Supporting Amphibious Forces with Partnered U.S: Japan Cyber Operations

Harrison Rashley[1], Timothy Shives[2] and Wade Huntley[2]
[1]United States Naval Academy, Annapolis, Maryland, USA
[2]Naval Postgraduate School, Monterey, California, USA

rashley@usna.edu
timothy.shives@nps.edu
wlhuntle@nps.edu

Abstract: The first island chain is a threat environment characterized by persistent and sophisticated cyber activities by state and non-state actors, as well as strategic competition with China, North Korea, and Russia. To operate in these conditions the United States Marine Corps has proposed the Stand-in Force, a small, low-signature force establishing the forward edge of a partnered defense-in-depth in the United States Indo-Pacific Command area of operations. This paper examines the efficacy of utilizing partnered and allied cyber infrastructure to support persistent reconnaissance and counter-reconnaissance operations by Stand-In Forces within contested maritime zones. It focuses on Japan, a key ally in the Western Pacific. Through a case study approach, it examines the nation's cyber command structure, defense network security, existing cyber agreements with the United States, and barriers to cooperation, congruently assessing their cyber capabilities and willingness to cooperate in cyberspace. The result is a summary of their ability to support the Stand-In Forces in defensive and offensive cyber operations, an analysis of current barriers, and the requirements of an ideally cyber-capable Stand-In Force.

Keywords: Cyber, Cyber reconnaissance, Marine Corps, Stand-in force, Amphibious force, Partners, Allies, Policy, Doctrine, Operations

1. Introduction and Background

In 2019 the United States Marine Corps identified the need for sweeping force design changes to fill the role as an expeditionary force-in-readiness. One proposed addition in Force Design 2030 (FD2030) is the Stand-In Force (SIF), a small, low-signature force comprised of Navy and Marine Corps units operating within a maritime contested area. Stand-In Forces establish the forward edge of a partnered defense-in-depth, denying the adversary freedom of action through persistent reconnaissance and counter reconnaissance (*A Concept for Stand-In Forces,* 2023). Reconnaissance is conducted to confirm or deny enemy presence, and the SIF will be tasked with locating the enemy fleet while denying their ability to locate our own. Due to the nature and location of their mission, these forces will have a limited organic cyber capability, especially to conduct offensive cyberspace operations or reconnaissance, and will be required to leverage resources from external sources to maintain contact with adversaries in cyberspace. The SIF are a crucial part of the FD2030 plan, and their mission is a cornerstone of the Marine Corps' *21st Century Amphibious Operations* concept.

The United States has a wealth of allies and partners in the West Pacific, each with their own cyber capabilities and accompanying policies. Of note, Japan is in geographic proximity to China and has long established relationships with the United States. The country has an established cyber program and has recently engaged in talks to deepen ties with the United States in cyberspace ("United States-Japan-ROK Working Group on Cyber Activities," 2024). Their infrastructure is geographically closer and more accessible to forces in the zone of conflict, but it comes with challenges of its own. Unaligned regulatory and strategic goals, combined with a lack of technical solutions to enable intelligence sharing between nations, greatly increases difficulty in conducting joint cyber operations even in peacetime (Moroney et al., 2023). This regulatory and technical divide is the primary obstacle in the conduct of a partnered multi-domain campaign. This research provides a synopsis of each ally or partner's cyber capabilities in support of the United States successfully leveraging these relationships for SIF missions.

1.1 Cyber Threats to Amphibious Forces

The Stand-In Forces are the United States Marine Corps' answer to an increasingly complex battlespace. The SIF will not be able to persist in the zone of conflict without interference. The major concern across all domains is the inevitability of adversary attempts to degrade positioning, navigation, and timing systems, and interfere with communications (*A Concept for Stand-In Forces,* 2023). The SIF will be able to provide these services to nearby naval forces, but only if their own has not been disrupted. Thus, they will need highly capable defensive cyberspace operations (DCO) assets organic to their units and will need capable cyber operators in their midst.

Remaining entirely unseen is nearly impossible, so the SIF will have to keep their actions in the contact layer below a certain threshold of activity. In this way they should be able to persistently engage in both cyberspace and the physical domain without being directly engaged themselves.

