NATIONAL SECURITY RESEARCH DIVISION

U.S.–Japan Alliance Conference

Strengthening Strategic Cooperation

Scott W. Harold, Martin C. Libicki, Motohiro Tsuchiya, Yurie Ito, Roger Cliff, Ken Jimbo, Yuki Tatsumi

For more information on this publication, visit www.rand.org/t/CF351

Published by the RAND Corporation, Santa Monica, Calif.

Preface

In 2015, after two years of study and policy coordination, the United States and Japan publicly issued new defense guidelines, updating and expanding upon the previous guidance of 1997. The new guidelines enable a much broader set of cooperative engagements, including in geographic areas beyond the areas surrounding Japan and in the new domains of outer space and cyberspace. While no single threat or challenge spurred the allies to issue new guidelines, they have clearly emerged in an environment characterized by a rising China, a provocative North Korea, and rapid defense-related technological change. The evolution of U.S. and Japanese security strategies, as well as partner states' willingness to engage in collaborative security building and regional cooperation, have shaped the prospects for using the U.S.–Japan alliance in new ways to protect the allies' security and contribute to peace and stability in the Asia-Pacific region.

In order to explore, explain, and advance security cooperation in the various spaces and domains described above, RAND undertook a seven-month project that brought together a series of leading specialists on Asian security, cybersecurity, and building partner capacity. In March 2016, about a year after the announcement of the new security guidelines, RAND convened the research team to present their findings in a pair of public conferences keynoted by former Japanese Minister of Defense Itsunori Onodera and former U.S. Secretary of Defense Chuck Hagel. This conference report describes the findings of the research effort and the context in which the two allies are operating now and into the future. It also lays out a series of options for how the United States and Japan can further strengthen cooperation on cybersecurity, enhance the safety and hygiene of the online ecosystem, improve partner states' military capabilities and compliance with democratic norms and values in Southeast Asia, and deepen cooperation and collaboration with Australia. In so doing, this conference report seeks to advance a future security environment characterized by strong and consistent cooperation among democratic allies and their security partners, oriented toward peace, security, development, and an international order based on rule of law in which disputes are settled peacefully and without coercion.

This research was sponsored by the Government of Japan and conducted within the International Security and Defense Policy Center of the RAND National Security Research Division (NSRD). NSRD conducts research and analysis on defense and national security topics for the U.S. and allied defense, foreign policy, homeland security, and intelligence communities and foundations and other nongovernmental organizations that support defense and national security analysis.

For more information on the RAND International Security and Defense Policy Center, see www.rand.org/nsrd/ndri/centers/isdp or contact the director (contact information is provided on the web page).

Contents

Abbreviations

A2/AD	anti-access/area denial
ACTIVE	Advanced Cyber Threats Response InitiatiVE
ADF	Australian Defence Force
AFP	Armed Forces of the Philippines
ARF	ASEAN Regional Forum
ASEAN	Association of Southeast Asian Nations
AUSMIN	Australia–United States Ministerial Consultation
BPC	building partner capacity
CBA	capacity-building assistance
CCC	Cyber Clean Center
CDC	Centers for Disease Control and Prevention
CERT	computer emergency response team
CIRO	Cabinet Intelligence Research Office
CNAS	Center for a New American Security
CSH	Cybersecurity Strategic Headquarters
CSIRT	computer security incident response team
DARPA	Defense Advanced Research Projects Agency
DDoS	distributed denial of service
DHS	U.S. Department of Homeland Security
DNS	domain name server
DoD	U.S. Department of Defense
DPRK	Democratic People's Republic of Korea [North Korea]
EDCA	Enhanced Defense Cooperation Agreement
EWI	East West Institute
FMS	Foreign Military Sales
GSOC	Government Security Operations Coordination team
HA/DR	humanitarian assistance and disaster relief
HUMINT	human intelligence
IMINT	imagery intelligence

IMR	Indicator and Measurement Registry
ISIS	the Islamic State of Iraq and Syria
ISR	intelligence, surveillance, and reconnaissance
JASDF	Japan Air-Self-Defense Force
JGSDF	Japan Ground Self-Defense Force
JMSDF	Japan Maritime Self-Defense Force
JPCERT/CC	Japan Computer Emergency Response Team Coordinating Committee
JPS	Japan Pension Service
JSDF	Japan Self-Defense Forces
KHI	Kawasaki Heavy Industries
MHI	Mitsubishi Heavy Industries
MOD	Ministry of Defense [Japan]
NATO	North Atlantic Treaty Organization
NDPG	National Defense Program Guidelines
NISC	National Center for Incident Readiness and Strategy for Cybersecurity
NSS	National Security Strategy [Japan]
ODA	official development assistance
PCG	Philippines Coast Guard
QDR	Quadrennial Defense Review
SDMX	Statistical Data and Metadata Exchange
SEATO	Southeast Asia Treaty Organization
SIAS-J	situations in areas surrounding Japan
SIGINT	signals intelligence
SPE	Sony Pictures Entertainment
WHO	World Health Organization

1. Deepening Dialogue on Asia Strategy

Scott W. Harold, Ph.D.
Political Scientist
RAND Corporation

Introduction

How are the United States and Japan responding to the rise of an assertive China, employing cyber capabilities and paramilitary forces backed by increasingly powerful air, naval, and missile forces, to challenge the established order in the Asia-Pacific region? What options do the allies have for tightening their collaboration on cybersecurity in the wake of the North Korean hacking of Sony Pictures Entertainment in America, which could demonstrate an ambition to employ cyberwarfare more broadly in the future? In the face of these challenges, in April 2015, the United States and Japan issued new guidelines on defense cooperation, expanding military cooperation into new physical and electronic domains, including outer space, cyberspace, and assistance to regional partners in Southeast Asia. The new guidelines replace a previous set of revised guidelines issued in 1997 in the wake of the 1993–1994 North Korean nuclear crisis and China's missile exercises in the Taiwan Strait in 1995 and 1996. The previous document clarified Japan's ability and intention to cooperate with the United States in responding to security challenges in situations in areas surrounding Japan (SIAS-J), a somewhat ambiguous geographic region intended to incorporate both the Korean Peninsula and Taiwan without explicitly naming them. The new 2015 guidelines expand on this cooperation by improving the allies' ability to respond to gray zone or paramilitary contingencies, establishing a new alliance coordination mechanism, and encouraging coordinated efforts to shape the regional security environment. In accordance with this last step, both Washington and Tokyo have sought to enhance their own capabilities and further tighten their defense relationships with other countries, such as Australia, and have begun providing military assistance to maritime states in Southeast Asia facing Chinese pressure over competing claims in the South China Sea.

Recognizing the importance of understanding these changes in depth, RAND brought together leading U.S. and Japanese experts on cybersecurity and the two countries' relations with Southeast Asia and Australia, which were among the most important new areas of cooperation identified in the 2015 defense guidelines. RAND convened a pair of public conferences in Santa Monica, California, in March 2016 to share the project's research findings with policymakers and the general public. Keynoted by remarks from former Japanese Minister of Defense Itsunori Onodera and former U.S. Secretary of Defense Chuck Hagel, the two-day event received substantial media attention and public participation. The two former defense leaders focused

their remarks on explaining the reasons for the revision of the defense guidelines and described how the U.S.–Japan alliance can serve as a force for peace and stability in the years ahead.

The scholarly presentations made at the two conferences (and the papers included in this report, which the experts' public remarks were based on) explored the following questions: How can the United States best cooperate with Japan on improving cybersecurity? What is the best model for enhancing the health of the cyber ecosystem? Is there a threshold beyond which a cyberattack on an ally would occasion a kinetic response under the U.S.–Japan Mutual Security Alliance? What steps should the United States and Japan take to bolster Southeast Asian nations' military capabilities to defend themselves? Why is Japan interested in playing a more active role today, and what steps are open to it as it seeks to assist Southeast Asian states? How far can trilateral U.S.–Japan–Australia cooperation go? These are explored more fulsomely in the papers that follow.

Summaries of Included Papers

Chapter 2: In his essay on U.S.–Japan cooperation on cybersecurity, Martin Libicki of RAND notes that Japan has made significant strides in improving its cybersecurity over the past decade and can make many of the remaining changes on its own without substantial U.S. assistance, largely by purchasing commercially available off-the-shelf cybersecurity technologies. Nonetheless, the United States can assist Japan in a number of areas, including by reinforcing overall deterrence and security commitments, sharing intelligence indications and warning, encouraging and assisting with improvements in active defenses, making enhancements to post-attack remediation, and sharing lessons learned. He concludes by arguing that while some of the options above may be most useful to pursue in a bilateral context, others would actually be more valuable if multilateralized so as to provide (for example) information about threat vectors and vulnerabilities to all potential victims of cyberattack. Such an approach, Libicki notes, would potentially have the added benefit of shaping and reinforcing global norms, institutions, and multilateral cooperation.

Chapter 3: Presenting a Japanese perspective on U.S–Japan cybersecurity cooperation, Keio University's Motohiro Tsuchiya starts by describing the rapidly evolving history of cyberintrusions that have affected Japan, including the hacking of Mitsubishi Heavy Industries, Sony Pictures Entertainment (a U.S.-based subsidiary of Japan's Sony Corporation), and the unauthorized entry into the systems of the Japan Pension Service. These high-profile hackings got the attention of the Japanese government and private sector, which are evaluating the need for a plan to defend the country's systems from the onslaught of intrusions expected around the time of the 2020 Tokyo Olympics. The government's responses have included passing the 2014 *Cybersecurity Basic Law*, establishing the National Center for Incident Readiness and Strategy for Cybersecurity, setting up a Cybersecurity Strategic Headquarters to coordinate closely with the country's new National Security Council, and publishing a *Cybersecurity Strategy* in 2015.

While these steps have been substantial, the government's ability to respond remains seriously limited by historical legacies from the fascist period prior to the end of World War II, most notably in the form of a prohibition on establishing a capacity for domestic surveillance and signals intelligence collection. Tsuchiya argues that addressing the challenge of balancing civil liberties concerns with the imperative of protecting vulnerable networks and critical infrastructure remains a task for the nation's political leaders. Given the constraints on the Japanese government at present, it relies heavily on U.S. assistance to deter and respond to threats to computer network systems and critical infrastructure that rise above mere cybercrime to the level of a cyberattack. Tsuchiya also argues that the new defense guidelines that the two sides have issued can also usefully focus joint cooperative efforts on intelligence-sharing and capacity-building. He closes by suggesting that the two sides pay greater attention to the protection of undersea submarine cables that serve as the backbone of the Internet.

Chapter 4: Shifting from a perspective defined largely in national security terms to one framed through the lens of public health, Yurie Ito, the executive director of CyberGreen, shares information about this recently formed nonprofit organization. CyberGreen got its start with Japanese government funding and works to link together national computer emergency response teams in the Asia-Pacific to provide insights into the global cyber threat environment. In socializing and providing cross-national data for comparison and lessons-learning, CyberGreen seeks to encourage good cyber hygiene, enhance the "health" of the Internet by quickly and effectively directing resources to problem areas as they emerge, and move away from a simple "name and shame" approach to an approach that will give localities and national governments more incentive to remediate problem areas in their portions of the Internet. To that end, they are striving to establish and encourage the adoption of common metrics and standards for cyber ecosystem health on the premise that "you can't manage what you can't measure."

Chapter 5: Turning from the allies' attempts to shape the online environment to their collective efforts to determine the broader security environment in the physical domain in the Asia-Pacific, Roger Cliff of the Atlantic Council explores a wide variety of assistance and capacity-building options that the United States and Japan have or could undertake with respect to Southeast Asia. Focusing primarily on efforts to assist Association of Southeast Asian Nations members in ways that are commensurate with U.S. and Japanese national security interests and with broader democratic values, Cliff finds that the most promising areas include helping to ensure continued democratic development and security, counterterrorism, counterpiracy, ensuring the peaceful and equitable resolution of territorial disputes, and engaging in humanitarian assistance and disaster relief (HA/DR) in the wake of natural or man-made crises. Because many countries in Southeast Asia are only nominally or tenuously democratic, Cliff argues that they should only receive two types of assistance: aid that does not help their militaries engage in repression and assistance that actively encourages their armed forces to accept civilian control. Others appear to be much further along the pathway to consolidated democratic governance and can be given more fulsome military assistance. In almost all

countries across the region, however, there are at least some options for pursuing a positive agenda that may contribute to consolidation of a southern tier of democratic states that are positively disposed to the United States and Japan and supportive of mainstream international norms and values.

Chapter 6: Ken Jimbo of Keio University echoes Cliff's finding that there are promising options to assist Southeast Asian nations on security affairs, but he focuses his analysis more narrowly on areas that may hold promise for addressing concerns over a rising, assertive China seeking to change the status of disputed maritime areas through coercion. To that end, he describes how the notion of building partner capacity (BPC) emerged in Japanese government strategy, focused most specifically on assisting the nations bordering the South China Sea with the development of maritime domain awareness. Japan has relaxed its rules on the export of defense articles in recent years and adopted a new approach to provision of excess defense articles that characterizes these as "strategic overseas development assistance" (or "strategic ODA"). The Japan Self-Defense Forces have also helped train and educate some regional militaries' personnel, while Japan's International Cooperation Agency has been investing in port and road development that could benefit regional militaries. Overall, Jimbo argues, helping to enhance the human resources; infrastructure; hardware; and intelligence, surveillance, and reconnaissance capabilities of regional militaries (especially navies) to resist coercion and demand the peaceful settlement of territorial disputes through international law is and should be the focus of Japan and the United States.

Chapter 7: In the final essay, Yuki Tatsumi of the Henry L. Stimson Center explores the growing bilateral and trilateral cooperation among the United States, Japan, and Australia. She argues that the increasingly close cooperation among these allies and security partners is being driven by three factors: developments within each country's own security strategy; positive signals and opportunities in the three relationship dyads (the United States and Japan, the United States and Australia, and Japan and Australia); and considerations stemming from the worsening regional security environment, driven primarily by the rise of an aggressive, increasingly well-armed and ambitious China that appears bent on changing the status of contested territories and bodies of water, most notably in the South and East China Seas, through intimidation and coercion. The allies' shared assessments of the risks of North Korean nuclear and missile capabilities, as well as the positive experiences of joint response to such disasters as the Indian Ocean tsunami of 2004 and the Great East Japan earthquake and triple disaster of 2011 have also helped drive cooperation forward. Tatsumi notes that HA/DR is an area in which the three sides are already cooperating extremely closely, while capacity-building in Southeast Asia is a growing focus and (writing before Canberra's decision late in April 2016 to award its next-generation submarines contract to French firm DCNS) joint defense industrial development appears set to take off. Tatsumi highlights that certain forms of security cooperation (HA/DR and BPC) are likely to continue, while others (joint defense industrial development) appear more contingent on the continuance of shared threat assessments, something that can be affected

deeply by political developments internal to each country. While neither a trilateral alliance nor a Japan–Australia alliance are likely to take the place of the bilateral U.S. alliances that both Tokyo and Canberra rely on, the prospects for continued deepening of collaboration on defense nonetheless appear bright.

Conclusion

Through the opportunity to dialogue with senior defense leaders, policy analysts, scholarly counterparts, and the assembled audience members, the participants deepened their own understandings of the issues under consideration, expanded their personal networks, and helped to inform the public about the reasons and implications for the evolution of the U.S.–Japan alliance in important new directions. Looking ahead, cooperation between the two biggest status quo powers in the Asia-Pacific appears likely to both deepen and grow ever more important if the region is to remain peaceful and shaped by a set of common rules and institutions. Whether through joint efforts to enhance cybersecurity or as a result of unilateral (but sometimes coordinated) attempts to bolster vulnerable Southeast Asian nations, as the research and analyses in this volume show, the prospects for the U.S.–Japan alliance to play a positive role in shaping the regional and online security environments are promising, timely, and important.

2. U.S.–Japanese Cooperation in Cyberspace: Potential and Limitations

Presenter: Martin Libicki, Ph.D.
Senior Management Scientist
RAND Corporation

Introduction

How can close allies like the United States and Japan cooperate most effectively in cyberspace? In October 2012, then–U.S. Secretary of Defense Leon Panetta warned of the prospect of a future cyber "Pearl Harbor," a metaphor that highlights the extent to which U.S. officials worry about the prospect of attack through cyberspace.[1] In 2014, Sony Pictures Entertainment, an American subsidiary of the Japanese Sony Corporation, was hacked in an attack attributed to North Korea. And in 2015, the United States and Japan issued revised Defense Guidelines that identified cybersecurity as a key new area in which they would cooperate. This paper examines some of the ways in which the United States and Japan can cooperate to enhance their cybersecurity and assesses the benefits that may result.

A recent RAND report[2] that analyzed the hundreds of policy options that can be employed to increase the cybersecurity of an organization concluded that only a small fraction of these options are things that a government can do to enhance nongovernment cybersecurity. Furthermore, most of these—such as catching more cybercriminals and facilitating standards-setting—are highly indirect. For the most part, it is up to organizations to defend their own systems. This year they will spend close to $80 billion doing so.[3]

Similarly, the ability of any government, including the United States, to help another country, such as Japan, defend its computer systems is likely to be highly constrained. Perhaps the most meaningful step the United States can take is to bolster the ability of the government of Japan to ensure the cybersecurity of its own systems. Still, since most of the critical computer systems in

[1] Elisabeth Bumiller and Thomas Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.," *New York Times*, October 11, 2012.

[2] John S. Davis II, Martin C. Libicki, Stuart E. Johnson, Jason Kumar, Michael Watson, and Andrew Karode, *A Framework for Programming and Budgeting for Cybersecurity*, Santa Monica, Calif.: RAND Corporation, TL-186-DHS, 2016.

[3] Markets and Markets, "Cyber Security Market Worth $170.21 Billion by 2020," news release, undated; see also data from Gartner, "Gartner Says Worldwide Information Security Spending Will Grow Almost 4.7 Percent to Reach $75.4 Billion in 2015," September 23, 2015; and Martin Giles, "Defending the Digital Frontier," *The Economist*, July 12, 2014.

Japan are not run by the government of Japan, such gains are likely to be very limited (though some, such as My Number, the national identification system, are critical and do constitute likely targets of attack). The same limitations apply when Japan helps the United States.

Despite the caveats noted above, cooperation on cybersecurity between the United States and Japan can be valuable even if the amount of money spent addressing the threat environment is several orders of magnitude less than the aforementioned $80 billion. Indeed, most of what each country can do to help its allies, friends, and partners is to extend the results of activities that each already does today. There already have been multiple agreements over the past several years between the United States and Japan that touch on cooperation in cyberspace. The most relevant recent U.S.–Japan cybersecurity agreement is the Joint Statement of the Security Consultative Committee[4] (April 27, 2015), which "called for continued progress in cooperation on cyberspace issues, particularly in the areas of threat information sharing, mission assurance, and infrastructure protection." Furthermore, the Joint Statement of the U.S.–Japan Cyber Defense Policy Working Group observed,

> The MOD [Japan's Ministry of Defense] and DOD [U.S. Department of Defense] are already using and refining existing channels to share cyber threat and vulnerability information and best practices. The sharing of information will include best practices on military training and exercises, education and workforce development; this may include site visits and joint training and exercises, as appropriate. The MOD and DOD, in cooperation with other relevant government agencies, are to explore how to improve cyber information sharing through various channels in a crisis environment, and work toward timely, routine, two-way information sharing and the development of common cyber threat indicators and warning.[5]

This paper explores and evaluates these policy options, starting with deterrence and then turning to indications and warning, improvements in active defenses, enhancements to post-attack remediation and lessons learned, and other forms of improvements to cybersecurity. It concludes with some thoughts on the value of such cooperation and its limitations.

Deterrence by Punishment

Countries typically defend themselves in part by promising that attacks on them will be met by punishment. Although the United States and Japan are bound in a mutual defense treaty and cyberwar has been deemed to fall under that treaty, the degree to which such deterrence—much less extended deterrence—can actually improve Japan's cybersecurity is unclear.

Estonia, for instance, was covered under the North Atlantic Treaty Organization's (NATO's) Article V guarantees, but NATO declared that the 2007 cyberattacks on Estonia from Russia—

[4] U.S. Department of State, "Joint Statement of the Security Consultative Committee: A Stronger Alliance for a Dynamic Security Environment—The New Guidelines for U.S.-Japan Defense Cooperation," April 27, 2015.

[5] Joint Statement of the U.S.–Japan Cyber Defense Policy Working Group, May 30, 2015.

which disrupted financial and government functions carried out online but created no casualties—did not invoke such guarantees. The official explanation was no one could prove that the Russian government (as opposed to Russian citizens and ethnic Russians) carried out the attacks. But it hardly helped that many Europeans doubted that a cyberattack was an actionable use of force, much less one sufficient to trigger common defense obligations (in any event, such attacks stopped well before the NATO ruling). In 2014, NATO asserted that cyberattacks did constitute actionable activities, but this is only the first step in a long process of figuring out how cyberwar fits into NATO doctrine.

Difficulties in implementing effective deterrence, notably those associated with determining attribution and communicating red lines, still persist and are relevant for the U.S.–Japan alliance. Since 2012, U.S. officials have argued that U.S. attribution capabilities are much better than people might assume. But would the U.S. ability to attribute attacks be as good as it is if countries that employed or sheltered attackers actually paid a price for their doing so—or would the imposition of such penalties persuade attackers to cover their tracks better? To date, most of what has been attributed appears to reflect an assumption that attribution can be done by combining motivation and data reflecting past *modus operandi*.

The attribution of the Sony attack to North Korea, for example, was facilitated because the hackers used signatures and techniques similar to those used a year and a half earlier in attacks on South Korean institutions (for which, presumably, only North Korea had a motive). Even if the United States has other ways of knowing who carried out a cyberattack, it is unclear how to publicly respond to a putative attacker when relevant evidence is not for public eyes.

The threshold issue also has to be resolved in order to cope with cyberattacks that are less severe than those that are obviously tantamount to war—as an extended takedown of the power grid might be. Prior to the Sony attack, the United States hinted that cyberattacks on its critical infrastructure would cross a red line—but afterward it argued that the attack on Sony's moviemaking arm demanded a response because it implicated free-speech principles, one of the "fundamental American values."[6] In the meantime, it is not easy to identify what exactly the United States did to North Korea in response to Sony (apart from naming and shaming) that would deter a repeat performance.

During the Cold War, there was also an expectation that the United States would respond to a nuclear attack on its allies the same way that it would respond to a nuclear attack on its own homeland. (France, for one, was not entirely sure that the United States would "trade New York for Paris" and went on to develop its own deterrent.) But while everyone assumed that the United States would not let a nuclear detonation on its soil go unanswered in kind, there is no such expectation for cyberattacks and thus there are comparable doubts about extending the U.S. deterrent umbrella for cyberattacks on U.S. allies. Furthermore, while the United States said that

[6] Joseph Marks, "White House Cyber Czar: Even Non-Critical Infrastructure Vulnerable—Top Sony Corp. Exec Condemns Hack at CES," *Politico*, January 6, 2015.

it would not retaliate for a kinetic attack on an ally if that ally failed to provide for its own defense (since defense was supposed to reflect *mutual* effort), the analogy breaks down in cyberspace, where defense is *not* a mutual effort. Instead, in cyberspace it is primarily the responsibility of the network system's owner to provide for its own security. As a consequence, it would be plausible that one country could refuse to respond to a cyberattack on another by citing the other's failure to protect its own assets.

Fortunately, deterrence policy does not have to be absolutely unquestioned to be effective. An attacker may doubt that a response is coming, but it may also doubt that it can act with impunity. The larger the attack, the greater the likelihood that the mutual defense treaty will be invoked. Thus, even absent formal red lines, there should be some understanding by potential attackers that the United States would not stand by if a costly and/or deadly cyberattack were launched against Japan. Although a U.S. response may not necessarily come in the form of a kinetic military response or even a cyber hack-back, there would likely be a response that would hurt the attacker sufficiently to make it and others rethink the value of such an action. In that sense, the mutual defense treaty is a reflection of the importance of Japan's national security to the United States, and any U.S. response to a cyberattack would reflect that importance.

Indications and Warning

Apart from deterrence, every other element of cooperation in cyberspace between the United States and Japan (or any two countries, for that matter) entails the exchange of information. When one reflects that cyberspace is a medium through which information alone can travel, this limitation is quite understandable. In the following sections, I review the many pieces of information that can travel between the United States and Japan, starting with indications and warning: actionable information that warns of a possible imminent cyberattack or, at least, indicates conditions under which the odds of a cyberattack are significantly elevated.

The process of sharing indications and warning data is not necessarily problematic; the United States can choose to share actionable intelligence with Japan or vice versa. At present, the United States and Japan share many types of intelligence and some of these, when combined, may indicate a heightened risk of a forthcoming cyberattack. Indeed, if the subject is a cyberattack on Japan, the chances are good that a combination of various types of information derived from a number of different sources will be required to make such a determination about an elevated threat level.

One problem comes when assessing how reliable and actionable such information might be. To start with an easy example, imagine that the United States finds out that a group in a hostile country is preparing a cyberattack against Japan. Furthermore, assume that the United States can distinguish between a credible cyberthreat and idle talk. Here, the indications and warning data can be valuable—but not by itself sufficient. The reason why is that characteristic of most cyberattacks (apart from distributed denial of service [DDoS] and border gateway protocol

attacks) is that they are enabled by exploitable flaws in the system being attacked. Thus, if the nature of the attack were known with sufficient specificity, it would also be possible to disarm the attack by fixing the flaw in the target system. The United States could simply write and send out the requisite patch if the attack had yet to be implanted or a detect-and-clean kit if the attack had been implanted but not yet activated. This not only helps protect the intended targets but also other targets. But the knowledge that Japan is going to be attacked, without an indication of *how* it is to be attacked, is not so actionable. By way of analogy, consider the difference between an intelligence report that asserts that al Qaeda is going to attack the United States soon and one that asserts that it will do so by using its operatives to hijack airplanes for suicide missions that would crash into U.S. landmark buildings. The first piece of knowledge was not specific enough to lead to changes in behavior by the United States. The second, even though its information was still fairly general, could have been used to inform the flying public that resistance, rather than acquiescence, was the wiser choice following a hijacking—contrary to prevailing wisdom before the September 11, 2001, attacks. The differences in approach can be seen by comparing the flights that crashed into the World Trade Center and the Pentagon and United Airlines Flight 93, which the passengers helped to bring down in a field near Shanksville, Pennsylvania.

Other indicators are much better at saying *what* than *when*. Destructive malware found in a system can indicate that a system has been targeted, but discovering this may not provide much clue as to when such malware will be set off or who created it. Removal and timing are also important considerations. If the price of warding off an attack is to limit a system's connectivity or a user's privileges, how disruptive will it be to take the system offline or reduce access to it in order to clean it? In addition, because some cyberattacks are prefatory to the use of force, knowing when the attack is set to take place helps in knowing whether to mobilize against the use of such force (particularly when sustained mobilization is costly).

Unless the United States is actually looking into Japanese systems (or vice versa), it is unlikely to discover implanted malware code directly. However, if the United States has other ways of determining that, for example, a particular code set is malware, it can devise methods for hunting for such code (or correlated evidence of the code's presence, such as suspiciously altered settings) and pass them on to Japan. A variation of such indications and warning is to look at the characteristics of a brand of attack in other parts of the world, conclude that such an attack would work in Japan (or the United States), and develop countermeasures (and then share these). Another variation exploits the fact that carrying out catastrophic cyberattacks is a chancy process, and thus there may be many failures on the road to success as hackers work out the successive barriers to scaling up attacks. Thus, evidence of near-successes (or near-catastrophic attacks) indicates that a catastrophic attack is probably coming. The United States and Japan could and should, in such a case, share such evidence in order to ascertain the odds of such an event in ways that neither could do alone without the evidence that the other has. Unfortunately, while such warnings might, for example, nudge the management of infrastructure systems in the direction of cybersecurity, they rarely say much about when or where such an attack may come.

Another indicator of the timing of an attack is that countries that intend to carry out cyberattacks of a serious nature (well in excess of what we have seen to date) are, as noted above, likely also planning to carry out other moves as well. Conversely, evidence that other moves may be imminent could also signal an impending cyberattack. What a country or organization can do in advance of cyberattacks whose nature is no clearer than before this type of warning is limited: Actions include accelerating patch installation, responding to the discovery of ambiguous or subtle anomalies by network management systems (at the cost of generating more false positives), and limiting exposure of systems to the outside.

