NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

JAPAN'S PLEDGE FOR AN ACTIVE CYBER DEFENSE STRATEGY

by

Isabella C. Colandrea

December 2023

Thesis Advisor: Scott E. Jasper
Second Reader: Robert J. Weiner

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2023	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE JAPAN'S PLEDGE FOR AN ACTIVE CYBER DEFENSE STRATEGY	**5. FUNDING NUMBERS**
6. AUTHOR(S) Isabella C. Colandrea	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

This research examines why Japan has pledged to implement an active cyber defense (ACD) strategy. An ACD strategy enables nations to discover, detect, analyze, and mitigate threats in cyberspace. Although Japan's pacifist constitution limits its military capabilities, an ACD strategy would allow Japan to act in real-time to a detected intrusion and, if necessary, use offensive cyber capabilities. To answer why Japan pledged to adopt an ACD strategy, this research identifies the reasons why nations adopt an ACD strategy and reviews the risks associated with the strategy. Japan's decision to adopt an ACD strategy reflects its wish to decrease the number of new attackers, incorporate flexible layered cybersecurity techniques, and develop norms amongst allies. However, Japan's changing perceptions of its security environment, its relationship with the U.S., and its pacifist culture provide unique explanations for why Japan pledged to implement ACD. The research concludes with an evaluation of Japan's current cyber infrastructure and plans for implementation. Japan's current cybersecurity infrastructure provides a foundation for the future integration of ACD, but to ensure successful and safe employment of ACD, Japan must honor its planned pledges, compose an ACD doctrine, clarify its command structure, invest in an educated cyber core supported by defensive and offensive technology, and integrate its cyber core into an ACD's functional areas.

14. SUBJECT TERMS active cyber defense, ACD, cybersecurity, Japan, national security strategy	**15. NUMBER OF PAGES** 91
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

JAPAN'S PLEDGE FOR AN ACTIVE CYBER DEFENSE STRATEGY

Isabella C. Colandrea
Second Lieutenant, United States Air Force
BS, United States Air Force Academy, 2022

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(STRATEGIC STUDIES)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2023**

Approved by: Scott E. Jasper
Advisor

Robert J. Weiner
Second Reader

Afshon P. Ostovar
Associate Chair for Research
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This research examines why Japan has pledged to implement an active cyber defense (ACD) strategy. An ACD strategy enables nations to discover, detect, analyze, and mitigate threats in cyberspace. Although Japan's pacifist constitution limits its military capabilities, an ACD strategy would allow Japan to act in real-time to a detected intrusion and, if necessary, use offensive cyber capabilities. To answer why Japan pledged to adopt an ACD strategy, this research identifies the reasons why nations adopt an ACD strategy and reviews the risks associated with the strategy. Japan's decision to adopt an ACD strategy reflects its wish to decrease the number of new attackers, incorporate flexible layered cybersecurity techniques, and develop norms amongst allies. However, Japan's changing perceptions of its security environment, its relationship with the U.S., and its pacifist culture provide unique explanations for why Japan pledged to implement ACD. The research concludes with an evaluation of Japan's current cyber infrastructure and plans for implementation. Japan's current cybersecurity infrastructure provides a foundation for the future integration of ACD, but to ensure successful and safe employment of ACD, Japan must honor its planned pledges, compose an ACD doctrine, clarify its command structure, invest in an educated cyber core supported by defensive and offensive technology, and integrate its cyber core into an ACD's functional areas.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACD	Active Cyber Defense
CDU	Cyber Defense Unit
CYMAT	Cyber Incident Mobile Assistance Team
DBP	Defense Buildup Plan
DPB	Defense Programs and Budget
DOD	Department of Defense
GSOC	Government Security Organization Coordination Team
IISS	International Institute for Strategic Studies
JPCERT/CC	Japan Computer Emergency Response Team Coordination Center
MOD	Ministry of Defense
NCPI	National Cyber Power Index
NCSC	National Cyber Security Centre
NOCP	Defence National Offensive Cyber Programme
NISC	National Center for Incident Readiness and Strategy for Cybersecurity
NSS	National Security Strategy
OEWG	Open-Ended Working Group
PSIA	Public Security Intelligence Agency
SDF	Self Defense Force
SNMS	Systems and network management systems
USCYBERCOM	U.S. Cyber Command

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank my two thesis advisors, Dr. Jasper and Dr. Weiner, for their constant support and constructive feedback. Thank you both for your time and patience. I would also like to thank Professor George Lober (retired) for his assistance at the Graduate Writing Center. Thank you for providing valuable advice throughout the writing process.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

As Japan expands its military capabilities and perception of defense, the major research question this thesis asks is, why did Japan pledge to implement an active cyber defense (ACD) strategy? An ACD strategy allows nations to act in real-time to intrusions by enabling nations with the ability to discover, detect, analyze, and mitigate threats in cyberspace. Although Japan's pacifist constitution limits the nation's military capabilities, an ACD strategy allows the nation to use offensive cyber capabilities when an adversary intrusion is detected. Nations practicing the policy employ techniques such as honeypots, white worms, hack-backs, and other limited offensive actions or counterattacks after detection. However, when nations engage with actors on external networks to penetrate and neutralize servers, ACD methods may cause escalation and unintended collateral damage or fail to establish conducive cyber norms.

While Japan's government pledged to implement an ACD strategy, it has yet to outline a plan to achieve the pledge, and Japan's legislature has yet to approve the implementation. To evaluate Japan's decision to normalize cyber policy, this thesis answers the following related sub-questions: 1) What are the reasons for, and risks of adopting an ACD strategy? 2) Do the general factors that drive other nations to adopt an ACD strategy similarly influence Japan's decision, or does Japan's case reflect unique incentives and obstacles? and 3) What cyber related changes are necessary for Japan to execute an ACD strategy?

This chapter discusses the significance of the research, then outlines hypotheses attempting to answer the three sub-questions, followed by the research methodology and thesis overview. Relevant literature and scholarly arguments related to the sub-questions are woven into the chapters rather than presented in a stand-alone literature review section.

A. SIGNIFICANCE OF THE RESEARCH QUESTION

Cyber policy is essential to directing how a nation will operate in cyberspace and protect the domain from malicious actors. For example, in 2011, the U.S. Department of Defense (DOD) released its cybersecurity doctrine calling for the implementation of an

"ACD capability to prevent intrusions onto DOD networks and systems."[1] The strategy explains that an ACD framework allows the U.S. to detect and interrupt adversarial activity in real-time before an attack occurs on the DOD network or systems. ACD is a policy practiced by nations to secure the cyber domain; however, the term does not have a universal definition and consists of a range of methods. For this thesis, Robert Dewar's definition of ACD is used due to the research's methodology and the definition's acceptance in the field. Dewar's report defines ACD as

> an approach to achieving cyber security predicated upon the development of measures to detect, analyze, identify, and mitigate threats to and from communications systems and networks in real-time as well as the malicious actors involved. This requires that defenders have the capability and resources to take proactive or offensive action against threats as well as interact with malicious actors, both in the defended system and in those malicious actors' home networks.[2]

Dewar's analysis summarizes the commonalities between ACD interpretations and compares different cyber security policies to determine the utilization of an ACD strategy. Cyber scholar Dorothy Denning explains that "ACD is a direct defensive action taken to destroy, nullify, or reduce the effectiveness of cyber threats against friendly forces and assets."[3] An effective ACD strategy is a deterrence strategy. The strategy seeks to prevent the adversary from conducting malicious operations due to the defenders credible and convincing threats. The adoption of an ACD strategy by the DOD illustrates the evolution in the U.S. perception of the nature of cyberspace operations in the last decade.

Despite the U.S. DOD's adoption of ACD in 2011, U.S. cyberspace policy transitioned to a more offensive cyber policy known as persistent engagement and advocated for allied integration. Before 2018, U.S. cyber policy reflected a deterrence theory framework; however, nations operate in constant contact in cyberspace and

[1] U.S. Department of Defense, *Strategy for Operating in Cyberspace* (Washington, DC: Department of Defense, 2011), https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf, 6.

[2] Robert S. Dewar, "Active Cyber Defense" (ETH Zurich, 2017), https://doi.org/10.3929/ethz-b-000169631, 19.

[3] John Arquilla et al., "Active Cyber Defense: Applying Air Defense to the Cyber Domain," in *Understanding Cyber Conflict: 14 Analogies* (Georgetown University Press, 2017), 194.

adversaries continue to disrupt networks below the level of an armed attack. General Nakasone, Commander of U.S. Cyber Command (USCYBERCOM), explains that due to the nature of cyberspace operations, the U.S. must "compete with and contest adversaries globally, continuously, and at scale."[4] In an attempt to establish norms reflecting the nature of the domain, the U.S. adjusted its cyber policy to reflect the persistent engagement theory. The persistent engagement theory allows nations to act by anticipating and disabling malicious adversary operations before they act. Unlike ACD policy, persistent engagement permits action on external networks prior to an adversary's attack or detection within the defender's internal network. As the U.S. commits to a persistent engagement strategy in cyberspace – and transitions away from ACD while advocating for increased partner engagement – U.S. allies must understand how their current cyber policies fit into USCYBERCOM's new direction and how the offensive implications of persistent engagement may limit the U.S.'s call for integrated deterrence. The U.S.'s cyber policy evolution is particularly interesting for Japan, which is an important ally to the U.S. in the region, since Japan faces significant obstacles in implementing offensive-minded strategies like persistent engagement.

As Japan communicates its intent to modernize its military capabilities and increase military integration with allies, Japanese leaders face the decision of transforming cyber policy alongside their allies. In a 2023 joint press conference, President Biden and Prime Minister Kishida communicated their concerns for maintaining a secure Indo-Pacific region and stressed the importance of working with allies to deliver results on cybersecurity.[5] However, Japan's defensive constitution and pacifist culture does not align with the "defend forward" premise of U.S. persistence engagement theory methods. Article 9 of Japan's constitution guides the nation's use of force. Benjaman Bartlett explains that "Article 9 of Japan's constitution prohibits war making potential or the use of force or even the threat of force, as a political instrument…however…it does not deny the inherent right

[4] Paul M. Nakasone, "A Cyber Force for Persistent Operations," *Joint Force Quarterly: JFQ*, no. 92 (2019), 12.

[5] The White House, "Joint Statement of the United States and Japan," The White House, January 13, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/01/13/joint-statement-of-the-united-states-and-japan/.

to self-defense."[6] Japan's defense-oriented constitution creates a unique security environment in East Asia.

Japan's defense-oriented constitution and military infrastructure create unique hurdles for Japanese military normalization. Japanese normalization refers to Japan's changing defense posture and military buildup since the installment of their defense-oriented constitution following World War II. Over time, especially in the twenty-first century, Japanese military normalization has occurred. Japan is pledging to increase its defense budget, acquire counterstrike capabilities, and increase its role in security cooperations.[7] Japan's normalization efforts are driven by increasing regional threats and changing political attitudes, as well as U.S. encouragement to modernize its defense apparatus. Japan's most recent National Security Strategy (NSS) states that Japan must "strive to proactively foster a desirable security environment."[8] The strategy highlights Japan's desire to protect democratic values against nations not practicing these universal values. The strategy concludes that Japan is facing the "most severe and complex security environment since the end of WWII."[9] Japan's normalization has evolved in a gradual process of deciding whether and how to shift from more passive strategies to active or even persistent ones. Although Japan's move to an active cyber strategy is significant for the nation, its most recent NSS did not go as far as the United States' transition to a persistent engagement strategy in cyberspace. For the scope of thesis, the research uncovers why Japan is implementing ACD rather than why Japan did not adopt persistent engagement.

Japan's introduction of ACD principles, in the 2022 NSS, is still a shift in Japan's perception of cybersecurity. An ACD strategy would allow Japan to monitor potential hackers and neutralize their systems once a potential risk is established. Analyzing Japan's

[6] Benjamin Bartlett, "Japan: An Exclusively Defense-Oriented Cyber Policy," *Asia Policy* 27, no. 2 (2020): 93–100, https://doi.org/10.1353/asp.2020.0013, 94.

[7] Teresa Chen, Alana Nance, and Summer Han-ah, "Water Wars: Japan's Defense Buildup Signals a Shift Away from Post-WWII," *Lawfare* (blog), February 6, 2023, https://www.lawfareblog.com/water-wars-japans-defense-buildup-signals-shift-away-post-wwii.

[8] National Security Council, *National Security Strategy of Japan* (Tokyo, Japan: Ministry of Foreign Affairs of Japan, 2022), https://www.mofa.go.jp/fp/nsp/page1we_000081.html, 1–2.

[9] National Security Council, 25.

decision to implement an ACD strategy aids in understanding the nation's normalization tendencies and constraints in modernizing the cyber domain, as well as the complications of varying cyber policy between strong allies. The U.S.'s 2022 NSS emphasizes the importance of integrated deterrence and calls upon partner integration in developing a cooperative deterrence posture.[10] Similarly, the U.S.'s 2023 Cybersecurity Strategy prioritizes allied and partner collaboration. The strategy insists that the U.S. will work with "allies and partners to strengthen norms of responsible state behavior" in the domain.[11] However, the U.S. and Japan are implementing cyber strategies that employ cyber tools and methods at different times in the intrusion timeline. For integrated deterrence to be successful and to establish responsible international cyber norms, the U.S. and Japan must understand each other's respective perceptions of successful cyber strategies.

Still, the basic nature of cyberspace operations and cyber threats do not differ for Japan. Japanese leaders must follow through on their commitment to an ACD posture in order for the policy to deter adversary aggression. Japanese leaders have yet to clearly define and agree upon their perception of ACD strategy. While Prime Minister Kishida's Cabinet supported the implementation of an ACD strategy, Japan's Diet has tabled the discussion of implementing the pledge. Similarly, the language within Japan's NSS is vague and leaves aspects of the policy up to interpretation. The strategy outlines that "for serious cyberattacks that pose security concerns against the Government, critical infrastructure, and others, the Government will be given the necessary authorities…[to] allow it to penetrate and neutralize attacker's servers and others in advance to the extent possible."[12] In addition to the policy's subjectivity, Japan has not released a new Cybersecurity Strategy document or ACD doctrine for future operations. Japan's Defense Buildup Plan (DBP) called for an increase of cyber personnel by 2027 and an improvement to cyber education within the military. The document did not outline plans for the

[10] The White House, *National Security Strategy of the United States of America* (Washington, DC: White House, 2022), https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf, 22.

[11] The White House, *National Cybersecurity Strategy* (Washington, D.C.: White House, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/, 2.

[12] National Security Council, National Security Strategy of Japan, 22–23.

acquisition of offensive cyber capabilities, define a clear cyber leadership/organization chart, or outline necessary legal changes for its Self Defense Force (SDF) law. This raises the question of how Japan's current cyber infrastructure will need to change in order to properly implement this policy change, given concerns associated with an ACD strategy. Japanese leaders must now weigh the political, social, and procurement constraints of practicing an ACD strategy against their perception of cyber threats that jeopardize Japan's national security.

B. POTENTIAL EXPLANATIONS AND HYPOTHESIS

This research utilizes the three sub-questions as a method to determine why Japan's government leaders supported the implementation of an ACD strategy, how the factors that enable Japan's normalization efforts relate to the cyber domain, and what cyber related changes are necessary for Japan to execute an ACD strategy.

Chapter II's research analyzes the general reasons and risks for a nation to adopt an ACD strategy. This thesis hypothesizes that given the nature of current cyberspace operations, the reasons for a nation to adopt an ACD strategy outweigh the possible risks associated with the policy. The U.S. introduced an ACD strategy in 2011 with the goal of mitigating malicious cyber-attacks and deterring adversary activity. Similar to the U.S.'s decision making process, the possible reasons for Japan's government deciding to pursue an ACD strategy are to prevent future malicious cyber activity and to possibly establish favorable cyber norms alongside like-minded allies. However, implementing ACD also requires the use of limited offensive actions that can possibly cause escalation and unintended collateral damage, or fail to establish responsible cyber norms. After identifying the reasons and risks associated with ACD, this research evaluates how the reasons and risks associated with a nation adopting an ACD strategy explain why Japan pledged to a new cybersecurity policy.

This thesis compares the reasons why Japan's government is pursuing an ACD strategy to the general factors outlined in Chapter II. Chapter III determines how Japan's case is similar and different to the general reasons for implementation. Japan's perception of defense is evolving as regional actors exhibit more aggressive rhetoric and practice

undesirable behavior. In the 21st century, Japan increased its security capabilities to counter regional security threats. Shelia Smith, in her book *Japan Rearmed*, explains that "Japan has relaxed its restraints on its military, and the [Self Defense Force] plays a far more visible role in national policy."[13] In addition to the changing security environment, the U.S.-Japan alliance contributes to Japan's perception of defense. The U.S. has repeatedly called upon Japan to increase its defense cooperation in order to contribute to extended deterrence.[14]

Japan's government may be supporting the implementation of an ACD strategy in cyberspace because leaders view current policy inadequate in addressing adversary activity in cyberspace. Japan may have pledged to implement an ACD strategy because it perceived cyberspace as a vulnerable warfighting domain and current counter measures as unable to maintain the cyber domain's integrity against adversary cyber activity. Japan may have perceived the escalation risks and possible collateral damage as less detrimental to their security than the status quo. Therefore, this thesis hypothesizes that Japan's government decided to follow an ACD policy in its NSS to support the establishment of acceptable cyber norms alongside allied initiatives, to maintain a strategic advantage, and to combat malicious cyber actors. Although Japan's government may be pursuing cyber normalization, it is important to evaluate how capable and integrated Japan's cyber infrastructure is by evaluating where Japan's technical cyber apparatus stands.

The third question of this research discusses what cyber related changes are necessary for Japan to execute an ACD strategy. This thesis hypothesizes that Japan's current cyber infrastructure is not yet able to support the shift to an ACD strategy. This thesis investigates how Japan's current cyber infrastructure limits Japan's ability to execute an ACD strategy. ACD emphasizes detection, but the theory still requires the defender to hold the ability to neutralize the attacker once detected. Japan's strategy will fail if adversaries do not perceive Japan's ACD measures to be convincing. Employing an ACD

[13] Sheila Smith, *Japan Rearmed: The Politics of Military Power* (Cambridge: Harvard University Press, 2019), 4.