Another issue faced by forward-deployed units has been highlighted by the conflict in Ukraine. Beginning in 2014, Russian advanced persistent threat (APT) group FANCY BEAR implemented malware in a legitimate Android application developed by a Ukrainian artillery officer for fire direction. Since the application required location data for targeting, this malware facilitated reconnaissance against Ukrainian troops, allowing Russian forces to precisely target Ukrainian artillery forces (Crowdstrike Global Intelligence Team, 2016). The malware was originally proliferated on Ukrainian message boards and was unknowingly given access to the application by Ukrainians using it for targeting. As similar applications, like the widely used Android Team Awareness Kit (ATAK), become more popular in the U.S. military, expeditionary forces will be required to guard against similar attempts. This is especially important for the SIF if they intend to remain undetected within the zone of conflict.

1.2 Barriers to Allied and Partner Integration

The DoD defines an alliance as a "formal agreement between two or more nations," adding, "in national defense, [alliances are] promises that each nation will support the other, particularly during war" (Roulo, 2019). The 2023 DoD Cyber Strategy directly addresses the importance of partners and allies as a line of effort to combat current and future cyber threats. The goals outlined include reinforcing norms of behavior in cyberspace, continuing hunt forward operations and technical collaboration, and expanding avenues of cyber cooperation (*Cyber Strategy*, 2023). This final objective includes timely information and best practice sharing, but also addresses the institutional barriers that limit cooperation in cyberspace. These barriers can stem from many areas, but generally fall into two categories: technical, and strategic.

1.2.1 Technical barriers

Technical barriers can range from a lack of compatible systems to a lack of domain knowledge or expertise (Moroney et al., 2023). Many countries use systems or software that are not directly compatible with American versions due to age differing technology, and others have security concerns due to systems purchased from the United States' competitors. U.S. prioritization of technological advancement also puts many partners at a disadvantage if they are not on an even technological footing. All U.S. information systems are governed by National Institute of Security and Technology (NIST) publication 800–53, which mandates the security and privacy controls (JTF Interagency Working Group, 2020). Other nations are all governed by their own security controls, and thus have differing levels of security requirements. These differences make it difficult for the United States to maintain confidence in an ally or partner's ability to adequately protect classified or operationally significant information.

1.2.2 Strategic barriers

States also have significantly different strategic goals. Even limited to the West Pacific, each American partner or ally has their own strategic goals and relationships with other states. For example, while South Korea has been a U.S. military ally for decades, they have also attempted to retain a policy of "balanced diplomacy" with China as the U.S.-China rivalry has grown, and they have extensive economic ties with Beijing (Lee, 2020). Likewise, Japanese interests in the region have historically mirrored those of the United States, but aligning goals can be difficult due to Japan's predisposition to a defensive strategy (Katagiri, 2021). Many countries also support different methods towards similar goals; some will support "direct" military intervention in a conflict, while others will prefer an indirect approach (Moroney et al., 2023). These strategic misalignments not only present an obstacle to conventional security cooperation, but also cybersecurity cooperation.

2. Methodology

This paper utilizes the case study method for inductive reasoning, a research strategy which focuses on understanding the dynamics present within a setting using a combination of data collection methods like document review, interviews, and observation (Eisenhardt, 1989). As a comparative analysis and qualitative comparison of the capabilities, relationships with the United States, and willingness of another sovereign nation, the case study method is appropriate for this research.

2.1 Framework

This section details the framework for this study, based on the approach to qualitative case study research designed by Robert Yin (Yin, 2013). There is no comprehensive or standardized catalog for case study research,

but Yin's 2013 model lays out a step-by-step approach to design that is flexible enough for application to most case studies while remaining detailed enough to ensure academic rigor. Yin's process contains five component steps: choosing study research questions, developing propositions, assigning units of analysis, linking data to propositions, and creating criteria for interpreting the findings (Yin, 2013).

Following Yin's model, this paper attempts to answer the following question: do allies and partners in the contested area have the capability and willingness to support Navy and Marine Corps cyber operations? To narrow the scope of the question, we propose that allies and partners in the contested area have varying levels of cyber infrastructure and competence in cyber operation, and cyber cooperation will vary greatly between nations, depending as much on willingness and established relationships as it does on viable infrastructure. Units of analysis are labeled in Figure 2.