Missing from this list are traditional, straightforward indications and warning data (for example, evidence that a rocket is being fueled would indicate that its use was imminent). Twenty years ago, it was believed that a series of small cyberattacks would presage a large one (granted, hackers do sometimes test attacks in the 24 hours before deploying them worldwide); today, this assumption is increasingly open to question. The fact is that there is no sequence of events that must proceed a major cyberattack in a given time frame. Furthermore, in a world that has yet to see a large cyberattack, there is no basis in empirical experience to say what presages a catastrophic cyberattack.

Although this discussion has been framed in terms of bilateral cooperation, it raises the question of whether an indications and warning discussion should be bilateral, or even multilateral. If the value of indications and warning is to motivate action *and* the primary targets of a cyberattack are private actors, then they are the ones most at risk, and they must be informed so as to take action to defend themselves. In most of these cases it is difficult to argue why such indicators should not be broadcast publicly instead of merely shared bilaterally through official channels.[7] Unfortunately, because many of these indicators come from the intelligence community, they come wrapped in a shroud of secrecy—to the point where the direst warnings are those hardest to transmit to the parties best placed to act on them.

Active Defense

One of the reasons that deterrence by punishment has risen to prominence as a way of dealing with cyberattacks is that deterrence by denial (sometimes referred to as "passive defense") is deemed unsatisfactory, despite the tens of billions of dollars that have been spent on it. Believing that the best defense is a good offense, many analysts have argued for "active defense," or a practice of reaching out into red space (adversary networks) or at least gray space (networks that belong to neither the attacker nor the defender, such as those that connect countries) to disable cyberattacks before they start. Thus, part of the cooperation between the United States and Japan might include preemptive U.S. operations against those who would attack Japan.

[7] There is an argument about crying wolf too often, but it applies to bilateral sharing as well.

But can active defense actually help? In some cases, it might. International efforts to dismantle large botnets (large numbers of remotely controlled computers), for instance, reduce the severity of DDoS attacks, in which such computers are commanded to contact a targeted website, thereby preventing legitimate users from doing so. But because botnets can be used against a wide variety of targets, this sort of active defense probably constitutes general rather than country-specific relief.

Active defense also presents some serious unknowns, notably the requirement that exquisite, actionable intelligence will actually be available and the willingness to run the risk that reaching out into red space to disable an attack before it is launched does not set off an escalatory spiral. Indeed, without compelling and publicly releasable proof, such actions could conceivably be portrayed (even by a malicious adversary who was preparing to execute an imminent attack) as a violation of sovereignty that could shift global public opinion against those that moved preemptively to stop the attack before it was launched.

A more fundamental problem is that success in countering cyberthreats in this way is hard to repeat. Once attackers know that their malware or command-and-control servers have been corrupted, they can employ fairly straightforward countermeasures—such as digital signatures or sleeper command-and-control servers—and get back in business very quickly. As with cyberattacks themselves, the essence of active defense is surprise. It may work once—and if the forestalled attack was going to do substantial damage then it may be worth the United States doing so for Japan—but it should not be counted upon as a long-term strategy or approach for preventing cyberattacks.

Lessons Learned and Threat Indicators

To paraphrase one leading cybersecurity thinker, Ross Anderson, the reason that airplane safety keeps improving and cybersecurity seems to get worse every year is that airplanes crash outdoors and computers crash indoors.[8] When airplanes crash (or have near-misses or other incidents that might have resulted in crashes), there is an intensive investigation on what went wrong. When computers go down (in the face of cyberattack), the facts, much less the analyses of how they were taken down, are often hidden. Even the United States government—which urges private firms to talk about cyberattacks and imposes such requirements on their contractors—is usually careful not to reveal the causes of its own network security failures (the hack on the U.S. Office of Personnel Management being a case in point). Nevertheless, because every successful or even partially successful cyberattack is a potential case study in failure, and every failure is a learning opportunity, much learning about how to improve cybersecurity is simply not happening. Accordingly, sharing lessons can be part of the cooperation between the

[8] Inferred from Ross Anderson, "Why Cryptosystems Fail," presented at the 1993 Association for Computing Machinery Computer and Communications Security Conference, p. 1.

United States and Japan, allowing each to learn from the other. Indeed, such cooperation is implied by current agreements.

Threat indicators, or sets of common markers that are believed to be (or actually have been) associated with cyberattacks, are more specific. Some threat indicators may include malware signatures or social engineering tricks. They can be fed into firewalls and intrusion detection systems as well as shared with systems administrators. Indicators of compromise are similar but are detected within a system (e.g., a suspicious file in an unexpected directory) rather than at the border of a system. Some threat indicators may include malware signatures or social engineering tricks. They can be fed into firewalls and intrusion detection systems and shared with systems administrators. Indicators of compromise are similar but are detected within a system (e.g., a suspicious file in an unexpected directory) rather than at the border of a system.

But the same question about indications and warning can be raised about lessons learned and threat indicators: Why share bilaterally what you can broadcast? One reason might be the sensitivity of the information. Yet, whereas it is considered unprofessional to withhold information on aviation or medical mistakes, withholding information on cybersecurity mistakes is for some reason seen as acceptable by segments of the cyber community, something which should be rethought. There may be ways to talk about how attacks happened without talking about who they happened to. Another reason that is sometimes cited for a bilateral approach to sharing is that by sharing insights with Japan, the United States can persuade it to reciprocate on this or other sensitive issues on which the United States seeks deeper intelligence-sharing. In practice, this might be true, but in terms of cyberhygiene, at least, it is clearly a second-best approach.

Assistance with Cybersecurity

The United States boasts the world's deepest wells of cybersecurity expertise, whether measured among competing military organizations or more broadly to include commercial services (though, on a per capita basis, Israel probably has a better-developed industry). It would therefore seem logical for the United States to offer its services to Japan to help protect that nation. But if the best assistance is private, then assisting means subsidizing Japan's purchase of U.S. commercial services. Japan, which is a rich country, should arguably be the one to pay to secure its own systems, not the U.S. taxpayer. Several years ago, one could argue that Japan was behind the curve and was largely ignorant of the threat to its systems—threats that were clearly visible in the United States, which was at the time rapidly ramping up spending on cyberdefense. In that environment, U.S. assistance could arguably have helped to jump-start Japan's efforts to recognize and react to the threat environment it was operating in. Today, however, this argument no longer holds water; for several years now, Japan has been acutely conscious of the threat it faces from cyberspace—a threat it estimates will only continue to grow as the 2020 Tokyo Olympics approach.

There is, however, at least one fundamental problem with relying on commercial service providers for cybersecurity, and that is that they are, in fact, commercial. Vendors may be prone to exaggerating the cybersecurity problem or characterizing it in ways that highlight their own cybersecurity product. Experienced organizations can more easily identify qualified vendors, but it takes time to become experienced, and initial levels of distrust between Japanese organizations and international cybersecurity firms may lead to underinvestment. Military and civilian assistance from the United States could serve a role as an honest broker. The National Institute for Standards and Technology in the United States has decades of experience in identifying optimal levels of cybersecurity investment and could play an important role in helping Japan assess where best to focus its cybersecurity investments.

When it comes to protecting *military* systems, the United States and Japan have a mutual legitimate interest in each other's cybersecurity in ways that do not apply as much with civilian systems (even if both Japan and the United States have an interest in the other not buckling to coercion from a cyberattack). An infection that spreads from a poorly controlled system to a well-controlled system harms the efficiency of coalition warfare and erodes mutual trust. Here, the U.S. military is not necessarily the better-protected organization; what it gains through deeper cybersecurity expertise, it may lose by connecting systems that might more prudently be left unconnected (or by digitizing content unnecessarily). In many cases, what is needed is not only an exchange of expertise to improve cybersecurity but also a fine-grained understanding of how missions carried out jointly by U.S. and Japanese forces may be imperiled through inattention to cybersecurity (or from enthusiasm for networking that outruns the ability to secure networked systems). In other words, although information assurance is often understood as the purpose of cybersecurity, and this is something that can be supplied by systems specialists, mission assurance is the true purpose of cybersecurity, and that is something that can only be supplied by military specialists. Therefore, there is a basis for the U.S. and Japanese military to assist each other's cybersecurity efforts.

Other Forms of Cooperation

Last but not least on the list of areas for U.S.–Japan cybersecurity cooperation are the everyday forms of cooperation between U.S. and Japanese officials and bureaus (including private but government-supported institutions) to promote cybersecurity. These are hardly controversial (cost is essentially the only reason not to continuously increase such cooperation), but not necessarily unimportant for that reason.

Information-sharing, particularly internationally, can offer a great deal of value. Listening to those with very different perspectives on difficult topics (of which cybersecurity is surely one) is an effective antidote to stale thinking. Cooperation among national computer emergency response teams provides a venue for exchanging technical knowledge. Information-sharing also helps each side understand why the other side may respond to cyberattacks or other serious

systems intrusions in the way they do. There are also number of ways in which the United States and Japan could cooperate at the human level—for example, to cultivate a culture of operational security or improving cyber-defense. Thus, if cyberattacks rise to a serious international issue—as the Sony intrusions may have—better understanding should facilitate mutual support in such crises. A history of information-sharing also helps grease the wheels of justice in those cases where the United States or Japan may have to indict each other's citizens over a cybercrime.

Conclusions

The relationship between the United States and Japan is the bedrock of international security in the Asia-Pacific region. Correspondingly, cooperation between the United States and Japan to improve mutual cybersecurity is as important a component of this relationship as cyberspace is to international security in general.

As argued above, international cooperation can be divided into two spheres: those that relate directly to the U.S.–Japan alliance and those that make sense because the United States and Japan share mutual interests in establishing norms and maintaining and improving cybersecurity. Among the former are improvements to deterrence, indications and warning, and active defenses. Deterrence is ineluctably bilateral, but if either country finds an attack in the making (e.g., sitting in red or gray space) or other evidence that an attack is coming, it may not always be clear where the attack is going. Thus, what would be a bilateral issue for kinetic conflict may be a multilateral or public issue in cyberspace. The more general forms of information-sharing, notably lessons learned and threat indicators, can and perhaps should be done publicly, or at least multilaterally, rather than bilaterally, unless they involve information that is *justifiably* deemed sensitive. Nevertheless, if the choice is between bilateral cooperation or no cooperation at all, the former is clearly preferable.

Finally, expectations for what such cooperation can achieve should be tempered. When it comes to critical systems operated by private-sector actors, governments are usually on the outside looking in; when it comes to what governments can do for each other, allies are on the outside looking in as well.

3. Japan–U.S. Cooperation on Cybersecurity

Presenter: Motohiro Tsuchiya, Ph.D.
Professor, Graduate School of Media and Governance
Keio University

Introduction

Most of the cyberattacks reported in the mass media are actually better characterized as cybercrimes, cyber espionage, or cyber sabotage. These cyberattacks employ "weapons of mass disturbance" rather than real weapons, which cause physical damage. However, we cannot deny the possibility of a real cyberattack in the future—that is, a "cyber operation . . . [that causes] injury or death to persons or damage or destruction to objects."[9] In the six years that have passed since the revelation of the Stuxnet attack on Iran's nuclear facility in 2010, it is possible that state and nonstate actors may have developed the ability to employ such destructive cyber weapons.

The first shocking cyber operation against the Japanese government occurred in 2000. Some government web sites were taken over, and their contents were falsified. This incident occurred right after the government published a policy against cyberterrorism. However, it was regarded as a technical problem, not as a national security issue that would directly affect Japanese society and the Japanese economy.

Nowadays, broadly defined cyberattacks (including cybercrimes and cyber espionage) are everyday things in Japan and the world. Not only web falsifications but also the deliberate sabotaging of critical infrastructure, the causing of disorder in financial markets, and the penetration of defense systems constitute possible risks.

This paper begins by introducing the three most impactful cyber operations conducted against Japan in the past. It then moves on to review the Japanese government's responses to such cyberthreats. Finally, it concludes by exploring possible options for cybersecurity cooperation between Japan and the United States.

Major Cyber Incidents in Japan

Mitsubishi Heavy Industries

According to *Defense News*, Mitsubishi Heavy Industries (MHI) is the 36th largest defense contractor in the world, and its size is around one-fifteenth of Lockheed Martin (the world's

[9] Michael N. Schmitt, ed., *The Tallinn Manual on the International Law Applicable to Cyber Warfare*, New York: Cambridge University Press, 2013, Rule 30.

largest defense industrial firm). However, MHI is the largest defense firm in Japan, 1.38 times larger than Kawasaki Heavy Industries (KHI), Japan's second-largest defense contractor.[10] MHI produces special-purpose vehicles, ships, combat aircraft, helicopters, engines, aircraft equipment, and derivation equipment. It plays a core role in developing and maintaining Japan's defense industrial base and defense technologies.

In September 2011, it was reported that 86 personal computers and servers at MHI had been compromised. The company did not recognize this intrusion initially, and it is possible that a variety of defense technologies were stolen (though exactly what information was stolen, if any, has not been publicly confirmed). However, MHI was not the first target. Attackers had previously compromised the Society of Japan Aerospace Companies, an industry association related to MHI, KHI, and others. The Society did not assume that it had valuable information and did not employ sufficiently robust security methods in defense of its computer networks. An account at the association was taken over, and disguised email messages were sent to several defense contractors. This is how MHI was tricked into infecting its own systems.

This incident impressed upon the Japanese nation that Japan itself was a target of hostile cyber operations; it also strengthened the tendency of private-sector companies to hide evidence of having been hacked for fear of damaging their reputations with capital markets.

Sony Pictures Entertainment

In November 2014, Japan watched the developing story of the cyberattacks against Sony Pictures Entertainment (SPE) with great interest and a high degree of shock. While the company is an American firm, the Sony brand has Japanese origins, and many Japanese citizens view the hack as if it had happened to a Japanese company.

The U.S. government pointed the finger at the Democratic People's Republic of Korea (DPRK; North Korea). Despite their frequently bombastic rhetoric, the DPRK leadership tends to be cautious in calculating the impact of their actions when they attack or engage in confrontations with foreign countries. Launching a kinetic attack is much riskier than carrying out cyber operations and is much more likely to result in severe repercussions. The plausible deniability of cyberattacks and the use of proxies is thus an ideal alternative for Pyongyang.

Since the MHI case, many Japanese companies have become sensitized to the possible fallout of cyberattacks, particularly as nation states have begun to target private companies. This rarely happened in the Cold War era, but it now seems a defining characteristic of cyber conflict.

Sony had been cyberattacked in April 2011 by users of the company's PlayStation Network. Some users were angry about Sony's policy on hacking of Sony devices, which led to cyberattacks against the company. Sony thus should have been well-prepared for cyberattacks, though it is also true that 100-percent security is impossible. This incident also taught Japanese society an important lesson: Any company, big or small, can be a target of cyberattacks.

[10] Defense News, "Top 100 for 2015," undated.

Japan Pension Service

In May 2015, the servers of the Japan Pension Service (JPS) were compromised by four different computer viruses, and the personal pension information of up to 1.25 million enrollees was leaked. This attack became a major political issue. In all likelihood, the theft will not directly result in any serious damage, as the information pilfered included only names, postal addresses, telephone numbers, and pension numbers. Without credit card or other account numbers, these will not be enough to tap into personal finances, but monetizing the theft may not have been the thieves' primary motive.

More likely, the culprits were looking to use the internal information hacked from the JPS's computer system as an inroads to other agencies and organizations. The same method was used in the MHI case. Japan's central ministries have continued to beef up their cybersecurity systems, and accomplishing a breach would be no easy task. Hackers have instead turned their sights on peripheral targets, including government-affiliated organizations, think tanks, private companies working with the government, and universities. Media attention has focused largely on the theft of pension records, but this breach may represent only the tip of a more extensive operation.

Later investigations by NHK (*Nippon Hoso Kyokai*; Japan Broadcasting Corporation), Japan's public broadcasting service, revealed that more than 1,000 organizations were under cyberattack at the same time as the JPS. It was a huge operation, much larger than previously thought. At least 20,000 documents and files may have been stolen from the affected government and private organizations. According to NHK, data were sent to a commercial company in Shanghai, China. And those transmitted data were forwarded to another company in Guangzhou, China. NHK could not prove the involvement of the Chinese government, but Chinese actors were seen behind the incidents.[11]

The Japanese Government's Response

Cybersecurity Basic Law

Even before the SPE incident became public, the Japanese Diet was taking steps to reinforce cybersecurity. In November 2014, the Diet passed the Cybersecurity Basic Law,[12] and it became effective in January 2015; in the Japanese system, a basic law sets the country's long-term strategic goals in a certain policy area.

---

[11] NHK, "NHK Special: CYBER SHOCK," February 7, 2016.

[12] The text in Japanese is available at House of Representatives, "サイバーセキュリティ基本法案 [Cyber Security Basic Bill]," 2014.

After passing the law, the National Information Security Center was transformed into the National Center for Incident Readiness and Strategy for Cybersecurity (NISC).[13] It acquired more authorities and strengthened its legal basis to oversee cybersecurity issues in Japan. The Information Security Policy Council, which set cybersecurity policies across the government and reported to the Chief Cabinet Secretary, was renamed the Cybersecurity Strategic Headquarters (CSH), and today this body cooperates closely with the new Japanese National Security Council, chaired by the Prime Minister. The CSH's mandate is broad, covering the setting of Japan's strategic goals for cyberspace, protection of critical infrastructure, raising of public awareness, research and development, and information-sharing.

There is an international component of the Cybersecurity Basic Law. Article 23 requires Japan to contribute to international arrangements that improve its cybersecurity. The SPE incident came at a timely moment to test Japan's new responsibilities.

Cybersecurity Strategy 2015

Based on the Cybersecurity Basic Law, the CSH laid out its draft of a new Cybersecurity Strategy on May 25, 2015. Chief Cabinet Secretary Yoshihide Suga, who heads the CSH, immediately ordered a second version of the draft when the JPS was found to have been hacked. The new strategy was finalized on August 20, 2015, and was approved by the Cabinet on September 4. While the Cabinet's approval did not make the strategy law, it did confer it quasi-legal status. The strategy demonstrated Japan's high-level commitment to cybersecurity and formed the basis of measures to be implemented henceforth at ministries, agencies, and other government organizations.

Looking at the new strategy, the first thing to note is the stepped-up capabilities of the Government Security Operations Coordination team (GSOC). As a part of the NISC, GSOC has mainly been responsible for watching over the computer systems and networks of central government ministries. It was GSOC that first discovered the hacking of JPS and informed it of the intrusion, though (owing to the nature of the hack) the breach could not be addressed quickly. In response to this, the government extended GSOC's monitoring abilities to cover government-affiliated organizations as well, including incorporated administrative agencies and special public corporations (the JPS falls under the latter). It is also expected to bolster the budgets and staff of the NISC and GSOC to enable them to fulfill their roles as cybersecurity control towers.

A second point of the strategy is the government's efforts toward not only post-incident response but also proactive prevention. The strategy promotes understanding among relevant parties of the need to report even small-scale damage and signs of suspicious activity to safeguard against large-scale cyberattacks. It also puts an emphasis on bolstering both internal and external systems of cooperation and information-sharing. It goes without saying that a

[13] The NISC tried to keep its acronym as NISC and ended up with a strange name with "cybersecurity" and without "information security."

speedy response and recovery is essential following a cyberattack, but it also should be possible to prevent incidents from occurring by monitoring networks and systems and sharing information about hacking incidents among different agencies and with global partners.

A third point is the strategy's effort to strike a balance between security and free access. It underscores the impossibility and impracticality of tasking the government with maintaining order in cyberspace. In global cybersecurity talks, China and Russia have called on states and governments to take greater roles in policing unlawful activities by boosting surveillance and control measures. In response, Japan, the United States, and European countries have argued for the need to guarantee freedom of speech and the free flow of information. Entrusting cybersecurity solely to the state may result in the kind of surveillance society that exists in China and Russia. Japan has openly expressed its opposition to such a scenario. The Japanese strategy articulates the government's firm stance against state use of cyberspace to control, censor, steal, or destroy information, as well as its "illicit use" by terrorists and other nonstate actors. It goes on to establish the government's commitment to proactively contribute to conserving cyberspace for "peaceful purposes" while also ensuring the safety of the country.

Looking at the language of the revised strategy, the 40-page document contains 51 derivations of the word "sharing" and 80 usages of "cooperation." By comparison, "sharing" appeared 48 times and "cooperation" just 62 times in the earlier, 43-page Cybersecurity Strategy approved in June 2013. Information-sharing in the wake of hacking incidents and cooperation among organizations can be seen as pillars of Japan's Cybersecurity Strategy. Those activities are actually becoming more common domestically and internationally.

Signals Intelligence Capabilities

After the Edward Snowden revelations in 2013, the U.S. National Security Agency and the United Kingdom's Government Communications Headquarters were criticized for their data collection efforts. In contrast, however, the Japanese government's signals intelligence (SIGINT) capabilities have maintained a lower profile due to the legal and political restrictions they operate under. After its defeat in the Second World War, Japan's intelligence agencies were abolished, and the General Headquarters of the Allied Forces took over their authorities. Brigadier General Charles A. Willoughby was in charge of intelligence activities under General Douglas M. MacArthur until the San Francisco Peace Treaty entered into force in 1952.

In the early spring of 1952, about one month before Japan's regained its full independence, Jun Murai, secretary for Prime Minister Shigeru Yoshida, sought to reestablish Japan's intelligence capabilities. He tried to organize a Japanese version of the U.S. Central Intelligence Agency with Yoshida and Taketora Ogata, then serving as Deputy Prime Minister. Murai's plan was not fully realized due to political turmoil, and he ultimately went on to become Chief of the Cabinet's Research Office (today's Cabinet Intelligence Research Office [CIRO]) in April 1952. The intelligence capabilities of this body were quite limited. Today, human intelligence (HUMINT) activities are covered by the CIRO, the Public Security Intelligence Agency, and the

National Police Agency; the scale of Japanese HUMINT today, however, is extremely small compared with the activities of most nations of Japan's economic and population sizes.

After the end of Cold War, when the DPRK launched a Taepodong missile over Japan's main island in 1998, things began to change. This event triggered discussions within Japan on the need for the country to have its own satellites for imagery intelligence (IMINT) activities. Previously, Japan had relied on the United States for IMINT. The need to monitor the DPRK at all times accelerated the deployment of satellites, but Japanese government policy did not permit the use of space for military purposes; as such, the government described its new space-based intelligence, surveillance, and reconnaissance assets as information-gathering satellites.

The last missing piece in Japan's intelligence capabilities is SIGINT. Article 21 of the Japanese Constitution protects secrecy of communications. Since the end of the Second World War, the government, postal service providers, and telecommunications service providers have been under strict legal restraints that prevent the interception of most signals and communications.

In 1999, the Diet passed the Act on Wiretapping for Criminal Investigations to deal with organized crime, drug-related crime, and other serious crimes. This act allowed law enforcement agencies to tap communications with judicial warrants. Many Japanese telecommunications providers are still reluctant to cooperate with law enforcement agencies based on this act. Around 20 cases using this act occur every year, and almost all of them involve mobile phone communications. The scale of Japanese communications interceptions is very small compared with other countries, such as the United States and the United Kingdom.

This lack of SIGINT capabilities with respect to the Internet is becoming more serious in terms of impeding Japan's ability to ensure cybersecurity. SIGINT capabilities have been and are still used for preventing physical terrorist attacks, war, conflicts, and other diplomatic surprises. But today they are also used for preventing cyberattacks and detecting covert cyber operations. Without them, it would be quite difficult to solve attribution problems related to cyber incidents.

Japan–U.S. Cooperation

Defense Guidelines

The Japanese and American governments agreed upon and published versions of *The Guidelines for Japan-U.S. Defense Cooperation* in 1978, 1997, and 2015. Needless to say, no mention of cybersecurity was included in the 1978 and 1997 guidelines. The 2015 guidelines have eight chapters, and the sixth chapter outlines cooperation in outer space and cyberspace. The full text of the "Cooperation on Cyberspace" portion reads as follows:[14]

[14] Ministry of Defense of Japan, *The Guidelines for Japan-U.S. Defense Cooperation*, April 27, 2015.

> To help ensure the safe and stable use of cyberspace, the two governments will share information on threats and vulnerabilities in cyberspace in a timely and routine manner, as appropriate. The two governments also will share, as appropriate, information on the development of various capabilities in cyberspace, including the exchange of best practices on training and education. The two governments will cooperate to protect critical infrastructure and the services upon which the Self-Defense Forces and the United States Armed Forces depend to accomplish their missions, including through information sharing with the private sector, as appropriate.
>
> The Self-Defense Forces and the United States Armed Forces will:
>
> - maintain a posture to monitor their respective networks and systems;
> - share expertise and conduct educational exchanges in cybersecurity;
> - ensure resiliency of their respective networks and systems to achieve mission assurance;
> - contribute to whole-of-government efforts to improve cybersecurity; and
> - conduct bilateral exercises to ensure effective cooperation for cybersecurity in all situations from peacetime to contingencies.
>
> In the event of cyber incidents against Japan, including those against critical infrastructure and services utilized by the Self-Defense Forces and the United States Armed Forces in Japan, Japan will have primary responsibility to respond, and based on close bilateral coordination, the United States will provide appropriate support to Japan. The two governments also will share relevant information expeditiously and appropriately. In the event of serious cyber incidents that affect the security of Japan, including those that take place when Japan is under an armed attack, the two governments will consult closely and take appropriate cooperative actions to respond.

The most important of the paragraphs above is the last one. The meaning of "in the event of serious cyber incidents that affect the security of Japan" is critical. The Ministry of Defense of Japan and the U.S. Department of Defense have not yet clarified in what kind of situations they can deploy Japan Self-Defense Forces and U.S. military forces. In the case of a cyberattack defined narrowly according to the Tallinn Manual, there would be human loss or physical damage—people would have to be killed and/or things in the real world would have to be broken for a cyber operation to qualify as an "attack" under this definition.[15] Such an attack would clearly fall within the scope of exercise of the right of self-defense. Cyberattacks that did not result in the loss of life or physical damage to property could more accurately be characterized as cybercrimes, cyber espionage, or cyber sabotage in most cases, and it would be difficult to deploy the Self-Defense Forces or the U.S. military to respond to such events. Instead, law enforcement organizations or intelligence agencies should be in the lead in responding through criminal indictments; economic sanctions might also be a useful tool to employ.

One possible scenario is a cyberattack against command and control systems that support the Japan Self-Defense Forces. If those systems were lost and a possible enemy was moving military

[15] Schmitt, 2013, Rule 30.

forces, cyber counterstrikes (also known as "hack back") by Japan might be considered. But how to respond proportionally to such a crisis requires careful consideration. Without enough understanding on both sides, a cyberconflict might escalate to a physical conflict or a war.

One idea to consider is to think of cyberintrusions as analogous to airspace incursions or intrusions into territorial waters. When we think of cyberspace in terms of data location, it can be quite difficult to identify national borders. However, when we think of cyberspace in terms of a particular facility's geographical location, it can be easier to identify national borders and legal jurisdictions. If we find any event that causes harm to facilities inside our national borders, we can respond to such an event.

Aircraft are usually not permitted to come into a country's territorial airspace without preauthorization. By contrast, entering into a country's territorial waters is usually allowed provided that the ship entering does so in a mode known as "innocent passage." Cyberspace is more similar to sea space than to territorial airspace, as harmless communications are allowed without requiring preauthorization. However, we can still reserve the right to respond to harmful digital bits in our own facilities-based portion of cyberspace. This idea might ease international cooperation, including between Japan and the United States.

The Ministry of Defense of Japan and the Self-Defense Forces are not considering employment of active "offensive" measures in cyberspace due to Article 9 of the Japanese Constitution. Even in cyberspace, the use of weapons for undertaking a first strike would be difficult under the current legal frameworks. However, if we can clearly identify sources of cyberattacks in foreign countries, we would be able to stop them using cyber measures (by not sending troops). In that sense, active "defense" measures in cyberspace are within available options.

Information-Sharing and Diplomatic Partnership

As stated many times in the 2015 Cybersecurity Strategy, the Japanese government is stressing "information-sharing" and "cooperation" in developing its bilateral cyber relationships with the United States, the United Kingdom, Estonia, and India; its trilateral cyber relationship with the Republic of Korea and China; and its multilateral relationships with ASEAN and NATO.

Between Japan and the United States, there are formal frameworks, including the Japan-U.S. Cyber Dialogue and the Japan-U.S. Policy Cooperation Dialogue on the Internet Economy. When Prime Minister Abe and President Obama met in April 2015, they issued a joint statement agreeing to "ensure the safe and stable use of cyber space based on the free flow of information and an open internet."[16]

[16] Ministry of Foreign Affairs of Japan, "U.S.-Japan Joint Vision Statement," April 28, 2015.