[14] The White House, "U.S.- Japan Joint Leaders' Statement," April 17, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/16/u-s-japan-joint-leaders-statement-u-s-japan-global-partnership-for-a-new-era/.

strategy requires specific capabilities alongside proper signaling to adversaries and commitment to threats. It is necessary to determine the state of Japan's cyber infrastructure due to decades of investment in military defensive technology and limited military normalization before the 21st century. After formal adoption, shifting to an active defense strategy may take years even if Japan does invest in updates in the cyber domain and implement necessary command structures that support the implementation of the strategy. It is possible that U.S. investment into Japan's cyber apparatus may speed up Japan's shift to an ACD strategy. Additionally, an increase of adversary cyber activity may entice Japan to quickly integrate ACD methods.

C. RESEARCH DESIGN

This research analyzes components of the main research question to determine the applicability of the three hypotheses. The thesis utilized primary and secondary sources to determine the motivation for Japan's adaptation of an ACD strategy in the 2022 NSS. Scholarly literature on Japanese normalization efforts is analyzed to investigate why and how Japanese military normalization occurs. First, to determine the reasons and risks associated with an active defense strategy, this thesis relied upon published literature discussing the justifications and implications of adopting the strategy. Second, to understand how the general factors for adaptation of the strategy relate to Japan, the research reviewed the state of Japan's current passive cyber methods. The chapter utilized scholarly research and primary sources from Japan's government leaders to determine what motivates the nation's military normalization and how those factors relate to cyber normalization. Third, Japan's current SDF cyber apparatus, infrastructure, and structure is evaluated and compared to the basic general foundations of ACD strategy to determine the cyber related changes necessary to practice a successful ACD strategy.

D. THESIS OVERVIEW

The thesis is divided into five chapters. The introduction of this thesis serves as an overview of the research questions, hypotheses, and methodology. Chapter II reviews literature discussing what an ACD strategy is to determine the general reasons and risks associated with the strategy. Chapter III analyzes how the factors determined in Chapter II

relate to Japan's decision to adopt the strategy. The chapter also investigates how Japan's case differs from the general reasons for adoption. Chapter IV evaluates Japan's current cyber apparatus and plans for implementation, as well as identifies the necessary changes required if the nation was to formally implement a successful active defense strategy. Finally, Chapter V concludes with discussion of the research, recommendations for policy makers, and proposals for future research.

THIS PAGE INTENTIONALLY LEFT BLANK

II. GENERAL REASONS AND RISKS OF ACD STRATEGY

To determine why Japan pledged to implement an ACD strategy it is necessary to outline why any nation would transition to the strategy. This chapter reviews the literature on ACD to determine the general reasons and risks for adopting an ACD strategy. The first section of this chapter discusses the general reasons why a nation implements an ACD strategy, and the second section reviews the risks associated with the policy. After reviewing the literature on ACD, the chapter concludes that nations adopt an ACD strategy in order to harden their cyber infrastructure and deter future attacks through the integration of layered defensive and offensive cyber methods. Nations also commit to the guidelines of ACD strategy to aid in the development of responsible cyber behavior. The risks associated with the policy include escalation due to misattribution and unintended collateral damage. Implementing safeguards can reduce the possibility of these risks.

A. REASONS FOR ADOPTING ACD STRATEGY

The main reason for adopting an ACD strategy is to ensure better cybersecurity and decrease adversary intrusions. Once implemented, ACD strategy allows nations to respond in real-time to detected intrusions and prevent future intrusions. As noted in the previous chapter, Denning explains that "active cyber defense is a direct defensive action taken to destroy, nullify, or reduce the effectiveness of cyber threats against friendly forces and assets."[15] When a nation invests in ACD strategy and technology, its goal is to convince adversaries that the layered defensive cyber infrastructure and limited offensive tools available to the defender are not worth an attack. ACD strategy does not necessarily mean that the number of attempted attacks will automatically decrease. However, ACD methods will enable better detection and prevention, while attempting to prevent the adversary from conducting malicious operations due to the defender's credible convincing threats. Over time, if the strategy is implemented successfully, ACD methods can become a deterrent to adversaries and possibly reduce the number of attempted attacks.

[15] Arquilla et al., "Active Cyber Defense: Applying Air Defense to the Cyber Domain."

ACD is reliant upon elements of deterrence policy. The strategy is only successful if the defender's threats are viewed as credible by the opponent, the defender's properly signals to the adversary, and the defender follows through with its threats. Thomas Schelling's book *Arms and Influence* articulates how military capabilities, specifically nuclear weapons, shape international relations through elements of power, coercion, and bargaining. He explains that "the threat of damage, or of more damage to come…[makes] someone yield or comply."[16] Schelling adds that expressed threats must be viewed as credible and rational by the opponent. He also notes that the deterring nations must be committed to following through on their threats. For coercion to work in the cyber domain, the defender's communicated offensive course of action must force the adversary to weigh the costs of imposing harm on another network and influence the adversary to not follow through. Even if the actor is unknown, active cyber methods can deter the adversary from initially acting and in turn strengthen the nation's defenses. Joseph Nye also examines how power and deterrence are related to cyber methods in modern conflicts. Nye's analysis remarks that "offensive capabilities for immediate response can create an active defense that can serve as a deterrent even when the identity of the attacker is not fully known."[17] In addition to Nye, Robert Jervis considers how the cyber domain relates to deterrence strategy. Jervis argues that the domain's unique characteristics "leave some fundamental principles of deterrence intact and introduces new elements."[18] Cyber operations occur quickly, and, in some instances, attacks are difficult to attribute. Still, ACD is a deterrence policy attempting to strengthen a nation's cyber infrastructure and prevent intrusions by an adversary. Through the implementation of limited offensive cyber techniques, the defender can communicate the threat of these tools in order to prevent future attacks.

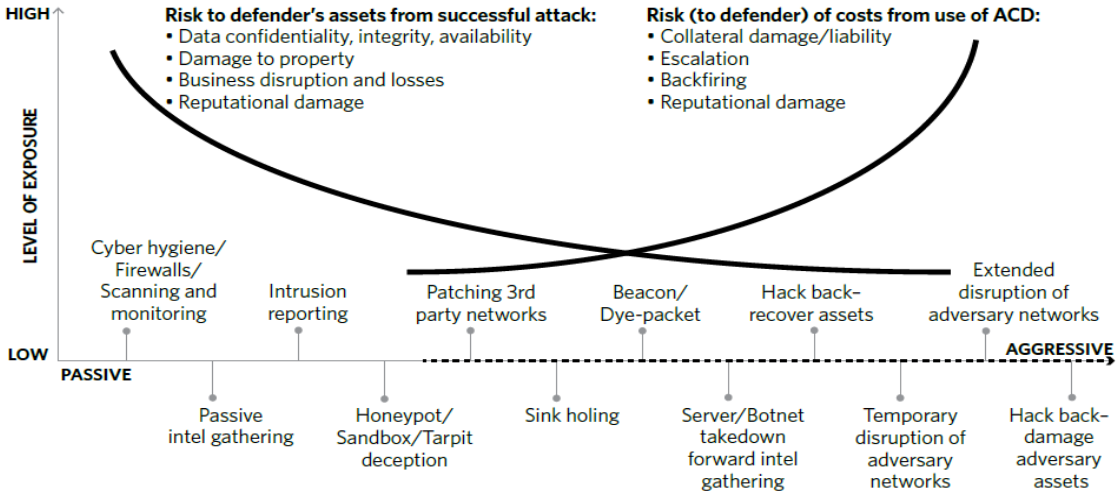
The successful implementation of an ACD strategy allows for a spectrum of responses to adversary cyber behavior. An ACD policy implements the means to detect,

[16] Thomas C. Schelling, *Arms and Influence*, Veritas paperback edition., Veritas Paperbacks (New Haven, CT: Yale University Press, 2020), https://doi.org/10.12987/9780300253481, 3.

[17] Jr Nye, "Cyber Power," *Belfer Center for Science and International Affairs*, May 2010, https://apps.dtic.mil/sti/citations/ADA522626, 17.

[18] R. Jervis, "Some Thoughts on Deterrence in the Cyber Era," *Journal of Information Warfare* 15, no. 2 (2016): 66–73, 67.

analyze, identify, and mitigate threats. Wyatt Hoffman and Ariel Levite explain that ACD "includes a diverse range of cyber measures and practices."[19] They continue by explaining the range of ACD activity from less aggressive measures, such as intrusion-prevention systems, to the most aggressive measures of ACD, such as hack-backs. Hoffman and Levite demonstrate how ACD measures occur on a spectrum depending on the tool utilized. Figure 1 demonstrates the range of ACD methods from passive to aggressive.



Source: Hoffman, Wyatt, and Ariel E. Levite. "Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?" *Carnegie Endowment for International Peace*, 2017. https://search.proquest.com/docview/1917694386?pq-origsite=primo, 20.

Figure 1. Spectrum of ACD Methods and Balancing Cyber Risks

ACD is not a single or extreme action. It is the implementation of various cybersecurity methods. MJ Herring and KD Willett emphasize how ACD strategy is designed to "accommodate a wide spectrum of…scenarios with performance occurring in cyber-relevant time."[20] They add that the integration of various tools is a strength to ACD

[19] Wyatt Hoffman and Ariel E. Levite, "The Spectrum of Active Cyber Defense," Private Sector Cyber Defense (Carnegie Endowment for International Peace, 2017), https://www.jstor.org/stable/resrep26906.7, 7.

[20] Mj Herring and Kd Willett, "Active Cyber Defense: A Vision for Real-Time Cyber Defense," Journal of Information Warfare 13, no. 2 (2014): 46–55, 47.

strategy. The variety of tools available to the defender comes from the implementation of layered cybersecurity techniques. Herring and Willett explain that ACD includes three methods—proactive, active, and regenerative—that occur simultaneously.[21] They go on to assert that proactive defenses harden the system, active measures halt real-time damage, and regenerative methods remediate the system following a successful attack. Developing layered cyber defense measures gives a nation more protection and flexibility.

Leading cybersecurity nations have strengthened their cyber apparatus with ACD methods. The United Kingdom adopted an ACD strategy in 2016. The U.K. stated that "ACD is the principle of implementing security measures to strengthen a network or system to make it more robust against attack."[22] Stuart Russell and Nadiya Kostyuk summarized the U.K.'s National Cyber Security Centre (NCSC) published report on the strategies programs. They highlight how "after only one year, the ACD program is already making a difference to cyberspace in the United Kingdom."[23] They go on to discuss that the ACD program brought about positive results and better protected the government and public from cybersecurity threats. However, it is important to note that U.K.'s ACD program is different to Japan's current pledge. A King's College London research report wrote that "the U.K's understanding of active cyber defence differs from other countries' more offensive-minded interpretations of the term. ACD is purely defensive in the UK context and does not hint at 'hacking back' or other actions that risk escalation or retaliation."[24] The report goes on to explains that the U.K.'s joint GCHQ/Ministry of Defence National Offensive Cyber Programme (NOCP) ability and willingness to employ offensive cyber capabilities are not a part of the ACD program the U.K. launched. Still, the less aggressive ACD methods are beneficial to a nation's overall cybersecurity.

[21] Herring and Willett, 46–47.

[22] HM Government, "National Cyber Security Strategy 2016–21," November 2016, https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021, 33.

[23] Russell and Kostyuk, "Evaluating the U.K.'s 'Active Cyber Defence' Program," Lawfare, February 14, 2018, https://www.lawfareblog.com/evaluating-uks-active-cyber-defence-program.

[24] Tim Stevens et al., "UK Active Cyber Defence: A Public Good for the Private Sector," *Policy Institute at King's College London*, January 2019, 4, 10.

Another reason nations may commit to an ACD strategy is to work alongside allies in the development of conducive cyber norms. Cybersecurity has become a national security issue for three reasons: the global reliance on the cyber domain, the use of cyber operations as an instrument of power, and low barrier of entry for malicious actors. As democratic nations seek to secure the cyber domain and counter adversary aggression, allied nations must collaborate to determine a cyber policy that establishes desired international cyber norms. As noted earlier, the U.K. adopted an ACD strategy in 2016 and the U.S. implemented a persistent engagement strategy in cyberspace in 2018. Neither strategy is solely a passive defensive system. Both strategies require a more active role in cyberspace, but at different levels. ACD allows for the use of limited offensive cyber techniques after intrusion. Persistent engagement in cyberspace allows for nations to disable a potential attack prior to detected intrusions on the defenders' network. Despite the strategies' differences, the two strategies illustrate how prominent nations on the international stage are altering their perspective on how to secure the domain. Norms guide nations' behavior in cyberspace and developing similar policies in cyberspace allows nations to collaborate more efficiently. In James Lewis's commentary on the U.N. Open-Ended Working Group's (OEWG) framework for responsible cyberspace behavior, he argues that "actions by one nation, no matter how powerful, are likely to be ineffective. The same is true for responses that are sporadic and occasional."[25] For Western nations to achieve their desired norms in the cyber domain, a majority must agree to how they will respond to attackers and consistently follow through on their guidelines.

If nations have conflicting cyber strategies or differ on what defensive responses are acceptable, then no norms will be developed. Experts at the NATO Cooperative Cyber Defense Center noted the development of cooperative measures, through means such as national cybersecurity strategies and legislation, can "strengthen [nations] collective capacity to deal with…cyber threat [s]."[26] Developing similar cybersecurity strategies that

[25] James Andrew Lewis, "Creating Accountability for Global Cyber Norms," February 23, 2022, https://www.csis.org/analysis/creating-accountability-global-cyber-norms.

[26] Anna-Maria Osula and Henry Roigas, eds., *International Cyber Norms: Legal, Policy & Industry Perspectives* (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2016), https://ccdcoe.org/library/publications/international-cyber-norms-legal-policy-industry-perspectives/, 140.

outline comparable capabilities, structures, and guidelines allows nations to work alongside one another more effectively, as well as aid in the development of acceptable cyberspace behavior.

In summary, nations adopt an ACD strategy for its efficiency and protection of the nation's cyber infrastructure. The method provides the user with a layered defensive system incorporating a spectrum of cybersecurity techniques. The implementation of the strategy to harden the system, halt real-time damage, and remediate the system can encourage responsible behavior in cyberspace. Still there are risks associated with the policy that nations consider when adopting the most aggressive ACD methods.

B. RISKS OF IMPLEMENTING AN ACD STRATEGY

The risks associated with adopting an ACD strategy that penetrates external systems to halt damage include the possibility for escalation and increased tension amongst nations due to misattribution and unintended damage. To properly employ the most aggressive measures of ACD techniques seen in Figure 1, the defender must first establish where the attack originates from. Unintended follow-on incidents may occur politically, economically, or even militarily if attribution is not properly assigned. Sean Harrington summarizes the concerns cybersecurity experts have with employing these ACD methods. He discusses that before a defender utilizes techniques such as hack-backs, they "would not only have to establish proper intent, but also attribution."[27] He goes on to point out that the most aggressive ACD activity can lead to misattribution, collateral damage, and escalation. If a nation incorrectly identifies the malicious actor or is unable to accurately identify who conducted the intrusion, but still engages with offensive ACD techniques, the nation risks future political hostility. A nation that wishes to execute the limited offensive measure provided in ACD's framework must correctly determine the malicious actor or risk misattribution.

The risk of escalation is heightened if a nation's cyber infrastructure is inadequate in practicing and carrying out ACD methods external to the network. If a nation commits

[27] Sean L. Harrington, "Cyber Security Active Defense: Playing with Fire or Sound Risk Management?," *Richmond Journal of Law & Technology* 20, no. 4 (2014), 41.

to an ACD policy and its technical mechanisms are unprepared, it may jeopardize political stability and increase the probability for escalation. Hoffman and Levite discuss how ACD risks are "especially pronounced if the defender is ill-equipped to attribute the attack and control its effects."[28] Executing offensive ACD methods takes preparation, training, and experience. When a nation decides to initiate an attack in response to an intrusion, it risks causing unintended damage within other nation's systems, and possibly civilian systems. While ACD methods would not cause physical harm, Sasha Romanosky and Zachary Goldman note that the manipulation of data may lead to financial, political, and other consequences.[29] In their analysis of cyber collateral damage they argue that "only when cyber operators can predict in advance what the intended consequences of their operations may be, can they design meaningful approaches to mitigate unwanted and harmful effects."[30] The defender who conducts an attack risks escalation if its cyber technicians are unable to confidently predict collateral damage and create mitigate measures. To decrease the possibility for escalation, nations must develop capable cyber operators aware of ACD method consequences and understand mitigation methods.

Nevertheless, an ACD strategy can reduce these risks if safeguards are integrated and effective. To reduce the threat of escalation, collateral damage, and misattribution, nations can employ measures to reduce these risks. David Herpig's report addressing ACD operations highlights safeguards to reduce concerns. The safeguards he outlines include defining the scope, establishing a national legal framework, setting up guidelines for tools and services, and also adapting confidence-building measures.[31] ACD risks can be mitigated if a nation can confidently employ its limited offensive tools, communicate to the aggressor, and develop oversight. Similarly, Scott Jasper explains that "through open

[28] Wyatt Hoffman and Ariel E. Levite, "Rethinking Corporate Active Cyber Defense," Lawfare, July 17, 2017, https://www.lawfareblog.com/rethinking-corporate-active-cyber-defense.

[29] Sasha Romanosky and Zachary Goldman, "What Is Cyber Collateral Damage? And Why Does It Matter?," *Lawfare – Cybersecurity & Tech* (blog), November 15, 2016, https://www.lawfaremedia.org/article/what-cyber-collateral-damage-and-why-does-it-matter.

[30] Sasha Romanosky and Zachary Goldman, "Understanding Cyber Collateral Damage," *Journal of National Security Law & Policy* 9, no. 2 (2017): 233–57, 256.

[31] David Herpig, "Active Cyber Defense Operations: Assessment and Safeguards" (Transatlantic Cyber Forum, November 2021), https://www.stiftung-nv.de/sites/default/files/active_cyber_defense_operations.pdf.

communication of intentions to deliver credible responses outside the network, coupled with emergence of automated capability to stop attacks inside the network, ACD is well postured to serve as an alternative strategy to achieve deterrence within the cyber arena."[32] Nations that utilize automated platforms for detection inside the network and communicate their objective in response outside the network can safely prevent against intrusion in real-time. Still, to mitigate risks and employ these safeguards, nations must develop the necessary personnel and cyber cadre to oversee ACD methods. While ACD methods may have risks, an effective safe employment of ACD methods can deter adversaries from pursuing malicious cyberattacks.