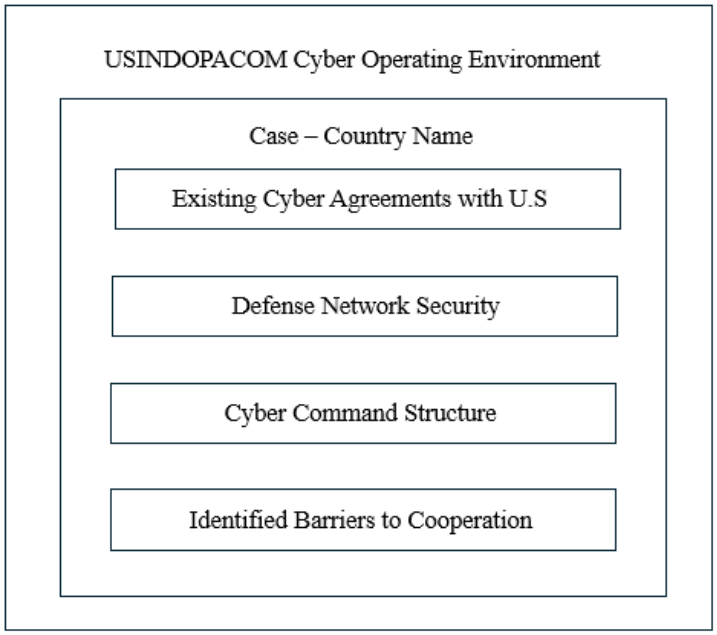

Figure 1: Individual Case Study Design. Adapted from (Yin, 2013)

Data was largely collected through a document review, compilation of previous case studies, and select interviews with experts. References only include recent policies, agreements, and technical specifications. For relevance, only recent agreements, policies, and technical specifications were considered.

2.2 Selection of Cases

We originally examined three cases for the study: Japan, South Korea, and the Philippines. This paper has been reduced to one study on Japan for brevity. The three countries have different relationships and established partnerships with the United States, providing a useful juxtaposition of examples for analysis. As major military powers in the region threatened by a common adversary, they also have the greatest incentive to conduct partnered cyber operations with the U.S. South Korea has recently reaffirmed their commitment to creating offensive cyber capabilities, and remains a witting ally in both offensive and defensive U.S. cyber operations (Saballa, 2023). Japan has long been a defensive ally in the U.S. Indo-Pacific Command (USINDOPACOM) region, and April, 2024 talks between the U.S., Japan, and the Philippines not only established an enhanced Japanese-American military partnership, but served to bring the latter country into the fold as well (Erickson and Watson, 2024).

3. Case Study - Japan

Japan and the United States have been treaty allies since 1951 and the two countries have made efforts to deepen ties and improve joint operational capabilities since the early 2000s (Manyin et al., 2023). This alliance has been central to current Indo-Pacific strategy, and Japan plans to increase its defense spending to 2% of its national gross domestic product (GDP) in an effort to face the unprecedented strategic challenge that results from their proximity to China (Manyin et al., 2023). Japan's military posture is currently limited by their

constitution, which constrains their spending to just 1% of their GDP, by their reluctance to become involved in military conflict, and by the defense-oriented national policy that they have maintained since 1945 (Bartlett, 2020). These factors have limited collaboration with American forces in the past, but as Japan shifts its national focus to address growing threats from adversaries, they will become more a more promising ally for prospective offensive and defensive cyber operations.

3.1.1 Cyber command structure

Unlike the contemporaneous establishment of USCYBERCOM and its subordinate service components, the branches of the Japanese Self-Defense Forces (JSDF) each independently established cyber-capable forces in the early twenty-first century. This began with the creation of the of the Air Self-Defense Force's cyber-surveillance unit in December 2000, followed by those of the Ground Self-Defense Force and Maritime Self-Defense Force (Kallender and Hughes, 2017). In 2008, the Ministry of Defense created a centralized command, the Command Control Communication Computers Systems Command (C4SC) to act as a coordinator between the cyber units from each individual service, but these components were still largely responsible for their own efforts (Bartlett, 2020). In 2012, the Japanese Government formally acknowledged the status of cyberspace as an operation domain under international law, and thus could be considered a domain in which Japan could exercise self-defense (Kallender and Hughes, 2017). This led to the establishment of the joint Cyber Defense Unit under the C4SC in 2014. This unit started with around 90 personnel, but was reorganized in 2022 with 540 members and plans to expand up to 4,000 ("Japan's SDF launches new cyber-defense unit," 2022). By July of 2023 they had 890, a number far behind the United States at 6,200 and vastly outnumbered by China's estimated 30,000 ("Japan to speed up SDF cybersecurity personnel development," 2023). This limited number of personnel is in large part due to Japan's "denial defense" approach, which focuses on mitigation over neutralization and greatly limits their ability to respond offensively.