Technology and Capability

As stated above, Japan has legal restrictions on its SIGINT capabilities. In order to work around these limitations, the government and the private sector have utilized all other available technologies and capabilities in their efforts to mitigate cyber threats. For example, the National Institute of Information and Communications Technology, under the Ministry of Internal Affairs and Communications, is building a vast network of academic institutions and nonprofit organizations inside and outside Japan and is developing tools for visualizing cyberattacks. Those networks allow sharing of incidents and signatures of attacks and thereby facilitate attribution of attackers.

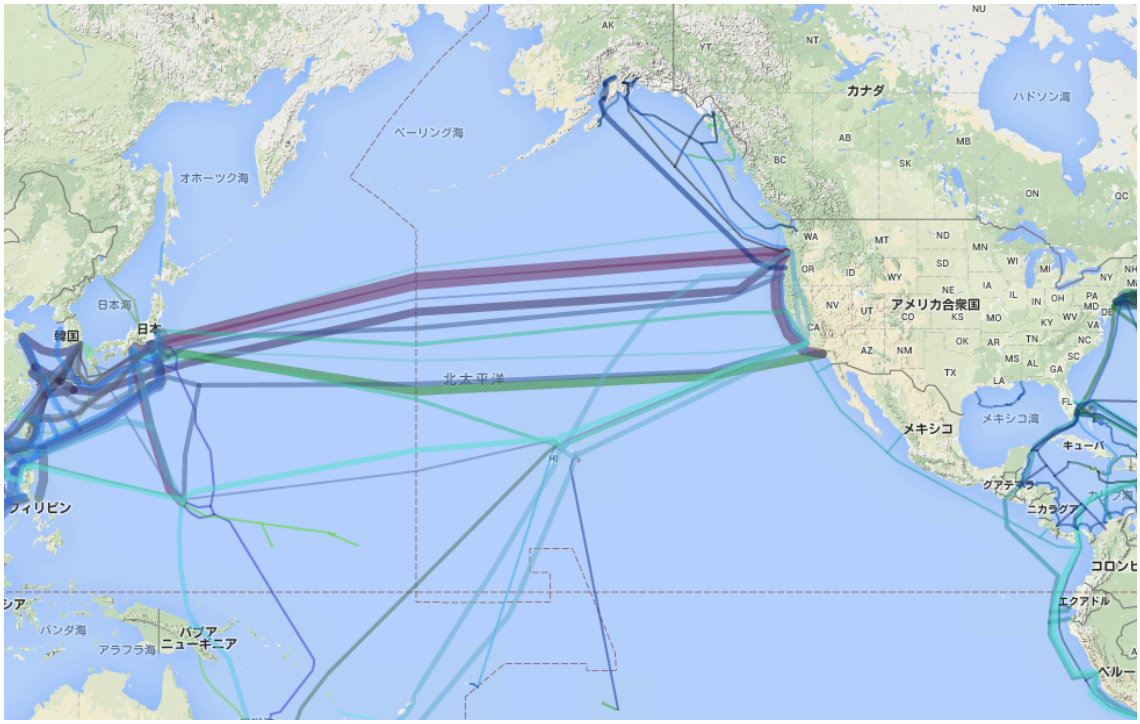
Examples of the Japanese government's technological operations to respond to cyber threats are the Cyber Clean Center (CCC) and the Advanced Cyber Threats Response InitiatiVE (ACTIVE). CCC has set up honeypots to catch malware and observe their behaviors. Commercial Internet service providers acquired security alerts from the CCC and identified infected customers. Customers who received alerts installed security updates or anti-malware software and deleted malware from their computers. In January 2013, CCC was reorganized as an ACTIVE project, and the project is still under operation to mitigate cyber incidents inside Japan's jurisdiction.

The Japanese government is also promoting education and the training of skilled computer engineers who can become specialists in cybersecurity beginning as early as junior high school and running through high school, college, and post-graduate education. Many competitions to raise cybersecurity awareness have been held in Japan.

Submarine Cables

One point that deserves attention is the need for Japan and the United States to cooperate in ensuring the protection of the submarine cables that link Japan and the United States across the floor of the Pacific Ocean. As Figure 3.1 shows, there are many telecommunications cables that cross the Pacific Ocean. The United States is at the center of global Internet connections, while Japan is located at the northeast entrance to Asia. Connections between the two countries are critical for ensuring the free flow of information to and from the Asia-Pacific region. Private companies own most of the cables and landing stations. The physical protection of those cables is increasingly important, as global communications are more reliant on submarine cables than they are on space-based satellites; in Japan's case, 99 percent of international communications go through such cables. Military and financial communications are also heavily dependent on high-speed trans-Pacific cables.

Figure 3.1. Submarine Cables Between Japan and the United States



SOURCE: Google map with overlay by Greg's Cable Map, 2016.
Data available under GNU General Public License, version 3.

Conclusion

There is more to cybersecurity than building sturdy walls and hiding behind them. The value of an interconnected society comes from the free flow of information. There is no such thing as a perfect defense, since black hat hackers will exploit the tiniest holes and cracks in any system of fortifications to infiltrate, steal information, or even carry out attacks.

The first step in guarding against cyberattacks, as called for in the 2015 cybersecurity strategy, is to develop highly capable human resources to work in both government and the private sector, overcoming sectionalism to share information and promote cooperation at the individual and organizational levels. Going forward, this will form the core of Japan's approach to cybersecurity.

As Tokyo looks to host the Olympic Games in 2020, organizers will need to be mindful of the impact that cyberattacks could have. Strengthening Japan–U.S. cooperation in this area will not only provide a united front against hackers in the short term, but it will also seek to prepare for any contingencies that might occur during the Tokyo Olympics.

4. CyberGreen: Improving the Cyber Ecosystem's Health Through Mitigation, Metrics, and Measurement

Presenter: Yurie Ito
Executive Director, CyberGreen
Director, Global Coordination, Japan Computer Emergency Response Team Coordinating Committee (JPCERT/CC)

Introduction

Cyberspace provides an open environment facilitating global connections. This environment allows individuals and organizations around the world to share data and ideas rapidly, greatly increasing efficiency and the power of innovation. However, the openness and speed of the Internet also makes security difficult, facilitating growing levels of malicious activity in the ecosystem. This situation poses many challenges without simple solutions.

The current Internet environment also enables high levels of spam, phishing emails, and domain name server (DNS) amplification to create denial of service attacks and many other types of attacks due to vulnerable systems and other weaknesses. These problems directly or indirectly lead to a profusion of unsolicited traffic, compromised hosts, and vulnerable nodes of activity, such as websites and DNS servers. Malware exploitations follow on and take advantage of these vulnerabilities. Proactively eradicating the technical weakness that enables attacks through a stronger ecosystem is a better cure than trying to react to growing swell of malicious cyberactivity.

CyberGreen started as a two-year pilot project for concept and initial capability development initiated in April 2014. For the last two years, CyberGreen has operated under the sponsorship of the Japan Computer Emergency Response Team Coordinating Committee (JPCERT/CC) and has focused on piloting capabilities with the computer emergency response team (CERT) community starting in the Asia-Pacific region. CyberGreen is now transitioning from pilot project to a long-term operation run by a global nonprofit organization.

As it evolves into a globally focused nonprofit, CyberGreen seeks to improve cyber health by providing reliable information and best practices to national CERTs and network operators to facilitate cleanup efforts and provide policymakers insight into the systemic risk conditions for the cyber ecosystem.

CyberGreen views cyberspace as a globally shared ecosystem. All members of the Internet community must understand their contribution to the health of the cyber environment. CyberGreen can improve the cyber ecosystem by providing data and transparency into the risk conditions. We must have a healthy cyber ecosystem to sustain the trust of individuals and

companies and ensure that cyberspace remains an innovative, dynamic place that drives both economic growth and social dialogue.

CyberGreen's driving concept originated from approaching cybersecurity from a public health perspective. Internet security incidents are symptoms of underlying problems. By identifying the root causes of these problems and treating them, we can make large-scale improvements to Internet security. One of CyberGreen's primary objectives is to aggregate and display metrics for cyber risk observed on the Internet for use by all parties involved in improving health of the system. Creating transparency in the cybersecurity environment will foster global collaborative efforts to assess risk and to act to clean up cyberspace proactively, rather than reacting to malicious activity once it becomes a chronic disease. Just as the public health system improves life conditions, CyberGreen is doing the same for life on the Internet.

Introduction to CyberGreen: Defining Cyber Health

The driving concept behind CyberGreen comes from approaching global cybersecurity from a health perspective, rather than a traditional national security perspective. It focuses on the identification of underlying factors in the global cyber ecosystem that pose risks to stakeholders across the globe, which enables remediation by those who can act. CyberGreen is intended to be collaborative rather than divisive and proactive rather than reactive. Thus, it is imperative that we first define the concept of cyber health as a basis for discussion about CyberGreen's mission and organization. *Cyber health* is defined as "a condition of cyber systems and networks that are not only free from infection, from malware, and [from] botnets but [that] also contributes more broadly to the overall trust and usability of the cyberspace for the well-being of all."[17] This definition helps to clarify what a healthy cyber ecosystem is and will provide future CyberGreen stakeholders a consistent definition that will enable effective participation.

Background

The international community has grappled with the challenge of achieving meaningful cooperation in cyberspace for some time. Particularly in recent years, cyberspace has been increasingly characterized as a competitive environment more prone to conflict than cooperation, moving away from the original concept that cyberspace is a shared global resource that fosters an open environment for all to interact and share information. Distrust in cyberspace increased with more nation states acquiring and employing offensive cyber capabilities, leading some to advocate a need for greater national control of cyberspace, akinto raising fences. This growing atmosphere of distrust in cyberspace raised concerns about a "Balkanization" of the Internet,

[17] Yurie Ito, "Managing Global Cyber Health and Security Through Risk Reduction," thesis, Medford, Mass.: Fletcher School of Law and Diplomacy, Tufts University, July 18, 2011.

contrary to the core values upon which various stakeholders have built and managed this shared resource to date.

However, such hyperbolic characterization of cyberspace as a primarily competitive environment can be misleading. In fact, many actors facing complex international issues find that cooperation is also just as necessary, and there is also potential for cooperative structures to emerge in cyberspace.[18] Actors will find themselves subject to cyberattacks from many sources, including nation states, proxies, and terrorist actors, to which they will need to respond competitively, but they simultaneously find that for many other issues—such as botnet reduction—cooperation is both needed and mutually desirable in order to enhance each other's overall security in cyberspace. Furthermore, the transnational nature of cyber risk and the involvement of both state and nonstate actors increase the importance of achieving cooperation in a way that brings together previously discordant communities. When such cooperation occurs, the collective benefit that emerges for all participating actors may be greater than the sum of their individual actions.

The challenge lies in recognizing that despite the benefits of cooperation in principle, individual actors often fail to achieve cooperation naturally under a state of "anarchy."[19] As Jean-Jacques Rousseau's story of the stag hunt illustrates, individuals may still choose to hunt a small hare for themselves rather than participate in a group hunt for a large deer despite the better payoff the latter provides if the incentive structures they face based on environmental conditions such as risk drive them to "defect," or seek more reliable, but suboptimal, payoffs.[20] Both independent action (hare hunting) and collaborative action (stag hunting) are rational choices for each actor to make, depending on their expected weight of personal risk versus mutual benefit. When faced with these two choices, such factors as trust among players and environmental structure play a significant role in creating an environment more conducive to cooperation.

In cyberspace, conditions that foster cooperation are still in their infancy. Despite the existence of common underlying challenges that undermine the health of the overall ecosystem and the existence of efforts to mitigate such problems by individual entities, sustained and robust cooperation in this domain has yet to occur. The lack of reliable global regimes for coordination and cooperation, uncertainties about the benefits of cooperation, concerns about the sharing of

---

[18] Thomas Schelling, "An Essay on Bargaining," *American Economic Review*, Vol. 46, No. 3, June 1956, pp. 281–306.

[19] Robert Axelrod and Robert Keohane, "Achieving Cooperation Under Anarchy," *World Politics*, Vol. 38, No. 1, October 1985, pp. 226–254.

[20] Jean-Jacques Rousseau, *A Discourse on Inequality*, 1755: "If it was a matter of hunting a deer, everyone well realized that he must remain faithful to his post; but if a hare happened to pass within reach of one of them, we cannot doubt that he would have gone off in pursuit of it without scruple"; and Brian Skyrms, *The Stag Hunt and the Evolution of Social Structure*, Cambridge, UK: Cambridge University Press, 2003.

sensitive information, and the lack of appropriate global norms have kept stakeholders from achieving the full potential from collaboration.

CyberGreen aims to facilitate such cooperation and trust among key stakeholders for the continued robust utilization of cyberspace for routine communications and activity. As a concept, CyberGreen promotes approaching global cybersecurity from a public health perspective, aimed at improving the health of the global cyber ecosystem. Its primary mission will be to motivate stakeholders at the international, national, and local levels to participate in coordinated remediation and prevention activities by establishing robust metrics and standards for cross-comparable cyber risk measurement and mechanisms for sharing actionable information for timely, coordinated measures.

Cyber Health: Applying Lessons from Global Public Health

Traditional approaches to cybersecurity from a national security or law enforcement perspective have limitations in that they mainly take reactive postures to threats or incidents. They also rely heavily on the decisionmaking of nation states rather than a variety of key stakeholders comprising the cyber ecosystem. Such approaches often overlook proactive measures to improve underlying conditions and do not necessarily reduce risk at a systemic level. These approaches are analogous to treating a case of malaria through medicine while leaving the nearby mosquito swamp untouched or developing cancer treatment technology while paying little attention to the population's tobacco use.[21]

The advantage of approaching global cybersecurity issues from a public health perspective is that it compels stakeholders, including governments and network operators, to act based on an inclusive, holistic view of security. The focus is not only on response to threats and incidents but also on proactive measures to improve the general resiliency of a system or network. As stakeholders increasingly approach global cybersecurity from a public health perspective, they will not only mitigate malicious activity on their respective networks and systems but will also view their activities as one part of a larger effort to make the global cyber ecosystem clean, safe, and reliable.

Currently, few incentives exist to invest in cyber hygiene in the global commons, thereby making the overall ecosystem safer. Sources of technical weakness are hard to identify and measure. Technical sophistication can be needed and talent is expensive, while best practices for cleanup are not established and readily available. Standards for and comparative measurement to guide what constitutes a "clean, healthy, reliable" potion of cyberspace do not exist.

Much can be learned from the missions of global health organizations, such as the World Health Organization (WHO), and national-level agencies, such as the U.S. Centers for Disease Control and Prevention (CDC). Their missions include limiting the spread of infectious diseases,

[21] Ito, 2011.

information-sharing and response to outbreaks, and prevention measures that include immunization, education and awareness campaigns about hygiene, and the development of key metrics and standards in medicine. These organizations, by pooling resources at the local, state, national, and international levels in a coordinated fashion, have been playing a central role in combating complex transnational challenges and have been tremendously successful in improving global health conditions.

Likewise, the establishment of initiatives in cyberspace focused on prevention and remediation on a global scale has the potential to bring together previously disjointed efforts to secure the cyber ecosystem and develop common norms on cyber health. Currently, many cyber risks faced by public- and private-sector entities are symptoms enabled by an "unhealthy" cyber ecosystem, such as the prevalence of botnets and the unabated spread of malware. A collaborative and concerted effort to target such underlying causes of systemic cyber risk, rather than merely mitigating its symptoms, will have far-reaching impacts in establishing confidence in the safety and resiliency of the global cyber ecosystem.

If a hub can be created to provide data detailing where technical weaknesses exist, such as unpatched servers, then the underlying conditions that cause such weakness can be addressed. Examples of how such an initiative might improve the cyber's ecosystem health include raising awareness of the merits of avoiding pirated software, spreading best practices for cleanup, improving procedures for downloading and using cleanup tools, and aiding already existing efforts by national CERTs and network operations teams, especially in areas where less technical prowess exists. At a higher level, pairing transparency with technical credibility about nations and networks that harbor or facilitate malicious activity that impacts others will provide the dual-edged incentive of shaming those who do not keep their cyber ecosystem healthy and enabling the targeting of assistance to those who lack the resources to do so effectively.

Cross-Comparable Statistics Are Key

One of the most important conditions for enabling robust cooperation in cyberspace is the availability of cross-comparable statistics that empower decisionmakers to set policies based on evidence, establish priorities, and see trends. By *cross-comparable*, we mean that measurements are conducted and metrics are established based on strong scientific methods across what currently is a wide variety of data sources using different technical techniques with widely varying fidelity and challenges. The key focus is on making various statistics produced at the national and organizational levels cross-comparable, rather than merely sharing information. Today, many national-level CERTs and computer security incident response teams (CSIRTs) around the world generate their own statistics from internally collected data. The problem is that data collection varies greatly, dependent on CERT and CSIRT capabilities and mandates. These data are then turned into statistics using a range of different standards and methods. Added to that are third-party data providers who also use their own data collection and statistical

methods.[22] This becomes a significant impediment to collaboration as decisionmakers end up comparing apples to oranges and cannot generate meaningful aggregate statistics for use.

There are generally two approaches to achieving cross-comparability: (1) establishing standards prior to collection and encouraging each entity to adhere to them when producing statistics or (2) developing statistical methods after collection to adjust for differences and normalize statistics to maximize comparability. The two approaches are not mutually exclusive, and organizations have relied on both to produce meaningful information for stakeholders. For example, WHO maintains the WHO Indicator and Measurement Registry (IMR) for producing global statistics on such health risk factors as obesity and blood pressure. IMR is a central source of metadata of health-related indicators that include indicator definitions, code lists, data sources, and methods of estimation.[23] It further provides a mechanism for interoperability through the Statistical Data and Metadata Exchange—Health Domain (SDMX-HD) indicator exchange format, allowing entities to incorporate appropriate international standards such as the SDMX Metadata Common Vocabulary (MCV), ISO (International Organization for Standardization) 11179, Data Documentation Initiative (DDI), and Dublin Core (DCMES). IMR provides an avenue for individual organizations to achieve harmonization without imposing mandatory standards. Additionally, WHO also uses statistical methods to make adjustments to national-level data, adjusting for such factors as risk factor definition, age groups reporting, reporting year, and representativeness of population. WHO also takes into account uncertainty in estimates, produces age-standardized comparable estimates, and publishes its statistical methods online for transparency.

Several principles are imperative in achieving cross-comparability using the above two approaches. The first is a focus on enabling voluntary adoption of good standards rather than issuing mandates. Individual organizations often have vastly varying capacities and operate in different environments, and imposing high standards may hinder data collection and reporting itself. Instead, an approach based on developing frameworks, such as IMR, makes available user-friendly databases for access, comparison, and translation of data that better meet international standards. The second is an emphasis on transparency. When possible, such information as data sources, sampling methods, and methods for estimation should be made available in a transparent and accessible manner. The disclosure of such information builds confidence and trust in the system and encourages open discussion about improving methodology and analysis techniques.

The potential for global collaboration stemming from cross-comparable statistics in cyber health is enormous. Decisionmakers across the world in various industries will be able to not only see which regions have the greatest botnet infection rates and which regions have the most

[22] OECD Working Party on Security and Privacy in the Digital Economy, "Guidance for Improving the Comparability of Statistics Produced by Computer Security Incident Response Teams (CSIRTs)," June 8, 2015.

[23] World Health Organization, "WHO Indicator Registry," 2016.

unpatched systems, but over time they will also see trends, such as activity patterns or the "half-life" of zero-day vulnerabilities. Such statistics would enable individuals to make decisions based on evidence rather than perception and help justify investment and budgetary decisions, as well as help make predictions based on patterns. Most importantly, these statistics enable organizations, such as CERTs, to mitigate underlying risk factors and provide a way to measure their progress.

Building on Past and Existing Efforts: Leveraging the Public Health Model in Cybersecurity

The application of public health models in cybersecurity is not a new concept. As early as 1996, a Defense Advanced Research Projects Agency (DARPA)-sponsored RAND report recommended that one of the steps that the U.S. government could initiate immediately to reduce U.S. vulnerability in cyberspace was to adopt the information-sharing functions of the CDC:[24]

> The CDC acts as a worldwide clearinghouse for health and disease information; it is a central source of information when needed, from routine queries to tracking the spread of epidemics. This same clearinghouse function is needed to collect and assess information on disparate cybersecurity incidents.

The RAND report, however, mentioned this possibility only briefly and did not extend the application beyond information-sharing. The analogy between public health and cybersecurity grew stronger as the number of Internet users skyrocketed and more networks and systems came to be interconnected, resulting in a global "cyber commons."[25] Computer security expert and biostatistician Dan Geer says that like in dealing with cybersecurity challenges, public health practitioners focus on "macro scale effects due to micro scale events."[26] Due to the high degree of interconnectivity and rapid transmission of information in cyberspace, approaches to public health came to be viewed as increasingly applicable. From 2010 to 2012, various reports exploring this nexus have been published, each from a distinct perspective.

In 2010, Gregory Rattray, Chris Evans, and Jason Healey extensively explored this model in a Center for a New American Security (CNAS) report, exploring how such concepts as

---

[24] Robert H. Anderson and Anthony C. Hearn, *An Exploration of Cyberspace Security R&D Investment Strategies for DARPA: "The Day After . . . in Cyberspace II,"* Santa Monica, Calif.: RAND Corporation, MR-797-DARPA, 1996, p. xii.

[25] The author acknowledges that this characterization is not wholly accurate, as such networks and systems are bound to physical infrastructures often within a state's jurisdiction and thus are not a globally shared resource. The characterization nonetheless is used to explain the wide reach and interconnectivity of cyberspace.

[26] Dan Geer, "Measuring Security," presentation, 2007.

epidemiology and preventive health can be applied in cybersecurity.[27] Their study focused on measures used by epidemiologists to prevent and respond to disease outbreaks, including sanitization, diagnosis, early warning, and isolation. The report conducted a comparison of outbreak alert systems with existing cyber incident alert systems, as well as a comparative analysis of WHO and the CDC. Finally, realizing the limits of achieving security through deterrence in cyberspace, the authors recommended that United States should lead global efforts to clean up the cyber environment.

Scott Charney, leader of the Trustworthy Computing Group at Microsoft, took a slightly different approach by framing the topic under collective defense.[28] While focusing on the idea of "device health" and the proposition of issuing health certificates to consumer machines before allowing Internet access, much of the paper examined achieving international cooperation when collectively defending against a threat, which does not address the public health focus on proactive measures. Collective defense is contingent on a premise of shared threat; in cyberspace, however, not every actor shares the same threat perception, nor do some of the underlying risk factors constitute threats in and of themselves. Just as WHO not only responds to pandemics, such as severe acute respiratory syndrome (SARS), but also researches tobacco use and obesity, CyberGreen's mission must look beyond the collective defense analogy.

In 2011, the U.S. Department of Homeland Security (DHS) published "Enabling Distributed Security in Cyberspace," which focused on building a healthier cyber ecosystem by increasing automation.[29] DHS proposed that in the face of increasing cyberattacks that propagate at machine speeds, we must explore ways to have cyber devices "work together in near-real time to anticipate and prevent cyberattacks, limit the spread of attacks across participating devices, minimize the consequences of attacks, and recover to a trusted state." This model draws upon the immune system of the human body rather than a public health model and cites interoperability and authentication as also important for building a healthier cyber ecosystem. The report mentions that incentivizing individuals to adopt cyber best practices and configuration guidelines remains a challenge, stemming from the difficulty in defining a level of harm incurred as a result of a cyberincident. The report recommended that a "Cyber CDC" in the future should provide stakeholders with the information needed to diagnose problems through increased sharing of anonymized cyberincident and mitigation data.

---

[27] Gregory Rattray, Chris Evans, and Jason Healey, "Chapter 5: American Security in the Cyber Commons," in Abraham M. Denmark and James Mulvenon, eds., *Contested Commons: The Future of American Power in a Multipolar World*, Center for a New American Security, 2010, pp. 139–176.

[28] Scott Charney, "Collective Defense: Applying Public Health Models to the Internet," Microsoft, 2010.

[29] U.S. Department of Homeland Security, "Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action," March 2011.

Finally, the East West Institute (EWI) published "The Internet Health Model for Cybersecurity" in 2012,[30] presenting a comprehensive overview of functions in public health that could be applied to cybersecurity. Like others, EWI also looked to WHO and the CDC and identified five basic functions as applicable: education, monitoring, epidemiology, immunization, and incident response. It also outlined some limitations and dangers of relying on the public health analogy, such as how malware originates with human intent, as opposed to diseases (which are organic in nature); that devices do not have natural immune systems like living creatures do; and the negative connotations associated with surveillance and quarantine in cyberspace. Most importantly, the EWI report notes that while individuals must take ultimate responsibility for their online safety, they cannot do so in isolation. In this regard, EWI notes the importance of establishing sound metrics, measurement, and information-sharing schemes to provide the foundations of cooperation.

To move toward a cybersecurity approach that implements lessons from the public health model, CyberGreen seeks to enable similar collaborative information-sharing processes between CERTs and CSIRTs. Based on the work of global public health organizations, CyberGreen will identify comparable risk conditions in cyberspace and empower stakeholders to remedy those fundamental issues.

Establishing CyberGreen

CyberGreen, acknowledging past and current efforts to improve cyber health, seeks to establish itself as an increasingly effective hub for collaborative efforts to address systemic cyber risk and improve the general health of the cyber ecosystem.

Statement of Need

"You can't manage what you can't measure." This management axiom certainly holds true in the complex world of cybersecurity. Measurement of malicious activity today focuses on counting the number of infected machines and organizations. However, our current efforts fail to capture underlying conditions causing the worsening global cyber health challenges that we face and give little in the way of leverage to address these challenges efficiently or in a globally collaborative way.

The Problem

Infections and malicious activities in cyberspace continue to rise every year. Symantec reports that more than 317 million new pieces of malware were created in 2014, or close to 1 million new pieces of unique malware each day. We have now identified 1.7 billion different

[30] Karl Frederick Rauscher, "The Internet Health Model for Cybersecurity," East-West Institute, June 2, 2012.

types of malicious software.[31] The specific case of the DNS Changer malware provides a good example of how underlying weakness in the ecosystem leads to emergence of major cybersecurity challenges. Exploiting a weakness as simple as altering a user's local DNS settings, DNS Changer infected approximately 4 million computers in more than 100 countries around the world. By manipulating users' DNS queries, the criminals who created the virus were able to generate at least $14 million in illicit gains.[32] In certain instances, the malware simultaneously prevented users' antivirus software and operating systems from updating, thereby exposing infected machines to even further malicious software infection. Analysts have found that economic losses in the billions of dollars per year for the United States alone can be tied to Internet security incidents.[33]

The cybersecurity community at times has responded to specific challenges, such as the Conficker and GameOver Zeus botnets. While such efforts have had positive impacts on Internet health, past mitigation initiatives have been specific in nature and focused on addressing one or two risk factors for a limited time period. Additionally, the data used in specific efforts usually are not normalized and tracked over time. As a result, metrics do not exist to track impact across different initiatives or time periods, and we cannot compare the effectiveness or efficacy of remediation efforts.

Two primary challenges must be overcome to foster a cyber ecosystem health improvement approach:

Focus on symptoms, not causes: Traditional approaches to cybersecurity have crucial limitations based on the fact that they are typically characterized as reactive approaches to addressing threats or incidents. Reactive approaches do not improve underlying conditions and reduce risk at a systemic level.

Establish statistical rigor: Existing cybersecurity metrics, specifically for evaluating risk conditions, have long suffered from a lack of statistical rigor. Challenges stem from many sources, including issues in collection, the inability to compare data across organizational or institutional lines (such as national boundaries), and a failure to apply normalization techniques. The absence of statistically meaningful cybersecurity metrics prevents comparisons of infection rates within organizations and regions, comparisons of the efficacy of various efforts to improve cyber ecosystems' health over time, and an effective evaluation of cybersecurity investments.

We need a sustainable approach to measuring cyber health and providing data to assist those seeking to improve the underlying conditions in the ecosystem. CyberGreen seeks to provide the global collaborative hub that overcomes these challenges.

---

[31] Symantec, *2015 Internet Security Threat Report*, Volume 20, 2015.

[32] Federal Bureau of Investigation, "Operation Ghost Click: International Cyber Risk That Infected Millions of Computers Dismantled," November 9, 2011.

[33] Gordon M. Snow, Assistant Director, Cyber Division, Federal Bureau of Investigation, "Statement Before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit," Washington, D.C., September 14, 2011.