In addition to ACD's technical liabilities, the long-term success of ACD policy is unknown since the policy is uncommon and benchmarks for success must be determined. As a consequence, nations may fail to establish their desired norms. Rather than contributing to desired global cyber norms, committing to an ACD strategy may contribute to a more contentious domain. Employing ACD techniques external to one's own network can create a precedent for more aggressive cyber techniques. Jervis points out that the political implications of offensive cyber weapons are still unknown and cautions against allowing nations to view the domains as lawless.[33] When nations commit to the most aggressive ACD policies and practices they contribute to a precedent within the international community in the cyber domain. A precedent of more offensive ACD methods may cause adversaries to carry out similar methods. As Hoffman and Levite point out, unrestricted ACD conduct could result in opponents utilizing similar techniques and increasing tensions amongst already hostile nations.[34] Even if an adversary does not have the same means as the defender, the adversary could reuse and recycle code implemented by the defender.

Furthermore, there is debate over whether ACD and a deterrence framework is effective in countering adversary cyber operations. Given the constant contact, speed, and

[32] Scott Jasper, *Strategic Cyber Deterrence: The Active Cyber Defense Option* (Lanham, Maryland: Rowman & Littlefield, 2017), 185.

[33] Jervis, "Some Thoughts on Deterrence in the Cyber Era," 67.

[34] Hoffman and Levite, "Rethinking Corporate Active Cyber Defense."

anonymity within the cyber environment some argue that applying elements of deterrence are challenging, as well as unapplicable. Mariarosaria Taddeo discusses the limitations of a deterrence framework in the cyber domain by examining to what extent aspects of deterrence theory are effective. She argues that in cyberspace, defense is required, "but primarily as a means to guarantee the resilience of a system once an attack has been launched (and also after it has breached the system), rather than as a means of deterring attackers."[35] Taddeo goes on to point out that mitigating risks following an attack is not avoiding conflict. Similarly, Michael Fischerkeller, Emily Goldman, and Richard Harknett argue that a deterrence framework is failing to protect nation-states from adversary behavior.[36] Goldman argues that a paradigm shift has occurred within USCYBERCOM to combat the malicious operations carried out within the domain.[37] Due to the limitations that a deterrence policy allows, the U.S. committed to a persistent engagement strategy in 2018. Unlike an ACD policy, a persistent engagement strategy allows a nation to disable an attack on an external network before an intrusion is detected.

Other scholars note that committing to more escalatory policy is worrisome for allies, sets an undesired precedent for adversaries, and can lead to unintended conflict. Although deterrence analogies are argued by some to be ineffective in the cyber domain due to the constant interaction in cyberspace and ubiquitous anonymity, policy makers should be aware of the concerns associated with adopting policies. Max Smeets argues that a nation committing to a being a disrupter in the domain can cause "friction by allies undermining trust" and allied nations adopting a similar policy could "further undermine the alliance relationship."[38] Similar to Hoffman and Levite, Smeets also points out that offensive techniques could be utilized by opponents. Jason Healey also analyzes the

[35] Mariarosaria Taddeo, "The Limits of Deterrence Theory in Cyberspace," *Philosophy & Technology* 31, no. 3 (2018): 339–55, https://doi.org/10.1007/s13347-017-0290-2, 347.

[36] Michael P. Fischerkeller, *Cyber Persistence Theory: Redefining National Security in Cyberspace*, Bridging the Gap (New York, NY: Oxford University Press., 2022), 23.

[37] Jacquelyn Schneider et al., "Ten Years In: Implementing Strategic Approaches to Cyberspace," *U.S. Naval War College* Special Collections (2020), https://digital-commons.usnwc.edu/usnwc-newport-papers, 31.

[38] Max Smeets, "U.S. Cyber Strategy of Persistent Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection," *Intelligence and National Security* 35, no. 3 (2020): 444–53, https://doi.org/10.1080/02684527.2020.1729316, 6.

strengths and weaknesses of adopting a cyber policy not reflective of deterrence principles. Healey comments that committing to USCYBERCOM's policy may result in "mistakes, misperception, and miscalculations."[39] Although adopting an ACD strategy includes risks, the strategy's offensive measures and guidelines for when offensive methods can be utilized by the defender are less aggressive than the persistent engagement theory. Adopting an ACD strategy may result in unintended damage and conflict amongst nations; however, the outcome of ACD strategy does not risk as much as persistent engagement that relies on preemption before an intrusion is detected.

C. CONCLUSION

Nations adopt an ACD strategy to develop a more robust cybersecurity infrastructure able to mitigate intrusions and deter future attacks. Integrating a layered defensive system with limited offensive capabilities allows the defender a variety of tools to ensure security. ACD strategy is not the most aggressive cyber strategy a nation can implement since the strategy requires initial intrusion and allows the defender flexibility in determining their responsive techniques. Although offensive measures include risks, there are means to reduce the possibility of misattribution and escalation. Implementing safeguards such as developing a proficient cyber core able to mitigate risks and communicate intentions to adversaries can reduce the liabilities correlated with the most aggressive aspects of the strategy.

[39] Jason Healey, "The Implications of Persistent (and Permanent) Engagement in Cyberspace," *Journal of Cybersecurity* 5, no. 1 (January 1, 2019): tyz008, https://doi.org/10.1093/cybsec/tyz008, 11.

III. FACTORS INFLUENCING JAPAN'S PLEDGE FOR ACD

Japan's pacifist constitution and self-defense force restrict its ability to enact policies most nations pursue when modernizing their national defense apparatus. Japan's unique political, military, and social limitations raises the question: how do the general factors that drive other nations to adopt an ACD strategy similarly influence Japan's decision? Or does Japan's case reflect unique incentives and obstacles? The first section of this chapter will review how Japan's decision to pledge an ACD strategy relates to the general reasons and risks associated with the policy. The second section of the chapter will investigate factors unique to Japan's case that motivated its government to pledge to an ACD strategy. This analysis determines that the general reasons for adoption – intrusion mitigation, development of norms alongside allies, and layered defense – are all reflected in Japan's decision to pledge to an ACD strategy. However, there are reasons specific to Japan's case. Japan's perception of its security environment, cyber-attacks from regional actors, and the U.S.-Japan alliance are all unique reasons why Japan's government announced its pledge to an ACD strategy. Similarly, Japan's defensive constitution and pacifist society introduce a new set of explanations for why Japan pledged to adopt an ACD strategy compared to other more aggressive cyber policies. Japan's case still reflects the general concerns policy makers express when discussing ACD's risks; however, Japan's pacifist constitutional heightens the manner in which Japan weighs the risks associated with the policy.

A. JAPAN'S SIMILARITIES TO GENERAL REASONS FOR ADOPTION

Japan's recognition of cyber as a national security issue and its new perception of future defense is encouraging the nation's leader to adopt an ACD strategy. The government's perception of cybersecurity and success in halting detected attacks with its passive cyber strategy contributed to Japan's cyber normalization evolution. Yet empirical evidence and Japan's new defense strategies showcase its recognition that current passive defensive methods are failing to protect against new attacks, and aid in explaining why new policy is being considered. Achieving decreased intrusions and the option to utilize

various cybersecurity methods on top of Japan's defensive cyber capabilities reflect the general reasons why Japan would pledge to an ACD strategy. In addition to cyber specific reasons, Japan is also pledging to an ACD strategy to develop responsible cyber norms alongside allies.

Japan's government leaders across the political spectrum and various interest groups in Japan agree that securing the cyber domain is essential to the nation's prosperity. Japan's recognition of the domain's importance motivates the nation to discover methods which decrease the threat of intrusions. A Congressional Research report noted in the early 2000s that Japan's government cyber efforts were perceived as weak, until "high-profile cyberattacks…affected Japan, the United States, and South Korea between 2009 to 2014 raised awareness of the issue."[40] They add that the awareness from the attacks paved the way for Japan's cybersecurity legislation. Paul Kallender and Christopher Hughes, in their article discussing Japan's evolution as a 'cyber power', argue that since the late 2000s "Japanese policy-makers from all political spectrums and agencies, and provided with some momentum under the...Abe...administration, have moved cybersecurity to the very core of national security policy to create more centralized institutions for formulating responses on cyber security."[41] They go on to conclude that Japan's perception of cybersecurity experienced a swift move towards centralization and expanded the military's role in the domain. Recognizing cyber espionage as a national security issue justified Japan's initiation of cyber legislation and protection at the national level. Gradual centralization of the cybersecurity apparatus established the foundation for national cybersecurity strategy. Japan stated in its most recent NDS that there are "increasing serious risks in the cyber and other domains" [42] and note that the "way of warfare has also drastically changed."[43] Japan's recognition of the cyber domain as a national security issue

[40] Emma Chanlett-Avery and Caitlin Campbell, "The U.S.-Japan Alliance" (Congressional Research Service, June 13, 2019), https://crsreports.congress.gov/product/pdf/RL/RL33740, 48.

[41] Paul Kallender and Christopher W. Hughes, "Japan's Emerging Trajectory as a 'Cyber Power': From Securitization to Militarization of Cyberspace," *Journal of Strategic Studies* 40, no. 1–2 (2017): 118–45, https://doi.org/10.1080/01402390.2016.1233493, 138.

[42] National Security Council, *National Defense Strategy* (Tokyo, Japan: Ministry of Foreign Affairs of Japan, 2022), https://www.mofa.go.jp/fp/nsp/page1we_000081.html, 5.

[43] National Security Council, 8.

and the changing nature of warfare explains why Japan is considering new cybersecurity policy. Similar to ACD strategy's objective, Japanese leaders wish to accomplish intrusion mitigation at the national level in order to secure the domain and protect the nation's prosperity.

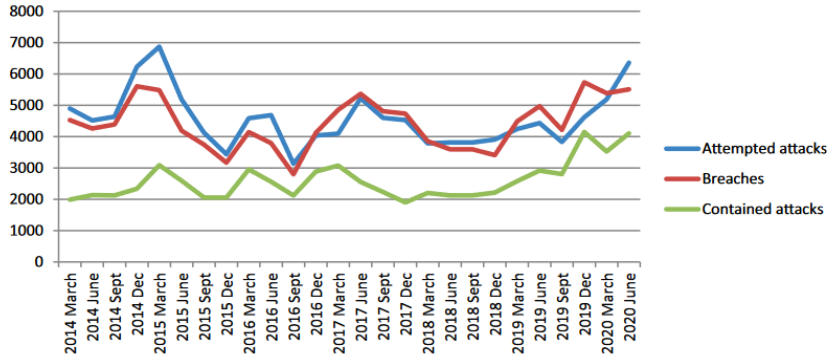
In addition to government officials, other groups within Japan's society recognize how important securing the cyber domain is and believe intrusion mitigation is essential to the nation's prosperity. Nori Katagiri's analysis on the role of interest groups in democracies uncovers, in a Japanese case study that "interested groups have worked closely with the government to strengthen defense against cyberattacks."[44] He goes on to point out that Japan's three main interest groups – industry unions, policy advocacy groups, and academics – believe in security advancement in the cyber domain. These groups showcase how securing the domain is viewed as an essential issue within society's interest groups. Japan's overall recognition of cybersecurity as a national security issue and the desire to secure the domain explains why Japan's government is considering new ways to ensure intrusion mitigate.

Despite Japan's desire to achieve a secure domain and reduce intrusions, Japan's passive cyber methods are failing to prevent new attackers and motiving Japanese political leaders to consider other cyber strategies. Japan's previous cybersecurity methods are proving to be ineffective. The Japan Computer Emergency Response Team Coordination Center (JPCERT/CC), publishes quarterly reports that overview incidents.[45] As shown in Figure 2, the number of attempted cyberattacks within Japan has increased since 2019. Katagiri discovers through empirical data from the JPCERT/CC that Japan is able to utilize passive defense to "suppress a rise in the number of breaches, [but] it is not deterring new attack. In other words, even if passive defense may have deterred some [attacks], it has

[44] Nori Katagiri, "The Soft Underbelly of Cyber Defence in Democracy: How Interest Groups Soften Japan's Cyber Policy," *Journal of Cyber Policy* 7, no. 3 (September 2, 2022): 336–52, https://doi.org/10.1080/23738871.2023.2192227, 347.

[45] "JPCERT/CC Incident Handling Quarterly Report," n.d., https://www.jpcert.or.jp/english/ir/report.html.

not…[deterred] to the extent that we see a reduction in the number of attacks."[46] Katagiri's data analysis highlights how passive cyber defense is able to detect and halt intrusions, but not doing enough to deter new attacks. Japan's inability to deter new cyber-attacks with its passive defense system aid in explaining why Japan is pledging to a new cyber policy.



Source: Katagiri, Nori. "From Cyber Denial to Cyber Punishment: What Keeps Japanese Warriors from Active Defense Operations?" *Asian Security* 17, no. 3 (September 2, 2021): 331–48. https://doi.org/10.1080/14799855.2021.1896495, 336.

Figure 2. JPCERT/CC Reported Cyberattacks on Japan 2014–2020

Cyber-attacks and intrusions from adversaries are also motivating Japan to reevaluate its cyber strategy. The primary adversarial threats Japan faces in the domain originate from China, Russia and North Korea. Barlett discusses how cyber threats from these nations threaten Japan's national security. He writes that "China, has…stolen information from a number of Japanese public and private organizations. Likewise, North Korea has hacked into and stolen money from Japanese Bitcoin exchanges. Russia does not yet seem to have targeted Japan, but Japan has noted Russia's activities elsewhere."[47] Cyber espionage affects Japan's overall stability. James Lewis explained in a Nikkei Asia article that "Japan is a primary target for Chinese cyber activities both for traditional

[46] Nori Katagiri, "From Cyber Denial to Cyber Punishment: What Keeps Japanese Warriors from Active Defense Operations?," *Asian Security* 17, no. 3 (September 2, 2021): 331–48, https://doi.org/10.1080/14799855.2021.1896495, 337.

[47] Bartlett, "Japan: An Exclusively Defense-Oriented Cyber Policy," 93.

political/military intelligence gathering, and also for economic espionage."[48] Cyber aggression threatens Japan politically, militarily, and economically. Bartlett states that Japanese leaders believe adversaries "will use 'grey zone' operations that do not rise to the level of military force in order to change the status quo."[49] Japan perceives cyber as a national security issue because it is aware of the strategic advantage attacker's gain due to the nature of cyberattacks. Nations utilize cyber espionage to gain a strategic advantage in the grey zone because most attacks occur under the threshold of an armed attack. Plus, attacks are hard to attribute and may not be immediately identified.

Intrusions from adversaries in the cyber domain have gained the attention of Japanese leaders and aid in explaining why Japan is reevaluating its current cyber strategy. Increased intrusions and the motivation to deter attackers is encouraging Japan to implement new cybersecurity policy. Japan's National Center for Incident Readiness and Strategy for Cybersecurity's (NISC) 2021 Cybersecurity Strategy noted that the nation must "place higher priority on cyber issues in [the] diplomatic and national security agenda in light of the threats from China, Russia and North Korea."[50] Kallender and Hughes explain that "the result of rising concerns about APTs [advanced persistent threat] and China's potential involvement has been for Japan to now begin to elevate cybersecurity into the top echelons of security concerns."[51] Japanese leaders acknowledge the threats adversaries pose in the cyber domain and highlight Japan's desires to mitigate future attacks from adversaries. For Japan's case, some may argue that cyber intrusions from these actors are unique reasons for ACD adoption. However, Japan's objective is to mitigate future intrusions from state and non-state actors rather than just mitigate cyber intrusions from regional actors. Japan's Public Security Intelligence Agency (PSIA) identifies that

[48] Ryo Nakamura, "Chinese Cyberattacks on Japan Prompts U.S. Push for Stronger Defenses," Nikkei Asia, August 10, 2023, https://asia.nikkei.com/Politics/International-relations/US-China-tensions/Chinese-cyberattacks-on-Japan-prompts-U.S.-push-for-stronger-defenses.

[49] Benjamin Bartlett, "Why Do States Engage in Cybersecurity Capacity-Building Assistance? Evidence from Japan," *The Pacific Review*, February 28, 2023, https://nps.primo.exlibrisgroup.com/discovery/fulldisplay/cdi_webofscience_primary_000942176100001/01NPS_INST:01NPS, 8.

[50] The Government of Japan, "English Translation of the Pamphlet of Cybersecurity Strategy (Cabinet Decision)" (National Center of Incident Readiness and Strategy for Cybersecurity, September 2021), https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-en-booklet.pdf, 12.

[51] Kallender and Hughes, "Japan's Emerging Trajectory as a 'Cyber Power,'" 7.

"threat actors include a wide variety of actors, such as hacktivist groups, money-grubbing criminals…as well as cyberattack groups with the involvement or support of states and other entities."[52] To deter new attacks from all threat actors, new policy may be necessary. Overall, the increase of attacks since 2019 and the recognized threat of adversaries in the cyber domain showcases motives for why Japan is pledging to implement a new cyber strategy.

To deter new attacks, mitigate intrusions and build upon Japan's passive cyber infrastructure, Japan's government must consider implementing cybersecurity methods other than passive methods to reduce attacks. As discussed earlier, ACD is a strategy that is implemented alongside passive cyber tools with the ability to inflict active cyber methods. The spectrum of techniques that strategy consistently and simultaneously provides allows for more resilience, as well as a tailored response to intrusions. Katagiri argues that "one of the primary reasons for [Japan's] deterrence failure is the absence of active defense options."[53] Successfully acquiring, integrating, and utilizing active defense methods such as dye packets, sink holes, and hack-backs would aid in the Japanese government's ability to deter adversaries from attacking. Similarly, another Japanese scholar, Takahisa Kawaguichi, believes if Japan wishes to improve its cybersecurity they must "deter cyberattacks while also taking preemptive actions."[54] An ACD strategy reflects preemptive actions by proactively strengthening the system and deterrence methods by nullifying the actor. Committing to an ACD strategy builds upon Japan's previous passive cybersecurity methods and allows the nation the ability to deter future attacks by employing offensive capabilities after intrusion. While ACD's layered defense is appealing to Japan since it builds upon previous efforts, the strategy also allows Japan scalability. Japan does not have to employ the most aggrieve ACD methods such as hack-backs and distribution of adversary networks; however, for deterrence to work and norms to be established, Japan

[52] Public Security Intelligence Agency, "Overview of Threats in Cyberspace" (Ministry of Justice, 2023), https://www.moj.go.jp/content/001398997.pdf, 9.