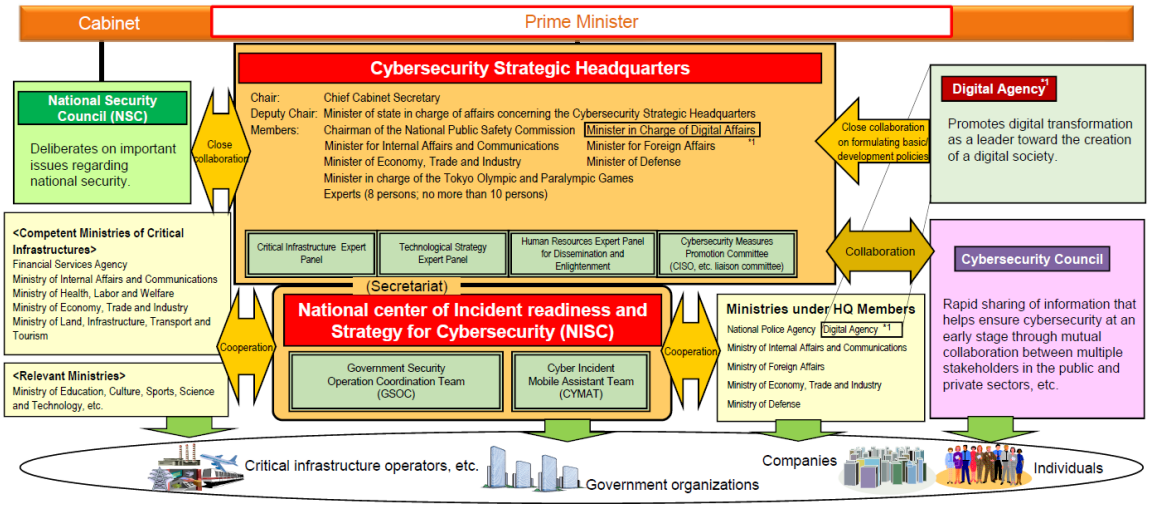

Figure 2: Japanese Cybersecurity Implementation Framework. Source: (NISC, 2021)

As shown in Figure 6, the Cybersecurity Strategic Headquarters forms the primary cyber operations entity in Japan. It is headed by the Chief Cabinet Secretary, and composed of relevant ministers and knowledgeable experts ("National center of Incident readiness and Strategy for Cybersecurity | NISC," n.d.). The National center of Incident readiness and Strategy for Cybersecurity (NISC) serves as its secretariat and regulatory body, handling international cooperation, incident response, and general strategy and management. The NISC owns one of two existing Government Security Operation Coordination (GSOC) Teams; GSOC 1 monitors government networks, analyzes malware, collects on cyberthreats, and distributes info to ministries and agencies, while GSOC2 is owned by the Information-technology Promotion Agency and monitors the incorporated agencies (Bartlett, 2020). The Cyber Incident Mobile Assistance Team within NISC provides support and technical expertise when a government body is attacked. The NISC and all the ministries with representatives in the Cybersecurity Strategic Headquarters collaborate with critical infrastructure operators, government organizations, companies, and individuals to ensure cybersecurity standards and effective incident response (NISC, 2021).

Japan has consistently worked toward centralization of cyber capabilities since the inception of the first service cyber branches at the turn of the millennium. While their cyber command structure is still not as centralized as the United States with CYBERCOM and the NSA, they have a solid foundation and have established a working bureaucratic model for cyber defense.

3.1.2 Existing cyber agreements

The United States and Japan signed the first Treaty of Mutual Cooperation and Security on September 8, 1951, then a revised and renewed version in 1960 that still stands today. This created an alliance between the two nations, and the 1960 revision required a mutual defense agreement. Specifically, in Article V, the treaty states that "an armed attack against either Party in the territories under the administration of Japan would be dangerous to its own peace and safety and declares that it would act to meet the common danger" ensuring an attack against either nation within the territory of Japan would be responded to by both countries (Christian A. Herter et al., 1960).