The Solution

The greatest hurdle to improving cyber health today is the lack of common metrics and an operational hub to provide and collaboratively use the global data and metrics we can collect to enable proactive improvement efforts. Progress can be significant when the data is available and easily digestible. For example, the Anti-Phishing Working Group's quarterly report, which publishes statistics on phishing on a regular basis, enables organizations to focus defensive efforts on identified sources of these attacks. Similarly, the Open Resolver project, by regularly notifying and publishing specific statistics around openly recursive name servers and misconfigured time services, enables significant reduction in the presence of vulnerable infrastructures.

CyberGreen seeks to enable improved cyber health by

- gathering key risk conditions from a growing number of quality data sources
- providing statistically mature, comparable measurements of cyber ecosystems' healthiness, including an overall CyberGreen Index score
- assisting CSIRTs through documentation, tools, and best practices to take action to improve Internet health in their own region utilizing indicators from freely available data sources
- promoting cooperation among experienced CSIRTs and other practitioners to contribute case studies and best practices for the improvement of cyber health conditions
- advocacy for improving cyber health as a key public policy goal
- improving the overall health of the global cyber ecosystem, providing a safer place for customers, and restoring trust in the technology that we all rely on.

The vision for the development of CyberGreen's capabilities is as follows:

Improving measurement: The development and application of statistical methods to data will allow measurement of key indicators of malicious activity and risk conditions. These methods will provide analytical insight about patterns, priorities, and trends for action by the CERT/CSIRT community and others. As of summer 2015, CyberGreen has conducted an analysis of current measurement practices used to measure cyber health, identified limitations, and established an initial set of metrics. CyberGreen analysis of statistical methods and explanation of current metrics are available on the CyberGreen portal.[34] Leveraging ever-improving data, CyberGreen will seek to continuously improve the practice of cyber health and risk condition measurement. Establishment of partnerships with universities, research organizations, and thought leaders on applying information generated by CyberGreen to other issues in cybersecurity will also result. CyberGreen will provide regular reports on the state of cyber health and sponsor forums for improving measurement and analytic methods. As the repository of data and statistics grows, so too will our ability to conduct stronger analysis of

[34] CyberGreen, "Tracking the State of Global Cyber Health," 2016.

patterns, priorities, and trends, eventually strengthening the effectiveness of CyberGreen's collaborative risk reduction efforts.

Sourcing data: Establishing accurate and comprehensive data sources will enable CyberGreen to produce valuable cyber health risk metrics. As of summer 2015, CyberGreen has access to a number of openly available data sources and a small number of private data sets for the exclusive purpose of enhancing metrics. Data ranges from network scanners probing for vulnerable nodes to compromised websites hosting phishing lures to known botnet addresses directing compromised nodes on what commands they should execute next. Today, much of the data focus on larger economies, where bandwidth and resources are much more plentiful. This bias can overshadow challenges in countries with smaller subscriber bases that are inadequately accounted for. By the time of its launching in spring 2016 with the collaboration of national CSIRTs, CyberGreen seeks to expand visibility into other regions of the world where there is very little in terms of openly available risk data.

Providing a clearinghouse for mitigation: The primary means for CyberGreen to enable those mitigating cyber health risks is through the development and operation of a CyberGreen platform. The platform provides a mechanism for gathering the data produced and the tools for conducting statistical analysis. CyberGreen will also establish processes for disseminating data and aggregated risk metrics provided through the CyberGreen platform to existing entities in the global remediation community. As of summer 2015, a pilot operating platform is providing participants with initial metrics based on the CyberGreen Index approach using mostly openly available data sources. Early feedback and interest across the global CSIRT community has been positive, and CyberGreen strives to engage users in every step of the platform development. By the time of its launch in spring 2016, CyberGreen will provide an enriched set of metrics based on improved data via its portal to an expanded base of users.

Capacity-building: CyberGreen will identify potential partners in the developing world and provide the necessary training to enable their participation in risk mitigation and cyber health improvement efforts. A key subset of this effort includes CERT capacity-building and information-sharing workshops to encourage further integration. This knowledge will improve interactions and information flow throughout the cybersecurity community. By doing so, developing countries will stand to benefit from mentoring and assistance that will aid in the improvement of their local cyberspace environment. By the time of its launch in the spring 2016, CyberGreen will have established a training cadre, training materials, and a dedicated portion of the portal for capacity-building with developing nation partners. The uniqueness of this capacity-building program is that it will consist not only in the provision of training but also in the provision of actual data and tools to support continued cleanup and hygiene-raising operations. The CyberGreen Index can serve as the scoreboard for the effectiveness of those efforts.

Advocacy: CyberGreen will also engage the policymaking and media communities as active participants in pursuit of cyber health. CyberGreen is working with partners to initiate a public awareness campaign to ensure that governments, businesses, and individuals recognize the value

of a healthy cyber ecosystem. As CyberGreen matures, it will promote education and awareness about cyber health among governments and the media. As of March 2016, CyberGreen has begun its advocacy campaign through presentations in such policy forums as the Global Conference on Cyberspace 2015 in The Hague and at the Internet Governance Forum. By the time of its launch in spring 2016, CyberGreen will be able to engage with leading government organizations to educate them on the necessity of making cyber health a key public policy goal. It will also work with media and other global actors to raise awareness of the importance of cleaning up the Internet.

Making Cyberspace Healthier Through CyberGreen

As CyberGreen approaches its first phase of implementation, present-day cyber conflict, the growth of botnets, and the prevalence of malware all serve as signs that a global collaborative approach to cybersecurity is needed now more than ever. Applying the lessons of global health approaches, defining cyber health, and converting threat information into practical metrics will help CyberGreen and its future CERT/CSIRT partners improve the cyber ecosystem. CyberGreen looks forward to developing, implementing, and refining this model in conjunction with members of the global CERT/CSIRT community. Through collaboration between the members of this community, CyberGreen will improve cyber health for all global users.

5. U.S.–Japan Cooperation on Capacity-Building in Southeast Asia

Presenter: Roger Cliff, Ph.D.
Senior Fellow
The Atlantic Council

Introduction

The administration of U.S. President Barack Obama has put increased emphasis on U.S. interests in the Asia-Pacific since it took office in 2009, a policy known as the "rebalance to Asia."[35] One element of this policy has been increasing the capabilities of the security forces of countries in the region that are believed to support U.S. interests. In 2015, the U.S. Department of Defense (DoD) announced a Southeast Asia Maritime Security Initiative, an effort to increase the maritime capabilities of countries in Southeast Asia in particular.[36] Under this initiative, $425 million in funding will be provided over five years to Indonesia, Malaysia, the Philippines, Thailand, and Vietnam for, among other things, "training to ministry, agency, and headquarters level organizations."[37]

Like the United States, Japan has also been increasing its defense cooperation and capacity-building efforts with Southeast Asian nations over the past several years. Prior to 2010, building partner capacity was not a significant emphasis of Japan's Ministry of Defense (MoD). However, the 2010 version of the MoD's National Defense Program Guidelines (NDPG), a document setting the strategic direction for the MoD and updated every few years, for the first time specified that "Japan will . . . support the capacity-building of countries" in the Asia-Pacific region and globally.[38] Accordingly, in 2012 the MoD created a Capacity-Building Assistance Office and began engaging in capacity-building activities with various nations in the Asia-Pacific region, particularly in Southeast Asia. Southeast Asian nations involved initially included Timor-Leste, Cambodia, Vietnam, and Indonesia. In 2014 Myanmar (formerly Burma) and the Philippines were added, and in 2015 Malaysia was added. Activities have included training in field maintenance of military equipment, civil engineering, underwater medicine, meteorology

[35] See Daniel R. Russell, "Remarks on the U.S.-Asia Rebalance and Priorities," U.S. Department of State, January 27, 2015.

[36] U.S. Department of Defense, *Asia-Pacific Maritime Security Strategy*, July 2015c, p. 26.

[37] Aaron Mehta, "Carter Announces $425M In Pacific Partnership Funding," *Defense News*, May 30, 2015.

[38] Ministry of Defense of Japan, *National Defense Program Guidelines for FY2011 and Beyond*, December 17, 2010.

and oceanography operations, peacekeeping operations, humanitarian assistance and disaster relief (HA/DR), aviation safety, aviation meteorology, international aviation law, and aviation transportation. Although the number of activities has increased, the scale has been small, with no more than 23 people from Japan visiting the subject country at a time and no more than six people from the subject country visiting Japan at a time.[39]

Since 2013, Japan has made cooperation with the United States an explicit goal of its capacity-building efforts. The 2013 version of the NDPG declared that Japan would strengthen its cooperation with the United States in the field of capacity-building assistance, and the 2015 *Guidelines for Japan-U.S. Defense Cooperation*, the first new version since 1997, stated that "The two governments will cooperate in capacity-building activities, as appropriate, by making the best use of their capabilities and experience . . . . Examples of cooperative activities may include maritime security, military medicine, defense institution building, and improved force readiness for HA/DR or peacekeeping operations."[40] Consistent with this, Japan's partner capacity assistance efforts have indeed included military medicine, peacekeeping operations, and HA/DR. However, none of these activities appear to have been conducted cooperatively with the United States, nor is it clear that their planning and selection was coordinated between Japan and the United States.

Given the finite resources available to both countries for building partner capacity, the United States and Japan should focus their efforts on areas in which they have common security interests and coordinate their capacity-building activities to maximize the benefits. In Southeast Asia, the United States and Japan have common security interests in ensuring the security and stability of Southeast Asian democracies,[41] countering terrorism, countering piracy, upholding a rules-based international order in general, and ensuring that territorial disputes are resolved peacefully and fairly in particular, and mitigating the effects of natural and man-made disasters in the region. This paper examines each of these areas and, based on the examination, makes recommendations for areas in which the security forces of the United States and Japan should cooperate in the building of partner capacity.

---

[39] Ministry of Defense of Japan, "Past Programs," undated(b).

[40] Ministry of Defense of Japan, *National Defense Program Guidelines for FY 2014 and Beyond*, December 17, 2013c, p. 9; Ministry of Defense of Japan, *The Guidelines for Japan-U.S. Defense Cooperation*, April 27, 2015.

[41] The United States and Japan have an interest in the security and stability of Southeast Asian democracies because democracies are more likely to support the interests of other democracies and because they rarely, if ever, go to war with each other. In addition, by definition, democratic governments protect and promote, albeit imperfectly, the freedom and human rights of their populations, something that is valued by the majority of people in the United States and Japan. For the same reasons, the United States and Japan do not necessarily have an interest in the security and stability of nondemocracies in Southeast Asia, as it is possible that the lack of these things could result in these countries becoming democracies. This does not mean, however, that the United States and Japan necessarily have an interest in the insecurity and instability of nondemocracies in Southeast Asia, as insecurity and instability in these countries could negatively affect the interests of the United States and Japan (as well as of the people living in these countries) without necessarily resulting in them becoming democracies.

Ensuring Security and Stability

No Southeast Asian democracy currently faces a plausible threat of invasion and conquest of the nation as a whole by a neighboring state. The greatest threats to the security and stability of Southeast Asian democracies, therefore, are from internal sources. In particular, both the Philippines and Indonesia face significant internal threats to their security and stability. The Philippines faces two main internal threats. One is a Communist insurgency that has been under way since the late 1960s. More than 40,000 people have been killed over the course of the conflict, and, as of the most recent year for which information is available (2014), at least 80 people were dying each year as a direct result of the conflict.[42] The second internal threat in the Philippines is an Islamic separatist movement based on and around the southern island of Mindanao. This conflict has been ongoing for more than a century and has resulted in 120,000 people being killed and more than 2 million people displaced in recent decades alone. The Philippine government reached a peace agreement with the largest Muslim insurgent group, the Moro Islamic Liberation Front (MILF), in 2014, but conflict with other groups, some of whom have linkages to such international extremist organizations as al-Qaeda and the Islamic State, continues, and whether the peace agreement with the MILF will hold is uncertain.[43]

Ultimate resolution of both conflicts hinges largely on improvements in civilian governing capacity in the often remote and poor areas where the insurgencies are active,[44] but improving the capacity of Philippine security forces to provide development assistance and security in these areas would contribute to the peaceful resolution of these conflicts. Since 2001, the U.S. military has been engaged in just such an effort, training Philippine security forces in such areas as leading engineering projects and providing medical and veterinary care.[45] Japan, however, has not been involved in building Philippine capacity in these areas.[46] Improving the capacity of Philippine security forces to provide development assistance or security in conflict areas within the Philippines, therefore, is an area in which contributions from Japan could be valuable.[47]

---

[42] International Crisis Group, "The Communist Insurgency in the Philippines: Tactics and Talks," Asia Report No. 202, February 14, 2011, p. 1; U.S. Department of State, Bureau of Democracy, Human Rights, and Labor, "Country Reports on Human Rights Practices for 2014: Philippines," undated.

[43] *New York Times* Editorial Board, "The Philippines' Insurgency Crisis," *New York Times*, August 1, 2014; Prashanth Parameswaran, "Philippine Peace Deal Suffers Another Blow," *The Diplomat*, June 12, 2015.

[44] International Crisis Group, 2011, p. 25.

[45] Army Sgt. 1st Class Michael J. Carden, "Trainers, Advisors Help Philippines Fight Terrorism," American Forces Press Service, February 22, 2010.

[46] Japanese capacity-building assistance with the Philippines has been limited to related to aviation transport and aviation safety. See Ministry of Defense of Japan, undated(b).

[47] Although the Japanese constitution is interpreted as prohibiting Japan from engaging in such operations itself, nothing in the constitution prohibits Japan from increasing the capabilities of other countries in this area.

Indonesia also faces two main internal threats to its security and stability: violent Islamic extremist groups and regional separatist movements.[48] Islamic extremists have been responsible for multiple terrorist attacks in Indonesia since 2000, including the 2002 Bali resort bombings that killed 202 people, and as recently as January 2016.[49] Although the Indonesian government has been successful in neutralizing some of these organizations, such as Jemaah Islamiyah, new ones are constantly emerging.[50]

Indonesia has had two significant separatist movements in recent years, one in the western province of Aceh and the other in Indonesia's easternmost territory of Papua (the western half of the island of New Guinea). The separatist conflict in Aceh ended in 2005 with the signing of a peace accord that granted Aceh a significant degree of autonomy and a share of the revenues from Indonesia's extraction of natural resources in the province. Although tensions and friction remain, this agreement has now held for more than a decade.[51]

Papua was ostensibly granted autonomy in 2001, but in practice this autonomy has not been fully implemented, and other promised benefits for Papua have failed to materialize as well. Meanwhile, Indonesia's police and military have faced widespread accusations of torture, excessive force, and extortion in Papua. As a result, members of the indigenous population of Papua continue to agitate for independence, and over a dozen people died in violence related to the independence movement in 2014.[52]

As noted, the Indonesian government has had some success neutralizing Islamic extremist organizations. This has been due in part to antiterrorism assistance that the United States has provided since 2003, but Japan's security forces may have capabilities to contribute as well.[53] In Papua, as in the Philippines, resolution of the conflict hinges largely on improvements in civilian governing capacity, but improving the capacity of Indonesian security forces to provide development assistance and security in Papua would contribute to such resolution.[54] The Japan Self-Defense Forces' (JSDF's) capacity-building assistance to Indonesia has been limited to training in meteorology, oceanography, and international aviation law.[55] Thus, it appears that it

---

[48] David Timberman, "Violent Extremism and Insurgency in Indonesia: A Risk Assessment," Washington, D.C.: Management Systems International, January 7, 2013.

[49] Tara John, "Indonesia's Long Battle With Islamic Extremism Could Be About to Get Tougher," *Time*, January 14, 2016.

[50] Hannah Beech, "What Indonesia Can Teach the World About Counterterrorism," *Time*, June 7, 2010; International Crisis Group, "How Indonesian Extremists Regroup," July 16, 2012a; John, 2016.

[51] M. Nur Djuli, "To Improve Peace Process in Aceh, Return to Sanity," *Jakarta Post*, August 24, 2015.

[52] International Crisis Group, "Indonesia: Dynamics of Violence in Papua," Asia Report No. 232, August 9, 2012b; U.S. Department of State, "Country Reports on Human Rights Practices for 2014: Indonesia," undated(b).

[53] "U.S.-Funded Detachment 88, Elite of Indonesia Security," Reuters, March 18, 2010.

[54] No public information was found indicating that the U.S. military currently provides such assistance, but it is possible that it is doing so without publicizing it.

[55] See Ministry of Defense of Japan, undated(b).

would be in the interest of the United States and Japan to provide Indonesia with capacity-building assistance in the areas of development assistance and security provision in Papua.

In addition to the Philippines and Indonesia, Thailand and Myanmar also suffer from internal threats to their security and stability. In Thailand, one threat is an ongoing struggle between primarily urban elites and rural populists. The inability of these two constituencies to reach a mutually acceptable formula for governing the nation has threatened to split the country and resulted in military coups twice in the last decade, most recently in 2014.

The second domestic threat to Thailand's security and stability is an insurgency in southern Thailand that results from ethnic, religious, and historical differences between people living in Thailand's four southernmost provinces and those in the rest of Thailand. This conflict has been exacerbated by the tactics used by Thailand's security forces in response to separatist violence in these provinces. Thus, improving the effectiveness of Thailand's security forces in counterinsurgency operations, such as security provision and development assistance, would appear to be an area in which the U.S. and Japanese militaries could potentially provide capacity-building assistance. Without democratic checks on Thailand's security forces, however, increasing their capabilities would likely contribute to further repression and abuse and potentially delay the return to democracy in Thailand without ameliorating either internal conflict. Although these conflicts threaten Thailand's security and stability, therefore, until democracy is restored in Thailand, capacity-building assistance to its security forces should be limited to increasing their capabilities in such noncombat areas as HA/DR and development assistance.

Myanmar suffers from ethnic violence and numerous separatist movements that have been at war with the central government virtually since the independence of the country. Although Myanmar recently held what were regarded as free and fair elections, there has not yet been time for any type of reconciliation process between the Myanmar government and the country's various ethnic groups. Myanmar's security forces, moreover, are not under the control of its civilian government and have been accused of numerous human rights abuses, including killings, torture, and rape.[56] Increasing their capacity to combat internal threats, therefore, carries a risk of contributing to repression and abuse and preventing an equitable resolution of Myanmar's ethnic conflicts. Thus, until Myanmar becomes a fully functioning democracy, capacity-building assistance to its security forces should also be limited to increasing their capabilities in such noncombat areas as HA/DR and development assistance.[57] Japan's assistance has been small-

[56] U.S. Department of State, "Country Reports on Human Rights Practices for 2014: Thailand," undated(c); and U.S. Department of State, "Country Reports on Human Rights Practices for 2014: Burma," undated(a). Myanmar (Burma) recently held elections in which the opposition party was victorious. Myanmar's armed forces, however, are independent of the control of its civilian government.

[57] No public information was found indicating that the United States has provided assistance to Myanmar's armed forces, but it is possible that it is doing so without publicizing it.

scale and has consisted of seminars and visits to SDF facilities in the areas of underwater medicine, aviation meteorology, and HA/DR.[58]

Countering Terrorism

Both the Philippines and Indonesia suffer from terrorist attacks. In the Philippines, these are associated with the Communist insurgency and the Islamic separatist movement. In the case of the Communist insurgency, the New People's Army, the armed wing of the Communist Party of the Philippines, has carried out "killings, raids, kidnappings, acts of extortion, and other forms of violence . . . against domestic and security force targets" throughout the Philippines.[59] In the case of the Islamic separatist movement, most terrorist acts have been committed by the Abu Sayyaf Group, which "engages in kidnapping for ransom, bombings, ambushes of security personnel, public beheadings, assassinations, and extortion," and the Bangsamoro Islamic Freedom Fighters.[60] In 2014, the Abu Sayyaf Group and the Bangsamoro Islamic Freedom Fighters both pledged allegiance to the Islamic State of Iraq and Syria (ISIS), raising concerns about increased terrorist attacks inspired or directed by ISIS and the possibility of ISIS elements traveling to the Philippines from the Middle East. The Indonesia-based terrorist organization Jemaah Islamiyah is also believed to operate in the Philippines, although it has moved away from violent attacks in recent years.[61] Since 2001, the U.S. military has been engaged in training Philippine security forces in counterterrorism operations.[62] This training should continue and is an area in which Japan's SDF or National Police Agency could potentially contribute as well.

As noted earlier, Islamic extremists have been responsible for multiple terrorist attacks in Indonesia since 2000. Although the Indonesian government has succeeded in neutralizing some organizations—most notably al Qaeda–linked Jemaah Islamiyah, perpetrator of the 2002 Bali bombings—new Islamic extremist organizations are constantly emerging. At least 22 Indonesian groups have pledged loyalty to ISIS, and over 600 Indonesians are believed to have traveled to ISIS-held territories in the Middle East.[63] As noted above, the United States has provided counterterrorism assistance to Indonesia since 2003. This assistance should continue, and, if Japan's security forces have useful capabilities to contribute, Japan should provide assistance in this area as well.

---

[58] Ministry of Defense of Japan, undated(b).

[59] U.S. Department of State, "Country Reports on Terrorism 2014," undated(d).

[60] U.S. Department of State, undated(d).

[61] U.S. Department of State, undated(d).

[62] Army Sgt. 1st Class Michael J. Carden, "Trainers, Advisors Help Philippines Fight Terrorism," American Forces Press Service, February 22, 2010.

[63] John, 2016.

Thailand has suffered from multiple terrorist attacks. Some of these have been perpetrated by Thailand's southern separatists, including the March 2012 vehicle bombings in the southern cities of Yala and Hat Yai that killed 14 and injured more than 400 and an April 2015 vehicle bombing on the tourist island Koh Samui that injured seven.[64] A bombing in Bangkok in August 2015 that killed 20 and injured 125, however, was apparently committed by Chinese Uighurs, possibly with assistance from individuals or government officials in Turkey.[65] Thai security officials have reportedly expressed concern about operational linkages between Thailand's southern separatists, who are ethnic Malay Muslims, and ISIS or other international terrorist networks. As of 2015, however, there was no direct evidence of such linkages or of Thais joining ISIS.[66] As with increasing the capacity of Thailand's security forces to combat internal threats, however, increasing their capacity to combat terrorism carries a risk of contributing to repression and abuse. Until democracy in Thailand has been restored, therefore, capacity-building assistance to its security forces should also be limited to increasing their capabilities in such noncombat areas as HA/DR and development assistance.

Malaysia has not experienced a terrorist attack in recent years, but Malaysian security authorities arrested numerous people allegedly involved in terrorism in 2015, including more than 100 people linked to ISIS. In addition, Philippine-based terrorist organizations, such as the Abu Sayyaf Group, have conducted attacks and kidnappings for ransom on Malaysian territory. Malaysia's antiterrorist capabilities, which reside in both its armed forces and its police, are regarded as strong. There are concerns, however, that the increased legal powers that the Malaysian government recently granted itself might be used to stifle legitimate political dissent. In addition, the Malaysian government's promotion of religious intolerance and a conservative version of Islam is seen by some experts as contributing to an environment that encourages religious extremism and terrorism.[67] Thus, providing capacity-building assistance to Malaysia's internal security forces does not seem appropriate at this time.

Myanmar has also seen terror attacks in recent years. In the case of Myanmar, however, these have primarily been committed by Burmese Buddhists against the Muslim Rohingya community, a minority group regarded by some Burmese as noncitizens and illegal immigrants. Policies of the Myanmar government have encouraged these attacks, and the government has done little to prevent or combat them.[68] Accordingly, any counterterrorism capacity-building assistance that

---

[64] Zachary Abuza, "The Southern Thailand Insurgency in the Wake of the March 2012 Bombings," *CTC Sentinel*, June 21, 2012; "Thailand Explosion: Seven Injured in Koh Samui," *BBC News*, April 11, 2015.

[65] Susan Cunningham, "Bangkok Shrine Bombing—Case (Pretty Much) Closed," *Forbes*, December 23, 2015.

[66] U.S. Department of State, undated(d).

[67] "Malaysia Steps Up Security to Counter Terror Threat," *DW*, January 21, 2016; U.S. Department of State, undated(d).

[68] Peter A. Coclanis, "Terror in Burma: Buddhists vs. Muslims," *World Affairs*, November/December 2013; Peter Popham, "Burma's 'Great Terror' Moves a Step Closer as Taliban Urges Rohingya To 'Take Up the Sword,'" *Independent*, June 14, 2015.

the United States or Japan provided to Myanmar's security forces would likely do little to reduce the incidence of terrorism in Myanmar.

Piracy

Piracy has been a growing problem in Southeast Asia in recent years. Roughly half of the world's piracy attacks occurred in Southeast Asia in 2014 and 2015. Virtually all of these attacks have occurred in the territorial waters of one country or another, mostly Indonesia, as opposed to on the high seas.[69] The United States and Japan, therefore, could usefully provide counterpiracy capacity-building assistance to the navies and coast guards of Southeast Asian countries, particularly Indonesia. Rather than providing the assistance separately to individual countries, however, the United States and Japan might consider providing joint training for the maritime security forces of Indonesia, Malaysia, and Singapore so that those three nations can closely coordinate their antipiracy efforts. The close proximity of their territorial waters, particularly in the Malacca and Singapore Straits, where most piracy attacks occur, requires that they coordinate their efforts. Without such coordination, pirates can easily escape pursuit by one nation's maritime security forces simply by crossing into the territorial waters of a different nation. Effective counterpiracy measures in this area, therefore, require close coordination between the three countries. As noted above, the SDF's capacity-building assistance to Indonesia has been limited to training in meteorology, oceanography, and international aviation law. The SDF has not provided capacity-building assistance to Singapore, and, as of January 2016, its assistance to Malaysia had consisted of a single seminar on international aviation law.[70] The United States, however, has provided significant assistance to Indonesia and Malaysia in this area. In the case of Indonesia, this has included an Integrated Maritime Surveillance System consisting of 18 coastal surveillance stations, 11 ship-based radars, and two regional and two fleet command centers worth a total of $51 million, as well as funding for sustainment and integration of the system in subsequent years. The United States has also been providing assistance to Indonesia to increase its maritime patrol capacity; capability to integrate intelligence, surveillance, and reconnaissance information; and capabilities to maintain its maritime security equipment and to support the Indonesian Coast Guard's organizational development. In the case of Malaysia, it has also included provision of an Integrated Maritime Surveillance System, in this case consisting of eight coastal surveillance radar stations, 28 small boats, and associated maritime interdiction training, as well as a Joint Regional Command Center, worth a total of $21 million. The United

[69] Sara Sjolin, "Forget Somalia—This Is the New Sea Piracy Hot Spot," *MarketWatch*, October 7, 2015; Oceans Beyond Piracy, *The State of Maritime Piracy 2014: Assessing the Economic and Human Cost*, Denver, Colo.: One Earth Future Foundation, 2014.

[70] Ministry of Defense of Japan, undated(b).

States has also provided funding to Malaysia to work with the United States to build its maritime law enforcement training capacity and interagency coordination.[71]

Ensuring That Territorial Disputes Are Resolved Peacefully and Fairly

The most significant territorial disputes in Southeast Asia are over islands in the South China Sea. The Paracel Islands are claimed by Vietnam, China, and Taiwan but have been occupied by China since a clash between Chinese and South Vietnamese forces in 1974. Vietnam, China, and Taiwan also all claim the entire Spratly Island group, the Philippines claims much of it, Malaysia claims seven of its islands and rocks, and Brunei claims one above-water feature.[72] The Philippines, China, and Taiwan all claim Scarborough Reef, an isolated feature that is separate from both the Spratlys and the Paracels.[73]

During the late 20th century, all of the claimants except for Brunei established multiple outposts on previously unoccupied features in the South China Sea. In 2002, however, China and all ten members of the Association of Southeast Asian Nations signed a "Declaration on the Conduct of Parties in the South China Sea" in which the signatories promised to refrain from establishing outposts on "presently uninhabited islands, reefs, shoals, cays, and other features," and it appears that none of the claimants has established additional outposts on any of the features in the Spratly group since that time.[74] China has, however, engaged in a massive expansion of its facilities in both the Spratlys and the Paracels, which certainly violates its promise, in the Declaration on Conduct, "to exercise self-restraint in the conduct of activities that would complicate or escalate disputes and affect peace and stability."[75]

---

[71] U.S. Department of Defense, *Asia-Pacific Maritime Security Strategy*, August 14, 2015d, pp. 26–27; White House, Office of the Press Secretary, "Fact Sheet: U.S. Building Maritime Capacity in Southeast Asia," November 17, 2015.

[72] J. Ashley Roach, "Malaysia and Brunei: An Analysis of Their Claims in the South China Sea," CNA Occasional Paper, August 2014; Joe Burgess, "Territorial Claims in South China Sea," *New York Times*, May 31, 2012. The various claimants also claim and/or occupy numerous reefs, shoals, and banks that are below water at high tide. According to the United Nations Convention on the Law of the Sea, however, if these features are more than 12 nautical miles from the claiming country's territory, they have no territorial seas or exclusive economic zones, and the right to build artificial islands, installations, and structures on them belongs to the country on whose continental shelf they are. See Roach, 2014; and United Nations, *United Nations Convention on the Law of the Sea*, undated, pp. 29–30, 43–45.