[53] Katagiri, "From Cyber Denial to Cyber Punishment," 338.

[54] Takahisa Kawaguchi, "Japan's Defense Policy in Cyberspace" (Stimson Center – Asia, March 2020), https://www.stimson.org/wp-content/uploads/2020/03/KeyChallengesInJapansDefensePolicy-March2020-V3-web.pdf.

must have the capability to employ offensive techniques, and also be willing to utilize the capability when necessary. However, for this scope of this research, the chapter is uncovering why Japan has pledged to adopt ACD rather than determine Japan's willingness to utilize limited offensive cyber capabilities.

Finally, Japanese leaders wish to increase the nation's own cyber infrastructure to prevent attacks while also working alongside allies in establishing responsible cyber norms. Japan hopes to make itself capable of cyber defense independently, and, when necessary, compatible with allies. Japanese leaders wish to collaborate with allies and prompt norms that reflect a free and secure cyber domain. In an International Institute for Strategic Studies (IISS) research paper addressing cyber capabilities and national power, Japan's global leadership in cyberspace affairs was discussed. The research stated that "Tokyo aims to solidify international rules and norms of behaviour for states in cyberspace and, as part of that norms-based approach, actively promotes the multistakeholder model of internet governance."[55] The paper goes on to note how Japan repeatedly participated and promoted norms in sessions with the UN Group of Governmental Experts, the G7 Cyber Expert Group, and the AESAN-Japan Information Security Policy Meeting. Japan's vulnerabilities and its priority for allied collaboration in the cyber domain motivates Japan to normalize its cyber policy. A recent Washington Post article reported that "in the fall of 2020…Chinese military hackers had compromised [Japan's] classified defense networks."[56] Nakashima goes on to point out that the intrusion, coupled with U.S. pressure—a unique factor for Japan in adopting ACD that will be discussed in the following section—motivated Japan to increase its cybersecurity budget and align its cybersecurity guidelines alongside international allies. For Japan to prosper in the digital age, Japan's leaders need to secure their nation's networks. Working alongside allies and

[55] "Cyber Capabilities and National Power: A Net Assessment" (International Institute for Strategic Studies, June 28, 2021), https://www.iiss.org/research-paper//2021/06/cyber-capabilities-national-power, 84.

[56] Ellen Nakashima, "China Hacked Japan's Sensitive Defense Networks, Officials Say," *Washington Post*, August 17, 2023, https://www.washingtonpost.com/national-security/2023/08/07/china-japan-hack-pentagon/.

participating in international forums that prompt democratic norms in cyberspace is one way Japan can gradually achieve cybersecurity.

In summary, intrusion mitigation evolved into an issue of high importance by the government and interest groups due to the nation's recognition of cybersecurity as a national security issue. Now that securing the domain is an essential issue to Japan, leaders recognize the threats new attacks originating from malicious actors and adversaries have against Japan's security and prosperity. Increased protection of Japan's cybersecurity apparatus, integration of various cybersecurity methods, and the establishment of cyber norms alongside allies reflect the general reasons why Japan would commit to an ACD strategy.

B. FACTORS UNIQUE TO JAPAN'S ADOPTION

In addition to the general factors the Japanese case reflects, Japan also presents unique reasons for adoption of ACD. New solutions to cybersecurity were deemed necessary by Japan's government due to continuation of new cyber-attacks, the perception of the changing security environment, and importance of the U.S.-Japan alliance. Japan's perception of its security environment and the U.S.-Japan alliance are unique factors for why Japan decided to pledge to ACD adoption. Japan's government also displays the same concerns regarding the risks associated with ACD, but the gravity Japan places on the general risk is heightened due to Japan's pacifist constitution and society.

In addition to Japan's recognition of declining success with passive measures and the increase of new attacks, the evolving security environment is contributing to Japan's new perception of overall national defense and its desire to decrease malicious attacks. Threats to Japan's security are motivating government leaders to alter previous security policies. Scholars analyzing Japanese military normalization explain how regional threats are leading to Japan's security perception. Andrew Oros writes that "Japanese elites and public alike are reconsidering past positions on security-related issues in the face of Japan's new security environment."[57] Smith also believes that "the Japanese military had to

[57] Andrew Oros, "Japan's Relative Decline and New Security Challenges in a Multipolar Asia," in *Japan's Twenty-First-Century Security Renaissance* (New York: Columbia University Press, 2017), 66–79.

increase its defense operations and add new missions and capabilities to keep pace with the growing military might of its neighbors."[58] Japan's efforts to normalize its security policy are also due to its reputation in the region. Japanese competition in the region stems from pride, and influences Japan's approach to regional threats. Michael Green believes that "the Chinese military threat punctured not only the Japanese sense of physical security but also Japan's rank and prestige within Asia."[59] Oros, Smith and Green's respective analyses showcase how regional threats are motivating Japan to reconsider its security apparatus. The desire to maintain security and prestige in the region have justified Japanese leaders to normalize security efforts.

Cyber-attacks from adversaries—China, Russia, and North Korea—were pointed out in the last section; however, attacks from these actors better reflect Japan's desire for intrusion mitigation. Japan wishes to decrease the number of new cyber-attacks in general rather than just mitigate regional adversary intrusions. The changing security environment and regional actors give context for why Japan released a new NSS and is reevaluating its defense strategy overall. Understanding Japan's perception of the security environment is an important factor in terms of Japan's broad normalization efforts and aids in Japan's justification for overall normalization.

The U.S.-Japanese alliance is another unique reason for why Japan is pledging to an ACD strategy. There are two U.S.-specific factors that influence Japan's normalization efforts and therefore Japan's pledge to commit to ACD. First, the increased strength of the U.S.-Japan alliance is due to U.S. attention to the region and Japan's perception of security in the region. These factors contribute to Japan's overall normalization and the U.S. ability to leverage Japan's security efforts. Second, the importance of the U.S.-Japan relationship encourages and pressures Japan to modernize its capabilities in order to achieve successful integrated deterrence amongst allies. The partnership of the U.S.-Japanese alliance will be discussed first in order to understand why Japan pledged to a new cybersecurity strategy

[58] Sheila Smith, *Japan Rearmed: The Politics of Military Power* (Cambridge: Harvard University Press, 2019), 90.

[59] Michael Green, "China," in *Line of Advantage: Japan's Grand Strategy in the Era of Abe Shinzo* (New York: Columbia University Press, 2022), 58.

and then how U.S. encouragement of integrated deterrence motivates Japan to reevaluate its cybersecurity strategy.

The rise of great power competition in the twenty-first century and focus on the Indo-Pacific region is strengthening the U.S.-Japanese alliance. While the U.S. and Japan have expressed discontent with Chinese behavior in the region, Japan is still cautiously balancing its relationship between China and the United States. Quansheng Zhao's book analyzing the dynamic relationship between the U.S., China and Japan aids in understanding the historical and modern factors that influence the three great power strategies. Zhao's conclusion suggests that Japan acts as a balancer between the two nations and points out how Prime Minister Kishida "emphasizes the importance of the US-Japanese alliance and the Quad, [while] at the same time notes the importance of stability in the two neighbors' relations."[60] While Japan attempts to stabilize international relations, its NSS still references Chinese behavior as a primary security concern. Japan's strategy claims that "China's external stance, military activities, and other activities…present an unprecedented and the greatest strategic challenge in ensuring the peace and security of Japan."[61] The growing Sino-U.S. rivalry and recent Chinese behavior in the region is deepening the U.S.-Japanese alliance.

The importance of the U.S.-Japanese relationship to each country in the shadow of the Sino-U.S. rivalry is allowing for Japanese normalization and integration alongside the United States. Hughes and Matsuda identify how Sino-U.S. rivalry is encouraging U.S.-Japanese defense integration and influencing Japan's response to national security interests. Hughes notes Japan's changing military posture in the last three decades and argues that the U.S.-Japanese alliance was re-strengthened due the strategic environment.[62] Similarly, Takuya Matsuda argues that "the resurgence of great power rivalry in the Western Pacific calls for a comprehensive national strategy, one in which Tokyo not only

[60] Quansheng Zhao, *Great Power Strategies – the United States, China and Japan*, China Policy Series (Milton: Taylor & Francis Group, 2022), https://doi.org/10.4324/9781003298502, 282.

[61] National Security Council, National Security Strategy of Japan, 9.

[62] Christopher W. Hughes, *Japan as a Global Military Power: New Capabilities, Alliance Integration, Bilateralism-Plus*, 1st ed., Cambridge Elements. Elements in Politics and Society in East Asia (Cambridge, United Kingdom ; New York: Cambridge University Press, 2022).

plays a proactive role in regional security, but which also serves to revitalize Japan's economic resilience."[63] Matsuda also notes how Japan's latest defense commitments possibly pave the way for a better integrated military alliance and reach the Biden administration's goal of integrated deterrence amongst allies. Hughes and Matsuda's respective arguments showcase how Japan's recent security commitments display how Japan plans to cooperate with the U.S. militarily in response to great power rivalry. As Japan attempts to maintain stability in the region and chooses to prioritize strengthening its relationship with the U.S., a U.S.-Japanese alliance must address how they will combat the cyber activity.

Some may argue that Japan is pursing the ACD strategy to become independent from the United States. In an interview, Prime Minister Kishida's press secretary claimed that "Japan intends to strengthen its cybersecurity response capabilities to be equal to or surpass the level of leading Western countries."[64] The goal to strengthen Japan's cybersecurity infrastructure stems from Japan's recognition of the threat cyber-attacks pose to its stability in its new security environment and pressure from the U.S. alliance. Richard Armitage and Nye argue that Japan's more proactive role in Asia is due to "an increasingly harsh national security environment…[and] inconsistent leadership in the United States."[65] Although previous U.S. policy, which called for a decrease to allied dependence on the U.S., may have motivated Japan to normalize, recent U.S.-Japanese efforts in the cyber domain showcase how the two nations are individually increasing their respective cyber infrastructure and collaborating to ensure optimal cyber defense. There is a balance between independently strengthening a nation's cybersecurity apparatus while simultaneously working alongside an ally to create compatible systems and norms.

[63] Takuya Matsuda, "Japan's Emerging Security Strategy," *The Washington Quarterly* 46, no. 1 (2023): 85–102, https://doi.org/10.1080/0163660X.2023.2190218, 97.

[64] Tim Starks, "Analysis | China's Hacking of Japan's Defense Networks 'Was Bad — Shockingly Bad,'" *Washington Post*, August 8, 2023, https://www.washingtonpost.com/politics/2023/08/08/chinas-hacking-japans-defense-networks-was-bad-shockingly-bad/.

[65] Richard L. Armitage et al., "The U.S.-Japan Alliance in 2020," December 7, 2020, https://www.csis.org/analysis/us-japan-alliance-2020.

The U.S. is motivated to encourage Japan to normalize its cybersecurity strategy and infrastructure because normalization efforts benefit both nations by deterring future attacks and ensuring network stability. Christopher Johnstone explains how Japan's focus on strengthening its cybersecurity is beneficial to the U.S. because "weak cybersecurity practices across the Japanese government have been a critical impediment to deeper alliance cooperation and expanded information-sharing."[66] Without a revision to Japan's cyber security policy and infrastructure, any success of integrated deterrence is limited and leaves the domain vulnerable. However, leaders in the U.S. and Japan recognize the important of updating Japan's cyber apparatus. In a bilateral press conference with President Biden and Prime Minister Kishida, Kishida noted that the two nations are "facing the most challenging and complex security environment."[67] He went on to explain that in order for future security in the region Japan wrote a new NSS to address areas of concern. Japan's vulnerabilities in the cyber domain, alongside the U.S.'s desire to work with capable allies in the domain, illustrate how the U.S.-Japan alliance motivated Japan to pledge to a new cyber strategy and is a unique reason not outlined in the general reasons for ACD adoption.

The importance of the U.S.-Japan alliance and the threat of cyber espionage legitimizes Japan's call for cyber normalization and the necessity for U.S. collaboration in mitigating threats. The U.S.-Japanese alliance aims to prepare Japan for future conflicts in the cyber domain. Kallender and Hughes believe that alliance is allowing Japan to "deliberately and progressively integrate its capabilities and strategy with those of the U.S. in order to…proactively…[counter] cyber threat [s] from China and other actors."[68] U.S. encouragement of increased allied capabilities in Asia and integration amongst allies is allowing the U.S. to encourage Japan to reevaluate its cybersecurity policy. Since the U.S. has altered its cybersecurity strategy, Japan must understand how the character of cyber deterrence is evolving amongst adversaries and even allies. Recent U.S. cybersecurity

[66] Christopher B. Johnstone, "Japan's Transformational National Security Strategy," December 8, 2022, https://www.csis.org/analysis/japans-transformational-national-security-strategy.

[67] The White House, "Joint Statement of the United States and Japan."

[68] Kallender and Hughes, "Japan's Emerging Trajectory as a 'Cyber Power,'" 2.

policy calls for integration and cooperation in the domain amongst allies. The 2023 U.S. National Cybersecurity Strategy insisted that the U.S. enable and collaborate with allies.[69] In addition to allied integration, the U.S. has specifically called upon Japan to "deepen defense cooperation across all domains, including cyber and space…to bolster extended deterrence."[70] The U.S. values the Japanese alliance and emphasizes the need for allied collaboration in the cyber domain. Influence from the U.S.-Japanese alliance is encouraging Japanese leaders to adopt an ACD strategy to meet U.S. allied integration efforts. The pledge to implement an ACD strategy as a means to integrate alongside the U.S. justifies Japan's military normalization in the domain while strengthening the U.S.-Japanese alliance.

While there is increasing cooperation and motivation from Japan to update its cybersecurity policy to better reflect U.S. efforts, the U.S. has adopted and Japan is pledging to adopt active cyber tools, but employ them at different times. There are significant risks that the U.S. policy presents, and Japan's government is not willing to go as far as the U.S.'s cyber strategy of persistent engagement because of the risks that the policy entails. Following the 2020 Chinese cyber intrusion on Japan's classified defense network, Ryo Nakamura explained that USCYBERCOM offered Japan a 'hunt forward' team, but the Japanese were "uncomfortable having another country's military on their networks."[71] Nakamura adds that the U.S. and Japan agreed to a compromise which permitted Japan's commercial companies to review the intrusions, then allowed USCYBERCOM to the review the information and provide guidance for how to respond. U.S. 'hunt forward' teams are invited units deployed to allied nations to observe, detect and at times recommend neutralization of malicious cyber activity on the host nation's networks.[72] General Hartman, Commander of Cyber National Mission Force, explained

[69] The White House, National Cybersecurity Strategy, 31.

[70] The White House, "U.S.- Japan Joint Leaders' Statement."

[71] Nakamura, "Chinese Cyberattacks on Japan Prompts U.S. Push for Stronger Defenses."

[72] U.S. Cyber Command Public Affairs, "CYBER 101: Hunt Forward Operations," U.S. Cyber Command, November 15, 2022, https://www.cybercom.mil/Media/News/Article/3218642/cyber-101-hunt-forward-operations/ https%3A%2F%2Fwww.cybercom.mil%2FMedia%2FNews%2FArticle%2F3218642%2Fcyber-101-hunt-forward-operations%2F.

that "when we [the U.S.] execute a defensive hunt operation, we install that equipment on a partner's network based on an agreement with that partner. And when we identify either malware or some type of misconfiguration on a network, we instruct the partner and the partner will take the remediation actions on their own network."[73] Japan may be reluctant to grant another nation, who practices the more aggressive cyber strategy, access and protection of its networks due to the possibilities of unintended escalation. Japan's hesitation showcases its awareness to the risks of aggressive cyber policy. Japan is willing to cooperate with the U.S. in the domain, but Japan prefers U.S. guidance opposed to network access.

Japan may be willing to accept the escalatory implications of an ACD strategy rather than the higher risk of escalation associated with the U.S. persistent engagement strategy. As discussed in the last chapter, a persistent engagement strategy in cyberspace allows a nation to disable actors before a detected intrusion. Japan cannot commit to a persistent engagement strategy given its pacifist constitution. The ACD strategy reflects the intent of Japan's self-defense force more than an anticipatory strategy does. An ACD strategy allows the nation to act after a detected intrusion. Still, pledging to a new cyber strategy illustrates Japan's desire to update its cyber strategy alongside allies. By pledging to an ACD strategy rather than U.S. cyber strategy, Prime Minister Khisida's cabinet seems to be willing to accept the risks of ACD rather than the risks of the U.S. persistent engagement theory in cyberspace. ACD is a balance between previous passive methods and an anticipatory strategy that the U.S. follows.

The general risks associated with the ACD strategy are reflected in the Japan case, but the way Japan weighs the general risks are unique because of Japan's pacifist culture and legal restrictions. The risks of military overreach and the violation of legal parameters force Japan to consider the general cyber risks far more cautiously than other nations. Chapter II determined that the general risks associated with ACD include the following: misattribution, unintended collateral damage, and escalation. These risks are extremely

[73] Dina Temple-Raston, "Q&A with Gen. Hartman: 'There Are Always Hunt Forward Teams Deployed,'" June 20, 2023, https://therecord.media/maj-gen-william-hartman-interview-ukraine-russia-click-here.

worrisome for the Japanese due to Japan's pacifist constitution. Article 9 of Japan's constitution states that "the Japanese people forever renounce war as a sovereign right of the nation and the threat or use of force as means of settling international disputes."[74] If Japan were to conduct an offensive capability against an attacker after a detected intrusion, but later discover the believed attacker was misattributed, Japan would have not acted out of self-defense, but instead attacked another nation without provocation. Similarly, if Japan's offensive capability was employed and unintentionally caused harm on networks other than the attackers, some may argue that Japan used forced against another nation. Both scenarios demonstrate how the general risks associated with ACD could easily lead to escalation and violate Japan's defense-orient constitution. Although these risks are general risks applicable to any nation, the gravity Japan places on them makes these factors unique to Japan. Mitigating these risks – misattribution, unintended collateral damage, and escalation – is essential for Japan due to the nation's commitment to pacifism. Developing a professional cyber core is detrimental for Japan during the implementation phase of ACD. As noted in Chapter II, a proficient cyber core well versed in ACD methods provides a safeguard to the outlined risks and mitigates the possibility for escalation.