With the advent of cyberspace and the subsequent rise of cyber operations, the definition of an "armed attack" as stated in the treaty has come under scrutiny. Protocol I of the 1977 amendment to the Geneva Conventions of 1949 states that an attack is an "[act] of violence against the adversary, whether in offense or defense" (Norris, 2013). While many operations in cyberspace do not cross this threshold, there is a point at which these actions become a "cyber-attack." The *Tallinn Manual*, a non-binding study on the applications of international law to cyberspace, provides a specific interpretation of this threshold. Mirroring the Geneva Convention's definition of "armed attack," the *Tallinn Manual* defines a cyber-attack as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage and destruction to objects" and confirms that "consequential harm" resulting as a second order effect from a cyber operation may classify it as an attack (Norris, 2013).

By this rationale, should any malicious actor conduct a cyber-attack against American troops or base infrastructure in Japan, Japan would be required to defend them. This will likely depend on how each nation chooses to interpret the attack, however, and the *Tallinn Manual* is not a legally binding document. Japan specifically categorizes cyber-attacks as crimes unless they can be attributed to another country's military forces (Katagiri, 2021). An attack with a suitably low enough signature or diplomatic impact could result in a successful *fait accompli*, where either the U.S., Japan, or both choose not to respond.

Beyond the Mutual Defense Treaty, the United States and Japan maintain a healthy relationship in cyberspace. The two nations conduct annual cyber dialogues, with a ninth meeting held on June 26th, 2024 ("The 9th Japan-US Cyber Dialogue," 2024). Japan's desire to strengthen their military alliance with the United States, combined with an increased need for cyber defense due to recent attacks on their networks by Chinese APTs, has driven increased cooperation in recent years. They remain reluctant to let U.S. cyber forces "hunt forward" on their networks, however (Bartlett, interview, 2024).

3.1.3 Defense network security

After Japan explicitly named Russia, North Korea, and China as threats in their 2021 Cybersecurity Strategy, they saw an unprecedented 87% increase in ransomware attacks in the first half of 2022 (*Building a Cyber Workforce*, 2023). The JPCERT Coordination Center recorded 19,720 incident cases in fiscal year 2023, down from 24,419 in 2022 but still a considerable number compared to pre-2021 incidents (Figure 7) (*JPCERT/CC Incident Handling Report,* 2024). Rather than distinguish between military, government, public, or private incidents, JPCERT/CC reports only separate incidents into categories for domestic or overseas. Unclassified reports on military and government security breaches are understandably hard to come by. The Washington Post reported in 2023 that the Chinese military had compromised Japanese military computer systems, discovered by the NSA in 2020 (Nakashima, 2023).

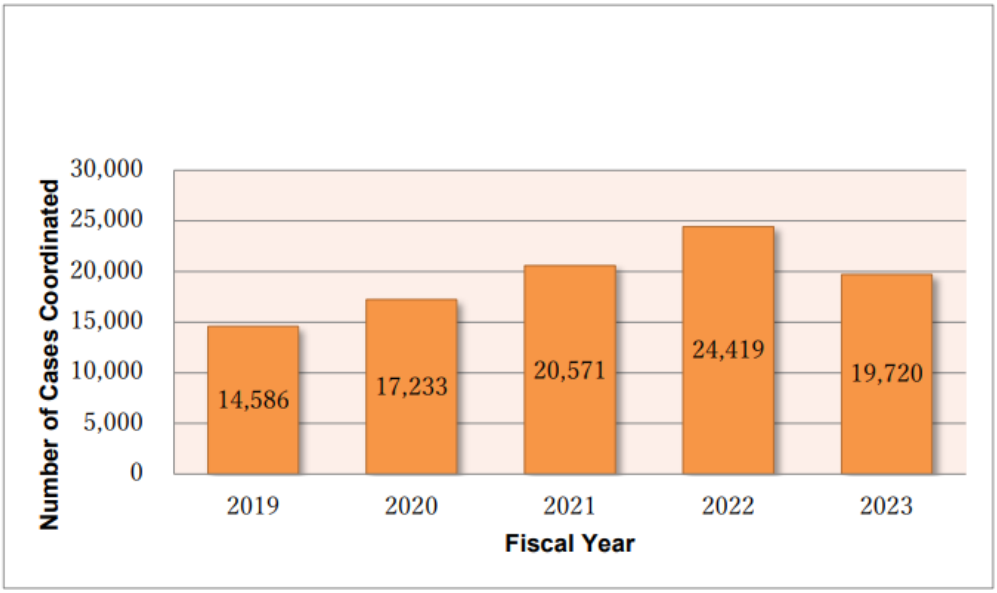

Figure 3: Change in Total Number of Cases Coordinated by Fiscal Year. Source: (*JPCERT/CC Incident Handling Report [January 1, 2024 - March 31, 2024]*, 2024)