[73] Richard Cronin and Zachary Dubel, "Maritime Security in East Asia: Boundary Disputes, Resources, and the Future of Regional Stability," Stimson Center, February 2013.

[74] Association of Southeast Asian Nations, "Declaration on the Conduct of Parties in the South China Sea," October 17, 2012.

[75] Greg Austin, professorial fellow with the EastWest Institute in New York and a professor at the Australian Centre for Cyber Security at the University of New South Wales, Canberra, at the Australian Defence Force Academy, has claimed, based on a Google Maps page, that between 1996 and 2015 Vietnam doubled the number of features it occupied. Careful comparison of the Google Maps page with a 2015 DoD map showing which country occupies each feature in the Spratly group, however, suggests that Vietnam in 1996 had already occupied most or all of the features it occupied in 2015. The misinterpretation likely stems from the fact many of the features shown on the

Neither Japan nor the United States has a position on the rightful ownership of the islands and rocks of the South China Sea. Both countries, however, have an interest in freedom of navigation and the settlement of disputes based on international law and international norms and in the dispute being handled peacefully and fairly. There have clearly been instances in which these principles were violated. These include the 1974 conflict between China and Vietnam over the Paracels, which left 36 dead, 110 wounded, and more than 160 missing, and a 1988 conflict between China and Vietnam at Johnson Reef in which 74 Vietnamese soldiers were killed and three Vietnamese ships were sunk.[76] More recently, after a standoff with the Philippines in 2012, China seized effective control of Scarborough Reef, preventing Philippine ships from approaching the area.[77] China has also tried to prevent the Philippines from resupplying one of its outposts (a grounded landing ship on Second Thomas Shoal, the BRP *Sierra Madre*, which is manned by a small number of marines from Philippines) in the Spratly Islands.[78]

These incidents, all of which, except for the last, resulted in China—by far the most militarily powerful of the claimants—taking effective control over disputed features, suggest that the territorial disputes in the South China Sea may not be resolved in a way that is equitable. To prevent such an outcome, it is in the interests of the United States and Japan to increase the capacity of the claimant countries other than China to monitor and patrol their claimed territories in the South China Sea, as well as to defend any current outposts they occupy. Such efforts could include the provision of both equipment and training to the coast guards and navies of the Philippines, Vietnam, Malaysia, and Brunei. Of these, the Philippines, both because China has been the most aggressive toward it in recent years and because of the weakness of its naval forces, is in the greatest need of assistance. The United States has provided such assistance to the Philippines. Japan has provided the Philippines with a loan to purchase ten 40-meter coast guard vessels from a Japanese shipbuilder and provided Vietnam with six used 600-ton patrol vessels.[79]

Although maritime disputes in the South China Sea dominate the headlines, Southeast Asia is the site of numerous other territorial disputes. One is a dispute between Cambodia and Thailand over the location of their border near the Preah Vihear Temple, where at least 34 people were killed in clashes between 2008 and 2011. In 2013, the International Court of Justice issued a ruling that favored Cambodia's claims in some areas and called on the two parties to decide on

---

2015 DoD map are so close to each other that they were represented by a single symbol on the map on which the Google map was based. See Greg Austin, "Who Is the Biggest Aggressor in the South China Sea?" *The Diplomat*, June 18, 2015; U.S. Department of Defense, *Asia-Pacific Maritime Security Strategy*, August 14, 2015d, p. 7.

[76] Lt. Cmdr. Jeff W. Benson, USN, "South China Sea: A History of Armed Conflict," *USNI News*, June 20, 2012.

[77] See Ely Ratner, "Learning the Lessons of Scarborough Reef," *The National Interest*, November 21, 2013.

[78] "China-Philippines Navy Spat Captured on Camera," *BBC News*, March 30, 2014.

[79] Department of Transportation and Commerce, Republic of the Philippines, "Japanese Firm to Build Ten 40-Meter Vessels for Philippine Coast Guard—DOTC," press release, 2014; "Japan Gives Vietnam 2 Ships to Beef up Maritime Security," *Stars and Stripes*, November 4, 2015.

the boundaries in other areas through negotiations.[80] Given that neither country appears to have the capability to unilaterally impose a solution on the other, and that neither is currently a democracy, it would not be appropriate for the United States or Japan to provide assistance to either that increased its capacity to enforce its territorial claims.

Thailand also has a border dispute with Laos. Although the dispute was the site of armed clashes in the 1980s and is still unresolved, the likelihood of armed conflict, or of one side attempting to unilaterally impose a resolution on the other, currently appears to be low.[81] Still, it would not be appropriate for the United States or Japan to provide assistance to either country that increased its capacity to enforce its territorial claims by force of arms.

Thailand, Cambodia, Vietnam, and Malaysia have overlapping territorial claims in the Gulf of Thailand. Malaysia and Thailand have agreed on a Joint Development Area where their claims overlap. Natural gas is currently being extracted from this area, with the revenues being shared equally.[82] Vietnam has also reached a joint development agreement with Malaysia, and Vietnam, Malaysia, and Thailand have agreed in principle on the joint development of the 875-km^2 area where the territorial claims of the three countries overlap. Cambodia's territorial claims in the Gulf of Thailand overlap with those of Thailand and Vietnam, but no agreement on border demarcation or joint development has been reached.[83] None of these disputes appears likely to result in armed conflict or a significantly inequitable resolution. Thus, there does not appear to be a need for U.S. or Japanese capacity-building assistance in this area.

A latent territorial dispute between the Philippines and Malaysia exists over the Malaysian province of Sabah, which once belonged to the Sultanate of Sulu, the remainder of which has been incorporated into the Philippines. In 2013, more than 100 Filipino followers of Jamalul Kiram III, who claimed to be the current Sultan of Sulu, invaded a village in Sabah. In the ensuing confrontation, 15 Malaysians and more than 50 Filipinos were killed. Manila has never formally renounced its claim to Sabah, but the invaders were not acting at the instigation of the Philippine government. Although there are concerns in Malaysia about a repeat of the 2013 incident, the Malaysian security forces had little difficulty defeating the invaders once Kuala Lumpur decided to use force against them.[84] Thus, Malaysia does not appear to need assistance in increasing its capacity to defeat this type of incursion.

---

[80] "Q&A: Thailand-Cambodia temple dispute," *BBC News*, November 7, 2013; Greg Raymond, "Thai–Cambodia Relations One Year After the ICJ Judgement," *East Asia Forum*, November 11, 2014.

[81] Luang Prabang, "Lao Border Talks Progressing," *The Nation* (Thailand), March 8, 2007; Ramses Amer and Nguyen Hong Thao, "Regional Conflict Management: Challenges of the Border Disputes of Cambodia, Laos, and Vietnam," *Austrian Journal of South-East Asian Studies*, Vol. 2, No. 2, 2009, pp. 53–80.

[82] Richard Cronin and Zachary Dubel, "Maritime Security in East Asia: Boundary Disputes, Resources, and the Future of Regional Stability," Stimson Center, February 2013.

[83] Amer and Thao, 2009; Manh Dong, "Maritime Delimitation Between Vietnam and Her Neighboring Countries," presentation to UN-Nippon Foundation Alumni Meeting, April 13–16, 2009.

[84] Najiah Najib, "Lahad Datu Invasion: A Painful Memory of 2013," *Astro Awani*, December 30, 2013; "Gathering Sulu Forces in Philippines Worrying Malaysia, Report Says," *Malay Mail Online*, May 28, 2015.

There are several other territorial disputes in Southeast Asia involving the location of the borders between Cambodia and Laos, Thailand and Malaysia, Thailand and Myanmar, and the Vietnamese and Indonesian exclusive economic zones. None of these disputes, however, are likely to result in major conflict or significantly inequitable resolutions.[85] Thus, there appears to be little need for capacity-building assistance in these cases.

Mitigating the Effects of Natural and Man-Made Disasters

All countries in Southeast Asia are subject to natural and man-made disasters, including typhoons, earthquakes, tsunamis, floods, volcanic eruptions, and industrial accidents. Since the benefits of providing such capacity-building would be primarily humanitarian, such assistance is appropriate for the United States and Japan to consider with respect to all Southeast Asian countries.

Conclusion

There are multiple opportunities for the United States and Japan to build partner capacity in Southeast Asia in ways that contribute to their mutual interests as well as those of their partners in the region. The United States and Japan should continue to assist the Philippines in increasing its capability to monitor and patrol its claimed territories in the South China Sea and to defend its current outposts in the Sea. The United States should also continue to aid Philippine security forces in increasing their capabilities to counter terrorism and to provide development assistance and local security. Japan could contribute in these areas as well. In Indonesia, the United States should continue to assist the Indonesian security forces in increasing their capabilities to counter terrorism, and Japan could also contribute in this area. In addition, the United States and Japan should consider aiding Indonesian security forces in increasing their capability to provide development assistance and security in Papua. The United States and Japan should provide assistance to Indonesia, Malaysia, and Singapore in increasing their joint counterpiracy capabilities. The United States and Japan should also consider assisting Malaysia and Brunei in increasing their capability to monitor and patrol their claimed territories in the South China Sea and, in the case of Malaysia, to defend its current outposts in the Sea. Japan should continue to assist Vietnam in increasing its capability to monitor and patrol its claimed territories in the South China Sea and to defend its current outposts in the Sea, and the United States could contribute in this area as well. In all countries in Southeast Asia, the United States and Japan

[85] Amer and Thao, 2009. A past dispute over the Cambodia-Vietnam border was officially settled in 2005, but opposition politicians have accused Cambodia's ruling party of using maps drawn by Vietnam in the border demarcation process, which is ongoing. In June 2015, fighting occurred between Vietnamese villagers and Cambodian activists who claimed that Vietnam had occupied approximately 75 acres of Cambodian territory. See "Hun Sen Asks Western Leaders to Help Resolve Cambodia's Border Disputes," *Radio Free Asia*, July 15, 2015.

should consider aiding the security forces of those countries in increasing their capabilities to mitigate the effects of natural and man-made disasters by providing HA/DR.

6. Japan–U.S. Cooperation on Capacity-Building in Maritime Asia

Presenter: Ken Jimbo, Ph.D.
Associate Professor
Keio University

Introduction

Capacity-building focused on enhancing the maritime security of Southeast Asian littoral states has become one of the primary pillars of regional security engagement for the Japan–U.S. alliance. Though the origins, scheme, and scope of engagement of the two countries with respect to Southeast Asia are significantly different, Tokyo and Washington are increasingly coordinating their efforts on maritime capacity-building. While the dominant form of capacity-building for both countries remains bilateral, there are growing efforts to coordinate, including through coordination of "bilateral plus" (e.g., U.S.–Japan–Philippines trilateral relations) mechanisms.

Japan's Capacity-Building in Southeast Asia

Japan's engagement in Southeast Asia, since the establishment of the Association of Southeast Asian Nations (ASEAN), has been driven primarily by strong commercial interests. Thanks in part to Japan's large-scale foreign direct investment over the past several decades, ASEAN has become the hub of production networks for many Japanese firms and their joint ventures in Asia. As early as in August 1977, then–Prime Minister Takeo Fukuda gave a landmark speech in Manila in which he rejected a role for Japan as a military power and resolved instead to contribute to peace and prosperity in Southeast Asia through support for ASEAN's solidarity and resilience. This speech ultimately came to be known as the Fukuda Doctrine.[86] In the decades following that declaration, Japan avoided playing a direct military role in the region while becoming the number-one donor of Official Development Assistance (ODA) to the ASEAN countries.[87] The principles Fukuda laid down in his speech thus set the strategic foundation of Japan's foreign policy toward the region that subsequent prime ministers, irrespective of their ideological affiliations, embraced for decades.[88]

---

[86] "Prime Minister Fukuda Takeo's Doctrine Speech" is available in Lam Peng Er, ed., *Japan's Relations with Southeast Asia: The Fukuda Doctrine and Beyond*, New York: Routledge, 2013, "Appendix 1: Fukuda Doctrine," pp. 158–162.

[87] Lam, 2013, pp. 11–14.

[88] Surin Pitsuwan, "Fukuda Doctrine: Impact and Implications on Japan-ASEAN Relations," in Lam, 2013, pp. 163–172.

In recent years, however, there has emerged a long-term shift in Japan's maritime security priorities with respect to Southeast Asia, driven mainly by the rise of China and its expanding influence in the maritime domain. In response, Japan's traditional focus on counterpiracy and sea-lane safety for merchant vessels has shifted in the direction of a greater emphasis on the balance-of-power paradigm. Under this latter framework, Japan benefits if regional actors who share its interest in an open, rule of law–based international order possess sufficient capabilities, especially in the area of maritime domain awareness, to identify potential threats, defend their interests, ensure good regional order, and resist aggression or coercion.[89]

The concept of maritime capacity-building first appeared in Japanese government policy with the issuance of the National Defense Program Guidelines (NDPG) in December 2010.[90] The NDPG 2010 held that "Japan will also strive to establish and strengthen regional cooperation practices and support the capacity-building of countries in the region" in the context of maintaining the stability of Asia-Pacific region. After this statement, the Ministry of Defense (MOD) established the Capacity-Building Assistance (CBA) Office under the International Policy Division in April 2011.[91] The CBA Office, launched with a relatively modest budget, encompasses five areas in its operational focus: (1) humanitarian assistance and disaster relief (HA/DR), (2) de-mining, (3) military medicine, (4) maritime security, and (5) United Nations peacekeeping operations.[92] The MOD's initial capacity-building efforts have focused on the "soft" approach of assisting recipient countries in human resource development.[93] In 2012, the Self-Defense Force was dispatched to Cambodia and Timor-Leste and provided development assistance for road-building and vehicle maintenance. Short-term seminars were also provided for Vietnam, Indonesia, and Mongolia for civil engineering, military medicine, aviation safety, and more.[94]

The Ministry of Foreign Affairs (MOFA) of Japan has also sought to promote maritime capacity-building in Southeast Asia through the use of "strategic ODA" (official development assistance). In June 2006, Japan donated three patrol boats to Indonesia, characterizing these as instances of ODA. The Japanese government was careful to make clear at the time that this

---

[89] Similar arguments can be found in Ken Jimbo, "Japan Should Build ASEAN's Security Capacity," *AJISS-Commentary*, May 30, 2012; Euan Graham, "Maritime Security and Capacity-Building: The Australia-Japan Dimension," in William Tow and Tomonori Yoshizaki, eds., *Beyond the Hub and Spokes: Australia-Japan Security Cooperation*, Tokyo: The National Institute for Defense Studies, 2014, pp. 43–57; Corey J. Wallace, "Japan's Strategic Pivot South: Diversifying the Dual Hedge," *International Relations of the Asia-Pacific*, Vol. 13, No. 3, 2013, pp. 479–517; and Celine Pajon, "Japan and the South China Sea: Forging Strategic Partnerships in a Divided Region," *Asie Visions 60*, Center for Asian Studies, IFRI, January 2013.

[90] Ministry of Defense of Japan, 2010.

[91] National Institute for Defense Studies, *East Asian Strategic Review*, May 2013, p. 124.

[92] Ministry of Defense of Japan, "Capacity Building Assistance," undated(a).

[93] National Institute for Defense Studies, *East Asian Strategic Review*, May 2013, p. 124; Tomoaki Honda, "Boeisho Jieitai Niyoru Hidentoteki Anzenhosho Bunya no Noryoku Kochiku Shien" [Ministry of Defense and Self-Defense Force's Capacity Building in the Non-Traditional Security], *Senryaku Kenkyu* [Strategy Studies], Vol. 15, 2015.

[94] See Ministry of Defense of Japan, undated(a).

constituted a one-off exception to its policy of strictly limiting arms exports, and prior to transferring the boats it mandated the removal of all onboard weapon systems and extracted a promise from Jakarta that the Indonesians would limit their usage to antiterrorism and antipiracy operations.[95] In 2009, the Japan International Cooperation Agency (JICA) transferred high-tech equipment to the Philippines Coast Guard (PCG) for use in maritime safety and security operations.[96] The transferred equipment included satellite communications systems, a VHF/HF radio system, a microwave communications system, and transmitting and receiving equipment. Since 2002, the PCG has regularly received staff visits from the Japan Coast Guard for antipiracy training and consultations on capacity-building.[97] In 2006, Japan helped Cambodia to improve the security facilities and equipment in its main international ports. Likewise, Japanese assistance to a number of Southeast Asian ODA recipients has helped with various infrastructure projects, including ports, airports, power generation stations, roads, and telecommunication systems and can be related to security capacity-building.[98]

Perhaps the most important benchmark for the "strategic use of ODA" is the decision to provide ten Japanese Coast Guard vessels to the Philippines.[99] In a February 2012 speech, then–Foreign Minister Koichiro Gemba made such connections explicit, saying: "I intend to strategically use ODA and other appropriate schemes to address maritime issues, which are also important for national security. Specifically, I will promote measures to defend the security of sea lanes and to improve the maritime security of coastal developing countries, including through the provision of patrol boats to fight piracy and terrorism at sea."[100] Japan's proposal to provide

---

[95] The Three Principles on Arms Exports were the basic policy governing Japan's arms exports from their declaration at the Diet session in 1967 until they were revised in April 2014. Under the Three Principles, arms exports to the following countries or regions were not permitted: (1) communist bloc countries, (2) countries subject to arms exports embargo under the United Nations Security Council's resolutions, and (3) countries involved in or likely to be involved in international conflicts. See Ministry of Foreign Affairs of Japan, "Japan's Policies on the Control of Arms Exports," 2014a. On exports to Indonesia specifically, see Ministry of Foreign Affairs of Japan, "Provision of Patrol Vessels to Indonesia," *Official Development Assistance White Paper 2006*, December 2006.

[96] See Johan Bergenas and Richard Sabatini, "Japan Takes the Lead in Coordinating Security and Development Aid," *World Politics Review*, August 1, 2012.

[97] Interview of a senior staff member from the Japan Coast Guard, September 8, 2014.

[98] Johan Bergenas and Richard Sabatini wisely describe the objective of this aid as not "aimed at militarizing a country or region, nor do the initiatives seek to 'securitize' aid. Instead, the programming is closely coordinated with recipient states' development needs, while seeking to respond to a more complex global environment in which sustainable development through security capacity-building is a critical component" (Johan Bergenas and Richard Sabatini, "Japan Takes the Lead in Coordinating Security and Development Aid," *World Politics Review*, August 1, 2012).

[99] For the details of Japan International Cooperation Agency's loan agreement, see Japan International Cooperation Agency, "Maritime Safety Capability Improvement Project for the Philippine Coast Guard," *Ex-Ante Evaluation (for Japanese ODA Loan)*, December 14, 2013.

[100] Foreign Minister Koichiro Gemba, "Japan's Efforts in the Global Agenda-Implementing 'Full-Cast Diplomacy' and Expanding the Frontiers of International Cooperation," speech delivered at the National Graduate Institute for Policy Studies, February 18, 2012.

ten patrol boats to the PCG is widely regarded as Japan's most visible commitment to engage in promoting maritime capacity-building in Southeast Asia.

After the landslide victory of the Liberal Democratic Party (LDP) in the general election of December 2012, the new administration led by Prime Minister Shinzo Abe further raised the priority on capacity-building in Japanese foreign and security policy. The Abe administration's National Security Strategy (NSS), released in December 2013, noted that "Japan will further strengthen capacity-building" in the fields of maritime order, outer space, and cyberspace.[101] The NSS also reiterated that the utilization of ODA and capacity-building assistance should contribute to seamless assistance in security-related areas. The 2013 National Defense Program Guidelines,[102] a key document issued by the Ministry of Defense to provide basic guidance of Japan's defense policy, further specified the objectives of Japan's capacity-building efforts as follows:

- Strengthening partnerships: Japan will further strengthen its relationships with partner countries in the Asia-Pacific region, including Southeast Asian countries, and will actively promote joint training and exercises and capacity building assistance.
- Capacity-building assistance: Utilizing the capabilities of the SDF, Japan will continuously engage in capacity-building assistance such as human resource development and technical support on a regular basis in order to enhance the ability of developing countries to help secure themselves, thereby improving the security environment in the Asia-Pacific region.
- Ensuring maritime security: As a maritime state, the maintenance of an "open and stable" maritime order is the cornerstone of peace and prosperity, and as such Japan will take all possible measures to secure the safety of maritime traffic. Japan will also conduct anti-piracy activities in cooperation with regional partner countries and will promote various efforts including capacity-building assistance, enhancement of joint training, and exercises in waters other than those surrounding Japan.

Japan's capacity-building in Southeast Asia, though modest to date, has the potential to expand further, especially as the Abe administration has significantly relaxed Japan's long-standing principles restraining the export of defense articles. On April 1, 2014, the Japanese government released "The Three Principles of Transfer of Defense Equipment and Technology."[103] In the new principles, transfers of defense equipment may be permitted if the case contributes to (1) the active promotion of peace and international cooperation or (2) Japan's security. Under the new principle, Japan will be able to pursue a wider range of options to transfer its defense equipment and technologies to Southeast Asia.

---

[101] Cabinet Secretariat of Japan, "National Security Strategy" (provisional translation, English version), December 17, 2013.

[102] Ministry of Defense of Japan, "National Defense Program Guidelines and Mid-Term Defense Program," December 17, 2013b.

[103] Ministry of Foreign Affairs of Japan, "The Three Principles on Transfer of Defense Equipment and Technology," April 1, 2014b.

U.S. Capacity-Building in Southeast Asia

The United States has a long-standing tradition of helping build the capacity of its allies and partners. During the Cold War, U.S. security assistance was a major component of the country's foreign engagement strategy, with a focus on Western Europe, Greece, South Korea, and Southeast Asia. The Defense Security Cooperation Agency (formally founded as the Defense Security Assistance Agency in 1961) has provided financial and technical assistance, transfer of military equipment, training, and services to allies and partners and has also promoted military-to-military contacts. The major forms of security assistance programs include Foreign Military Sales (FMS) and International Military Education and Training (IMET).

In Southeast Asia, the main component of security assistance was to build up the capacity of key U.S. allies in the region, namely the Philippines (with which the United States signed a Mutual Defense Treaty in 1951) and Thailand (as a party to the Manila Pact signed in 1954 and reaffirmed by the Thanat-Rusk Communique of 1962). During the Cold War years, one of the most important benchmarks for U.S. security engagement in Asia was the Nixon Doctrine (as articulated in 1969). Under this approach, the United States promised to "furnish military and economic assistance" while at the same time looking "to the nation directly threatened to assume the primary responsibility of providing the manpower for its defense."[104]

In the twenty-first century, U.S. capacity-building efforts in Southeast Asia have been shaped by two major dynamics. The first is DoD's initiative on security assistance reform. In 2007, the U.S. Navy, Marine Corps, and Coast Guard for the first time collectively articulated a unified maritime strategy.[105] This strategy emphasized an integrated approach to the employment of maritime forces to foster and sustain cooperative relationships with international partners through capacity-building. The 2010 Quadrennial Defense Review (QDR) pointed out that U.S. security assistance is designed to support long-term relationships and can take months or even years to fully build out and resource.[106] The 2010 QDR called for customized, whole-of-government, and interagency approaches to capacity-building. Then–Secretary of Defense Robert Gates reiterated that, given the global spread of terrorism and the threat of instability in weak or poorly governed states, "building the governance and security capacity of other countries must be a critical element of U.S. national security strategy."[107]

The second important factor is the Obama administration's strategy to rebalance to the Asia-Pacific region. The military dimension of the strategy was illustrated in the Defense Strategic Guidance announced in January 2012. Then–Secretary of Defense Leon Panetta, in announcing

---

[104] Richard Nixon, "Address to the Nation on the War in Vietnam," Nixon Library, November 3, 1969.

[105] U.S. Navy, U.S. Marine Corps, and U.S. Coast Guard, "A Cooperative Strategy for 21st Century Seapower," October 2007.

[106] U.S. Department of Defense, *Quadrennial Defense Review Report*, February 2010, p. 74.

[107] Robert Gates, "Helping Others Defend Themselves: The Future of Military Assistance," *Foreign Affairs*, May/June 2010.

the document's publication, stated that "The U.S. military will increase its institutional weight and focus on enhanced presence, power projection, and deterrence in the Asia-Pacific."[108] This pronouncement was followed by his speech at the Shangri-La Dialogue in June 2012, in which he stated that "by 2020 the Navy will re-posture its forces from today's roughly 50/50 percent split between the Pacific and the Atlantic to about a 60/40 split between those oceans. That will include six aircraft carriers in this region, a majority of our cruisers, destroyers, Littoral Combat Ships, and submarines."[109] Subsequently, Panetta emphasized that the United States would modernize and strengthen its alliances and partnerships in this region. While enhancing cooperation with traditional allies, such as Japan, South Korea, Australia, the Philippines, and Thailand, the U.S. government would also invest in new security partnerships with India, Singapore, New Zealand, Indonesia, and Vietnam. Among the most significant announcements included in the rebalance have been the rotational deployment of up to 2,500 U.S. Marines to Darwin, Australia; the rotational deployment of four Littoral Combat Ships to Singapore; and the enhancement of the U.S. military relationship with the Philippines.

DoD's role in the rebalance has emphasized the role of existing alliances as a vital foundation of regional security and the importance of expanding networks of security partnerships with emerging partners throughout the Asia-Pacific so as to "ensure collective capability and capacity" for securing common interests. The main focus of such efforts clearly aims at enhancing regional connectivity among U.S. allies and partners to ensure regional capacity.

The Case of the Philippines

Although the United States closed its military bases in the Philippines in 1992, joint counterterrorism operations and hedging against China's rise in the maritime domain have reinvigorated the security relationship between the two countries since 2001.[110] The U.S.–Philippines relationship gained new momentum under the Obama administration. U.S. military assistance to the Philippines in the 2000s had a predominant focus on counterterrorism capacity-building. For nearly a decade, U.S.–Philippines joint exercises and campaigns aimed primarily at operations in Western Mindanao and Sulu to attack Islamic terrorist groups operating in those territories, most notably the Abu Sayyaf Group.[111]

In recent years, however, U.S. military assistance to the Philippines has begun to shift focus toward potential maritime threats in the South China Sea. Such assistance has increasingly taken

---

[108] U.S. Department of Defense, "Transcript of the Press Conference: Defense Strategic Guidance from Pentagon," January 5, 2012.

[109] Leon Panetta, "The U.S. Rebalance Towards the Asia-Pacific" transcript of speech at the Shangri-La Dialogue IISS Asia Security Summit, June 2, 2012.

[110] Thomas Lum, "The Republic of the Philippines and U.S. Interests," *CRS Report for Congress*, April 5, 2012, p. 1.

[111] Lum, 2012, p. 14.

the form of enhanced joint training and exercises with the Armed Forces of the Philippines (AFP). The annual Balikatan (Shoulder-to-Shoulder) exercise, for example, has incorporated a maritime component to its drills since the early 2010s. In 2012, Balikatan included a joint combat drill off the coast of Palawan Island, which is close to the disputed Spratly Island chain and near the country's largest offshore oil field.[112] The Cooperation Afloat Readiness and Training (CARAT) exercises and the Philippines Amphibious Landing Exercise (PHIBLEX) constitute important platforms for the U.S. Navy and its Southeast Asian counterparts to conduct drills aimed at enhancing maritime patrol and HA/DR capacities.

In 2011, the United States and the Philippines agreed to upgrade the AFP's maritime security capabilities including through (1) U.S. funding support to the AFP's Capability Upgrade Program (CUP), which includes acquisition of equipment, as well as extensive refurbishing and maintenance of existing AFP materiel; and (2) the provision of an additional $40 million for Coast Watch South to boost the AFP's surveillance, communications, and interdiction capabilities.[113] The United States also transferred two former *Hamilton*-class U.S. Coast Guard cutters to the Philippine Navy through FMS. In December 2013, Secretary of State John Kerry announced the implementation of a three-year, $40 million program for the Philippines under the Global Security Contingency Fund (GSCF). The program will be used to improve maritime security and maritime domain awareness and to provide assistance for law enforcement counterterrorism capacity-building in the southern Philippines.[114]

In late April 2014, the two allies signed a framework agreement called the Enhanced Defense Cooperation Agreement (EDCA).[115] EDCA envisions the United States supporting the AFP by "addressing short-term capability gaps, promoting long-term modernization, and helping maintain and develop additional maritime security, maritime domain awareness, and humanitarian assistance and disaster relief capabilities."[116] On January 12, 2016, the Philippine Supreme Court upheld the legality of EDCA, and this led both governments to agree on the first five locations in which to begin implementing EDCA.

