019. We were granted an early opportunity to evaluate the ability of large language models to shape public opinion.[48] We have since studied the kill chain of automated disinformation, ways to mitigate its effects, ways to detect inauthentic content, and various other aspects of the threat.[49]

The threat is substantial. Language models can generate convincing text, especially when paired with human editors or filters who can quickly select promising outputs or tweak them to stay on message or remove incriminating errors or omissions. And the outputs can be extremely difficult to detect as inauthentic. But this does not necessarily imply a future of discourse that is written by malicious chatbots. Scaling up disinformation campaigns requires much more than simply writing more content. It requires an infrastructure of inauthentic accounts that often include inauthentic emails and possibly credit card numbers. It requires networks of servers, often through several countries, to communicate with those accounts in ways that are difficult to trace back to the source. It requires effort and maintenance which may be difficult to justify at times given how effective the old-fashioned human-driven operations already are.

The human-driven component is also a key to understanding how these models might affect scams. Examples, such as the fake Nigerian Prince who requests money, are notoriously transparent and usually filled with grammatical and typographical errors. Many observers suggest that language models will turn these scams from obvious to compelling, but that view treats the grammar and transparency as bugs to remove rather than as intentional tactics of the scammers. Since all but the most gullible will withdraw before wiring money to a stranger, a more convincing message could create more work for scammers.[50] That

does not apply yet for voice scams. A phone call that uses the AI-generated voice of a family member, friend, or colleague can fool those who are not so gullible, at least for now. It remains to be seen if these tricks will become so well-known that they too turn to obvious giveaways or if they remain successful as they become more renowned.

Phishing is evidence that scams remain effective. With click rates around three percent, a large campaign is almost certain to compromise at least one victim.[51] However, large phishing campaigns also have a high likelihood of alerting defenders. This suggests that perhaps the value to hackers of AI-generated phishing is not so much in increasing the odds of a successful intrusion but in decreasing the odds of alerting defenders. In that case, AI might actually shrink the number of phishing messages being sent.

Alternatively, the value may lie in compromising high-value targets. For spear-phising, there's only a small benefit from AI-generations because a handful of spear-phishing messages are easy enough to write by hand. But there might be a benefit in being able to spear-phish many different organizations. In that sense, AI-generations might increase the volume of carefully crafted messages directed at high-value accounts across the internet.

Malware Generation and Hacking

Beyond the initial foothold that phishing might provide, AI generations might play an important role in the subsequent operation. AI is capable of writing components of software, and since malware is just software, it can help write malware.[52] Presently, AI code generation systems do not seem to be adept at writing complete malware from start to finish except perhaps for the most common exploits where complete code is already a

simple internet search away. Still, it has likely decreased the time for new malware development.

But like phishing emails, writing malware is usually just one step in a larger operation. These operations take many steps and use many tools that are already highly automated. Once a hacker reaches a computer or device, they may use a tool to scan for nearby targets and another to search through directories and folders and a third to test billions of possible passwords. The human largely guides the process and selects the correct tools and settings. AI may also be able to help select and run those tools, but our initial tests suggest it is not yet as adept as some might fear.[53]

Defensive Coding

Just as generative AI can be used to help write malware, it is easy to imagine it being used to write the updates and patches that are needed to block malware. But that technology could only provide limited progress at best because patch writing is already relatively efficient. Defenders already know about the vulnerabilities and produce patches before they're announced about eighty percent of the time. For the remaining twenty percent of vulnerabilities too, patches come quickly. Eighty percent of those have a patch within the first two months. The delay is not so much in creating patches, it comes mainly in adopting those patches.[54]

With that in mind, there is an opportunity for AI to help defenders test their patches to understand which ones are most critical to apply. The defenders also need to understand the risk that updates may interfere with normal operations. Administrators are often reluctant to apply patches that are available because updates can require downtime or resets, or because updates may change how software that seems to be

working will operate. These are more challenging problems for AI to help solve, but addressing these challenges could provide more benefit than automating patch writers.