According to Katagiri, Japan's approach to network security is best described as "denial defense," a strategic posture designed to deny attacks by defensive methods, minimizing danger rather than attacking back (Katagiri, 2021). This leaves adversaries with little fear of reprisal, which combines with their expanded use of advanced command, control, communications, and intelligence equipment to leave Japanese forces highly vulnerable to cyber-attacks (Bartlett, 2020). Despite this, Japan has done much to harden their networks against enemy intrusion. Their "Common Standards for Cybersecurity" ("Common Standards for Cybersecurity Measures for Government Agencies and Related Agencies (FY2023)," 2023) lay out a robust framework for security from information sharing and handling to security requirements for computer systems. Of particular interest for cooperation, these standards require implementation of zero trust architecture for dynamic access control, though it is not clear how closely these standards are followed by military information systems ("Common Standards for Cybersecurity," 2023).

Japan also ranks highly in the International Telecommunication Union's Global Cybersecurity Index (GCI), which measures nations' commitment to cybersecurity ("Global Cybersecurity Index," 2020). GCI tracks legal, technical, and organizational measures to produce a score for each country evaluated. Japan came in seventh in the most recent report (2020), behind only South Korea and Malaysia in the USINDOPACOM region.

3.1.4 Barriers to cooperation

From 2021 to 2023 the Maureen and Mike Mansfield Foundation, an American policy thinktank, convened a working group to address growing concerns on a lack of human capital in cybersecurity, specifically in the relationship between the Japan and the United States. This group was comprised of twelve members, six from the United States and six from Japan, and was largely focused on cyber defense and policy recommendations, to include standardizing cybersecurity language, addressing obstacles to information sharing and joint action, and utilizing public-private partnerships to enhance collaboration (*Building a Cyber Workforce Through the U.S.-Japan Alliance*, 2023). The Mansfield report found that a lack of standardization was largely to blame for inherent barriers in cybersecurity like inconsistent training, lack of relevant skills, and difficulties in cross-sector permeation. The working group recommended the adoption of the NIST Cybersecurity Framework (CSF) and the National Initiative for Cybersecurity Education (NICE) Framework, which provide a set of building blocks for describing tasks, knowledge, and skills teams need to perform cybersecurity. Neither government has mandated conformance to these standards since NIST frameworks are only recommendations, but they could provide the two countries with a baseline to standardize cybersecurity procedures. As of 2023 the Japanese Cross Sectors Forum and the companies that comprise it have agreed to use the NICE framework but have not yet implemented it. Within the scope of standardization, the report mentions cultural barriers, operational differences, information sharing, structural differences, and career trajectories (*Building a Cyber Workforce Through the U.S.-Japan Alliance*, 2023).

Another limitation to Japan's ability to support American amphibious forces in the zone of conflict is their predisposition to defensive operations. As stated above, this is already compelled in large part by their own doctrine and agreements with the United States. However, given the nature of cyber persistence and the leeway granted by the unspecific language of "self-defense," there is much opportunity for cyber operations that Japan is currently neglecting.

Another major barrier is, ironically, Japan's relationship with the United States. The U.S. has a considerable cyber force, and the JSDF and Ministry of Defense rely heavily on the American cyber arsenal (Bartlett, 2020). Because they already work closely together, Japan can focus solely on their own defense and trust the United States to conduct offensive operations against APTs and other threat actors in response to attacks against Japanese networks.

4. Conclusion

Japan is a defense-minded nation. They are capable in cyberspace, with the appropriate policy and standards for cyber hygiene, but suffer from an inundation of attacks greater than their limited cyber force can confidently handle. Their porous network defense presents some concern and will need to be greatly improved before the United States is willing to risk operations on Japanese infrastructure. Despite their capability and willingness, Japan's cyber force is small and often overwhelmed, and their network defenses will require improvement to fully support U.S. operations. Cyber operations in defense of their homeland and infrastructure are likely to continue to be a priority for the Government of Japan, and while they may offer clandestine support to U.S. cyber forces, they are unlikely to be a collaborative ally in offensive cyber operations in the immediate future. Offensive cyber collaboration with Japan will require pushing them out of their traditional AO, leaning on their stated goals to delve more into offensive cyber operations by holding them to that proposal. However, they continue to be extremely willing partners in defense, and there is expectation that this will continue to improve in the future.