The Case of Vietnam

In December 2013, U.S. Secretary of State John Kerry announced an initial commitment of $32.5 million in new regional and bilateral assistance to advance maritime capacity building in

[112] Lum, 2012, p. 15.

[113] United States Embassy, Manila, "Co-Chair's Statement of the Philippines-United States Bilateral Strategic Dialogue," January 27–28, 2011.

[114] U.S. Department of State, Office of the Spokesman, "Global Security Contingency Fund Program for the Philippines," December 17, 2013.

[115] Government of the Philippines, "Agreement Between the Government of the Republic of Philippines and the Government of the United States of America on Enhanced Defense Cooperation," *Official Gazette*, April 29, 2014.

[116] Government of the Philippines, 2014.

Southeast Asia.[117] The United States intends to provide up to $18 million in funding for search and rescue, disaster response, and other activities, including through provision of five fast patrol vessels to the Vietnamese Coast Guard. Existing programs include efforts to combat piracy in and around the Malacca Strait, to counter transnational organized crime and terrorist threats in the tri-border region south of the Sulu Sea between the southern Philippines, Indonesia, and Malaysia, and to expand information-sharing and professional training through the Gulf of Thailand initiative.

In FY 2015, the United States increased its maritime assistance program spending to $19.6 million to support developing Southeast Asian maritime capabilities to bolster maritime intelligence, surveillance, and reconnaissance (ISR) and command and control, a program that has implications for assisting Vietnam's maritime agencies. The White House also stated that it has lifted "the ban on sales of maritime-related lethal capabilities to allow development of Vietnam's maritime capacity and encourage interoperability with other regional forces."[118] The United States also indicated that it would expand bilateral training and exercise with Vietnam.[119]

Conclusion

Although Japan and the United States have different historical experiences with maritime capacity-building in Southeast Asia, there is an increasing synergy and complementarity to their bilateral approaches to this issue. There are two underlying trends that have driven the two countries to adopt similar policy goals and measures.

First, there is an urgent need on the part of numerous Southeast Asian littoral states to build up their maritime patrol and defense capabilities in light of the growing challenge to their maritime claims posed by the Chinese Coast Guard and the Chinese People's Liberation Army Navy. China's rapid pace of fielding new coast guard vessels, its consolidation of its maritime law enforcement forces, its offshore resource development efforts, innovative use of its commercial fishing fleet as a de facto maritime militia, and massive construction of artificial islands capable of sustaining substantial military capabilities in the disputed maritime zone constitute "tailored coercion" against its Southeast Asian neighbors.[120] The substantial growth of Chinese naval power and airpower are likely to continue for the foreseeable future, putting China's Southeast Asian neighbors at a clear and growing disadvantage in the years ahead.

Second, the long-term shift in the maritime strategies of Japan and the United States, based on their shared strategic interests in an open, rule of law–based international order, has created

[117] U.S. Department of State, "Expanded U.S. Assistance for Maritime Capacity Building," December 16, 2013b.

[118] White House, Office of the Press Secretary, "Fact Sheet: U.S. Building Maritime Capacity in Southeast Asia," November 17, 2015.

[119] White House, Office of the Press Secretary, 2015.

[120] Patrick M. Cronin, Ely Ratner, Elbridge Colby, Zachary M. Hosford, and Alexander Sullivan, "Tailored Coercion: Competition and Risk in Maritime Asia," Center for New American Security, March 2014.

an opportunity for increased policy coordination between Tokyo and Washington. As noted above, Japan's maritime security priorities in Southeast Asia are increasingly strategy-driven and aimed at maintaining a balance of power that favors the status quo countries of the region. The U.S. rebalance has emphasized the importance of ensuring operational access to the East Asian strategic theater for U.S. forces, as well as encouraging allies and friends to build up their own capacities for maritime security.

The following are some recommendations for Japan and the United States to further enhance cooperation on maritime capacity-building in Southeast Asia. Tokyo and Washington and should enhance cooperation on the following areas.

Maritime Domain Awareness

At the top of the agenda is providing littoral states in Southeast Asia, especially the Philippines and Vietnam, with better (and shared) intelligence-gathering capabilities at sea. Currently, a lack of maritime domain awareness in the South China Sea is a strategic and operational problem. With countries in the region insufficiently equipped to monitor waters that they claim and that are proximate to their territory, they face basic challenges of simply knowing what activities are occurring in or near their waters. Japan and the United States should therefore enhance their cooperation by

- upgrading the Coast Watch System in the Philippines
- building capacity for data-gathering, processing, and distribution
- building up the capacity of regional coast guards
- enhancing the ISR capabilities of regional partner nations, including through assistance aimed at helping regional states acquire both air and maritime ISR assets[121]
- sharing real-time satellite information
- sharing real-time information on marine traffic via the Automatic Identification System and
- development of supporting infrastructure and communication systems.

Common Operating Picture

Japan and the United States need to develop a common operating picture (COP) in the maritime domain to share with Southeast Asia littoral states. This is important in two senses. First, "gray zone" contingencies are even more likely in the South China Sea than in the East China Sea. In order to respond effectively, the United States, Japan, and regional actors need to share a common understanding of the actual state of play, as well as clarity about their likely roles and responsibilities and the actions that their partners would be likely to take. Second, a COP is a critical aspect of "escalation management" if the United States is to use its full national means to respond to a crisis.

---

[121] See Renato Cruz De Castro and Walter Lohman, "Getting the Philippines Air Force Flying Again: The Role of the U.S.-Philippines Alliance," *Backgrounder*, The Heritage Foundation, September 24, 2012.

Strategic Financing

Japan's ODA and U.S. FMS and assistance need to be further coordinated in order to enhance maritime capacity-building in Southeast Asia. Aspects of ASEAN's critical infrastructure, such as airports, ports, roads, power generation stations and electricity supply, communications, and software development, are important—and often highly compatible—components of their security sectors. These could become significant force multipliers if the necessary financial aid, as well as investment promotion schemes, can be coordinated among Japan, the United States, and regional countries.

Maritime Security Order Based on Asymmetrical Equilibrium

In the end, Japan and the United States share the goal of a liberal, rule of law–based international order in the South China Sea. Such an order needs to be undergirded by a balance of power that favors the Japan–U.S. alliance. The only plausible model for the South China Sea will be one of "asymmetric denial." As China is acquiring anti-access/area denial (A2/AD) capabilities vis-à-vis the United States, the Philippines and Vietnam similarly may be able to collectively block a change in the status quo by force through the acquisition of their own asymmetric capabilities, a kind of reverse A2/AD approach. They may not need to achieve parity with China in order to achieve such an outcome; if a country acquires the ability to impose unacceptable costs and negative consequence on assertive unilateral behavior, this could create an effective denial capability. Such an "asymmetrical equilibrium" could help underwrite a new model of stable maritime order in Southeast Asia.

7. U.S.–Japan–Australia Trilateral Security Cooperation: Opportunities and Challenges

Presenter: Yuki Tatsumi
Senior Associate
The Henry L. Stimson Center

Introduction

The U.S.–Japan–Australia security relationship has quickly emerged as one of the most robust trilateral security relationships that the United States has with its allies in the Asia-Pacific region. This trilateral security relationship is anchored by but also transcends U.S. bilateral alliances, and the relationship has grown closer at an accelerating pace since 2013. The purpose of this chapter is to examine (1) the drivers for developing the U.S.–Japan–Australia security partnership, (2) the areas for cooperation, and (3) challenges of cooperation.

When President Barack Obama met with his Australian and Japanese counterparts on the sidelines of the G20 Summit in Brisbane, Australia, in 2014, the three leaders emphasized their commitment to "deepening the trilateral partnership . . . . to ensure a peaceful, stable, and prosperous future for the Asia-Pacific region."[122] Based on such shared values as their "commitment to democracy, open economies, the rule of law and the peaceful resolution of disputes,"[123] Washington, Canberra, and Tokyo have paid increasing attention to their rapidly deepening trilateral partnership as a framework to maintain and enhance the international order in the Asia-Pacific region.[124]

Although the U.S.–Japan–Australia trilateral security partnership has been developing steadily since the end of the Cold War, their security partnership first attracted increased attention in 2006 when the foreign ministers of the three countries met for the first trilateral security dialogue (TSD) ministerial meeting.[125] With the creation of the Security and Defense Cooperation Forum (SDCF) in 2007, the trilateral relationship evolved from a framework for

[122] White House, Office of the Press Secretary, "Australia-Japan-United States Trilateral Leaders Meeting Joint Media Release," November 16, 2014.

[123] White House, Office of the Press Secretary, 2014.

[124] Yuki Tatsumi, ed., *US-Japan-Australia Security Cooperation: Prospects and Challenges*, Stimson Center, 2015, p. 18.

[125] Tomohiko Satake, "The Origin of Trilateralism? The US-Japan-Australia Trilateral Relations in the 1990s," *International Relations of the Asia-Pacific Region*, Vol. 11, 2010, pp. 87–114, provides an excellent overview of the developments in the trilateral relationship in the years immediately after the Cold War.

policy consultation on terrorism and other nontraditional security issues to a mechanism that the three countries could employ for the purposes of practical defense cooperation.

Today, the U.S.–Japan–Australia trilateral security partnership is recognized as a critical instrument in each country's security policy. Leaders in the three countries recognize that it not only reinforces their bilateral security alliances and partnerships with one another but is also useful for broader regional engagement. Defense officials from the three countries have frequent opportunities for a variety of face-to-face meetings, ranging from regular ministerial meetings on the sidelines of multilateral conferences, such as Shangri-La Dialogue and the ASEAN Defense Ministers' Meeting-Plus (ADMM Plus), to working-level consultations on specific policy issues. The U.S. and Australian armed forces and the Japan Self-Defense Force also hold joint exercises and training with increasing frequency; recent such opportunities include

- a joint naval exercise by the U.S. Navy, the Royal Australian Navy, and the Japan Maritime Self-Defense Force (JMSDF) in August 2014
- the *Michinoku Alert 2014* exercise between the Japan Ground Self-Defense Force (JGSDF), the U.S. Army, the U.S. Marine Corps, and the Royal Australian Army in November 2014
- the *Cope North Guam 2015* exercise between the U.S. Air Force, the Royal Australian Air Force, and the Japan Air-Self-Defense Force (JASDF) in February 2015
- the *Southern Jackaroo* exercise between the U.S. Army and U.S. Marines, the Royal Australian Army, and the JGSDF in May 2016.[126]

In addition, Australia participated in *Dawn Blitz 2015*, hosted by the U.S. Marine Corps, in which the JGSDF also participated as an observer.[127] The three militaries also hold various staff-level consultations on a regular basis.

As the foregoing thumbnail sketch shows, trilateral defense cooperation has been moving forward in recent years. What factors are driving this growth in military-to-military relations and broader security cooperation? What specific forms does it take? And how far can it go? The remainder of the paper explores these questions in turn.

Drivers Behind the Accelerating Defense Relationship Among the Three Countries

The intensifying security cooperation between the United States, Japan, and Australia is a result of the developments that have occurred at three different levels—in each country's national security policies, in their bilateral alliances and partnerships, and in the broad regional security environment. These are explored below in turn.

[126] Australian Army Headquarters, "Exercise Southern Jackaroo Wraps Up," May 30, 2016.

[127] U.S. Marine Corps, "Dawn Blitz 2015," undated.

Evolving Trends in American, Japanese, and Australian National Security Policies

There has been a common trend among U.S., Australian, and Japanese national security policies toward greater emphasis on trilateral and multilateral security cooperation beyond traditional bilateral alliance cooperation. For the United States, while bilateral alliances remain the core of its strategy for maintaining peace and stability in the Asia-Pacific region, multilateral security cooperation with its allies and strategic partners has emerged as a key force multiplier that is beneficial to U.S. security policy goals in the region. In particular, since the Obama administration launched its "rebalance to the Asia-Pacific" strategy in 2011, the incentive to utilize existing alliances and partnerships in a more flexible manner has become an essential component of the effort led by the U.S. Department of Defense (DoD). U.S. Secretary of Defense Ashton Carter has described such efforts as "reinforcing the partnerships and alliances that are the bedrock of everything we do in the Asia-Pacific."[128] In his April 2015 speech, Secretary Carter described an "unprecedented" effort to "expand the reach of our alliances" by "networking our [U.S.] relationships."[129] U.S. defense spending will likely remain flat due to budgetary constraints over the next decade, making security cooperation with allies and partners that goes beyond the traditional "hub-and-spokes" approach—including encouraging enhancement of the relationships among the "spokes"—an attractive policy choice for a fiscally constrained Washington.

In Tokyo, the desire to expand its role both within the U.S.–Japan alliance and beyond is growing, especially following the inauguration of Prime Minister Shinzo Abe in December 2012. Abe first unveiled his vision for Japan's place in the international community during his February 2013 visit to Washington, describing his vision of Japan as "a rules-promoter, a commons' guardian, and an effective ally and partner to the U.S. and other democracies."[130] His views were further elaborated in Japan's first-ever *National Security Strategy,* which was published in December 2013. In this document, the improvement of the security environment in the Asia-Pacific region was defined as one of the key objectives for Japan's national security policy, and alliance cooperation with the United States and broader security cooperation with other partners that share Japan's values were identified as two key components to achieve this goal. In particular, Australia has been defined as Japan's most important regional partner. The *National Security Strategy* encourages Japan to utilize trilateral security cooperation with the United States and Australia "to shape regional order in the Asia-Pacific and to maintain and reinforce peace and stability in the international community."[131]

---

[128] U.S. Department of Defense, "Secretary of Defense Speech: Remarks on the Next Phase of the U.S. Rebalance to the Asia-Pacific," April 6, 2015a.

[129] U.S. Department of Defense, 2015a.

[130] Prime Minister of Japan and His Cabinet, "'Japan Is Back': Policy Speech by Prime Minister Shinzo Abe at the Center for Strategic and International Studies," February 22, 2013a.

[131] Prime Minister of Japan and His Cabinet, *National Security Strategy*, December 17, 2013b.

For Australia, its core strategic interest has been to prevent major power competition in the Asia-Pacific region and thereby maintain the stability in the region. Since 1945, a close alliance with the United States has been the key vehicle through which Canberra pursued this goal. It also led Australia to continue to prioritize close and robust defense ties with the United States in order to ensure Washington's engagement in the Asia-Pacific region.[132]

In its recently announced *Defence White Paper 2016*, the Australian Department of Defence identified three "Strategic Defence Interests" that will drive Australia's defense policymaking: (1) to deter or defeat any attack on, or attempt to coerce, Australia; (2) to secure "maritime Southeast Asia" and the South Pacific; and (3) to contribute to a stable Indo-Pacific region and a rules-based global order.[133] Further, discussing Australia's international engagement in defense sector, the *Defence White Paper 2016* emphasizes that Australia will strive to sustain a "deep and strong alliance" with the United States and continue to enhance its security relationship with Japan. It also indicates Australia's willingness to enhance its investment in capacity-building in the Indo-Pacific region "to contribute to our collective security."[134] Although the *Defence White Paper 2016* remains restrained in its tone, it still identifies "challenges to the stability of the rules-based global order, including competition between countries and major powers trying to promote their interests outside of the established rules" as one of the strategic trends that will shape Australia's security environment to 2035, acknowledging that the territorial disputes in East and South China Sea "have created uncertainty and tension in our region."[135]

Developments in Bilateral Relations

Secondly, there have been developments in bilateral security relations among the three bilateral relationships—the U.S.–Japan, U.S.–Australia, and Japan–Australia dyads—that reinforce the three countries' interests in continuing to cultivate deeper trilateral cooperation. When the United States and Japan signed the *Joint Declaration on Security* in April 1996, the two countries redefined the purpose of the U.S.–Japan alliance as being to serve as a "cornerstone" of peace and prosperity in the Asia-Pacific region.[136] Since then, the U.S.–Japan alliance has made steady progress toward creating a structure that (1) enables Japan to assume a larger amount of responsibility in the alliance and (2) facilitates a coordinated approach to engagement with other partners in the region.

---

[132] Peter Jennings, "The U.S. Rebalance to the Asia-Pacific: An Australian Perspective," *Asia Policy*, No. 15, January 2013, p. 38.

[133] Australian Department of Defence, *Defence White Paper 2016*, 2016.

[134] Australian Department of Defence, 2016, pp. 117–134.

[135] Australian Department of Defence, 2016, pp. 30, 40.

[136] Ministry of Foreign Affairs of Japan, *Japan-U.S. Joint Declaration on Security: Alliance for the 21st Century*, April 17, 1996.

Security cooperation with partners who share their support for the existing principles of the international order in the Asia-Pacific region has emerged as one of the priorities for the U.S.–Japan alliance in recent years. With Japan poised to play a bigger security role in the Asia-Pacific region in the wake of a series of important defense reforms, Tokyo and Washington have moved to modernize the existing mechanism of defense cooperation to reflect the changing nature of security challenges in the Asia-Pacific region and beyond. In the joint statement *Toward a More Robust Alliance and Greater Shared Responsibilities* issued at the Security Consultative Committee (SCC) meeting on October 3, 2013, the importance of trilateral security cooperation with Australia (as well as with South Korea) was recognized as a useful vehicle to "advance our shared security interests, promote common values, and enhance the security environment of the Asia-Pacific region."[137]

The two governments have completed the revision of the *Guidelines for Japan–U.S. Defense Cooperation*, which were announced on the eve of Prime Minister Shinzo Abe's April 2015 visit to Washington, D.C. Under the revised guidelines, Japan now assumes greater responsibility in defense of its homeland, as well as in regional emergencies. When Secretary of Defense Ashton Carter, Secretary of State John Kerry, Minister of Defense Gen Nakatani, and Minister of Foreign Affairs Fumio Kishida met for the Security Consultative Committee meeting (known as the "2 + 2" meeting) on April 27, 2015, to announce the modernized *Guidelines for Japan–U.S. Defense Cooperation*, they affirmed that "cooperation with regional and other partners" is also emphasized as one of the foci of the revised guidelines.[138] In the joint statement *A Stronger Alliance for a Dynamic Security Environment*, which was announced with the revised guidelines, the four ministers confirmed that the U.S.–Japan alliance serves as a "platform for promoting a more peaceful and stable international security environment."[139]

Likewise, the United States and Australia took their first step toward leveraging their bilateral alliance to boost their day-to-day engagement and respond to the security challenges in the Asia-Pacific region when they agreed on the Force Posture Initiative in 2011. Under the initiative, Australia agreed to host a rotational presence of U.S. Marines in Darwin. It also reaffirmed its alliance as an "anchor" of peace and stability in the Asia-Pacific region and beyond during the Australia–United States Ministerial Consultation (AUSMIN) Joint Statement on November 20, 2013.[140] At the AUSMIN in August 2014, Washington and Canberra signed the Force Posture Agreement, reaffirming both countries' commitment to fully implementing the

---

[137] Ministry of Defense of Japan, *Joint Statement of the Security Consultative Committee: Toward a More Robust Alliance and Greater Shared Responsibilities*, October 3, 2013a.

[138] Ministry of Defense of Japan, *The Guidelines for Japan-U.S. Defense Cooperation*, April 27, 2015.

[139] Minister for Foreign Affairs Fumio Kishida, Minister of Defense Gen Nakatani, Secretary of State John Kerry, and Secretary of Defense Ashton Carter, *Joint Statement of the Security Consultative Committee: A Stronger Alliance for Dynamic Security Environment*, April 27, 2015.

[140] U.S. Department of State, "Australia–United States Ministerial Consultation (AUSMIN)," November 20, 2013a.

Force Posture Initiative originally announced in 2011.[141] Furthermore, at the October 2015 AUSMIN, the defense officials of the two governments signed a Joint Defense Statement in which they reaffirmed their commitment to deepen their bilateral defense ties to "shape a rule-based international order that promotes peace, security, and opportunities for all" by working together bilaterally and with partners.[142]

Finally, the deepening of Japan–Australia security relations is a particularly noteworthy development in the last several years, as well as a driver of U.S.–Japan–Australia trilateral cooperation. In fact, one might argue that what makes the U.S–Japan–Australia trilateral relations unique is the depth and breadth of security relationships between Japan and Australia. Unlike U.S.–Japan–South Korea trilateral relations that have been strained by political tension between Tokyo and Seoul stemming from a sense of grievance in South Korea regarding Japan's handling of its wartime history, security relations between Tokyo and Canberra have steadily developed since the end of the Cold War. Security cooperation between the two countries initially began in the context of large multinational operations, such as the United Nations peacekeeping mission in East Timor and the post-conflict reconstruction of Iraq. However, security relations between Tokyo and Canberra quickly developed after the two countries signed the Japan–Australia Joint Declaration on Security Cooperation in 2007. Today, for both Canberra and for Tokyo, the security relationship they enjoy with one another constitutes their most important, institutionalized bilateral security relationship other than with the United States. Their foreign and defense ministers have met for 2+2 consultations annually since 2007. With the signing of the Acquisition and Cross-Servicing Agreement (ACSA) and General Security of Military Information Agreement (GSOMIA) in 2010 and 2012 respectively, the two countries have the key agreements in place to facilitate deeper defense cooperation between the Australian Defence Force (ADF) and the JSDF. In addition, when their foreign and defense ministers met in June 2014, both sides agreed to explore the possibility of defense equipment cooperation.[143] The joint statement issued at the end of the June 2014 2+2 meeting identified several areas in which the two sides agreed to boost cooperation, including joint training and exercises, personnel exchanges, HA/DR, maritime security cooperation, peacekeeping, and capacity-building. Trilateral security cooperation with the United States was also highlighted as a high-priority issue.[144]

---

[141] U.S. Department of State, "Joint Communique AUSMIN 2014," August 12, 2014.

[142] Australian Department of Defence and U.S. Department of Defense, "Statement on Defense Cooperation in the 21st Century," undated.

[143] Ministry of Defense of Japan, "5th Japan-Australia 2+2 Foreign and Defense Ministerial Consultations," June 11, 2014.

[144] Ministry of Defense of Japan, "5th Japan-Australia 2+2 Foreign and Defense Ministerial Consultations," June 11, 2014.

Regional Imperatives

Finally, the developments in the region have facilitated the desire of the three countries to enhance security cooperation with one another. China's assertive international behavior in recent years, especially in the East China Sea and the South China Sea, looms large as one of the leading drivers of this trend. Australia's *Defence White Paper 2013,* Japan's *National Security Strategy,* and the U.S. *Asia-Pacific Maritime Security Strategy* all point to concerns over the "excessive claims" by some of the claimants in the South China Sea, including China, which have had an adverse impact on the "maintenance of the rule of law" and the peaceful resolution of international disputes, threatening freedom at sea.[145] In particular, these reports note the intensification of China's assertive actions, which include its unilateral declaration of an air defense identification zone (ADIZ) in the East China Sea, its construction of artificial land features that include airstrips in the South China Sea, and an increase in aggressive behavior toward both the patrol and fishing boats of other claimants in South China Sea.

Indeed, China's behavior in the South China Sea has raised the urgency of cooperation among the three countries, all of which look at Chinese behavior as posing a serious challenge to the important principles that support the existing international order. The hardening of Australia's attitude toward China in the last couple of years is particularly noteworthy. After all, until Tony Abbott became prime minister in 2013, Australia had been hesitant to promote trilateral cooperation with the United States and Japan out of a concern that doing so might alienate China. Indeed, there is still an active debate within Australia among foreign policy intellectuals about the wisdom of aligning Australia too closely with the United States and/or Japan at the expense of relations with China, its biggest trading partner and the largest market for its natural resource exports.[146] The shift in Canberra's position, as illustrated first in the *Defence White Paper 2013* and continued in the *Defence White Paper 2016*, as well as Washington's intensified call to halt further reclamation and militarization activities in South China Sea,[147] reflect the rising sense of urgency.

In the last two years, Japan, for its part, has also demonstrated that its concern for Chinese assertive behavior is growing. In June 2015, Admiral Katsutoshi Kawano, JSDF's Chief of Joint Staff, suggested in an interview that the JSDF would consider joining the United States in joint

---

[145] U.S. Department of Defense, *Asia-Pacific Maritime Security Strategy*, August 14, 2015d; Prime Minister's Office and His Cabinet, *National Security Strategy*, December 17, 2013b; Australian Department of Defence, "Defence White Paper 2013," 2013.

[146] For recent discussion against Australia aligning itself too closely with the United States (and Japan), see, for example, Hugh White, *The China Choice: Why America Should Share Power*, Melbourne, Australia: Black Inc., 2012. Also see, for example, the "China Gap" argument by Tomohiko Satake in "Japan-Australia Relations: Towards Regional Order-Building," in Yuki Tatsumi, ed., *Japan's Global Diplomacy: Views from the Next Generation*, Stimson Center, March 2015, pp. 21–31.

[147] U.S. Department of Defense, "Secretary of Defense Speech: Remarks at ASEAN Defense Ministers' Meeting-Plus (ADMM-Plus)," November 4, 2015e.

patrol of the South China Sea.[148] When Vietnamese Community Party Chief Nguyen Phu Tong visited Tokyo to meet with Prime Minister Abe in September 2015, the two countries announced a grant program under which Japan would provide aid, including patrol boats, to the Vietnamese government to support Hanoi's effort to enhance its capacity in responding to China's reclamation activities.[149] Most recently, the Japanese government decided to loan retired JMSDF training aircraft to the Filipino Navy to enhance its surveillance capability.[150]

In addition, the three countries' collective experiences in working together in response to large-scale natural disasters in the Asia-Pacific region have given them confidence that they can play a role of "core partners" in orchestrating region-wide responses to natural and man-made disasters. As key allied militaries of the United States, both the JSDF and the ADF enjoy high levels of interoperability with the U.S. armed forces, which facilitated their cooperation in providing HA/DR in response to the 2004 Indian Ocean tsunami. When Japan was hit by the March 11, 2011, triple disaster of the biggest earthquake since the 1995 Hanshin-Awaji earthquake, the most severe tsunami in recent history, and the meltdown of the Fukushima Dai-ichi nuclear power plant, the U.S. military provided large-scale support under *Operation Tomodachi*, with the ADF also providing support through U.S. military facilities. When Typhoon Haiyan hit the Philippines, the United States, Japan, Australia, and Singapore played major roles in providing the military assistance essential for the initial recovery period.

Finally, the three countries share concern over other state-based (North Korea's nuclear and missile programs) and nontraditional (i.e., terrorism) national security challenges. They also share an interest in actively engaging in a wide variety of peacetime activities, including capacity-building in Southeast Asia and multinational operations, such as United Nations peacekeeping operations, in which three countries often contribute. This has motivated the defense establishments of three countries to share intelligence and information and to improve communications by increasing the frequency of trilateral consultations. The fourth nuclear test by North Korea on January 6, 2016, and the terrorist bombing in Jakarta on January 14, 2016, only reinforce the case for greater cooperation.

Areas of Cooperation

While there is an overall agreement among Washington, Canberra, and Tokyo on the need for trilateral cooperation, some areas are better established than others. This section explores examples of several types of ongoing or potential trilateral security cooperation.

---

[148] Yuka Hanashi and Chieko Tsuneoka. "Japan Open to Joining U.S. in South China Sea Patrols," *Wall Street Journal*, June 25, 2015.

[149] "Japan to Step Up Help for Vietnamese Maritime Security," Associated Press, September 15, 2015.

[150] "Kaiji-ki Hi-Kaigun ni Taiyo-he: Minami Shina-kai no Kanshi ni Riyou [Japan to Loan JMSDF Aircraft to Filipino Navy: To Be Used for South China Sea Surveillance]," *Yomiuri Shimbun*, February 29, 2016.

Humanitarian Assistance/Disaster Relief: Habits of Cooperation Firmly Established

The Asia-Pacific region is a disaster-prone area: From earthquakes to tsunamis, it is not uncommon for the region to suffer large-scale disasters several times throughout any given year. For this reason, HA/DR is considered a high-priority area of cooperation in region-wide multinational frameworks. For instance, in the ASEAN Regional Forum (ARF), Australia co-sponsors the ARF Disaster Relief Web Mapping Service, which facilitates voluntary provision of geospatial data on natural and man-made disasters by ARF member states so as to enable timely, region-wide cooperation on HA/DR.[151] Cooperation in provision of HA/DR in the aftermath of large-scale disasters contributes not only to the recovery of the countries affected by these disasters, but it is also useful in developing "habits of cooperation" among the participants, thereby contributing to confidence-building among them.