Defending with AI Beyond Detection

Deciding which patches to apply at any given time, or deciding when and how to change configurations more generally, is like a strategic multimove game that defenders play against attackers. Generative AI may become adept at game playing, but a different type of AI has been the most promising to date. Reinforcement Learning (RL) is an approach that lets a digital agent try to achieve some goals in what is usually a simulated environment. The agent chooses an action and receives some small reward or punishment based on how well that action progresses the agent toward achieving its goal. This is very similar to how humans learn, but it is also the technique that has created the best Chess and Go playing programs in the world.

Until very recently, RL was almost never applied to cyber problems, but that is changing.[55] Led mostly by the Defense and Intelligence arms of the Five Eyes and NATO countries, there are now several highly configurable cyber training environments. Several of these training gyms are openly available to download, and one of them, named CybORG, has been used to run a series of competitions with international entrants.[56]

These efforts to develop agents that can not only detect threats but that can also act quickly to reconfigure aspects of the network or devices are still in their early days. The networks being tested are still small and so are the number of variables the agents observe and the number of actions they can take. It is not clear how capable these agents can become but there is plenty of room for further improvement. The agents that have been trained to this point are still tiny compared to the state of the art AI systems in other domains.

Opportunities for International Collaboration

This context provides several opportunities for the US and Japan, as well as other international allies, to work together. As a start, there is much research to be done in applying AI for defense. Autonomous patch writing can still provide some benefit, but getting those patches into vulnerable networks faster would be even more beneficial. Beyond patches, autonomous controls that can reliably and quickly determine which configurations to change, which digital processes to kill, or which devices to isolate could be valuable. Along those lines, Japanese efforts to contribute to the early work being done on RL for autonomous cyber defenses would almost certainly be welcomed by other international partners and allies.

With an eye toward attackers, the US and Japan have many shared adversaries. If AI does increase the scale of the threat then it also increases the opportunity for information sharing and collaborative threat hunting. Increased scale of attacks usually requires increased scale of infrastructure such as covert identities and botnets of co opted devices, and the attacker often needs these to extend through allied countries. This infrastructure can provide clues to pass between nations and can also provide the breadcrumbs that lead back to the attackers' origins, where they can be more thoroughly defanged. While AI certainly introduces new threats, it may also introduce more opportunities for defense and for increased coordination among allies.

The views expressed are the author's own personal views and do not necessarily reflect the views of the White House or the Administration.

[48] Ben Buchanan, et al., "Truth, Lies, and Automation: How Langauge Models Could Change Disinformation," Center for Security and Emerging Technology (May 2021). https://cset.georgetown.edu/publication/truth-lies-and-automation/

[49] Katerina Sedova, et al., "AI and the Future of Disinformation Campaigns Part 1: The RICHDATA Framework," Center for Security and Emerging Technology (Dec 2021) https://cset.georgetown.edu/publication/ai-and-the-future-of-disinformation-campaigns/; Katerina Sedova, et al. "AI and the Future of Disinformation Campaigns Part 2: A Threat Model," Center for Security and Emerging Technology (Dec 2021) https://cset.georgetown.edu/publication/ai-and-the-future-of-disinformation-campaigns-2/; Josh A. Goldstein, et al., "Generative Language Models and Automation Influence Operations: Emerging Threats and Potential Mitigations," arXiv 2301.04246 (Jan 2023). https://arxiv.org/pdf/2301.04246.pdf; Josh A. Goldstein, Andrew J. Lohn, "Finding Language Models in Influence Operations," Lawfare (June 20, 2023) https://www.lawfaremedia.org/article/finding-language-models-in-influence-operations.

[50] Cormac Herley, "Why do Nigerian Scammers Say They are from Nigeria?," Microsoft (Jun 2012) https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/WhyFromNigeria.pdf.

[51] "Verizon: 2021 Data Breach Investigations Report," Computer Fraud & Security 2021, no. 6 (2021): 4.