This research identified significant challenges, both technical and policy-related, to cooperation with allies and partners in INDOPACOM. The case study methodology produced the following hypothesis: Current cyber relationships with Japan are sufficient for cooperative cyber operations in support of United States Marine Stand-In Forces. However, partner networks are not secure enough for independent U.S. cyber operations, and the SIF will be unable to utilize them directly without robust changes by each nation. Additionally, concerns over sovereignty will limit U.S. use of partner networks.

5. Future Work

As stated earlier, the full version of this paper is a multi-case study examining Japan, South Korea, and the Philippines. While this version focuses solely on Japan, publishing the full-length study would offer a more comprehensive comparison of cross-national variation in cyber posture, capabilities, and willingness to cooperate with the United States.

Future research could expand on several fronts, both in depth and breadth. First, comparative analysis of additional U.S. allies and partners in INDOPACOM, like Australia or Taiwan, would further broaden understanding of regional cyber capabilities. Second, deeper qualitative investigation into Japan's evolving domestic cyber policy, organizational structure, and military doctrine would help assess their future role in offensive cyber cooperation. Third, future work could explore the operational integration of partner nations into U.S. cyber planning frameworks, especially in support of concepts of like Marine Stand-In Forces.

Moreover, applying this methodology in a European context could yield valuable insights. The U.S. Marine Corps has mission responsibilities in regions like Norway and the Mediterranean, which could serve as the basis for similar studies of European allies. For instance, nations such as Norway, Denmark, or Italy might present interesting candidates for analysis, given their strategic importance in European defense and potential for cyber collaboration with the U.S. Expanding this research to include both Indo-Pacific and European contexts would not only enhance our understanding of global cyber dynamics but also provide critical insights into strengthening international cooperation in cyberspace, particularly within U.S. military strategies.

Disclaimer: The views expressed here are those of the authors and do not necessarily represent the views of the Naval Academy, the Naval Postgraduate School, the Department of Defense, or the U.S. Government.)

References

2023 Cyber Strategy of the Department of Defense Summary (2023). Department of Defense, Washington, DC, USA. Available at: https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.pdf

A Concept for Stand-In Forces, United States Marine Corps. Washington, DC, USA, 2023. Available: https://www.hqmc.marines.mil/Portals/142/Users/183/35/4535/211201_A%20Concept%20for%20Stand-In%20Forces.pdf

Bartlett, interview, B. (2024).

Bartlett, J. (2022) *U.S.-ROK Strategy for Enhancing Cooperation on Combating and Deterring Cyber-Enabled Financial Crime*. Washington, DC, USA: Center for a New American Security.

Building a Cyber Workforce Through the U.S.-Japan Alliance (2023). Washington, DC, USA: Mansfield Foundation. Available at: https://mansfieldfdn.org/wp-content/uploads/Building-a-Cyber-Workforce-Through-the-U.S.-Japan-Alliance-Policy-Brief.pdf.

Christian A. Herter *et al.* (1960) 'Treaty of Mutual Cooperation and Security between the United States of America and Japan'. Available at: https://afe.easia.columbia.edu/ps/japan/mutual_cooperation_treaty.pdf.

CISA (2023) *#StopRansomware: Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities*. Cybersecurity Advisory AA23-040A. Available at: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-040a

'Common Standards for Cybersecurity Measures for Government Agencies and Related Agencies (FY2023)' (2023). Cybersecurity Strategic Headquarters of Japan. Available at: https://www.nisc.go.jp/eng/pdf/kijyunr5-en.pdf.

Crowdstrike Global Intelligence Team (2016) *Use of FANCY BEAR Android Malware in Tracking of Ukrainian Field Artillery Units*. Intelligence Report.

'Cybersecurity Strategy' (2021). The Government of Japan. Available at: https://www.nisc.go.jp/eng/pdf/cs-senryaku2021-en.pdf.

Eisenhardt, K.M. (1989) 'Building Theories from Case Study Research', *The Academy of Management Review*, 14(4), pp. 532–550. Available at: https://doi.org/10.2307/258557.