C. CONCLUSION

The above analysis of Japan reflects all the general reasons for why nations adopt an ACD strategy, but points out factors unique to Japan. The Japan case also reflects the general risks associated with ACD policy, but highlights how Japan's pacifist constitution increases the seriousness of these factors. For Japan, cyber normalization efforts are driven by changing political attitudes resulting from previous policy failure in deterring future attacks, increasing regional threats, and U.S. encouragement to integrated defense capabilities. Japan's new security documents demonstrate the nation's recognition of cyber as a national security issue and the importance of reevaluating current cyber strategy. Empirical evidence showcases how previous cyber policy efforts are failing to deter new attackers and how the fear of cyber threats under the threshold of an armed attack are

[74] Ministry of Justice, "The Constitution of Japan and Criminal Statutes" (1947), https://japan.kantei.go.jp/constitution_and_government_of_japan/constitution_e.html.

motiving Japan to invest in modern cyber technology. Finally, the U.S. alliance is encouraging Japan to develop its own capabilities and integrate its policy parallel to U.S. efforts in the region. Although U.S. policy and Japan's pledge are not the same, Japan's pledge still allows for more offensive techniques and gradually moves its policy closer to the United States. Japan may never achieve the same level of offensive means the U.S. uses due to Japan's political, social, and legal limitations. Still, the commitment to an ACD strategy showcases Japan's recognition of how solely passive cyber efforts are failing to deter new attacks and secure the domain in the future. Pledging to ACD brings Japan a step closer to U.S. policy which aids in the development of responsible cyber behavior amongst allies.

IV. JAPAN'S CYBER INFRASTRUCTURE AND CHANGES NECESSARY TO EXECUTE ACD STRATEGY

Japan pledged to implement an ACD strategy, but its previous investment and attention to passive defensive systems may limit its ability to transition to a new strategy. This chapter investigates the question: what cyber-related changes are necessary for Japan to execute an ACD strategy? The chapter identifies the political, legal, and social hurdles Japan will face before entering the strategy's implementation phase. Japan can implement the necessary ACD elements, after it receives Diet approval, executes legal reforms, and obtains societal support for the strategy. The research will review general ACD literature regarding ACD's foundational components to determine the effectiveness of Japan's current cyber structure and pledged changes. The chapter then outlines Japan's current cyber infrastructure, analyzes Japan's pledges to execute ACD strategy, and provides recommendations for improvements. The chapter concludes that Japan's current cyber apparatus provides a foundation for the implementation of an ACD strategy, but to achieve ACD Japan still requires specific ACD doctrine, clarification of its cyber command structure, and investment in its cyber core's education, as well as offensive cyber technology.

A. REQUIREMENTS PRIOR TO IMPLEMENTATION

For an ACD strategy to be implemented, there are requirements Japan will need to address before the nation is able to restructure its cybersecurity apparatus. Japan must receive political approval of the new security documents by the Diet, execute legal reform to allow for ACD operations, and obtain societal support for the policy. In terms of political hurdles, the policy still requires approval outside of Prime Minister Kishida's Security Council. Jeffery Hornung and Adam Liff point out that "these documents [NSS, NDS, and DBP] are *not* legally-binding commitments, plans, or legislation that have received the imprimatur of Japan's National Diet, much less been fully resourced."[75] The documents,

[75] Jeffery Hornung and Adam Liff, "Japan's New Security Policies: A Long Road to Full Implementation," *Brookings* (blog), March 27, 2023, https://www.brookings.edu/blog/order-from-chaos/2023/03/27/japans-new-security-policies-a-long-road-to-full-implementation/.

referenced by Liff and Hornung, published in December of 2022 outline the vision and intent of Japan's Cabinet for ACD, but do not guarantee successful implementation. The Diet will have to consider the implications of a cyber policy that requires countermeasures. Due to Japan's pacifist culture and defensive legacy, political leaders will have to weigh the risks associated with the outlined normalization efforts against the possibility of societal pushback. Hornung and Johnstone also commented on how Japan's new cybersecurity objectives require new legislation and political will.[76] Leaders will have to advocate for why the new policy is necessary, commit to the costs that will sustain the new security objectives, and ensure the policy is implemented successfully. Therefore, publishing the new NSS and supporting documents does not automatically translate its objectives to law, and political approval will need to occur before the implementation phase.

In addition to Diet approval, executing legal reforms for certain ACD methods will be necessary for implementation of the strategy. Following Diet approval, Japan will have to develop regulations for the employment of offensive techniques, review domestic cybersecurity legislation, and update SDF law to allow the use of limited offensive ACD methods. In Katagiri's assessment of Japan's ability to achieve an ACD infrastructure, he argues that for ACD to be implemented "a new law would have to specify conditions under which countermeasures will be carried out…[and] reform would require lawmakers to revise all relevant [cybersecurity] laws."[77] He goes on to note how existing law enforcement penal codes limit Japan's actions in cyberspace. Amendments to law enforcement penal codes need to be approved to allow the use of limited offensive techniques such as hack-backs and dye-packs. Japan will also have to clarify the government's ability to respond to intrusions. Jun Osawa notes the Telecommunications Law and Unauthorized Computer Access requires reforms to allow the government to

[76] Jeffery Hornung and Christopher Johnstone, "Japan's Strategic Shift Is Significant, but Implementation Hurdles Await," War on the Rocks, January 27, 2023, https://warontherocks.com/2023/01/japans-strategic-shift-is-significant-but-implementation-hurdles-await/.

[77] Katagiri, "From Cyber Denial to Cyber Punishment."

conduct "administrative interception" of the intruders.[78] Similarly, changes to SDF law will have to allow the use of limited offensive techniques. Katagiri explains that "SDF law remains profoundly unclear about the conditions for force deployment, because it gives SDF no explicit authorization to carry out anything more than passive defense, leaving underspecified the way SDF would be permitted to conduct active cyber defense."[79] Japan will need to update SDF law to specify how and when ACD methods would be employed by the SDF. However, Japan's government does acknowledge the need for legislative reform prior to implementation. The NSS states that "the Government will work on legislation and strengthen operations for the purpose of materializing these new efforts [ACD strategy] in the field of cybersecurity."[80] In summary, following the Diet's approval of the new objectives outlined in the NSS, Japan's government will need to publish regulations for when ACD measures are sanctioned, clarify the legality of ACD countermeasures for law enforcement, reevaluate domestic privacy laws, and update SDF law to allow for ACD offensive operations.

Society serves as a barrier to political approval and legal reform. Japan's unique pacifist society makes it difficult to change previous legal frameworks and quickly enact an offensive policy. Katagiri argues that "the legal reform is hard to sell to the Japanese public because it has significant bearing on domestic politics and constraints on the use of force at home and because the existing legal system is so embedded in the society."[81] Before implementation, Japanese leaders need to weigh the domestic risk of undergoing legal reforms that allow for countermeasures. Japanese interest groups may also impede the direction of Japan's cybersecurity policy. By identifying how cybersecurity interest groups within Japan work closely with the government, Katagiri notes that interest groups have opposed controversial reforms to cybersecurity strategy to include ACD and military cross-domain operations.[82] To enact legal reform and implement ACD operations,

[78] Jun Osawa, "How Japan Is Modernizing Its Cybersecurity Policy," *Stimson Center* (blog), February 2, 2023, https://www.stimson.org/2023/japan-cybersecurity-policy/.

[79] Katagiri, "From Cyber Denial to Cyber Punishment," 340.

[80] National Security Council, National Security Strategy of Japan, 24.

[81] Katagiri, "From Cyber Denial to Cyber Punishment," 344.

[82] Katagiri, "The Soft Underbelly of Cyber Defence in Democracy." 347.

Japanese political leaders will need to satisfy interest groups and communicate to the public the domestic benefits of ACD.

Support from society could occur if society is educated on ACD's intent and methodology. As described in Chapter II, ACD is a layered system with flexible techniques that does not allow for the use of offensive techniques until an intrusion occurs. ACD operations require an intrusion on the defender's network prior to the sanction of limited offensive techniques. If Japan chose to use offensive techniques the nation would be responding and defending against an intrusion. Additionally, offensive cyberspace operations do not amount to the same risks as direct military action. Employing a hack-back on an attacker's system does not result in physical damage to the attacker. The offensive technique may result in damage to the attacker's system, but it does not directly threaten the intruder's life. Japan's society may interpret the risks of offensive operations in cyberspace more willingly than in the physical world. Societal support for the policy will occur if the government can communicate the intent of ACD, the flexibility of responses ACD allows, and the security ACD countermeasures provide to the public without risk to human life.

Once the Japanese government addresses the political, legal, and social hurdles, the nation can manage the transition of its cybersecurity infrastructure from a solely passive cybersecurity structure to an ACD structure. Political approval and legal changes are achievable, but altering Japan's pacifist culture is challenging due to the nation's commitment to defense. Still, the nature of the cyber domain compared to the nature of conventional counter measures may allow for support from society and lead to political approval of legal reform necessary to implement ACD strategy.

B. GENERAL ACD STRUCTURE

A nation must develop and recruit a component cyber core for ACD operations to successfully and safely be carried out. The development and recruitment of a competent cyber core are areas that require attention and funding. Herring and Willett believe that "achieving...efficiency requires aware and intelligent management of integrated cyber defense to understand the needs and function of the individual parts in the context of the

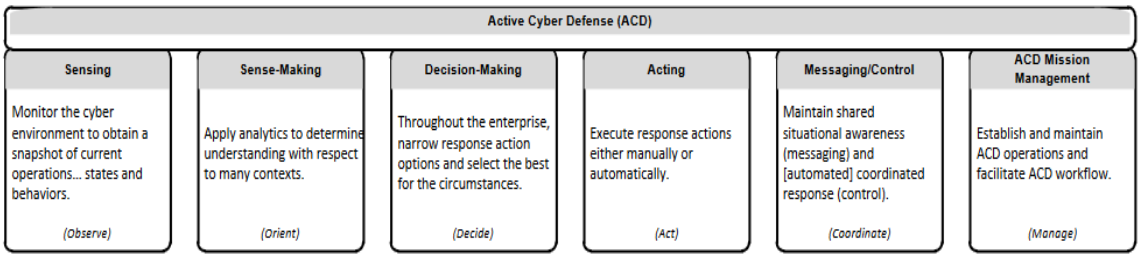
entire operation."[83] As discussed in Chapter II, establishing a proficient cyber core able to mitigate risks associated with ACD strategy is an important safeguard to spillover and escalation. If a nation wishes to implement an ACD strategy, it must confidently hire enough trained and experienced personnel capable of managing and executing the requirements of ACD strategy. Without the development and recruitment of a capable cyber core, the nation will be unable to safely execute the objective of ACD strategy.

The defender must develop a force structure that outlines roles to operate consistently and efficiently. Although one of the strengths of ACD is the spectrum of responses available to the user, it can be difficult for responses to be executed consistently in cyber-relevant time. Since Herring and Willett claim that ACD is "a comprehensive…solution require[ing] the integration of many tools,"[84] the defending nation must develop a component cyber core able to quickly evaluate intrusions and respond efficiently, as well as effectively. One way to achieve operability is through a structure that assigns clear roles and outlines intrusion procedures. Herring and Willett argue that since "ACD is not a single solution; it is a capability to provide context and interoperability among many solutions under the six functional areas. An integrated, cohesive ACD solution implies the use of many sensors, analytics, and displays to support many decision-makers."[85] They go on to describe the six functional areas: sensing, sense-making, decision-making, acting, messaging/ control, and ACD mission management. Figure 3 summarizes the role of the six different functional areas. Each functional area has specific objectives and required personnel. Initiating the six functional areas as the foundation for a nation's ACD structure will reduce the possibility of overlap, miscommunication, and failure.

[83] Herring and Willett, "Active Cyber Defense," 49.

[84] Herring and Willett, 49.

[85] Herring and Willett, 50.



Source: Herring, Mj, and Kd Willett. "Active Cyber Defense: A Vision for Real-Time Cyber Defense." *Journal of Information Warfare* 13, no. 2 (2014): 46–55, 49.

Figure 3. ACD Functional Areas

The functional areas aid in the decision-making process for the administrators, and real-time automation supports the administrators' decisions. Herring and Willett explain that "each decision-maker will have a unique context within which to make decisions."[86] They go on to explain that the decision-making process is based on decision drivers that originate from authoritative, negotiated, and self-imposed mandates. Once an intrusion is observed the decision-maker tailors the response and bases the act on the various guidelines. To address the unique nature of the cyber domain, the speed and the constant contact, the administrators work in partnership with automated platforms. Herring and Willett note this partnership by stating that "ACD accommodates the automation of decision-making as well as the cognitive supplement of human decision-makers."[87] The relationship between the decision-maker and the support from automation aids in not only the identification of issues, but also the speed in which decisions can be made. Although an educated cyber core is necessary for execution of the strategy, automation accelerates the process. It is essential for a cyber professional to be in the decision loop to reduce possible risks and weigh the various guidelines. In summary, the foundational elements of ACD's structure are a robust cyber core, the implementation of six functional areas, and the development of automation to support and enable the administrators in cyber relevant speed.

[86] Herring and Willett, 49.

[87] Herring and Willett, 49.

C. JAPAN'S CURRENT PLEDGES, PLANS AND LIMITATIONS

This section will review Japan's pledges and means for implementing an ACD structure. Japan is operating from a solely defensive cybersecurity structure. The pledges are designed to improve Japan's current cyber structure in order to carry out ACD operations. This chapter will analyze Japan's current cyber structure, NSS, DBP, and Defense Programs and Budget (DPB) to identify how effective the pledges will be in fulfilling an ACD strategy. Addressing the strengths and weaknesses of various categories—strategy and doctrine, organization, personnel, education and training, technology acquisition—will showcase the planned changes and future changes Japan must implement to achieve the foundations of an ACD apparatus.

1. Strategy and Doctrine

In addition to the NSS's pledge to ACD strategy, the NSS also outlines where Japan intends to improve its abilities to carry out ACD operations, when limited offensive techniques will be employed, and who will oversee the cybersecurity pledges. The NSS's directives aid in clarifying how Japan's cybersecurity apparatus will be improved and when countermeasures will be employed. Japan's NSS specifically states that for ACD to be realized the Government will do the following:

> (a) Japan will advance efforts on information sharing to the Government in case of cyberattacks among the private sector including critical infrastructures, as well as coordinating and supporting incident response activities for the private sector.
>
> (b) Japan will take necessary actions to detect servers and others suspected of being abused by attackers by utilizing information on communications services provided by domestic telecommunications providers.
>
> (c) For serious cyberattacks that pose security concerns against the Government, critical infrastructures, and others, the Government will be given the necessary authorities that allow it to penetrate and neutralize attackers' servers and others in advance to the extent possible.[88]

[88] National Security Council, National Security Strategy of Japan, 23–24.

The NSS goes on to direct the NISC to oversee the efforts outlined above. The NSS's directives showcase Japan's recognition for areas of improvement, intent for when limited offensive techniques would be utilized, and directs an organization to lead the transition. These efforts enable an agency to implement an ACD strategy and provide Japan a basic guideline for when to use ACD's limited offensive methods. However, the NSS does not provide details or a projected timeline with benchmarks for how the strategy will be realized. The 2022 DBP and 2023 DPB documents give a more detailed overview for how Japan will implement changes to its cybersecurity to achieve ACD operations. Guidance described in the DBP and DPB addresses some of the key changes needed to satisfy the foundations of an ACD structure determined in Section B. The DBP and the DPB outline how Japan's MOD/SDF will grow its SDF Cyber Defense Unit (CDU), address recruitment issues, alter its education system, update its cybersecurity technology, increase the cybersecurity budget, and continue to work with partners to achieve its objectives.[89] These documents published at the strategic level aid in developing an organized competent cyber core enabled with ACD's necessary technologies.

Yet one of the key elements not outlined in the NSS, NDS, and DBP is who will oversee the operations of the various ACD techniques across the private and public sector. If Japan wishes to implement the ACD concepts into its cyber apparatus, it is essential for the NISC to determine who will conduct the different elements of ACD operations and what regulations each agency will have. Hornung and Johnstone note that it is "unclear where the government's active defense capability would be housed."[90] In terms of the MOD's role in cybersecurity, the SDF CDU is only responsible for the oversight of defense networks. Stefan Soesanto explained that the group's task is to strengthen the SDF's defensive capabilities and "conduct persistent monitoring of SDF's information and communications networks."[91] Since the SDF is not allowed to protect networks outside of

[89] Ministry of Defense, "Defense Buildup Program," December 16, 2022, https://www.mod.go.jp/j/policy/agenda/guideline/plan/pdf/program_en.pdf, 11–12; Ministry of Defense, "Defense Programs and Budget of Japan: 'First Year' Budget for Fundamental Reinforcement of Defense Capabilities," 2023, https://www.mod.go.jp/en/d_act/d_budget/pdf/230330a.pdf, 20–21.

[90] Hornung and Johnstone, "Japan's Strategic Shift Is Significant, but Implementation Hurdles Await."

[91] Stefan Soesanto, Outward Defense: Comparing the Cyber Defense Postures of Japan, the Netherlands and the United States in Peace Time (Konrad Adenauer Stiftung, 2021), 3.

the defensive apparatus, Hidetoshi Ogawa and Motohiro Tsuchiya explain that the "MOD [Ministry of Defense] has traditionally taken an extremely prudent approach as to how it should be involved in general cybersecurity for fear of meddling in civilian domain."[92] Since Japan's SDF is unable to operate on non-defensive networks, the SDF will not protect against an attack on critical public infrastructure even though an attack on critical infrastructure is a national security issue. If Japan implements an ACD strategy that reacts to intrusions on the critical infrastructure systems, the SDF does not currently have the authority to respond. The NISC has yet to indicate who will oversee cybersecurity in the private sector. Considerations for how the private sector's cybersecurity will interact with the SDF during ACD operations are being discussed. Shusuke Shigeta writes that "the Japanese government is weighing how to expand the Self Defense Forces' cyber protection responsibility to businesses as increasing attacks threaten both confidential data and infrastructure."[93] He goes on to explain how companies supplying power, communications, and transportation will be protected by ACD concepts; however, he notes that these changes are not projected to occur until 2027 or 2028. Despite the long timeline, Japan's government is discussing the issue and considering the problem-sets ACD implementation brings to Japan's defense-oriented structure.