[52] Elias Groll, "ChatGPT shows promise of using AI to write malware," CYBERSCOOP (Dec 6, 2022). https://cyberscoop.com/chatgpt-ai-malware/.

[53] Lisa Lam, "Capturing the Flag with ChatGPT: Generative AI for Cyber Education," Center for Security and Emerging Technology (Jun 7, 2023). https://cset.georgetown.edu/article/capturing-the-flag-with-chatgpt-generative-ai-for-cyber-education/.

[54] Andrew Lohn, Krystal Jackson, "Will AI Make Cyber Swords or Shields?," Center for Security and Emerging Technology (Aug 2022) https://cset.georgetown.edu/publication/will-ai-make-cyber-swords-or-shields/; Andrew J. Lohn, Krystal Alex Jackson, "Will AI Make Cyber Swords or Shields: A few mathematical models," arXiv 2207.13825 (Jul 27, 2022) https://arxiv.org/abs/2207.13825.

[55] Andrew Lohn, et al., "Autonomous Cyber Defense: A Roadmap from Lap to Ops," Center for Security and Emerging Technology (Jun 2023) https://cset.georgetown.edu/publication/autonomous-cyber-defense/.

[56] The Technical Cooperation Program, "TTCP CAGE Challenge," GitHub https://github.com/cage-challenge.

Generative AI's Impact on Cybersecurity and US-Japan Cooperation

Mina Takazawa

Introduction

The landscape of cybersecurity is rapidly evolving, driven by the ever-expanding capabilities of technology. In this age of digital transformation, one technological advancement that has captured significant attention is Generative Artificial Intelligence (AI). Its potential impact on cybersecurity is profound, presenting both opportunities and challenges that warrant careful consideration. Furthermore, as the global community grapples with cyber threats, it becomes imperative for nations to cooperate and formulate effective strategies to harness the power of Generative AI for enhancing cybersecurity. This article explores the concerns surrounding Generative AI's impact on cybersecurity, delves into ways to leverage its potential for cyber defense, and emphasizes the significance of US-Japan cooperation in establishing a robust cybersecurity framework.

Concerns Looming Over Possible Impact of Generative AI on Cybersecurity

Generative AI, an innovation that has demonstrated remarkable capabilities in creative tasks such as image and text generation, holds the potential to revolutionize multiple domains. However, concerns are emerging regarding its potential negative impact on cybersecurity. Currently, the full sophistication of cyber-attacks leveraging Generative AI has not been realized, but the threat is real. Already, instances of propaganda and influence operations utilizing AI-generated content have been observed, signaling the need for proactive measures[57].

The ability of Generative AI to craft convincing fake content, such as news articles and social media posts, poses a significant risk to public trust and information integrity. Considering that global consensus to regulate generative AI, let alone AI, has yet to be created, there are no international guidelines that can prohibit Generative AI from being weaponized to pursue certain political or personal goals at the expense of maintaining social cohesion.

Disinformation and foreign influence operations have always been a threat to the information ecosystem throughout human history. However, the advent of Generative AI can vastly increase the scope, scale, and efficiency of malicious disinformation and misinformation campaigns that tarnish the global information ecosystem. Such malicious online operations have the potential to manipulate public perception, influence elections, and sow social discord at large. As the utilization of Generative AI in such operations becomes more sophisticated, the urgency to address its potential challenges is warranted.

Now more than ever developers of big foundational models such as the Large Language Model (LLM) should uphold high standards of responsible AI and ensure its application.

Data scientists and AI engineers must translate responsible AI standards into practice throughout the lifecycle of AI systems to develop appropriate guardrails against unintended or malicious uses. In such a best-case scenario, Generative AI systems could not be exploited by cyber criminals.

Leveraging Generative AI for the Sake of Cyber Defenders

While concerns surrounding Generative AI are legitimate, it is important to recognize that it can also be a powerful tool in the hands of cyber defenders.