HA/DR area is an area in which the United States has been increasing cooperation with Japan and Australia since the end of the Cold War. In addition to the track record of U.S.–Japan and U.S.–Australia cooperation in HA/DR, their successful experience of forming a core group within the international coalition to respond to the 2004 tsunami in the Indian Ocean has encouraged the three countries to approach HA/DR cooperation on trilateral basis since 2008. The cooperation among the U.S. military, the ADF, and the JSDF in the aftermath of the Great Eastern Japan Earthquake in 2011 further reinforced the importance of HA/DR operations.[152]

Capacity-Building in Southeast Asia

In the past, the United States, Japan, and Australia had pursued their respective engagements with Southeast Asia separately. The United States' post–World War II engagement with the region has been anchored by its security assistance to such allies as the Philippines and Thailand. Australia's relative proximity to Southeast Asia has encouraged Canberra to actively develop its relationship with Southeast Asia, including initiating the Colombo Plan in 1950 and participating in the Southeast Asia Treaty Organization (SEATO) when it was first launched in 1954. Japan, though initially handicapped by its World War II wartime atrocities in the region, developed over time into the region's most important economic partner (until the recent rise of China) and its biggest provider of official development assistance (ODA).

These three separate approaches have seen convergence in recent years. As the United States explores ways to effectively implement its Asia-Pacific rebalance, it has encouraged networking among its allies and partners in the region. Capacity-building in Southeast Asia is regarded as an important policy tool to achieve this goal by helping countries in Southeast Asia buttress their capacities to secure common interests. In his speech at the annual Shangri-La Dialogue in May

---

[151] ASEAN Regional Forum—Disaster Relief Mapping Service, home page, undated.

[152] H. D. P. Envall, "Community Building in Asia? Trilateral Cooperation in Humanitarian Assistance and Disaster Relief," in Yuki Tatsumi, ed., *US-Japan-Australia Security Cooperation: Prospects and Challenges*, Stimson Center, April 2015, pp. 51–59.

2015, Secretary of Defense Carter spoke about the U.S. desire to see an Asia-Pacific region "that is strong enough, capable enough, and connected enough to ensure that all Asia-Pacific peoples and nations have the opportunity to rise—and continue to rise—in the future."[153]

With respect to Japan, in both its *National Security Strategy* and its *National Defense Program Guidelines,* it identified capacity-building as one of its policy priorities. The *NSS* articulated the need for a "whole of government" approach to capacity-building in Southeast Asia that combines the strategic use of Japan's ODA toward this region and specific capacity-building activities conducted by the JSDF and the Japanese Coast Guard.[154] The *NDPG* clarified the objectives of Japan's capacity-building activities conducted by the JSDF in Southeast Asia as being designed to strengthen Japan's partner relationships with the countries in question by helping them acquire the capacity to play a role in stabilizing the regional security environment.[155]

Australia has engaged in capacity-building in Southeast Asia, first through SEATO and then primarily through defense diplomacy—bilaterally and through the Five-Power Defense Arrangement—with the countries in the region after SEATO was dissolved. It also launched Pacific Patrol, an effort specifically focused on maritime capacity-building.[156]

The three countries are increasingly focusing their trilateral security cooperation efforts of capacity-building in Southeast Asia on maritime capacity-building in the region. Japan has agreed to transfer its Coast Guard vessels and other maritime law enforcement assets to Southeast Asian countries. Secretary of Defense Carter launched the Maritime Security Initiative in his Shangri-La Dialogue speech on May 30, 2015.[157] When President Obama, Prime Minister Abe, and then–Prime Minister Tony Abbott met in Brisbane in November 2014, the three leaders reaffirmed their commitment to "deepen the already strong security and defense cooperation among the three countries and to strengthen the collective ability to address global concerns and promote regional stability through enhanced cooperation on: trilateral exercises; maritime security capacity building and maritime domain awareness; peacekeeping capacity building."[158]

The increased degree of coordination and cooperation among the three countries in the maritime capacity-building realm is clearly a response to the rather urgent needs on the part of Southeast Asian littoral states to build maritime patrol and defense capabilities, in light of their widening capability gap vis-à-vis China's Coast Guard and People's Liberation Army Navy. Just

---

[153] U.S. Department of Defense, "ISIS Shangri-La Dialogue: 'A Regional Security Architecture Where Everyone Rises,'" May 30, 2015b.

[154] Prime Minister of Japan and His Cabinet, *National Security Strategy*, December 17, 2013b.

[155] Ministry of Defense of Japan, *National Defense Program Guidelines for FY 2014 and Beyond*, December 17, 2013c.

[156] Ken Jimbo, "Japan-US-Australia Cooperation in Capacity-Building in Southeast Asia," in Yuki Tatsumi, ed., *US-Japan-Australia Security Cooperation: Prospects and Challenges*, Stimson Center, April 2015, pp. 61–75.

[157] U.S. Department of Defense, 2015b.

[158] Australia-Japan-United States Trilateral Leaders Meeting, "Joint Media Release," November 16, 2014.

as China's assertiveness facilitated the convergence of U.S., Japanese, and Australian strategic interests in the Asia-Pacific region to pursue greater cooperation among themselves in defense of the status quo and existing international norms and order, it has also helped sharpen the focus of the three countries' capacity-building efforts in Southeast Asia.[159]

Defense Technology and Equipment

In contrast with HA/DR and capacity-building in Southeast Asia—both of which are areas in which U.S.–Japan–Australia trilateral cooperation or coordination has been well established—cooperation in defense technology is still at a very nascent stage. This is because the defense industrial sector tends to remain one of the most protected sectors in any country that can afford to have one, despite globalization.

However, the failure on the part of the defense industrial sector in the three countries to fully catch up with the pace of technological change, combined with the rising cost of defense acquisition, has forced the defense establishments in all three governments to (1) look for ways to engage with companies beyond the fixed list of major defense contractors and (2) explore opportunities to collaborate with foreign industrial partners as a strategy to reduce costs by sharing them. These factors have collectively encouraged the United States, Japan, and Australia to put more emphasis on defense technology and equipment cooperation. In particular, Japan, which has undertaken policy changes that give it greater flexibility to export defense articles, has implemented considerable reform in its defense acquisition process, including the establishment of the Acquisition, Technology and Logistics Agency (ATLA) in October 2015.

The three countries are already collaborating on F-35 production and maintenance for the Asia-Pacific region, with Australia and Japan both designated as regional Maintenance, Repair, Overhaul, and Upgrade (MRO&U) centers in the Asia-Pacific for the F-35 by DoD. Should Japan win the bid for the *Collins*-class submarine replacement contract in Australia, it will open a new opportunity for the defense industries of the three countries to collaborate on a brand-new platform (since the United States will provide the guidance and weapons systems for the new Australian submarine). Japan and Australia, as close U.S. allies, need to maintain high levels of interoperability with the U.S. military in fiscal environments that are far more constrained than that of the United States. Given the anticipated lack of rapid growth in U.S. defense spending in the near term, it makes sense for the three countries to cooperate further in their defense acquisition to be more fiscally efficient. While it is unrealistic to expect the three countries to institutionalize their defense equipment cooperation at a very high level in the immediate future,

---

[159] Patrick M. Cronin, Ely Ratner, Elbridge Colby, Zachary M. Hosford, and Alexander Sullivan, "Tailored Coercion: Competition and Risk in Maritime Asia," Center for New American Security (CNAS), March 2014. See more at Ken Jimbo, "【東南アジア】南シナ海におけるコスト強要(cost-imposing)戦略 （１） －コスト強要戦略と非対称な均衡 [Southeast Asia Cost Extortion in the South China Sea (Cost-Imposing) Strategy (1)—Cost Extortion Strategy and Asymmetrical Balance]," Tokyo Foundation, October 14, 2014.

there will likely be future opportunities for collaboration on defense industrial development on a case-by-case basis.

Final Thoughts

When then–U.S. Secretary of State Condoleezza Rice and her Japanese and Australian counterparts Taro Aso and John Downer convened for the first trilateral strategic dialogue ministerial meeting in 2006, no one expected that the three countries' partnership would develop beyond an *ad hoc* policy consultation mechanism. Yet, despite initial skepticism, the security partnership among Canberra, Tokyo, and Washington has exceeded expectations and today represents one of the most institutionalized minilateral[160] relationships in the Asia-Pacific region.

As this paper has examined, the accelerated pace with which this trilateral partnership has grown in the last several years can be attributed to the parallel developments in each country's own national security policies, the evolution in the U.S.–Australia and U.S.–Japan alliances and in Japan–Australia relations, and the developments in the regional security environment. Its development as a framework that represents the three countries' commitment to promote and preserve a rule-based international order is particularly noteworthy.[161]

It is also important to take note that U.S.–Japan–Australia trilateral security cooperation does not and in all likelihood will not replace the U.S.–Japan and U.S.–Australia bilateral alliances any time soon, if ever. Rather, the dynamics in the three countries' relationships today are a direct result of the maturity in the U.S.–Japan and U.S.–Australia alliances, as well as the rapid institutionalization of Japan–Australia relations into a "quasi-alliance." In particular, since the Obama administration introduced its "rebalance" strategy directed toward strengthening Asia-Pacific security, the U.S. desire to see a greater role played by its allies and partners, along with Japan and Australia's strong interest in ensuring an enduring U.S. strategic engagement with the region, has worked as a mutually enforcing driver for the trilateral relationship.

Looking to the future, there are some challenges that could prevent U.S.–Japan–Australia trilateral security cooperation from sustaining its current momentum. First, the rapid progress in Japan–Australia relations while Tony Abbott, who called Japan "Australia's closest friend in Asia,"[162] was in office as Australia's prime minister demonstrates that leadership matters. Thus, how to sustain the current momentum over time through the political transitions in three capitals will be a challenge. When Abbott was replaced by Malcolm Turnbull in September 2015, it

---

[160] "Minilateral" in this paper refers to "usually three, but sometimes four or five states meeting and interacting informally (in the absence of a governing document) to discuss issue-areas involving mutual threats to their security or, more often, to go over specific tasks related to building regional stability and order." See William T. Tow, "The Trilateral Strategic Dialogue, Minilateral and Order-Building," in Yuki Tatsumi, ed., *US-Japan-Australia Trilateral Security Cooperation: Prospects and Challenges*, Stimson Center, April 2015, p. 24.

[161] Tow, 2015, pp. 23–35, and Ryo Sahashi, "Australia, United States and Japan in Regional Security Architecture," pp. 91–97, in Tatsumi, 2015.

[162] "Tony Abbott Invites Abe, Saying Japan Is Australia's 'Best Friend in Asia,'" *The Guardian*, October 10, 2013.

sparked some concern in Tokyo and Washington as to whether the new Australian prime minister would continue to support the foreign policy priorities set by his predecessor.

The United States, the anchor of the trilateral relationship, may be distracted. The Obama administration, now in its final year, continues to face multiple major foreign policy challenges, including civil war in Syria, implementation of the nuclear deal reached with Iran, and how to counter the growing influence of Islamic extremist groups aligned with ISIS. The biggest challenge for the United States in its implementation of the Asia-Pacific rebalance has been how to sustain high-level attention to this goal while it continues to face major national security challenges in the Middle East. This challenge will only become more difficult as the United States enters the election season, until the new administration fully staffs its key foreign policy and national security positions sometime in mid- to late 2017. In Japan, even though Prime Minister Abe technically does not have to face an election that could cost him the government until 2018, there is widespread speculation that he may decide to hold an election for the House of Representatives in summer 2016 together with the previously scheduled House of Councilors election, making it at least theoretically possible that he could lose power as soon as mid-2016 (though as of March 2016 he does not appear likely to lose his governing majority).

For the moment, these concerns appear to have dissipated. Malcolm Turnbull visited Tokyo in December 2015 for his first foreign visit as prime minister, despite the suggestion by some that he would postpone the visit to Japan until early 2016.[163] During his visit, Abe and Turnbull confirmed the two countries' united stance toward a variety of security issues, including their opposition to further land reclamation activities and other coercive measures in the South China Sea.[164] Prime Minister Turnbull visited Washington, D.C., on January 19, 2016. During his visit, he and President Obama discussed a range of global and regional security issues, including developments in the South China Sea. While there are questions on whether Australia can continue to sustain the current level of troop contribution to fight against ISIS, Turnbull's visit is considered successful in affirming that Australia's security policy outlook would not dramatically change under his new government. Abe's political standing in Japan seems solid (in part because of the absence of a credible alternative within the ruling Liberal Democratic Party and because the opposition parties are generally held in low regard by the public). And in the United States, despite criticism by some presidential candidates of U.S. allies for "free-riding,"[165] this is certainly not a mainstream view, and broad, bipartisan agreement continues to hold that maintaining robust alliances and partnerships is in the U.S. national interest. Still, no one knows

---

[163] Lenore Taylor, "Malcolm Turnbull's Flying Visit to Japan Includes 'Special Time' with Shinzo Abe," *The Guardian*, December 16, 2015; "Gou Shushou 18-Nichi Hounichi wo Happyou: Chuugoku-Tsuu no Taanburu Shi Nihon wo Yuusen [Australian PM Visits Japan on the 18th: China Hand Turnbell Prioritizes Japan]," *Sankei Shimbun*, December 16, 2015.

[164] "Abe, Turnbull Opposed to South China Sea Buildup," *The Nikkei Asian Review*, December 19, 2015.

[165] See, for example, Van Jackson, "Donald Trump's Asia Policy Would Be a Disaster," *The Diplomat*, September 11, 2015.

how the anticipated leadership changes in the three countries will impact the momentum of this specific trilateral relationship. Above all, the recent moves by China to explicitly militarize its artificial islands in the South China Sea by deploying military assets have heightened the sense of urgency among Washington, Canberra, and Tokyo to continue to focus on shared security concerns.

Secondly, how to expand security cooperation beyond peacetime cooperation is an open question. To be sure, both cooperation in HA/DR and capacity-building in Southeast Asia are important peacetime activities that go a long way toward reassuring the countries of Southeast Asia and carry value because they help these countries to acquire the capacities to contribute more to their own security. Also, building habits of cooperation through these peacetime activities, in addition to maximizing the opportunities for joint exercises and training, is important because it acclimates the bureaucracies and militaries of the three countries to cooperate with one another. Cooperation in defense technology will encourage the three governments to further prioritize interoperability in defense acquisition and procurement. But how much farther can the scope of trilateral defense cooperation, particularly those that involve the three countries' militaries, go beyond what already is happening? A great deal hinges on Japan in this regard. Even with the defense reform in Japan approved by the Diet in September 2015, it is unclear how these changes will translate into expansion of the lists of activities that the JSDF is authorized to undertake in various circumstances. For instance, despite the recent reforms, Japan's constitution still prohibits the three countries from establishing a combined command structure similar to NATO. Even though it is not impossible to imagine that the countries might move in this direction, current legal realities make it extremely difficult for them to address more tangible security challenges jointly.

Finally, the long-term sustainability of not only shared values but also shared threat perceptions will be an enduring challenge. Ensuring shared threat perceptions among trusted allies is challenging enough on a bilateral basis; sustaining this in a trilateral setting is even more challenging. Most notably, should the perception of the challenges that the rise of China represents noticeably diverge among the three nations, it will be difficult to sustain today's momentum. In order for their trilateral relations to sustain momentum, the three countries must pursue a closely coordinated and shared approach to China to send a clear message that, while their cooperation is not meant to contain Beijing, their relationship also stands for certain international norms and values which they expect China to respect and abide by. After all, their security cooperation is anchored by a shared threat perception, even if they strive to achieve positive goals.

8. Conclusion: Strengthening U.S.–Japan Strategic Cooperation

Scott W. Harold, Ph.D.
Political Scientist
RAND Corporation

With the Indo-Asia-Pacific security picture continuing to evolve rapidly in new and sometimes troubling directions, it will be important to sustain and further deepen the combined efforts by the United States and Japan to shape the strategic environment in ways that are stability-enhancing in the years ahead. The essays in this report explore and describe ways that Washington and Tokyo can reinforce the patterns of cooperation and the rules-based order that brought about nearly 40 years of unparalleled development and democratization in the region, transforming it into a global engine of growth. As Tatsumi notes, these actions will necessarily involve individual efforts, steps that require bilateral coordination, and, in some cases, measures that involve cooperation with third parties. The essays in this volume appear to confirm that this general direction is attractive for the two countries' interests and values moving forward. At the same time, a number of questions have arisen recently about where U.S.–Japan strategic cooperation will head in 2016 and beyond. Broadly speaking, these questions stem from domestic developments within both countries, regional receptivity to the two countries' foreign policy initiatives, and the evolving regional and technical threat environments. These are explored briefly in the following paragraphs.

First, a debate has clearly opened up within the United States about the value of alliances and whether the United States should continue to play its historic leading role in regional defense, order-shaping, and trade or whether it should instead shift its focus to prioritize domestic investments, social policy, and restoring the country to an imagined period of past "greatness." Such a sea change in U.S. national security policy, if fully implemented, would represent a substantial break with past practice. It is possible that it might call into question the extent to which Japan would continue to premise its overall national security strategy on cooperation with the United States to balance the rise of China, continue deterring North Korea, tighten collaboration on cybersecurity, assist in the bolstering of Southeast Asian nations, and further coordinate with such regional partners as Australia. While perhaps unlikely, traditional international relations theory would suggest that Tokyo might face a stark choice between confronting regional threats alone or bandwagoning with them, potentially in ways that would come at the expense of U.S. interests. Alternatively, were the United States to remove its extended deterrence guarantee, it is possible that Japan might seek to provide for its own security by revising its constitution, ramping up defense spending, procuring offensive strike capabilities, developing nuclear weapons, and enhancing outreach to other like-minded regional actors. In

either future, change could come rapidly, and the positive habits of cooperation identified by the authors of this report might be left partly or wholly unrealized or abandoned.

A second possibility is that a future Japanese government might decide to deprioritize cooperation with the United States in favor of either a more autonomous foreign policy or one oriented more toward integration into a Chinese-led regional order. While unlikely at present (especially since the 2010 and 2012 Senkaku Islands crises with China that appear to have come as something of a shock to many in Japan who favored a more engagement-heavy approach to managing relations with China), it is not impossible that a future Japanese administration might choose to negotiate with China over territorial disputes while increasing a focus on economic cooperation. Clearly, such an approach would represent a very substantial break with recent practice and thinking, but Japanese economic interests in China and the continuation of a strain of domestic antimilitarism could conceivably bring to power a Prime Minister and Cabinet with very different outlooks than have prevailed since 2010. A crisis in relations with the United States, such as might stem from a criminal incident committed by U.S. military or civilian personnel stationed in Japan or an operational military accident that claimed Japanese lives, could further fuel such a shift. A change in this direction would represent a break on par with that of a major abandonment by the United States of its leading regional role but is not altogether impossible to imagine.

Third, the receptivity to U.S.–Japan collaboration in the region could undergo a dramatic transformation. Indeed, with the 2014 coup in Thailand, the 2015 election in Indonesia, the 2015 leadership turnover in Australia, and the 2016 election in the Philippines, it is conceivable that we have already surpassed "peak rebalance" and may now be in an environment in which regional trends are shifting toward reduced interest in U.S. and Japanese assistance in countering expansive Chinese maritime claims. Political turmoil in Malaysia and the prospect of a possible return to progressive rule in South Korea in late 2017 could further complicate efforts to line up important regional partners behind a program of consistent signaling and strengthening of cooperation on behalf of the existing international order.

On the other hand, numerous regional actors have been moving toward closer collaboration with the U.S. and Japan in recent months, with positive signals coming from South Korea since late 2015, Taiwan in the wake of its January 2016 elections, Vietnam, and Myanmar, among others. In the realm of building partner capacity and tightening defense cooperation relationships with such third parties as ASEAN or Australia, substantial room for further development exists, as the U.S. decision to lift the ban on sales of lethal arms to Vietnam in May 2016 has demonstrated. While Cliff notes that such decisions may be fraught with difficult trade-offs between strategic balancing imperatives and the desire to support and enhance the spread of democratic values, they nonetheless represent areas in which the allies can take meaningful steps to shape the regional environment in ways that could complicate any prospective Chinese effort to dominate Southeast Asia or the South China Sea. As Jimbo points out, Japan's efforts to leverage a public-private partnership approach and offer "strategic ODA" to regional actors in

Southeast Asia is quite attractive to the region; indeed, such assistance may be easier and less politically sensitive for Southeast Asian states to accept from Tokyo than if it came from Washington, given Beijing's penchant for seeking to delegitimate U.S. assistance by characterizing it as reflective of a "containment"-based "Cold War mentality." And as Tatsumi notes, although Canberra opted to select the French bid as its *Collins*-class replacement submarine, there are still substantial reasons to think that the close ties between Japan and Australia are likely to continue developing in a positive direction, in part because the United States is likely to favor and encourage such an approach.

A fourth factor to keep an eye on is the potential for the regional security picture to transform in ways that might reduce or eliminate the logic that undergirds closer U.S.–Japan strategic cooperation. Most obvious in this regard would be a dramatic and, at present, difficult-to-foresee shift in Chinese foreign and security policy practice, away from a "salami-slicing" approach to coercively transforming the regional order without directly employing armed force. Whether such a change could occur in the absence of a fundamental transformation of China's one-party communist regime is unclear. At a minimum, China's decision to abandon its decade-long "charm offensive" from 1998 to 2008 suggests that the United States and Japan would have reason to sustain their cooperation until clear, unambiguous, and difficult-to-reverse signs of Chinese commitment to a new approach to regional cooperation emerge. Still, the Chinese government has undertaken substantial revisions to its foreign policy strategy in the past to address regional concerns over China's rise, and it is at least theoretically possible that Beijing might shift tactics (or even goals and strategy) again in the future.

Still, even if the threat that the United States and Japan perceive from China were to abate, the allies might nonetheless continue to cooperate until the regional challenges posed by North Korea and Russia also decline or disappear entirely. And even if all three revisionist actors were to transform into satisfied, system-oriented status quo powers, there might still be a case made in Washington and Tokyo that the very success of the allies' collaborative efforts had helped accomplish important goals, such as ensuring deterrence, stability, economic development, and regional democratization, and that these efforts should therefore continue because they support positive outcomes and should not be assessed exclusively on their value for achieving deterrence. For example, it is plausible to imagine that the stability and democracy-enhancing approach to building partner capacity in Southeast Asia that Cliff identifies would remain attractive to the United States, Japan, and ASEAN partner states even if perceived regional threats reduced in urgency. Similarly, the United States, Japan, and Australia would likely continue to deepen their collaboration on the basis of shared values and a common vision of good global order, as Tatsumi describes.

Finally, in the realm of technology, U.S.–Japan cooperation appears likely to deepen for years to come, irrespective of political change in Washington or Tokyo and quite apart from any regional developments. In part, this is because, in addition to threats that stem from state actors with advanced technical capabilities, such nonstate actors as terrorist groups and transnational

criminal actors will continue to have the capacity to brandish or use cyber capabilities to inflict harm on American and Japanese national interests. In some cases, as Libicki and Tsuchiya note with respect to cybersecurity, the bulk of the efforts to ensure the online health of the alliance may need to be taken by Japan investing more in its own cyberdefenses. There may, as the two authors note, be some room for bilateral cooperation in the realm of information-sharing and capacity-building, as well as in exercising specifically military-oriented forms of cyberdefense. In other cases, however, it might be better to focus less on bilateral information-sharing and more on approaches that broadly publicize threat vector information, a framework derived from a more public health-based model, as Libicki and Ito note.

In conclusion, domestic priorities, regional receptivity, a changing threat environment, and the continuing challenges of providing security in a rapidly evolving online cyber domain will shape the future sustainability and scale of strategic cooperation between the United States and Japan. While the shape, breadth, and depth of such collaboration are uncertain at present, the investments of the two sides to date in deeper diplomatic, economic, military, and people-to-people ties and the dividends these have already paid suggest that the ongoing evolution of the relationship between the United States and Japan is likely to be an important continuing component of both countries' national security strategies.

References

"Abe, Turnbull Opposed to South China Sea Buildup," *The Nikkei Asian Review*, December 19, 2015. As of January 6, 2016: http://asia.nikkei.com/Politics-Economy/International-Relations/Abe-Turnbull-affirm-opposition-to-South-China-Sea-buildup

Abuza, Zachary, "The Southern Thailand Insurgency in the Wake of the March 2012 Bombings," *CTC Sentinel*, June 21, 2012.

Amer, Ramses, and Nguyen Hong Thao, "Regional Conflict Management: Challenges of the Border Disputes of Cambodia, Laos, and Vietnam," *Austrian Journal of South-East Asian Studies*, Vol. 2, No. 2, 2009, pp. 53–80.

Anderson, Robert H., and Anthony C. Hearn, *An Exploration of Cyberspace Security R&D Investment Strategies for DARPA: "The Day After . . . in Cyberspace II,"* Santa Monica, Calif.: RAND Corporation, MR-797-DARPA, 1996. As of August 23, 2016: http://www.rand.org/pubs/monograph_reports/MR797.html

Anderson, Ross, "Why Cryptosystems Fail," presented at the 1993 Association for Computing Machinery Computer and Communications Security Conference. As of August 23, 2016: www.cl.cam.ac.uk/~rja14/Papers/wcf.pdf

ASEAN Regional Forum—Disaster Relief Mapping Service, home page, undated. As of January 5, 2016: http://www.arf-drms.com/geoportal/catalog/main/home.page

Association of Southeast Asian Nations, "Declaration on the Conduct of Parties in the South China Sea," October 17, 2012. As of February 26, 2016: http://www.asean.org/?static_post=declaration-on-the-conduct-of-parties-in-the-south-china-sea-2

Austin, Greg, "Who Is the Biggest Aggressor in the South China Sea?" *The Diplomat*, June 18, 2015.

Australia-Japan-United States Trilateral Leaders Meeting, "Joint Media Release," November 16, 2014. As of January 31, 2015: http://www.mofa.go.jp/mofaj/files/000059829.pdf

Australian Army Headquarters, "Exercise Southern Jackaroo Wraps Up," May 30, 2016. As of June 5, 2016: https://www.youtube.com/watch?v=or9LVVrsqQk

Australian Department of Defence, "Defence White Paper 2013," 2013 As of December 18, 2015: http://www.defence.gov.au/whitepaper/2013/docs/WP_2013_web.pdf

Australian Department of Defence, *Defence White Paper 2016*, 2016. As of February 29, 2016: http://www.defence.gov.au/whitepaper/Docs/2016-Defence-White-Paper.pdf

Australian Department of Defence and U.S. Department of Defense, "Statement on Defense Cooperation in the 21st Century," undated. As of August 23, 2016: http://www.defense.gov/Portals/1/Documents/pubs/2015_AUSMIN_Joint_Defense_Statement.pdf

Axelrod, Robert, and Robert Keohane, "Achieving Cooperation Under Anarchy," *World Politics*, Vol. 38, No. 1, October 1985, pp. 226–254.

Beech, Hannah, "What Indonesia Can Teach the World About Counterterrorism," *Time*, June 7, 2010.

Benson, Jeff W., Lt. Cmdr., USN, "South China Sea: A History of Armed Conflict," *USNI News*, June 20, 2012. As of February 26, 2016: http://news.usni.org/2012/06/20/south-china-sea-history-armed-conflict

Bergenas, Johan, and Richard Sabatini, "Japan Takes the Lead in Coordinating Security and Development Aid," *World Politics Review*, August 1, 2012. As of August 23, 2016: http://www.worldpoliticsreview.com/articles/12220/japan-takes-the-lead-in-coordinating-security-and-development-aid

Bumiller, Elisabeth, and Thomas Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.," *New York Times*, October 11, 2012. As of August 23, 2016: http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html

Burgess, Joe, "Territorial Claims in South China Sea," *New York Times*, May 31, 2012. As of February 25, 2016: http://www.nytimes.com/interactive/2012/05/31/world/asia/Territorial-Claims-in-South-China-Sea.html

Cabinet Secretariat of Japan, "National Security Strategy" (provisional translation, English version), December 17, 2013. As of August 23, 2016: http://www.cas.go.jp/jp/siryou/131217anzenhoshou/nss-e.pdf

Carden, Michael J., Army Sgt. 1st Class, "Trainers, Advisors Help Philippines Fight Terrorism," American Forces Press Service, February 22, 2010. As of February 17, 2016: http://archive.defense.gov/news/newsarticle.aspx?id=58031

Charney, Scott, "Collective Defense: Applying Public Health Models to the Internet," Microsoft, 2010.

"China-Philippines Navy Spat Captured on Camera," *BBC News*, March 30, 2014. As of February 26, 2016: http://www.bbc.com/news/world-asia-26806924

Coclanis, Peter A., "Terror in Burma: Buddhists vs. Muslims," *World Affairs*, November/December 2013.