Erickson, B. and Watson, K. (2024) 'Biden announces new steps to deepen military ties between the U.S. and Japan - CBS News', *CBS News*, 10 April. Available at: https://www.cbsnews.com/news/biden-kishida-to-announce-ramped-up-military-partnership/.

'Global Cybersecurity Index 2020' (2020). International Telecommunication Union, Geneva, Switzerland. Available at: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E.

Joint Task Force Interagency Working Group (2020) *Security and Privacy Controls for Information Systems and Organizations*. Revision 5. National Institute of Standards and Technology. Available at: https://doi.org/10.6028/NIST.SP.800-53r5.

JPCERT/CC Incident Handling Report [January 1, 2024 - March 31, 2024] (2024). Tokyo, Japan: JPCERT Coordination Center. Available at: https://www.jpcert.or.jp/english/doc/IR_Report2023Q4_en.pdf.

Kallender, P. and Hughes, C.W. (2017) 'Japan's Emerging Trajectory as a "Cyber Power": From Securitization to Militarization of Cyberspace', *Journal of Strategic Studies*, 40(1–2), pp. 118–145. Available at: https://doi.org/10.1080/01402390.2016.1233493.

Katagiri, N. (2021) 'From cyber denial to cyber punishment: What keeps Japanese warriors from active defense operations?', *Asian Security*, 17(3), pp. 331–348. Available at: https://doi.org/10.1080/14799855.2021.1896495.

Khan, S.A. and Abbasi, S.N. (2023) 'The U.S.-China Cyber Warfare in the 21st Century: Implications for International Security', *Insight Turkey*, 25(2), pp. 163–186.

Kyodo News+ (2022) 'Japan's SDF launches new cyber-defense unit', 17 March. Available at: https://english.kyodonews.net/news/2022/03/2009b0fac163-japans-sdf-launches-new-cyber-defense-unit.html.

Manyin, M.E. *et al.* (2023) *U.S.-Japan Relations*. CRS Report No. IF10199. Congressional Research Service, Washington, DC, USA.

Moroney, J.D.P. *et al.* (2023) *Overcoming Barriers to Working with Highly Capable Allies and Partners in the Air, Space, and Cyber Domains: An Exploratory Analysis*. RAND Corp., Santa Monica, CA, USA, RRA968-1. Available at: https://doi.org/10.7249/RRA968-1.

Nakashima, E. (2023) 'China hacked Japan's sensitive defense networks, officials say', *Washington Post*, 17 August. Available at: https://www.washingtonpost.com/national-security/2023/08/07/china-japan-hack-pentagon/ (Accessed: 26 February 2024).

National center of Incident readiness and Strategy for Cybersecurity | NISC (no date). Available at: https://www.nisc.go.jp/eng/index.html#sec1 (Accessed: 5 July 2024).

NISC (2021) 'Japan's Cybersecurity Strategy 2021 (Overview)'.

Norris, M.J. (2013) 'The Law of Attack in Cyberspace: Considering the Tallinn Manual's Definition of "Attack" in the Digital Battlespace', *Inquiries Journal*, 5(10). Available at: http://www.inquiriesjournal.com/articles/775/the-law-of-attack-in-cyberspace-considering-the-tallinn-manuals-definition-of-attack-in-the-digital-battlespace.

Roulo, C. (2019) 'Alliances vs. Partnerships', 22 March. Available at: https://www.defense.gov/News/Feature-Stories/story/Article/1684641/alliances-vs-partnerships/.

The Japan Times (2023) 'Japan to speed up SDF cybersecurity personnel development', 11 July. Available at: https://www.japantimes.co.jp/news/2023/07/11/national/sdf-cyber-capabilities/.

Yin, R. (2013) *Case Study Research: Design and Methods*. Fifth. SAGE Publications, Thousand Oaks, CA, USA.

(2024a) 'Second United States-Japan-Republic of Korea Trilateral Diplomatic Working Group Meeting on Democratic People's Republic of Korea Cyber Activities', 29 March. Available at: https://www.state.gov/second-united-states-japan-republic-of-korea-trilateral-diplomatic-working-group-meeting-on-democratic-peoples-republic-of-korea-cyber-activities/.

(2024b) 'The 9th Japan-US Cyber Dialogue', 27 June. Available at: https://www.mofa.go.jp/press/release/pressite_000001_00394.html.