Japan is missing clear ACD operational and tactical doctrines for the organizations within the NISC and MOD. Doctrine that provides clarification and guidance is essential for the proper employment of ACD operations. New doctrine is needed in an ACD structure because it aids in management of ACD techniques and provides guidance for how decision makers will carry out ACD operations consistently. Future doctrine and specific policy will need to be developed to maintain continuity across the different communities and set a precedent for how Japan will determine intrusions, communicate attribution, and employs limited offensive techniques across private and public networks. When the NISC works on its directed efforts assigned to them in the NSS, it should clarify the SDF's role in ACD

[92] Hidetoshi Ogawa and Motohiro Tsuchiya, "Cybersecurity Governance in Japan," *International Journal of Cyber Diplomacy*, 2021, 7–31, 20.

[93] Shunsuke Shigeta, "Japan to Extend Cyberdefense Umbrella to Private Sector," Nikkei Asia, December 31, 2022, https://asia.nikkei.com/Politics/Japan-to-extend-cyberdefense-umbrella-to-private-sector.

operations regarding the private sector to ensure Japan is able to neutralize intrusions across all sectors.

2. Organization

Japan's current cybersecurity structure provides a foundation for ACD strategy with existing cybersecurity administrators that have relationships across organizations reaching all relevant communities within government and society. Appendix A illustrates the formal and informal interactions of the organizations in Japan's cybersecurity apparatus. The organizations that exist in Japan's current cybersecurity structure that will lead ACD implementation or carry out ACD operations include the Cybersecurity Strategic Headquarters, NISC, Cyber Incident Mobile Assistance Team (CYMAT), Government Security Organization Coordination Team (GSOC), and the MOD's Joint SDF CDU.

The NISC, the organization directed to oversee ACD implementation, falls under the Cybersecurity Strategic Headquarters. Bartlett explains that the Cybersecurity Headquarters only "meets a few times a year to set overall policy…[while the NISC] handles much of the day-to-day affairs of government cybersecurity."[94] The NISC under the direction of the Cybersecurity Strategic Headquarters will ensure that ACD operations are developed. CYMAT currently provides support to the ministry or agencies when an intrusion occurs. The GSOC is responsible for monitoring government networks, analyzing threats, distributing information and oversight of administrative agencies. For ACD implementation, Japan will not need to develop brand new cybersecurity organizations at the operational levels. The CYMAT and GSOC can be enabled with ACD capabilities and new doctrine to achieve ACD operations. Additionally, the Joint SDF CDU already maintains a close relationship and collaborates with the NISC. The MOD states that "since it is difficult for the MOD/SDF alone to achieve stable use of cyberspace, they work closely with relevant ministries and agencies such as the [NISC]."[95] The relationship between the MOD and the NISC already provides a pathway for ACD operations collaboration. Once

[94] Bartlett, "Japan: An Exclusively Defense-Oriented Cyber Policy." 98.

[95] Ministry of Defense, "Regarding Response to Cyber Attack," Japan Ministry of Defense, n.d., https://www.mod.go.jp/en/.

the NISC writes doctrine that clarifies the abilities of the CYMAT and SDF CDU, the two organizations can collaborate to respond to intrusions. The centralized organizations across Japan's cybersecurity apparatus and the relationships between the organizations provide a foundation for ACD strategy to be implemented. Japan can use the preestablished organizations to communicate strategy changes and update the techniques and doctrine of the organizations to reflect ACD methods.

The details regarding how Japan will organize its cybersecurity apparatus, to protect the private and public sector with ACD concepts are still being discussed. Japan recognizes that there are organizational and leadership changes needed to implement ACD properly, but new command structures are still in the initial planning phase.[96] The NSS directs the NISC to "be constructively restructured to establish a new organization which will comprehensively coordinate policies in the field of cybersecurity, in a centralized manner."[97] Allocating a centralized expert group within the NISC ensures that ACD implementation is consistent across all organizations. Ogawa and Tsuchiya argue the NISC is a middle-level organization amongst Japan's other organization because the NISC's portion of the overall 2020 budget reflected that it is at "the middle ground between a full-fledge central agency and a coordinating Task Force-like organization."[98] The NISC may struggle to implement the directed efforts if it is not funded adequately or respected amongst the other agencies. Additionally, NISC has yet to publicly release guidance on how the cyber apparatus will be restructured or how the directed cybersecurity efforts outlined in the NSS will be realized. The NISC did acknowledge in this year's cybersecurity overview that it must address "research and development, public infrastructure development, cyber security, and international cooperation to enhance deterrence capabilities of Japan and other countries of the region under interagency framework, and to strengthen total defense posture."[99] Similarly, the MOD/SDF have not

[96] National Security Council, National Security Strategy of Japan, 23–24.

[97] National Security Council, 24.

[98] Ogawa and Tsuchiya, "Cybersecurity Governance in Japan," 14.

[99] Japan NISC, "Overview of Cybersecurity 2023," July 4, 2023, https://www.nisc.go.jp/eng/pdf/overview_of_cybersecurity2023_en.pdf, 6.

clarified how the new cyber defense squadron will be restructured to oversee ACD operations.[100] The new ACD responsibilities and restructuring of the NISC and MOD's cyber organizations are not fully defined yet. The respective roles of the organizations need to be defined to ensure credibility, allocate adequate funding, and provide coordination amongst different sectors.

To achieve implementation of ACD strategy across all organizations Japan must empower the NISC to a full-fledge central agency, follow through on the NSS's pledge for a new organization within the NISC to coordinate the new strategy, and organize the CYMAT and SDF CDU into ACD's six functional areas. To achieve organizational and leadership improvements, some argue that Japan needs to create a dedicated cyber ministry in addition to the Cyber Strategic Headquarters and NISC. In an interview with the *Diplomat*, Major General Tanaka Tatsuhiro, the retired commanding general of the GSF's Signal School, argued that Japan needed a cyber ministry. At the operational level, Major General Tatsuhiro explains that the NISC "is not a command center for cyber defense, but a coordination-based organization for responding to situations…[Japan] need [s] an organization that maintains a solid infrastructure for crisis management."[101] He adds that creating a cyber ministry would place cybersecurity at the same level as other ministries. He concludes by arguing that Japan "should aim to establish a large [cyber] ministry with large powers and responsibilities" to deal with cyber threats to the private and public sectors.[102] For consistency of ACD implementation and operations, Japan should consider creating a cyber ministry to properly execute ACD strategy across its entire cybersecurity apparatus.

3. Personnel

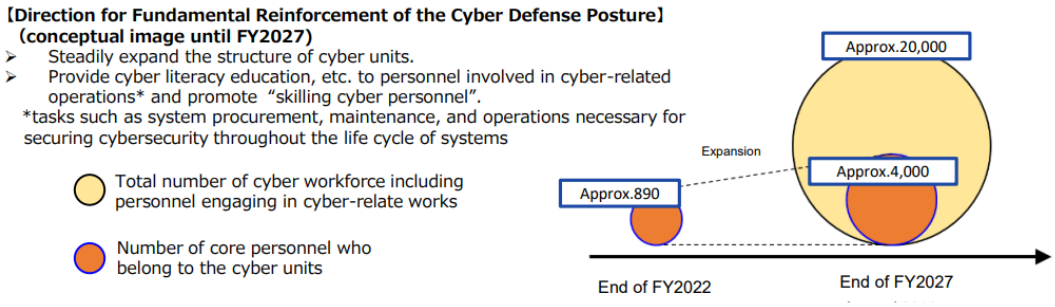
To build an educated cyber core capable of managing networks with ACD concepts Japan needs to expand its cybersecurity personnel first. The MOD intends to drastically

[100] Ministry of Defense, "Defense Buildup Program," 45.

[101] Takahashi Kosuke, "Japan Needs a Cyber Ministry: Former JGSDF Major General," Diplomat, September 19, 20222, https://thediplomat.com/2022/09/japan-needs-a-cyber-ministry-former-jgsdf-major-general/.

[102] Takahashi Kosuke.

increase its cybersecurity personnel from about 900 personnel to 4,000 by 2027. Figure 4 showcases the cyber defense personnel projection. The Japan Times reported that in the MOD "the total number of cyber-related personnel in the ministry, including the SDF unit, [would increase] to some 20,000."[103] For the SDF, Hornung and Johnstone note that Japan intends to achieve its personnel pledge "without increasing the size of the Self-Defense Forces. Instead, there will be some reallocation of personnel across services…but no growth in the overall size of the force."[104] They add that Japan will need to recruit the right people capable of fulfilling the highly technical positions and SDF personnel will need to be reclassed, as well as reeducated to fulfill the positions. As discussed in Section B, the development of a capable cyber core is essential to ACD operations. The drastic increase to Japan's cyber personnel aids in the oversight of ACD operations across the organizations Japan wishes to employ ACD methods. The MOD recognizes the necessity of increasing its current cyber core to achieve successful ACD operations.



Source: "Defense Programs and Budget of Japan: 'First Year' Budget for Fundamental Reinforcement of Defense Capabilities," 2023. https://www.mod.go.jp/en/d_act/d_budget/pdf/230330a.pdf, 21.

Figure 4. Cyber Defense Personnel Posture Projection

[103] Jiji, "Japan to Speed up SDF Cybersecurity Personnel Development," The Japan Times, July 11, 2023, https://www.japantimes.co.jp/news/2023/07/11/national/sdf-cyber-capabilities/.

[104] Hornung and Johnstone, "Japan's Strategic Shift Is Significant, but Implementation Hurdles Await."

Yet Japan's military faces a recruitment and retention issue due to Japan's changing demographics and private sector job opportunities. The SDF's ability to fulfill the pledged personnel increase will determine Japan's success in carrying out ACD operations across the functional areas outlined in Section B. Japan's demographics affect how Japan will fulfill its personnel changes in the SDF. Tom Phong Le discusses how Japan's "population decline, and aging society are constant constraining forces that are difficult to overcome because of economic and cultural realities that have developed over decades."[105] Japan's aging population and decreasing birthrate not only affect the country's overall prosperity, but also the SDF's recruitment of aspiring young cybersecurity professionals. Professor Fumika Sato stated that "in a booming economy, the motivation to choose the SDF as an employer is lost on those who can compete in the civilian job market."[106] Individuals who meet the SDF's targeted recruitment age range and are educated in cybersecurity will choose a higher-paying job in the private sector as opposed to the SDF. Japan will struggle in executing ACD without the recruitment or retention of SDF cyber personnel.

Outside the SDF's personnel challenges, realizing the other 16,000 cyber professionals in the ministry will be difficult due to Japan's limited cybersecurity professionals and employment tendencies. Without qualified and capable cyber professionals across the ministry Japan will be unable to transition its cyber apparatus and successful perform cybersecurity operations. In a Mansfield report, authors commented that society is "suffering from an acute shortage of skilled [cybersecurity] personnel needed even to sustain our current [cyber] posture; with a gap of 2.72 million globally, 377,000 in the United States, and 40,000 in Japan."[107] A shortage of cybersecurity professionals, combined with defense recruitment hurdles will hinder Japan's ability to achieve an ACD structure because capable personnel are an essential foundational element to ACD

[105] Tom Phuong Le, "Who Will Fight? The JSDF's Demographic Crises," in *Japan's Aging Peace: Pacifism and Militarism in the Twenty-First Century* (Columbia University Press, 2021), 64–105, 72.

[106] Gabriel Dominguez, "Recruitment Issues Undermining Japan's Military Buildup," The Japan Times, January 2, 2023, https://www.japantimes.co.jp/news/2023/01/02/national/japan-sdf-recruitment-problems/.

[107] "Building A Cyber Workforce: Through The U.S.-Japan Alliance" (The Maureen and Mike Mansfield Foundation, n.d.), https://mansfieldfdn.org/wp-content/uploads/Building-a-Cyber-Workforce-Through-the-U.S.-Japan-Alliance-Policy-Brief.pdf, 6.

operations. The Japan Times commented that "the government will look at appointing qualified civilians to cybersecurity roles at the ministry and in the SDF."[108] However, finding qualified cybersecurity professionals willing to leave current positions will be challenging. The Council on Foreign Relations noted how Japan's society "largely depends on a lifetime employment system, where an employee will start will one company and remain there until he or she retires."[109] They go on to claim that there is a limited amount of cross-pollination amongst the private sector and government. The MOD may be unable to incentivize the private sector to aid in the ministry's new ACD objectives. Japan's limited private-public sector overlap will make it difficult for Japan to fulfill its cyber personnel pledge and properly execute ACD operations.

Japan must follow through on its outlined recruitment efforts because increasing the cybersecurity core allows for oversight of ACD operations. MOD is aware of the recruitment and retention issue. The DBP and the DPB discuss general courses of action to deal with recruitment and retention. The DBP remarks that the SDF will review how it selects candidates, expand its SDF scholarship process, enable more flexible recruitment, reevaluate retirement services, and improve living and working environments for current personnel members.[110] Another way the MOD plans on achieving the personnel number is by "abolish [ing] units mainly composed of the SDF Ready Reserve Personnel, and allocate [ing] the regular uniformed SDF personnel belonging to the units to fulfill the personnel requirements."[111] The MOD's proposed solutions contribute to the cyber core's ability to maintain its current force presence and transition its cyber force to an ACD structure. Overcoming retention and recruitment issues will contribute to Japan's ability to fulfill the outlined personnel increase needed to satisfy ACD operations. Although a shortage of cyber professionals is not unique to Japan, Japan's education system should take steps to increase technology exposure by offering basic cybersecurity courses at lower levels in

[108] Jiji, "Japan to Speed up SDF Cybersecurity Personnel Development."

[109] Net Politics, "How Japan's Pacifist Constitution Shapes Its Approach to Cyberspace," *Council on Foreign Relations* (blog), May 23, 2018, https://www.cfr.org/blog/how-japans-pacifist-constitution-shapes-its-approach-cyberspace.

[110] Ministry of Defense, "Defense Buildup Program," 41–43.

[111] Ministry of Defense, "Defense Buildup Program," 20.

Japan's education system. Similarly, Japan must develop courses of action to incentivize public and private sector interaction. For example, the ministry could offer exchange programs where public sector officials shadow their counterparts in the private sector. Enabling public-private cross pollination aids in information sharing about possible intrusions and establishes relationships across the sectors that can help in responding to threats. If Japan is unable to overcome its recruitment and retention issues due to demographics and private sector opportunities, Japan should consider evaluating where automation can perform human tasks in ACD's defensive methods. Bartlett argues that one way Japan can overcome some of the personnel issues is by becoming more reliant on technology.[112] While relying on automation could solve some of Japan's personnel problems, developing a competent cyber core and increasing the number of cybersecurity professionals in the nation are still essential components to achieve security in the domain.

4. Education and Training

To improve Japan's ability to conduct ACD strategy, Japan will strengthen its cyber core through advanced education and training. As explained in Section B, an educated cyber core is an essential foundation to ACD operations. The MOD has a cyber education system it can build upon to create a competent cyber core able to oversee the new cybersecurity initiatives. The DBP indicates that the SDF will "reorganize…[and] expand the education infrastructure to train cyber personnel."[113] The MOD outlined internal education initiatives for educators and students by calling for the creation of a "cyber studies department at the National Institute for Defense Studies" for higher ranking officials and enhancement of cyber education at the SDF Academy.[114] Creating opportunities for senior officers allows for informed cyber commanders. Exposing younger SDF officers to cyber warfare encourages the next generation to serve in cyber roles, as well as educates them on the importance of the domain. The DBP identified how the military will develop a joint education training pipeline for SDF's cyber educators to ensure

[112] Bartlett, "Japan: An Exclusively Defense-Oriented Cyber Policy," 93.

[113] Ministry of Defense, "Defense Buildup Program," 11, 20–21

[114] Ministry of Defense, "Defense Programs and Budget of Japan," 21, 45.

all SDF branches receive the same cyber training no matter their service. The MOD states that Japan will "transform the Japan Ground Self-Defense Force High Technical School into a combined school of each service."[115] Identical education curriculums allows for integration across the SDF and ensures all cyber professionals receive the same cybersecurity terminology education. An integrated curriculum and cyber literacy across all services aids in developing a competent cyber core needed for ACD operations. MOD will also simultaneously improve internal cyber education and ally cooperation by offering higher education programs for Japanese cyber personnel within Japan and internationally. The MOD goes on to call for cyber competitions for the SDF and international actors, as well as an increase to international cyber dialogues and trainings.[116] The MOD's various education commitments demonstrate Japan's commitment to a professional cyber core, the importance the ministry places in future cybersecurity education, and highlights Japan's willingness to work with international partners in domain to develop its cyber core. The MOD's education pledges somewhat satisfy ACD's foundation requirement of a competent cyber core; however, the MOD does not specify if ACD curriculums will be integrate into Japan's education pledges.

Japan has not identified how the personnel will be reorganized or educated. The MOD does not communicate if or how ACD operations will be taught. Moving forward Japan will need to ensure its cyber core is taught the fundamentals of ACD operations. If Japan wishes to properly employ an ACD structure overseen by a professional cyber core, Japan should utilize the Ground SDF High Technical School's joint curriculum as an opportunity to educate its personnel on the spectrum of techniques ACD requires, outlined in Chapter II, and the six functional area of ACD management, outlined in Section B. An informed cyber core which understands the requirements and procedures from initial observation of an intrusion all the way to coordination of ACD methods will ensure Japan's cyber core is able to correctly employ the techniques of ACD. Similarly, Japan should utilize the cooperation avenues the DBP outlined as a way to educate its cyber core on the risks and rewards of limited offensive techniques. Since Japan has not implemented

[115] Ministry of Defense, "Defense Buildup Program," 43.