Cronin, Patrick M., Ely Ratner, Elbridge Colby, Zachary M. Hosford, and Alexander Sullivan, "Tailored Coercion: Competition and Risk in Maritime Asia," Center for New American Security, March 2014. As of August 23, 2016: http://www.cnas.org/sites/default/files/publications-pdf/CNAS_TailoredCoercion_report.pdf

Cronin, Richard, and Zachary Dubel, "Maritime Security in East Asia: Boundary Disputes, Resources, and the Future of Regional Stability," Stimson Center, February 2013. As of February 25, 2016: http://www.stimson.org/images/uploads/research-pdfs/MARITIME_TERRITORIAL_DISPUTES_AND_EAST_ASIA_2.pdf

Cunningham, Susan, "Bangkok Shrine Bombing—Case (Pretty Much) Closed," *Forbes*, December 23, 2015.

CyberGreen, "Tracking the State of Global Cyber Health," 2016. As of August 23, 2016: http://stats.cybergreen.net

Davis II, John S., Martin C. Libicki, Stuart E. Johnson, Jason Kumar, Michael Watson, and Andrew Karode, *A Framework for Programming and Budgeting for Cybersecurity*, Santa Monica, Calif.: RAND Corporation, TL-186-DHS, 2016. As of August 23, 2016: http://www.rand.org/pubs/tools/TL186.html

De Castro, Renato Cruz, and Walter Lohman, "Getting the Philippines Air Force Flying Again: The Role of the U.S.-Philippines Alliance," *Backgrounder*, The Heritage Foundation, September 24, 2012. As of August 23, 2016: http://www.heritage.org/research/reports/2012/09/getting-the-philippines-air-force-flying-again-the-role-of-the-us-philippines-alliance

Defense News, "Top 100 for 2015," undated. As of August 23, 2016: http://people.defensenews.com/top-100/

Department of Transportation and Commerce, Republic of the Philippines, "Japanese Firm to Build Ten 40-Meter Vessels for Philippine Coast Guard—DOTC," press release, 2014. As of February 26, 2016: http://www.dotc.gov.ph/index.php/2014-09-02-05-01-41/2014-09-03-06-43-32/123-japanese-firm-to-build-ten-40-meter-vessels-for-philippine-coast-guard-dotc

Djuli, M. Nur, "To Improve Peace Process in Aceh, Return to Sanity," *Jakarta Post*, August 24, 2015.

Dong, Manh, "Maritime Delimitation Between Vietnam and Her Neighboring Countries," presentation to UN-Nippon Foundation Alumni Meeting, April 13–16, 2009. As of February 25, 2016: http://www.un.org/depts/los/nippon/unnff_programme_home/alumni/tokyo_alumni_presents_files/alum_tokyo_dong.pdf

Envall, H. D. P., "Community Building in Asia? Trilateral Cooperation in Humanitarian Assistance and Disaster Relief," in Yuki Tatsumi, ed., *US-Japan-Australia Security Cooperation: Prospects and Challenges*, Stimson Center, April 2015, pp. 51–59.

Federal Bureau of Investigation, "Operation Ghost Click: International Cyber Risk That Infected Millions of Computers Dismantled," November 9, 2011.

Gartner, "Gartner Says Worldwide Information Security Spending Will Grow Almost 4.7 Percent to Reach $75.4 Billion in 2015," September 23, 2015. As of August 23, 2016: http://www.gartner.com/newsroom/id/3135617

Gates, Robert, "Helping Others Defend Themselves: The Future of Military Assistance," *Foreign Affairs*, May/June 2010.

"Gathering Sulu Forces in Philippines Worrying Malaysia, Report Says," *Malay Mail Online*, May 28, 2015. As of February 25, 2016: http://www.themalaymailonline.com/malaysia/article/gathering-sulu-forces-in-philippines-worrying-malaysia-report-says

Geer, Dan, "Measuring Security," presentation, 2007. As of August 23, 2016: all.net/Metricon/measuringsecurity.tutorial.pdf

Gemba, Koichiro, Foreign Minister, "Japan's Efforts in the Global Agenda-Implementing 'Full-Cast Diplomacy' and Expanding the Frontiers of International Cooperation," speech delivered at the National Graduate Institute for Policy Studies, February 18, 2012.

Giles, Martin, "Defending the Digital Frontier," *The Economist*, July 12, 2014. As of August 23, 2016: http://www.economist.com/news/special-report/21606416-companies-markets-and-countries-are-increasingly-under-attack-cyber-criminals

"Gou Shushou 18-Nichi Hounichi wo Happyou: Chuugoku-Tsuu no Taanburu Shi Nihon wo Yuusen [Australian PM Visits Japan on the 18th: China Hand Turnbell Prioritizes Japan]," *Sankei Shimbun*, December 16, 2015. As of January 8, 2016: http://www.sankei.com/world/news/151216/wor1512160023-n1.html

Government of the Philippines, "Agreement Between the Government of the Republic of Philippines and the Government of the United States of America on Enhanced Defense Cooperation," *Official Gazette*, April 29, 2014. As of August 23, 2016: http://www.gov.ph/2014/04/29/document-enhanced-defense-cooperation-agreement/

Graham, Euan, "Maritime Security and Capacity-Building: The Australia-Japan Dimension," in William Tow and Tomonori Yoshizaki, eds., *Beyond the Hub and Spokes: Australia-Japan Security Cooperation*, Tokyo: The National Institute for Defense Studies, 2014, pp. 43–57

Greg's Cable Map, home page, 2016. As of August 23, 2016: http://www.cablemap.info

Hanashi, Yuka, and Chieko Tsuneoka. "Japan Open to Joining U.S. in South China Sea Patrols," *Wall Street Journal*, June 25, 2015. As of February 29, 2016: http://www.wsj.com/articles/japan-may-join-u-s-in-south-china-sea-patrols-1435149493

Honda, Tomoaki, "Boeisho Jieitai Niyoru Hidentoteki Anzenhosho Bunya no Noryoku Kochiku Shien" [Ministry of Defense and Self-Defense Force's Capacity Building in the Non-Traditional Security], *Senryaku Kenkyu* [Strategy Studies], Vol. 15, 2015.

House of Representatives, "サイバーセキュリティ基本法案 [Cyber Security Basic Bill]," 2014. As of August 23, 2016: http://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/honbun/houan/g18601035.htm

"Hun Sen Asks Western Leaders to Help Resolve Cambodia's Border Disputes," *Radio Free Asia*, July 15, 2015. As of February 25, 2016: http://www.rfa.org/english/news/cambodia/hun-sen-asks-western-leaders-to-help-resolve-border-disputes-07152015160828.html

International Crisis Group, "The Communist Insurgency in the Philippines: Tactics and Talks," Asia Report No. 202, February 14, 2011.

International Crisis Group, "How Indonesian Extremists Regroup," July 16, 2012a.

International Crisis Group, "Indonesia: Dynamics of Violence in Papua," Asia Report No. 232, August 9, 2012b.

Ito, Yurie, "Managing Global Cyber Health and Security Through Risk Reduction," thesis, Medford, Mass.: Fletcher School of Law and Diplomacy, Tufts University, July 18, 2011.

Jackson, Van, "Donald Trump's Asia Policy Would Be a Disaster," *The Diplomat*, September 11, 2015. As of January 12, 2016: http://thediplomat.com/2015/09/donald-trumps-asia-policy-would-be-a-disaster/

"Japan Gives Vietnam 2 Ships to Beef up Maritime Security," *Stars and Stripes*, November 4, 2015. As of February 26, 2016:

http://www.stripes.com/news/japan-gives-vietnam-2-ships-to-beef-up-maritime-security-1.376884

Japan International Cooperation Agency, "Maritime Safety Capability Improvement Project for the Philippine Coast Guard," in *Ex-Ante Evaluation (for Japanese ODA Loan)*, December 14, 2013. As of August 23, 2016: http://www.jica.go.jp/english/our_work/evaluation/oda_loan/economic_cooperation/c8h0vm000001rdjt-att/philippines_131214_01.pdf

"Japan to Step Up Help for Vietnamese Maritime Security," Associated Press, September 15, 2015. As of February 29, 2016: http://www.thejakartapost.com/news/2015/09/15/japan-step-help-vietnamese-maritime-security.html

Jennings, Peter, "The U.S. Rebalance to the Asia-Pacific: An Australian Perspective," *Asia Policy*, No. 15, January 2013, p. 38. As of December 1, 2015: http://www.nbr.org/publications/asia_policy/free/AP15/AP15_B_Asia_balanceRt.pdf

Jimbo, Ken, "Japan Should Build ASEAN's Security Capacity," *AJISS-Commentary*, May 30, 2012. As of August 23, 2016: http://www2.jiia.or.jp/en_commentary/201205/30-1.html

Jimbo, Ken, "【東南アジア】南シナ海におけるコスト強要(cost-imposing)戦略 （１） －コスト強要戦略と非対称な均衡 [Southeast Asia Cost Extortion in the South China Sea (Cost-Imposing) Strategy (1)—Cost Extortion Strategy and Asymmetrical Balance]," Tokyo Foundation, October 14, 2014. As of February 2, 2015: http://www.tkfd.or.jp/research/project/news.php?id=1349#sthash.HSRS5os1.dpuf

Jimbo, Ken, "Japan-US-Australia Cooperation in Capacity-Building in Southeast Asia," in Yuki Tatsumi, ed., *US-Japan-Australia Security Cooperation: Prospects and Challenges*, Stimson Center, April 2015, pp. 61–75.

John, Tara, "Indonesia's Long Battle With Islamic Extremism Could Be About to Get Tougher," *Time*, January 14, 2016.

Joint Statement of the U.S.–Japan Cyber Defense Policy Working Group, May 30, 2015. As of August 23, 2016: http://www.mod.go.jp/j/press/news/2015/05/30a_1.pdf

"Kaiji-ki Hi-Kaigun ni Taiyo-he: Minami Shina-kai no Kanshi ni Riyou [Japan to Loan JMSDF Aircraft to Filipino Navy: To Be Used for South China Sea Surveillance]," *Yomiuri Shimbun*, February 29, 2016. As of February 29, 2016: http://www.yomiuri.co.jp/politics/20160228-OYT1T50110.html?from=ytop_ylist

Kishida, Fumio, Minister for Foreign Affairs, Minister of Defense Gen Nakatani, Secretary of State John Kerry, and Secretary of Defense Ashton Carter, *Joint Statement of the Security Consultative Committee: A Stronger Alliance for Dynamic Security Environment*, April 27, 2015. As of December 3, 2015: http://www.mod.go.jp/e/d_act/anpo/pdf/js20150427e.pdf

Lam Peng Er, ed., *Japan's Relations with Southeast Asia: The Fukuda Doctrine and Beyond*, New York: Routledge, 2013.

Lum, Thomas, "The Republic of the Philippines and U.S. Interests," *CRS Report for Congress*, April 5, 2012.

"Malaysia Steps Up Security to Counter Terror Threat," *DW*, January 21, 2016. As of February 23, 2016: http://www.dw.com/en/malaysia-steps-up-security-to-counter-terror-threat/a-18996395

Markets and Markets, "Cyber Security Market Worth $170.21 Billion by 2020," news release, undated. As of August 23, 2016: http://www.marketsandmarkets.com/PressReleases/cyber-security.asp

Marks, Joseph, "White House Cyber Czar: Even Non-Critical Infrastructure Vulnerable—Top Sony Corp. Exec Condemns Hack at CES," *Politico*, January 6, 2015. As of August 23, 2016: http://www.politico.com/tipsheets/morning-cybersecurity/2015/01/white-house-cyber-czar-even-non-critical-infrastructure-vulnerable-top-sony-corp-exec-condemns-hack-at-ces-212543

Mehta, Aaron, "Carter Announces $425M In Pacific Partnership Funding," *Defense News*, May 30, 2015.

Ministry of Defense of Japan, "Capacity Building Assistance," undated(a). As of August 23, 2016: http://www.mod.go.jp/e/d_act/exc/cap_build.html

Ministry of Defense of Japan, "Past Programs," undated(b). As of February 5, 2016: http://www.mod.go.jp/e/d_act/exc/cap_b/Past_programs.html

Ministry of Defense of Japan, *National Defense Program Guidelines for FY2011 and Beyond*, December 17, 2010. As of August 23, 2016: http://www.mod.go.jp/e/d_act/d_policy/pdf/guidelinesFY2011.pdf

Ministry of Defense of Japan, *Joint Statement of the Security Consultative Committee: Toward a More Robust Alliance and Greater Shared Responsibilities*, October 3, 2013a. As of December 3, 2015: http://www.mod.go.jp/e/d_act/us/JointStatement2013.pdf

Ministry of Defense of Japan, "National Defense Program Guidelines and Mid-Term Defense Program," December 17, 2013b. As of August 23, 2016: http://www.mod.go.jp/e/d_act/d_policy/national.html

Ministry of Defense of Japan, *National Defense Program Guidelines for FY 2014 and Beyond*, December 17, 2013c. As of January 9, 2016: http://www.mod.go.jp/j/approach/agenda/guideline/2014/pdf/20131217_e2.pdf

Ministry of Defense of Japan, "5th Japan-Australia 2+2 Foreign and Defense Ministerial Consultations," June 11, 2014. As of December 26, 2014: http://www.mod.go.jp/j/press/youjin/2014/06/11a_jpr_e.pdf

Ministry of Defense of Japan, *The Guidelines for Japan-U.S. Defense Cooperation*, April 27, 2015. As of February 5, 2016: http://www.mod.go.jp/e/d_act/anpo/shishin_20150427e.html

Ministry of Foreign Affairs of Japan, *Japan-U.S. Joint Declaration on Security: Alliance for the 21st Century*, April 17, 1996. As of December 10, 2015: http://www.mofa.go.jp/region/n-america/us/security/security.html

Ministry of Foreign Affairs of Japan, "Provision of Patrol Vessels to Indonesia," *Official Development Assistance White Paper 2006*, December 2006. As of August 23, 2016: http://www.mofa.go.jp/policy/oda/white/2006/ODA2006/html/honpen/hp202040400.htm

Ministry of Foreign Affairs of Japan, "Japan's Policies on the Control of Arms Exports," 2014a. As of August 23, 2016: http://www.mofa.go.jp/policy/un/disarmament/policy/

Ministry of Foreign Affairs of Japan, "The Three Principles on Transfer of Defense Equipment and Technology," April 1, 2014b. As of August 23, 2016: http://www.mofa.go.jp/press/release/press22e_000010.html

Ministry of Foreign Affairs of Japan, "U.S.-Japan Joint Vision Statement," April 28, 2015, As of August 23, 2016: http://www.mofa.go.jp/na/na1/us/page3e_000332.html

Najib, Najiah, "Lahad Datu Invasion: A Painful Memory of 2013," *Astro Awani*, December 30, 2013.

National Institute for Defense Studies, *East Asian Strategic Review*, May 2013. As of August 23, 2016: http://www.nids.go.jp/english/publication/east-asian/pdf/2013/east-asian_e2013_03.pdf

New York Times Editorial Board, "The Philippines' Insurgency Crisis," *New York Times*, August 1, 2014. As of February 17, 2016: http://www.nytimes.com/2014/08/02/opinion/the-philippines-insurgency-crisis.html

NHK, “NHK Special: CYBER SHOCK,” February 7, 2016.

Nixon, Richard, “Address to the Nation on the War in Vietnam,” Nixon Library, November 3, 1969. As of August 23, 2016: http://www.nixonlibrary.gov/forkids/speechesforkids/silentmajority/silentmajority_transcript.pdf

Oceans Beyond Piracy, *The State of Maritime Piracy 2014: Assessing the Economic and Human Cost*, Denver, Colo.: One Earth Future Foundation, 2014.

OECD Working Party on Security and Privacy in the Digital Economy, “Guidance for Improving the Comparability of Statistics Produced by Computer Security Incident Response Teams (CSIRTs),” June 8, 2015. As of August 23, 2016: https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2013)9/FINAL&doclanguage=en

Pajon, Celine, “Japan and the South China Sea: Forging Strategic Partnerships in a Divided Region,” *Asie Visions 60*, Center for Asian Studies, IFRI, January 2013. As of August 23, 2016: http://www.ifri.org/sites/default/files/atoms/files/asievisions60celinepajon.pdf

Panetta, Leon, “The U.S. Rebalance Towards the Asia-Pacific” transcript of speech at the Shangri-La Dialogue IISS Asia Security Summit, June 2, 2012. As of August 23, 2016: http://www.iiss.org/en/events/shangri%20la%20dialogue/archive/sld12-43d9/first-plenary-session-2749/leon-panetta-d67b

Parameswaran, Prashanth, “Philippine Peace Deal Suffers Another Blow,” *The Diplomat*, June 12, 2015.

Pitsuwan, Surin, “Fukuda Doctrine: Impact and Implications on Japan-ASEAN Relations,” in Lam, 2013, pp. 163–172.

Popham, Peter, “Burma's ‘Great Terror’ Moves a Step Closer as Taliban Urges Rohingya To ‘Take Up the Sword,’” *Independent*, June 14, 2015.

Prabang, Luang, “Lao Border Talks Progressing,” *The Nation* (Thailand), March 8, 2007.

Prime Minister of Japan and His Cabinet, “‘Japan Is Back’: Policy Speech by Prime Minister Shinzo Abe at the Center for Strategic and International Studies,” February 22, 2013a. As of January 2, 2016: http://japan.kantei.go.jp/96_abe/statement/201302/22speech_e.html

Prime Minister of Japan and His Cabinet, *National Security Strategy*, December 17, 2013b. As of January 2, 2016: http://www.cas.go.jp/jp/siryou/131217anzenhoshou/nss-e.pdf

"Q&A: Thailand-Cambodia temple dispute," *BBC News*, November 7, 2013. As of February 24, 2016:
http://www.bbc.com/news/world-asia-pacific-12378001

Ratner, Ely, "Learning the Lessons of Scarborough Reef," *The National Interest*, November 21, 2013.

Rattray, Gregory, Chris Evans, and Jason Healey, "Chapter 5: American Security in the Cyber Commons," in Abraham M. Denmark and James Mulvenon, eds., *Contested Commons: The Future of American Power in a Multipolar World*, Center for a New American Security, 2010, pp. 139–176.

Rauscher, Karl Frederick, "The Internet Health Model for Cybersecurity," East-West Institute, June 2, 2012. As of August 23, 2016:
https://www.eastwest.ngo/idea/internet-health-model-cybersecurity

Raymond, Greg, "Thai–Cambodia Relations One Year After the ICJ Judgement," *East Asia Forum*, November 11, 2014.

Roach, J. Ashley, "Malaysia and Brunei: An Analysis of Their Claims in the South China Sea," CNA Occasional Paper, August 2014. As of February 26, 2016:
https://www.cna.org/CNA_files/PDF/IOP-2014-U-008434.pdf

Rousseau, Jean-Jacques, *A Discourse on Inequality*, 1755.

Russell, Daniel R., "Remarks on the U.S.-Asia Rebalance and Priorities," U.S. Department of State, January 27, 2015. As of May 27, 2015:
http://www.state.gov/p/eap/rls/rm/2015/01/236764.htm

Sahashi, Ryo, "Australia, United States and Japan in Regional Security Architecture," pp. 91–97, in Yuki Tatsumi, ed., *US-Japan-Australia Trilateral Security Cooperation: Prospects and Challenges*, Stimson Center, April 2015. As of August 23, 2016:
http://www.stimson.org/images/uploads/research-pdfs/US-Japan_Australia-WEB.pdf

Satake, Tomohiko, "The Origin of Trilateralism? The US-Japan-Australia Trilateral Relations in the 1990s," *International Relations of the Asia-Pacific Region*, Vol. 11, 2010, pp. 87–114.

Satake, Tomohiko, "Japan-Australia Relations: Towards Regional Order-Building," in Yuki Tatsumi, ed., *Japan's Global Diplomacy: Views from the Next Generation*, Stimson Center, March 2015, pp. 21–31. As of January 5, 2016:
http://www.stimson.org/images/uploads/research-pdfs/Japans-Global-Diplomacy-WEB.pdf

Schelling, Thomas, "An Essay on Bargaining," *American Economic Review*, Vol. 46, No. 3, June 1956, pp. 281–306.

Schmitt, Michael N., ed., *The Tallinn Manual on the International Law Applicable to Cyber Warfare*, New York: Cambridge University Press, 2013, Rule 30.

Sjolin, Sara, "Forget Somalia—This Is the New Sea Piracy Hot Spot," *MarketWatch*, October 7, 2015.

Skyrms, Brian, *The Stag Hunt and the Evolution of Social Structure*, Cambridge, UK: Cambridge University Press, 2003.

Snow, Gordon M., Assistant Director, Cyber Division, Federal Bureau of Investigation, "Statement Before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit," Washington, D.C., September 14, 2011. As of August 23, 2016:
https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector

Symantec, *2015 Internet Security Threat Report*, Volume 20, 2015.

Tatsumi, Yuki, ed., *US-Japan-Australia Security Cooperation: Prospects and Challenges*, Stimson Center, 2015, p. 18. As of December 20, 2015:
http://www.stimson.org/images/uploads/research-pdfs/US-Japan_Australia-WEB.pdf

Taylor, Lenore, "Malcolm Turnbull's Flying Visit to Japan Includes 'Special Time' with Shinzo Abe," *The Guardian*, December 16, 2015. As of January 8, 2016:
http://www.theguardian.com/australia-news/2015/dec/16/malcolm-turnbulls-flying-visit-to-japan-to-include-special-time-with-shinzo-abe

"Thailand Explosion: Seven Injured in Koh Samui," *BBC News*, April 11, 2015. As of February 22, 2016:
http://www.bbc.com/news/world-asia-32259612

Timberman, David, "Violent Extremism and Insurgency in Indonesia: A Risk Assessment," Washington, D.C.: Management Systems International, January 7, 2013.

"Tony Abbott Invites Abe, Saying Japan Is Australia's 'Best Friend in Asia,'" *The Guardian*, October 10, 2013. As of January 5, 2016:
http://www.theguardian.com/world/2013/oct/10/aboott-invites-abe-japan-friend

Tow, William T., "The Trilateral Strategic Dialogue, Minilateral and Order-Building," in Yuki Tatsumi, ed., *US-Japan-Australia Trilateral Security Cooperation: Prospects and Challenges*, Stimson Center, April 2015, p. 24. As of August 23, 2016:
http://www.stimson.org/images/uploads/research-pdfs/US-Japan_Australia-WEB.pdf

U.S. Department of Defense, *Quadrennial Defense Review Report*, February 2010. As of August 23, 2016:
http://www.defense.gov/qdr/qdr%20as%20of%2029jan10%201600.pdf

U.S. Department of Defense, "Transcript of the Press Conference: Defense Strategic Guidance from Pentagon," January 5, 2012. As of August 23, 2016: http://www.defense.gov/transcripts/transcript.aspx?transcriptid=4953

U.S. Department of Defense, "Secretary of Defense Speech: Remarks on the Next Phase of the U.S. Rebalance to the Asia-Pacific," April 6, 2015a. As of December 10, 2015: http://www.defense.gov/News/Speeches/Speech-View/Article/606660/remarks-on-the-next-phase-of-the-us-rebalance-to-the-asia-pacific-mccain-instit

U.S. Department of Defense, "ISIS Shangri-La Dialogue: 'A Regional Security Architecture Where Everyone Rises,'" May 30, 2015b. As of January 10, 2016: http://www.defense.gov/News/Speeches/Speech-View/Article/606676/iiss-shangri-la-dialogue-a-regional-security-architecture-where-everyone-rises

U.S. Department of Defense, *Asia-Pacific Maritime Security Strategy*, July 2015c. As of February 26, 2016: http://www.defense.gov/Portals/1/Documents/pubs/NDAA%20A-P_Maritime_SecuritY_Strategy-08142015-1300-FINALFORMAT.PDF

U.S. Department of Defense, *Asia-Pacific Maritime Security Strategy*, August 14, 2015d. As of August 23, 2016: http://www.defense.gov/Portals/1/Documents/pubs/NDAA%20A-P_Maritime_SecuritY_Strategy-08142015-1300-FINALFORMAT.PDF

U.S. Department of Defense, "Secretary of Defense Speech: Remarks at ASEAN Defense Ministers' Meeting-Plus (ADMM-Plus)," November 4, 2015e. As of December 10, 2015: http://www.defense.gov/News/Speeches/Speech-View/Article/628351/remarks-at-the-asean-defense-ministers-meeting-plus-admm-plus

U.S. Department of Homeland Security, "Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action," March 2011.

U.S. Department of State, "Country Reports on Human Rights Practices for 2014: Burma," undated(a). As of February 22, 2016: http://www.state.gov/j/drl/rls/hrrpt/humanrightsreport/index.htm#wrapper

U.S. Department of State, "Country Reports on Human Rights Practices for 2014: Indonesia," undated(b). As of February 17, 2016: http://www.state.gov/j/drl/rls/hrrpt/humanrightsreport/index.htm#wrapper

U.S. Department of State, "Country Reports on Human Rights Practices for 2014: Thailand," undated(c). As of February 22, 2016: http://www.state.gov/j/drl/rls/hrrpt/humanrightsreport/index.htm#wrapper

U.S. Department of State, "Country Reports on Terrorism 2014," undated(d). As of February 22, 2016:
http://www.state.gov/j/ct/rls/crt/2014/index.htm

U.S. Department of State, "Australia–United States Ministerial Consultation (AUSMIN)," November 20, 2013a. As of December 2, 2015:
http://www.state.gov/r/pa/prs/ps/2013/11/217794.htm

U.S. Department of State, "Expanded U.S. Assistance for Maritime Capacity Building," December 16, 2013b. As of August 23, 2016:
http://www.state.gov/r/pa/prs/ps/2013/218735.htm

U.S. Department of State, "Joint Communique AUSMIN 2014," August 12, 2014. As of December 3, 2015:
http://www.state.gov/r/pa/prs/ps/2014/230524.htm

U.S. Department of State, "Joint Statement of the Security Consultative Committee: A Stronger Alliance for a Dynamic Security Environment—The New Guidelines for U.S.-Japan Defense Cooperation," April 27, 2015. As of August 23, 2016:
http://www.state.gov/r/pa/prs/ps/2015/04/241125.htm

U.S. Department of State, Bureau of Democracy, Human Rights, and Labor, "Country Reports on Human Rights Practices for 2014: Philippines," undated. As of February 17, 2016:
http://www.state.gov/j/drl/rls/hrrpt/humanrightsreport/index.htm?year=2015&dlid=252793

U.S. Department of State, Office of the Spokesman, "Global Security Contingency Fund Program for the Philippines," December 17, 2013. As of August 23, 2016:
http://www.state.gov/r/pa/prs/ps/2013/218823.htm

"U.S.-Funded Detachment 88, Elite of Indonesia Security," Reuters, March 18, 2010. As of February 19, 2016:
http://www.reuters.com/article/us-indonesia-usa-security-idUSTRE62H13F20100318

U.S. Marine Corps, "Dawn Blitz 2015," undated. As of December 21, 2015:
http://www.imef.marines.mil/Units/1STMEB/DawnBlitz2015/units.aspx

U.S. Navy, U.S. Marine Corps, and U.S. Coast Guard, "A Cooperative Strategy for 21st Century Seapower," October 2007. As of August 23, 2016:
http://www.navy.mil/maritime/MaritimeStrategy.pdf

United Nations, *United Nations Convention on the Law of the Sea*, undated. As of February 25, 2016:
http://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

United States Embassy, Manila, "Co-Chair's Statement of the Philippines-United States Bilateral Strategic Dialogue," January 27–28, 2011.

Wallace, Corey J., "Japan's Strategic Pivot South: Diversifying the Dual Hedge," *International Relations of the Asia-Pacific*, Vol. 13, No. 3, 2013, pp. 479–517.

White House, Office of the Press Secretary, "Australia-Japan-United States Trilateral Leaders Meeting Joint Media Release," November 16, 2014. As of January 4, 2016: http://www.whitehouse.gov/the-press-office/2014/11/15/australia-japan-united-states-trilateral-leaders-meeting-joint-media-rel

White House, Office of the Press Secretary, "Fact Sheet: U.S. Building Maritime Capacity in Southeast Asia," November 17, 2015. As of April 13, 2016: https://www.whitehouse.gov/the-press-office/2015/11/17/fact-sheet-us-building-maritime-capacity-southeast-asia

White, Hugh, *The China Choice: Why America Should Share Power*, Melbourne, Australia: Black Inc., 2012.

World Health Organization, "WHO Indicator Registry," 2016. As of August 23, 2016: http://www.who.int/gho/indicator_registry/en/