There has long been a perception that attackers possess the agility advantage. Adversaries with novel attack techniques typically enjoy a comfortable head-start before they are conclusively detected. But AI has the potential to swing the agility pendulum back in favor of defenders.[58] One of its significant advantages lies in its capacity to process, contextualize, and analyze vast amounts of security-related data much faster than a big team of security professionals can ever do. It could even propose possible options for remediation. This ability empowers organizations to rapidly identify potential threats, vulnerabilities, and anomalies, detect security incidents, and conduct effective investigations with speed thus giving defenders the ability to deny attackers their agility advantage. If we train and inform our Generative AI properly for security purposes, it could drastically reduce the time required to counter attacks by assisting cyber professionals throughout their investigation processes, enhancing the overall cybersecurity posture.

Another opportunity that Generative AI could bring about is its possibility to address the shortage of skilled cybersecurity professionals. The cybersecurity industry is grappling with a widening talent gap. By 2025, there will be 3.5 million

cybersecurity jobs open globally, representing a 350% increase over an eight-year[59]. Generative AI can contribute to bridging this divide. By facilitating the education and training of entry-level professionals through simulations and practical scenarios, Generative AI can expand the pool of capable cyber defenders. Highly capable cyber professionals will be released from drudgery or repetitive work and be able to focus on the most important jobs that require human ingenuity.

Making Generative AI Work through US–Japan Cooperation

The global nature of cyber threats necessitates international collaboration, and the partnership between the United States and Japan holds promise in addressing these challenges. As Japan recently revised its NSS that stipulated the Japanese government's determination to strengthen its cybersecurity capabilities, the time is ripe for enhanced US-Japan bilateral cooperation in this new strategic sphere. Given the possible impact of Generative AI which is expected to span a wide range of our economic and social life aspects, let alone cybersecurity, US-Japan bilateral cooperation should also consider Generative AI's impact, rather than solely focus on the AI-cybersecurity nexus.

First, the US and Japanese governments should jointly promote responsible AI practices to protect advanced Generative AI technologies from malicious cyber actors. As big foundational models such LLM necessitate huge computing, engineering, and financial resources, it would be difficult for malicious actors themselves to develop their own. Because timing is crucial, the two allies should start developing effective guardrails against malicious actors. In the United States, initiatives such as White House voluntary commitments for responsible AI [White House, 2023], and the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) have laid the foundation for responsible AI governance. Likewise, Japan's Liberal Democratic

Party is leading efforts to promote responsible AI adoption. The Japanese government is expected to release its revised AI guidelines, aimed at incorporating Generative AI's implications by the end of the year 2023[60]. However, given the rapidly evolving landscape of AI, the US and Japan should streamline and promote responsible AI practices across different sectors and players, particularly throughout the Generative AI development and deployment lifecycle.

Second, the US and Japan should also ensure coherence and interoperability in their regulatory and policy frameworks governing AI. The importance of regulatory and policy coherence and interoperability cannot be overestimated given the inherently global nature of AI technologies and the considerable barriers to innovation posed by fragmented regulatory frameworks among nations.

Also, to ensure that everyone can benefit from AI in a responsible way, societies around the world should develop, share, and access AI technologies. Ensuring coherence and interoperability across jurisdictions should be at the core. During its G7 chairmanship, Japan has undertaken the Hiroshima AI Process to ensure policy and regulatory coherence between member countries. This effort could serve as an important first step toward international regulatory interoperability and hopefully spark a more coherent global governance system. Fundamentally, this will be critically important to harness the power of AI while minimizing possible harms and risks across the globe.

On the development of global norms governing AI, OECD's foundational frameworks for responsible AI may provide useful insights. The US and Japan could cross-reference existing frameworks to further share best practices, and foster policy coherence and regulatory interoperability in the realm of Generative AI.