[116] Ministry of Defense, "Defense Buildup Program," 43.

countermeasures in the domain, cyber educators should encourage discussion in allied dialogue settings about the management of ACD's spectrum of techniques and utilize combined trainings as an opportunity to practice ACD methods. Additionally, the outlined efforts in the DBP do not address education of non-SDF personnel. Japan should clarify how the ministry plans to transform its non-military education platforms from solely passive defense operators to ACD operators. Japan should advocate for curriculum reform in university cybersecurity programs to include education on ACD strategy, structure, and operations.

5. Technology Acquisition

Prior to Japan's pledge to an ACD strategy, Japan was already regarded as a capable cyber nation due to its efforts in the late 2000s to centralize, invest, and develop its defensive cybersecurity structure. Japan's defensive cybersecurity efforts since the late 2000s support the nation's ability to build upon its defensive apparatus and introduce offensive ACD methods. Kallender and Hughes assert that since 2010, Japan has begun to emerge as a 'cyber power' due to Japan's centralized institutions able to detect cybersecurity intrusions.[117] Japan is not a powerless cyber nation, as Katagiri notes in Harvard's 2020 National Cyber Power Index (NCPI) report, Japan was ranked within the top ten of cyber powers.[118] Japan ranks highly as a capable cyber nation due to its defensive cyber capabilities. Katagiri believes that Japan should be considered as a capable cyber nation despite occasional network intrusions due Japan's investment in passive cyber defensives.[119] Additionally, Ogawa and Tsuchiya believe that the considerable increase in cybersecurity's budget since 2016 reflects how the "Japanese government has reasonably prioritized cybersecurity."[120] Chapter III identified that Japan's previous investment in passive cyber defense cyber may not halt new attacks, but defensive cybersecurity techniques are an essential aspect of ACD operations. Japan's previous investment in its

[117] Kallender and Hughes, "Japan's Emerging Trajectory as a 'Cyber Power,'" 26.

[118] Katagiri, "From Cyber Denial to Cyber Punishment," 336, 343.

[119] Katagiri, "The Soft Underbelly of Cyber Defence in Democracy," 343.

[120] Ogawa and Tsuchiya, "Cybersecurity Governance in Japan," 14.

cybersecurity apparatus and attention to passive resilient cybersecurity system provides a foundation for the development of future defense acquisition and fulfills ACD's defensive technology requirements.

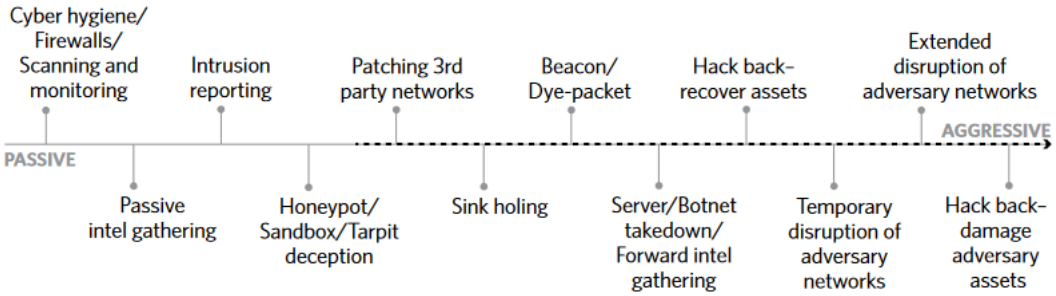
Japan pledged to standardize its cybersecurity systems for integration, introduce new defensive technologies and improve its cyber defenses with automation. These efforts will improve Japan's ability to consistently and effectively control ACD's defensive techniques. The MOD reviews the acquisitional steps that will occur to strengthen Japan's defensive cybersecurity. The DPB explains that Japan will develop a cloud system which will "integrate and standardize SDF systems that serve as the foundation of mission execution, and implement centralized cybersecurity measures."[121] It also notes several new systems being implemented: threat hunting equipment, cyber protection analyzers, systems and network management systems (SNMS), and physical protections to cyber facility infrastructure. Some of the technical updates outlined in the DPB satisfy the foundation of an ACD structure. Standardizing the SDF branches in the cyber domain and acquiring technology such as the threat hunting capabilities and protection analyzers grows Japan's defensive capabilities. Integration allows consistency of ACD techniques across all servers. Similarly, SNMS technology illustrates the relationship between human administrators and automation. Cisco explain that "network management systems have evolved to help IT teams operate in more agile ways, incorporating advanced analytics, machine learning, and intelligent automation to continually optimize network performance."[122] Managing multiple networks is challenging due to the speed and potential entry points in cyberspace. Administrators can reduce these challenges by implementing automation that can quickly and efficiently identify intrusions. While the DPB does not specify what specific network management systems will be acquired, the DPB still identifies that integration will occur across the MOD's networks and the administrators will be supported by automation to oversee all networks. The updates to Japan's cybersecurity integration, standardization,

[121] Ministry of Defense, "Defense Programs and Budget of Japan," 20.

[122] Cisco, "What Is Network Management?," n.d., https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-network-management.html.

and defensive technology aids in creating the foundation of ACD's technology and application.

However, the DPB and DBP do not mention how Japan will acquire limited offensive capabilities or how cyber personnel will receive trainings on these techniques. Japan has not announced what type of offensive capabilities would be acquired to respond to detected intrusions. Japan will be unable to deter new attackers if Japan is unable to implement offensive techniques that respond to intrusions. As mentioned in Chapter II, acquiring limited offensive capabilities is essential to ACD success. For deterrence to work within an ACD strategy, Japan must be able to neutralize and penetrate the attributed attacker if an intrusion occurs. To satisfy the countermeasure requirements of ACD strategy and develop a system with the spectrum of techniques identified in Figure 5, Japan should invest in dye-pack, hack-back, and botnet technology that can recover assets and disrupt adversary networks. Similarly, Japan must educate and train its cyber core on these offensive techniques to mitigate the possible risks of ACD techniques.



Source: Hoffman, Wyatt, and Ariel E. Levite. "The Spectrum of Active Cyber Defense." Private Sector Cyber Defense. Carnegie Endowment for International Peace, 2017. https://www.jstor.org/stable/resrep26906.7, 7.

Figure 5. Spectrum of ACD Methods

Katagiri and Soesanto mention that Japan approached private companies about offensive capabilities in the domain. Katagiri writes that "in 2012, the government

outsourced the development of offensive capabilities to firms like Fujitsu."[123] Soesanto then explains that "while the first developed 'seek and destroy' malware was shelved for unknown reasons, the status of the second project is currently unknown."[124] Both authors are cautious when making these statements. They each respectively note that there is no proof Japan ever utilized offensive techniques. Bartlett points out that "even these offensive capabilities are being built for defensive purposes to help prevent cyberattacks against Japan in a conflict scenario."[125] The offensive techniques ACD requires are not meant to be used before an intrusion is detected. An intrusion and malicious techniques must be utilized by the attacker on the defender's network before offensive techniques can be used to protect the defender. While Japan has previously invested in competent passive defense systems and outsourced the development of offensive cyber capabilities in the private sector, formal acquisition of limited offensive techniques and training to reduce possible risks will be necessary for Japan's public sector to properly apply an ACD strategy.

D. CONCLUSION

Japan's current cybersecurity infrastructure provides a foundation for the future integration of ACD strategy. To satisfy the basic requirements of ACD structure, Japan must develop an educated cyber core supported by technology and integrated into ACD's functional areas within the private and public sectors. To do this Japan must take the following steps: clarify how cyber stakeholders will respectively integrate ACD methods, develop ACD doctrine, follow through on its acquisition, education, and training commitments, and achieve its cyber personnel increase goals. While these pledges and plans are yet to be commitments due to political, legal, and social hurdles identified in Section A, efforts outlined in the NSS, DBP and DPB illustrate Japan's understanding of the changes necessary to execute an ACD strategy.

[123] Katagiri, "From Cyber Denial to Cyber Punishment," 338.

[124] Soesanto, Outward Defense: Comparing the Cyber Defense Postures of Japan, the Netherlands and the United States in Peace Time, 37.

[125] Bartlett, "Japan: An Exclusively Defense-Oriented Cyber Policy," 96.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

This thesis set out to explain the reasons and risks associated with Japan's pledge to implement an ACD strategy. Each chapter provides analysis that aids in explaining why and how Japan is pledging to transition its cyber strategy. Chapter II identifies the risks associated with ACD policy and outlines the reasons why nations execute ACD policy. The risks related to the ACD policy include unintended escalation, collateral damage, and misattribution, as well as the possibility for policy failure since the strategy cannot be immediately assessed. However, nations overcome these risks if they develop a competent cyber core and consistently communicate with the adversary. Nations adopt an ACD strategy to strengthen cybersecurity by mitigating intrusions and aiding in the development of responsible international cyber norms. The strategy also allows the defender flexibility by providing a spectrum of defensive and offensive techniques. The reasons and risks identified in Chapter II are then compared in Chapter III to Japan's current situation to determine why Japan pledged to adopt an ACD strategy.

Japan's case reflects the general reasons for adoption since Japan wishes to decrease the number of new attackers, incorporate flexible layered cybersecurity techniques, and develop norms amongst allies. Yet Japan's case also reflects unique reasons for adoption. Japan's perception of its security environment and its relationship to the U.S. are reasons unique to Japan's case. The general risks associated with the ACD strategy are reflected in the Japan case, but the manner in which Japan weighs the general risks are unique because of Japan's pacifist culture and legal restrictions governing its defense apparatus. The risks of military overreach and the potential violation of legal parameters force Japan to consider the general cyber risks far more cautiously than other nations.

Chapter IV evaluates what changes to cyber related structures are necessary for Japan's adoption of ACD. The chapter identifies the political, legal, and social hurdles Japan will face before implementation can occur. After reviewing the basics of general ACD, the chapter discusses Japan's plans for implementation of an ACD strategy and the limitations of Japan's current cyber apparatus. Japan's plan to increase its cyber core,

improve its cyber education system, and invest in updated defensive technology showcase its understanding that the nation must develop a professional cyber core supported by modern technology. Japan still must develop formal doctrine that clarifies who will oversee and execute ACD operations across the private and public sector, as well as identify how Japan will acquire and use limited offensive capabilities. To achieve the outlined pledges, Japan should consider creating the cyber ministry General Tatsuhiro proposed to oversee the implementation of the ACD strategy.[126] Overall, Japan is pledging to implement an ACD strategy to internally mitigate cyber intrusions and externally work alongside allies; however, Japan must follow through on its current plans for upgrading its cybersecurity apparatus and determine a command structure that ensures oversight on all essential networks.

A. IMPLICATIONS

Nations concerned with deterring intrusions in the cyber domain should consider implementing an ACD policy. The analysis on ACD policy in this thesis highlights the strategy's strengths and discusses ways to mitigate risk. The strategy allows a nation scalable protective defense and the option for tailored offensive capabilities. ACD is still a defensive strategy. As illustrated in Figure 1, p. 12, the strategy emphasizes the need for developed defensive techniques such as intrusion reporting technology and, if necessary, the strategy allows the defender to utilize limited offensive capabilities such as hack-backs after intrusions are detected. As states reevaluate the nature and characteristics of cyber warfare, it is apparent that intrusions are likely. Countries must develop methods to deter attackers, protect the defender and, when necessary, correct the attacker's actions. If a nation already has a defensive cyber apparatus maintained by a well-educated professional cyber core, nation should consider implementing an ACD strategy.

For Japan's case, the nation has already invested in passive defensive systems for the cyber domain. Still, Japan is failing to deter new attackers. Pledging to an ACD strategy showcases Japan's perception of the domain and its security environment. Japan understands that without cybersecurity, prosperity and national security is limited since the

[126] Takahashi Kosuke, "Japan Needs a Cyber Ministry: Former JGSDF Major General."

domain supports essential sectors. An ACD strategy highlights Japan's efforts for cyber normalization. While Prime Minister Kishida's announcements in December of 2022 do not allow for immediate implementation, the call for action in the cyber domain and directives for cybersecurity reorganizations showcase Japan's attention to cyber as a national security issue. Furthermore, the proposed changes outlined by the MOD indicate Japan's understanding that budget, personnel, education, and acquisition changes are necessary for future execution of ACD policy. Japan's previous endeavors in the late 2000s onward demonstrate Japan's willingness and ability to institutionalize cybersecurity at the national level. Although implementation may not happen for years, Japan's pledge illustrates that previous cybersecurity efforts are not protecting the nation well enough and new strategies should be explored.

Japan's recognition of cyber as a national security issue, its perception of its current cyber strategy, and its future pledge to policy transformation benefits not just Japan, but also its allies. Japan's policy transition may bring about more opportunities for allied engagement and dialogue. Increased communication and exchange between allies may lead to more robust partnerships. Although the U.S. experienced a different paradigm shift and transitioned to persistent engagement in the cyber domain, Japan's pledge to ACD policy moves Japan slightly closer to U.S. strategy. As the U.S.-Japan alliance values and pursues stability in East Asia, understanding one another's cyber doctrines diminishes the possibility for unintended escalation and strengthens the alliance cohesion. Overall, Japan's pledge to a new policy and attention to cybersecurity provide opportunities for more partnership and cooperation.

B. POLICY RECOMMENDATIONS

Japan should follow through on its pledge to implement ACD strategy to improve its ability to deter and respond to intrusions. Once Japan reaches the implementation phase by overcoming the political, legal, and social hurdles, Japan should ensure ACD concepts are integrated across all government and critical infrastructure systems. Since Japan directed the NISC to oversee the pledged cybersecurity changes, the NISC should establish a dedicated working group to oversee the pledges from start to finish. The group could be

composed of cyber professionals from the stakeholders outlined in Japan's cybersecurity structure (see Appendix A). It would also benefit the working group to reach out to cybersecurity professionals in the private sector and request representation from the U.S. and United Kingdom. The working group could draft implementation phases, establish benchmarks, and develop measures to test the policy's success. These efforts would aid in establishing a reasonable timeline for Japan and underscore the policy's progress. Additionally, the working group could split into various sub-groups by assigning people to different areas. The sub-groups could follow NATO's DOTMLPFI concept. The concept assists in the transformation of capability development by stepping through doctrine, organization, training, material, leadership, personnel, facilities, and interoperability.[127] Dividing the working group into these respective categories and stepping through them sequentially may provide a holistic approach to implementation and ensure all details of the policy are developed across Japan's cyber infrastructure.

Other efforts that would benefit the future of Japan's cybersecurity infrastructure include exposure to cyber education earlier in Japan's education system, opportunities for university cyber program exchanges, and incentives for private/public cross pollination. Exposing younger generations to tech conversations aids in developing an enthusiastic tech generation and responsible society online. A Manfield's report summarized existing U.S.-Japan cyber exchanges that aid in expanding Japan's cyber infrastructure.[128] The report concluded by outlining different policy recommendations, some of which emphasized standardizing cyber education amongst high school and university students. Japan should continue to collaborate with allies on problem sets in the cyber domain to deepen the partner relationship and solve complex personnel issues. Additionally, Japan should create opportunities for government cybersecurity experts to shadow private sector companies. The government experts could return to their ministries with new ideas and a better

[127] Inci Kucukaksoy, "NATO Capability Development & Interoperability," The Three Swords Magazine, 2016.

[128] The Maureen and Mike Mansfield Foundation, "Building A Cyber Workforce: Through The U.S.-Japan Alliance" (The Maureen and Mike Mansfield Foundation, August 2023), https://mansfieldfdn.org/wp-content/uploads/Building-a-Cyber-Workforce-Through-the-U.S.-Japan-Alliance-Policy-Brief.pdf, 8, 12–13.

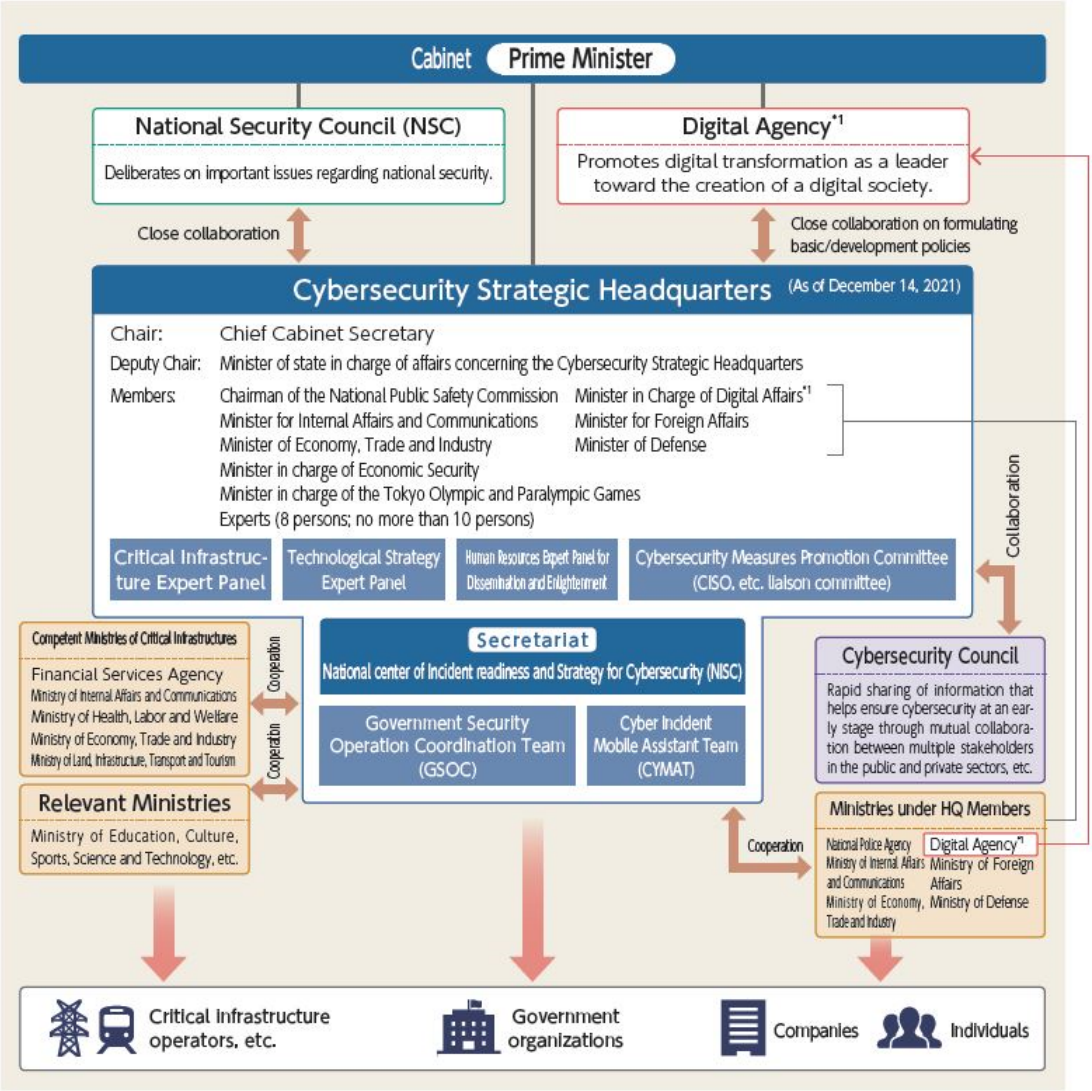
understanding of private sector responsibilities. Exchanges between the private and public sector in the domain will create relationships and assist in achieving a cooperative cyber apparatus.

C. FUTURE RESEARCH

Future research should assess Japan's willingness to implement ACD policy, investigate how the NISC plans to accomplish its assigned directives, and periodically review Japan's pledges to determine if the pledges are being carried out. Although Chapter IV assumed Japan's unique political, legal, and social challenges will be addressed in order to review how Japan will achieve implementation, future research may determine Japan's willingness to enact these policy pledges. The research could utilize previous normalization efforts that succeeded and failed to determine the probability of Japan successfully implementing ACD strategy. By analyzing the general characteristics of Japan's defense policy tendencies, policy makers could have a better understanding for how ACD will be carried out. Additionally, more research should be dedicated to how the NISC will reorganize Japan's cybersecurity apparatus to achieve an ACD concepts. As the most impactful cybersecurity stakeholder in Japan's cyber structure, it will be important to follow the NISC's developments. Future research could evaluate Japan's progress in accomplishing its pledges every six months to determine Japan's projected timeline and continued shortcomings. By building upon this research policy makers and cybersecurity professionals may achieve a better understanding of why Japan wishes to normalize in the cyber domain and what challenges Japan faces in executing cybersecurity policy.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX: JAPAN'S CYBERSECURITY STRUCTURE



(*1) Basic Act on Creation of a Digital Society (Act No. 35 of 2021), Act for Establishment of the Digital Agency (Act No. 36 of 2021). (effective since September 1, 2021)

Source: "About NISC," National center of Incident readiness and Strategy for Cybersecurity, https://www.nisc.go.jp/eng/index.html.

Figure 6. Japan's Cybersecurity Structure

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Armitage, Richard L., Joseph S. Nye Jr, Victor Cha, Matthew P. Goodman, and Michael J. Green. "The U.S.-Japan Alliance in 2020," December 7, 2020. https://www.csis.org/analysis/us-japan-alliance-2020.

Arquilla, John, Bradley J. Strawser, Steven E. Miller, Stephen Blank, Michael Sulmeyer, Emily Goldman, George Perkovich et al. "Active Cyber Defense: Applying Air Defense to the Cyber Domain." In *Understanding Cyber Conflict: 14 Analogies*. Georgetown University Press, 2017.

Bartlett, Benjamin. "Japan: An Exclusively Defense-Oriented Cyber Policy." *Asia Policy* 27, no. 2 (2020): 93–100. https://doi.org/10.1353/asp.2020.0013.

———. "Why Do States Engage in Cybersecurity Capacity-Building Assistance? Evidence from Japan." *The Pacific Review*, February 28, 2023. https://nps.primo.exlibrisgroup.com/discovery/fulldisplay/cdi_webofscience_primary_000942176100001/01NPS_INST:01NPS.

Chanlett-Avery, Emma, and Caitlin Campbell. "The U.S.-Japan Alliance." Congressional Reserach Service, June 13, 2019. https://crsreports.congress.gov/product/pdf/RL/RL33740.

Chen, Teresa, Alana Nance, and Summer Han-ah. "Water Wars: Japan's Defense Buildup Signals a Shift Away from Post-WWII." *Lawfare* (blog), February 6, 2023. https://www.lawfareblog.com/water-wars-japans-defense-buildup-signals-shift-away-post-wwii.

Cisco. "What Is Network Management?," n.d. https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-network-management.html.

"Cyber Capabilities and National Power: A Net Assessment." International Institute for Strategic Studies, June 28, 2021. https://www.iiss.org/research-paper//2021/06/cyber-capabilities-national-power.

Dewar, Robert S. "Active Cyber Defense." ETH Zurich, 2017. https://doi.org/10.3929/ethz-b-000169631.

Dominguez, Gabriel. "Recruitment Issues Undermining Japan's Military Buildup." The Japan Times, January 2, 2023. https://www.japantimes.co.jp/news/2023/01/02/national/japan-sdf-recruitment-problems/.

Fischerkeller, Michael P. *Cyber Persistence Theory: Redefining National Security in Cyberspace*. Bridging the Gap. New York, NY: Oxford University Press., 2022.

Green, Michael. “China.” In *Line of Advantage: Japan’s Grand Strategy in the Era of Abe Shinzo*. New York: Columbia University Press, 2022.

Harrington, Sean L. “Cyber Security Active Defense: Playing with Fire or Sound Risk Management?” *Richmond Journal of Law & Technology* 20, no. 4 (2014).

Healey, Jason. “The Implications of Persistent (and Permanent) Engagement in Cyberspace.” *Journal of Cybersecurity* 5, no. 1 (January 1, 2019): tyz008. https://doi.org/10.1093/cybsec/tyz008.

Herpig, David. “Active Cyber Defense Operations: Assessment and Safeguards.” Transatlantic Cyber Forum, November 2021. https://www.stiftung-nv.de/sites/default/files/active_cyber_defense_operations.pdf.

Herring, Mj, and Kd Willett. “Active Cyber Defense: A Vision for Real-Time Cyber Defense.” *Journal of Information Warfare* 13, no. 2 (2014): 46–55.

HM Government. “National Cyber Security Strategy 2016–21,” November 2016. https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.

Hoffman, Wyatt, and Ariel E. Levite. “Private Sector Cyber Defense : Can Active Measures Help Stabilize Cyberspace?” *Carnegie Endowment for International Peace*, 2017. https://search.proquest.com/docview/1917694386?pq-origsite=primo.

———. “Rethinking Corporate Active Cyber Defense.” Lawfare, July 17, 2017. https://www.lawfareblog.com/rethinking-corporate-active-cyber-defense.

———. “The Spectrum of Active Cyber Defense.” Private Sector Cyber Defense. Carnegie Endowment for International Peace, 2017. https://www.jstor.org/stable/resrep26906.7.

Hornung, Jeffery, and Christopher Johnstone. “Japan’s Strategic Shift Is Significant, but Implementation Hurdles Await.” War on the Rocks, January 27, 2023. https://warontherocks.com/2023/01/japans-strategic-shift-is-significant-but-implementation-hurdles-await/.

Hornung, Jeffery, and Adam Liff. “Japan’s New Security Policies: A Long Road to Full Implementation.” *Brookings* (blog), March 27, 2023. https://www.brookings.edu/blog/order-from-chaos/2023/03/27/japans-new-security-policies-a-long-road-to-full-implementation/.

Hughes, Christopher W. *Japan as a Global Military Power: New Capabilities, Alliance Integration, Bilateralism-Plus*. 1st ed. Cambridge Elements. Elements in Politics and Society in East Asia. Cambridge, United Kingdom ; New York: Cambridge University Press, 2022.

Japan NISC. "Overview of Cybersecurity 2023," July 4, 2023. https://www.nisc.go.jp/eng/pdf/overview_of_cybersecurity2023_en.pdf.

Jasper, Scott. *Strategic Cyber Deterrence: The Active Cyber Defense Option*. Lanham, Maryland: Rowman & Littlefield, 2017.

Jervis, R. "Some Thoughts on Deterrence in the Cyber Era." *Journal of Information Warfare* 15, no. 2 (2016): 66–73.

Jiji. "Japan to Speed up SDF Cybersecurity Personnel Development." The Japan Times, July 11, 2023. https://www.japantimes.co.jp/news/2023/07/11/national/sdf-cyber-capabilities/.

Johnstone, Christopher B. "Japan's Transformational National Security Strategy," December 8, 2022. https://www.csis.org/analysis/japans-transformational-national-security-strategy.

"JPCERT/CC Incident Handling Quarterly Report," n.d. https://www.jpcert.or.jp/english/ir/report.html.

Kallender, Paul, and Christopher W. Hughes. "Japan's Emerging Trajectory as a 'Cyber Power': From Securitization to Militarization of Cyberspace." *Journal of Strategic Studies* 40, no. 1–2 (2017): 118–45. https://doi.org/10.1080/01402390.2016.1233493.

Katagiri, Nori. "From Cyber Denial to Cyber Punishment: What Keeps Japanese Warriors from Active Defense Operations?" *Asian Security* 17, no. 3 (September 2, 2021): 331–48. https://doi.org/10.1080/14799855.2021.1896495.

———. "The Soft Underbelly of Cyber Defence in Democracy: How Interest Groups Soften Japan's Cyber Policy." *Journal of Cyber Policy* 7, no. 3 (September 2, 2022): 336–52. https://doi.org/10.1080/23738871.2023.2192227.

Kawaguchi, Takahisa. "Japan's Defense Policy in Cyberspace." Stimson Center – Asia, March 2020. https://www.stimson.org/wp-content/uploads/2020/03/KeyChallengesInJapansDefensePolicy-March2020-V3-web.pdf.

Kucukaksoy, Inci. "NATO Capability Developmet & Interoperability." *The Three Swords Magazine*, 2016.

Lewis, James Andrew. "Creating Accountability for Global Cyber Norms," February 23, 2022. https://www.csis.org/analysis/creating-accountability-global-cyber-norms.

Matsuda, Takuya. "Japan's Emerging Security Strategy." *The Washington Quarterly* 46, no. 1 (2023): 85–102. https://doi.org/10.1080/0163660X.2023.2190218.

Ministry of Defense. “Defense Buildup Program,” December 16, 2022. https://www.mod.go.jp/j/policy/agenda/guideline/plan/pdf/program_en.pdf.

———. “Defense Programs and Budget of Japan: ‘First Year’ Budget for Fundamental Reinforcement of Defense Capabilities,” 2023. https://www.mod.go.jp/en/d_act/d_budget/pdf/230330a.pdf.

———. “Regarding Response to Cyber Attack.” Japan Ministry of Defense, n.d. https://www.mod.go.jp/en/.

Ministry of Justice. The Constitution of Japan and Criminal Statutes (1947). https://japan.kantei.go.jp/constitution_and_government_of_japan/constitution_e.html.

Nakamura, Ryo. “Chinese Cyberattacks on Japan Prompts U.S. Push for Stronger Defenses.” Nikkei Asia, August 10, 2023. https://asia.nikkei.com/Politics/International-relations/US-China-tensions/Chinese-cyberattacks-on-Japan-prompts-U.S.-push-for-stronger-defenses.

Nakashima, Ellen. “China Hacked Japan’s Sensitive Defense Networks, Officials Say.” *Washington Post*, August 17, 2023. https://www.washingtonpost.com/national-security/2023/08/07/china-japan-hack-pentagon/.

Nakasone, Paul M. “A Cyber Force for Persistent Operations.” *Joint Force Quarterly : JFQ*, no. 92 (2019): 10–22.

National Security Council. *National Defense Strategy*. Tokyo, Japan: Ministry of Foreign Affairs of Japan, 2022. https://www.mofa.go.jp/fp/nsp/page1we_000081.html.

———. *National Security Strategy of Japan*. Tokyo, Japan: Ministry of Foreign Affairs of Japan, 2022. https://www.mofa.go.jp/fp/nsp/page1we_000081.html.

Net Politics. “How Japan’s Pacifist Constitution Shapes Its Approach to Cyberspace.” *Council on Foreign Relations* (blog), May 23, 2018. https://www.cfr.org/blog/how-japans-pacifist-constitution-shapes-its-approach-cyberspace.

Nye, Jr. “Cyber Power.” *Belfer Center for International Relations*, May 2010. https://apps.dtic.mil/sti/citations/ADA522626.

Ogawa, Hidetoshi, and Motohiro Tsuchiya. “Cybersecurity Governance in Japan.” *International Journal of Cyber Diplomacy*, 2021, 7–31.

Oros, Andrew. “Japan’s Relative Decline and New Security Challenges in a Multipolar Asia.” In *Japan’s Twenty-First-Century Security Renaissance*, 66–79. New York: Columbia University Press, 2017.

Osawa, Jun. "How Japan Is Modernizing Its Cybersecurity Policy." *Stimson Center* (blog), February 2, 2023. https://www.stimson.org/2023/japan-cybersecurity-policy/.

Osula, Anna-Maria, and Henry Roigas, eds. *International Cyber Norms: Legal, Policy & Industry Perspectives*. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2016. https://ccdcoe.org/library/publications/international-cyber-norms-legal-policy-industry-perspectives/.

Phuong Le, Tom. "Who Will Fight? The JSDF's Demographic Crises." In *Japan's Aging Peace: Pacifism and Militarism in the Twenty-First Century*, 64–105. Columbia University Press, 2021.

Public Security Intelligence Agency. "Overview of Threats in Cyberspace." Ministry of Justice, 2023. https://www.moj.go.jp/content/001398997.pdf.

Romanosky, Sasha, and Zachary Goldman. "Understanding Cyber Collateral Damage." *Journal of National Security Law & Policy* 9, no. 2 (2017): 233–57.

———. "What Is Cyber Collateral Damage? And Why Does It Matter?" *Lawfare – Cybersecurity & Tech* (blog), November 15, 2016. https://www.lawfaremedia.org/article/what-cyber-collateral-damage-and-why-does-it-matter.

Russell, and Kostyuk. "Evaluating the U.K.'s 'Active Cyber Defence' Program." Lawfare, February 14, 2018. https://www.lawfareblog.com/evaluating-uks-active-cyber-defence-program.

Schelling, Thomas C. *Arms and Influence*. Veritas paperback edition. Veritas Paperbacks. New Haven, CT: Yale University Press, 2020. https://doi.org/10.12987/9780300253481.

Schneider, Jacquelyn, Emily O. Goldman, Michael Warner, Paul Nakasone, and Chris Demchak. "Ten Years In: Implementing Strategic Approaches to Cyberspace." *U.S. Naval War College* Special Collections (2020). https://digital-commons.usnwc.edu/usnwc-newport-papers.

Shigeta, Shunsuke. "Japan to Extend Cyberdefense Umbrella to Private Sector." Nikkei Asia, December 31, 2022. https://asia.nikkei.com/Politics/Japan-to-extend-cyberdefense-umbrella-to-private-sector.

Smeets, Max. "U.S. Cyber Strategy of Persistent Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection." *Intelligence and National Security* 35, no. 3 (2020): 444–53. https://doi.org/10.1080/02684527.2020.1729316.

Smith, Sheila. *Japan Rearmed: The Politics of Military Power*. Cambridge: Harvard University Press, 2019.

Soesanto, Stefan. Outward Defense: Comparing the Cyber Defense Postures of Japan, the Netherlands and the United States in Peace Time. Konrad Adenauer Stiftung, 2021.

Starks, Tim. "Analysis | China's Hacking of Japan's Defense Networks 'Was Bad — Shockingly Bad.'" *Washington Post*, August 8, 2023. https://www.washingtonpost.com/politics/2023/08/08/chinas-hacking-japans-defense-networks-was-bad-shockingly-bad/.

Stevens, Tim, Kevin O'Brien, Richard Overill, Benedic Wilkinson, Tomass Pildegovics, and Steve Hill. "UK Active Cyber Defence: A Public Good for the Private Sector." *Policy Institute at King's College London*, January 2019.

Taddeo, Mariarosaria. "The Limits of Deterrence Theory in Cyberspace." *Philosophy & Technology* 31, no. 3 (2018): 339–55. https://doi.org/10.1007/s13347-017-0290-2.

Takahashi Kosuke. "Japan Needs a Cyber Ministry: Former JGSDF Major General." Diplomat, September 19, 20222. https://thediplomat.com/2022/09/japan-needs-a-cyber-ministry-former-jgsdf-major-general/.

Temple-Raston, Dina. "Q&A with Gen. Hartman: 'There Are Always Hunt Forward Teams Deployed,'" June 20, 2023. https://therecord.media/maj-gen-william-hartman-interview-ukraine-russia-click-here.

The Government of Japan. "English Translation of the Pamphlet of Cybersecurity Strategy (Cabinet Decision)." National Center of Incident Readiness and Strategy for Cybersecurity, September 2021. https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-en-booklet.pdf.

The Maureen and Mike Mansfield Foundation. "Building A Cyber Workforce: Through The U.S.-Japan Alliance." The Maureen and Mike Mansfield Foundation, August 2023. https://mansfieldfdn.org/wp-content/uploads/Building-a-Cyber-Workforce-Through-the-U.S.-Japan-Alliance-Policy-Brief.pdf.

The White House. "Joint Statement of the United States and Japan." The White House, January 13, 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2023/01/13/joint-statement-of-the-united-states-and-japan/.

———. *National Cybersecurity Strategy*. Washington, D.C.: White House, 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/.

———. *National Security Strategy of the United States of America*. Washington, DC: White House, 2022. https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

———. “U.S.- Japan Joint Leaders’ Statement,” April 17, 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/16/u-s-japan-joint-leaders-statement-u-s-japan-global-partnership-for-a-new-era/.

U.S. Cyber Command Public Affairs. “CYBER 101: Hunt Forward Operations.” U.S. Cyber Command, November 15, 2022. https://www.cybercom.mil/Media/News/Article/3218642/cyber-101-hunt-forward-operations/https%3A%2F%2Fwww.cybercom.mil%2FMedia%2FNews%2FArticle%2F3218642%2Fcyber-101-hunt-forward-operations%2F.

U.S. Department of Defense. *Strategy for Operating in Cyberspace*. Washington, DC: Department of Defense, 2011. https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

Zhao, Quansheng. *Great Power Strategies – the United States, China and Japan*. China Policy Series. Milton: Taylor & Francis Group, 2022. https://doi.org/10.4324/9781003298502.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Fort Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California