Third, the significance of public-private partnerships cannot be overstated in shaping the regulatory landscape of Generative AI in cybersecurity. Given the dynamic and evolving nature of technology, collaboration between governments and private sector entities is essential for regulations, standards, and protocols to keep pace with rapid technological development. In this regard, NIST's AI Risk Management Framework was developed through a consensus-driven and transparent process involving work by government agencies, civil society organizations, and several technology leaders[61]. The Framework provides a useful model borne out of public-private partnerships that other governments including Japan could leverage. The Japanese government also states the importance of "agile governance", which emphasizes the need for public-private partnership in forming regulations against the backdrop of today's rapid technological changes, in their draft skeleton of new AI guidelines. The Japanese government should grab this AI moment to innovate Japan's traditional regulatory process into a process that involves continuous and two-way communications between public and private sectors.

Fourth, both governments need to be cognizant of the fact that cloud adoption will be the key and prerequisite for strengthened cybersecurity cooperation in the new AI era. Lessons learned from the first days of the Russian invasion of Ukraine revealed that the Russian missiles first targeted the Ukrainian government's data center. Ukraine had passed laws to allow government data to move to the cloud only about one week before the attack. After 18 months into the war, the Ukrainian government continues to function regardless of relentless cyberattacks by Russian actors because of the cloud.

This means that data is far more secure in the cloud than on-premise, and even more so with the advent of AI when cybersecurity posture needs to be upgraded and enhanced at machine speed. As the next steps, the US and Japanese governments could collaborate for accelerated cloud adoption for

strengthened cybersecurity. Considering the breadth and depth of this issue, they can first start with strategically important sectors such as critical infrastructure operators by helping them move to the cloud.

Conclusion

In the age of Generative AI, technology, policy, and international cooperation is paramount for effective cybersecurity. While concerns persist, the potential benefits of Generative AI in bolstering cyber defense are also significant. The collaboration between the United States and Japan serves as an exemplar of international cooperation, highlighting the importance of working together to address the challenges posed by Generative AI in cybersecurity. As we stand at the crossroads of technological innovation, the path forward lies in harnessing the potential of Generative AI while remaining vigilant against its risks.

**The views and opinions expressed in this article are solely those of the author and do not necessarily reflect the official policy or position of Microsoft Corporation, its affiliates, or any other organizations mentioned. Microsoft Japan and the author are not responsible for any errors, omissions, or inaccuracies in the content, nor for any consequences arising from the use of the information provided in this article.*

[57] Chen May Yee, "Microsoft Interview with Tom Burt," Microsoft, June 13, 2023.
[58] Charlie Bell, "How AI will impact the future of security," LinkedIN, March 2, 2023, https://www.linkedin.com/pulse/how-ai-impact-future-security-charlie-bell/.
[59] Steve Morgan, "Cybersecurity Job Report: 3.5 million Unfilled Positions in 2025," Cybersecurity Ventures, April 14, 2023, https://cybersecurityventures.com/jobs/.
[60] "Generation AI, guidelines for businesses to be integrated by the government within the year," June 26, 2023, Nikkei, https://www.nikkei.com/article/DGX-ZQOUA2630A0W3A620C2000000/.
[61] "Governing AI: Blueprint for the Future," Microsoft, May 25, 2023, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW14Gtw.

About the Authors

MARK BRYAN MANANTAN EDITOR
is the Director of Cybersecurity and Critical Technologies at the Pacific Forum.

EMILY GOLDMAN, Ph.D. is a Strategist at the US Cyber Command.

MIHOKO MATSUBARA is the Chief Cybersecurity Strategist at NTT Corporation in Tokyo, Japan.

BENJAMIN BARTLETT, Ph.D. is Assistant Professor, Department of Political Science, Miami University.

ANDREW J. LOHN is a Senior Fellow at the Center for Security and Emerging Technology.

MINA TAKAZAWA is the Government Affairs Director at Microsoft Japan.

PACIFIC FORUM
INTERNATIONAL

pacforum.org | pacificforum@pacforum.org