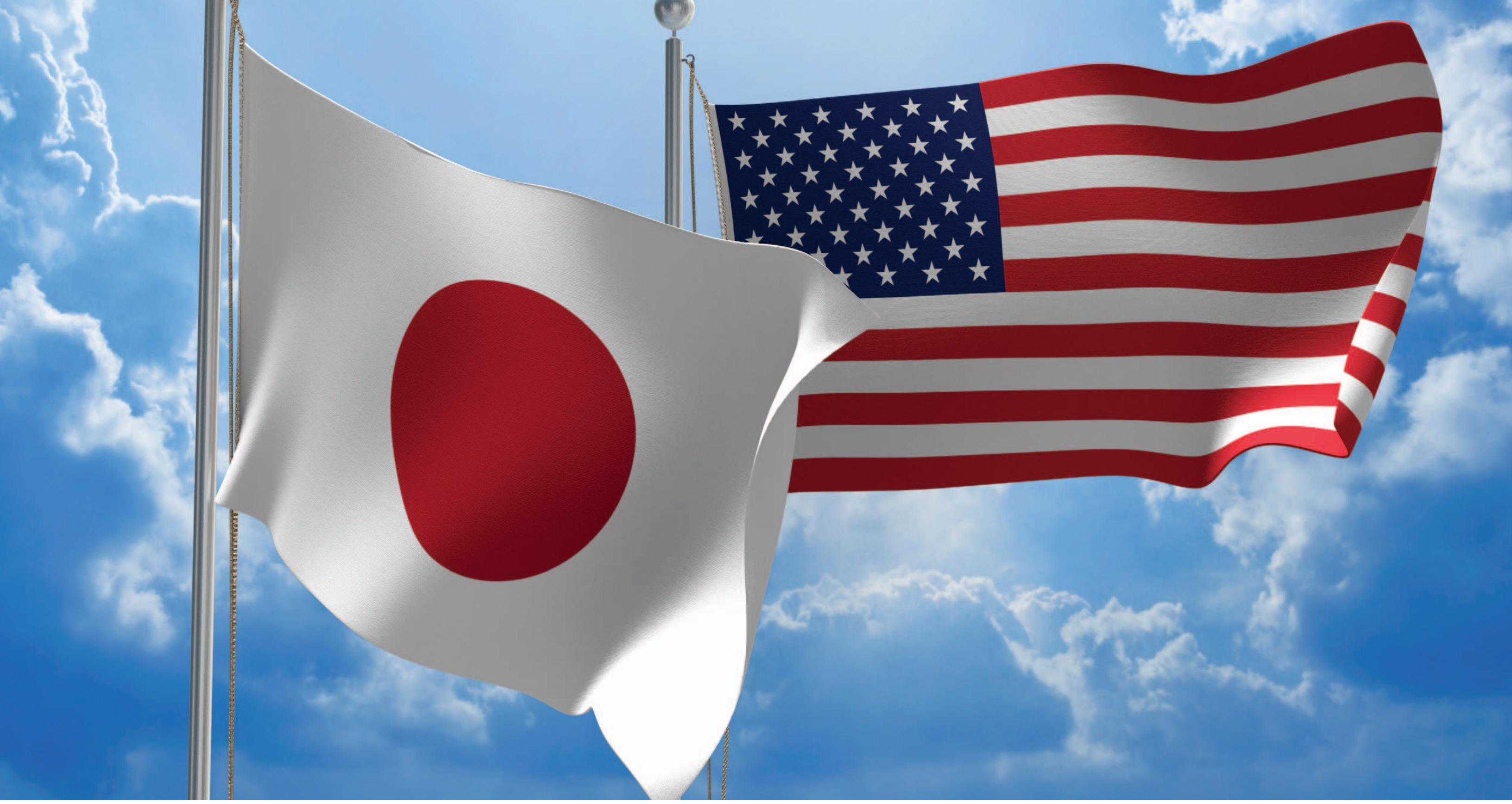


The U.S.-Japan Alliance and Deterring Gray Zone Coercion in the Maritime, Cyber, and Space Domains

Scott W. Harold, Yoshiaki Nakagawa, Junichi Fukuda, John A. Davis, Keiko Kono, Dean Cheng, Kazuto Suzuki

RAND
CORPORATION

For more information on this publication, visit www.rand.org/t/CF379

Published by the RAND Corporation, Santa Monica, Calif.

Cover image by Kagenmi, Getty Images.

Preface

To understand the importance of the U.S.-Japan alliance against the backdrop of a rapidly changing international environment in the Asia-Pacific, RAND convened a conference in early 2017 focused on the use of gray zone coercion in the maritime, cyber, and space domains. The conference brought together leading U.S. and Japanese experts to unearth areas of shared understanding and divergence in thinking on the two sides of the Pacific when it comes to dealing with Chinese efforts to reshape the international order through coercion designed to fall below the level that would invoke a treaty response under the U.S.-Japan alliance. The conference found numerous opportunities for the allies to collaborate in improving shared understandings, reducing ambiguities that China can exploit, stigmatizing gray zone coercion, hardening defenses, and preparing to impose costs. Although it will not be easy to deter gray zone coercion in the maritime, cyber, and space domains, the allies face strong incentives to improve their coordination and strengthen deterrence now, before China or other actors change the status quo at the expense of Washington and Tokyo.

This work was sponsored by the Government of Japan and conducted in the International Security and Defense Policy Center (ISDP) of the RAND National Security Research Division (NSRD). ISDP analyzes changes in the international political, strategic, economic, and technological environment and helps the Department of Defense and other clients develop policies to shape the environment and advance U.S. and allied interests. 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 webpage).

Contents

Figures and Tables

Figures

Tables

Abbreviations

A2/AD	antiaccess/area-denial
ACM	Alliance Coordination Mechanism
AOB	Amphibious Operations Brigade
ASAT	antisatellite
ASEAN	Association of Southeast Asian Nations
BPM	Bilateral Planning Mechanism
ASCM	antiship cruise missile
EEZ	exclusive economic zone
FDO	Flexible Deterrent Option
FY	fiscal year
GGE	UN Group of Government Experts
GOJ	Government of Japan
GPS	Global Positioning System
ICJ	International Court of Justice
ISR	intelligence, surveillance, and reconnaissance
ITLOS	International Tribunal on the Law of the Sea
JASDF	Japan Air Self-Defense Forces
JAXA	Japanese Aerospace Exploration Agency
JCG	Japan Coast Guard
JGSDF	Japan Ground Self-Defense Forces
JMSDF	Japan Maritime Self-Defense Forces
JSDF	Japan Self-Defense Forces
MLE	maritime law enforcement
MSO	maritime security operation
NATO	North Atlantic Treaty Organization
NISC	National Center of Incident Readiness and Strategy for Cybersecurity

NIST	National Institute of Standards and Technology
PCA	Permanent Court of Arbitration
PLA	People's Liberation Army
PNT	positioning, navigation, and timing
PSO	public security operation
SAM	surface-to-air missile
SAR	synthetic aperture radar
SSA	space situational awareness
THAAD	Terminal High-Altitude Aerial Defense
TT&C	tracking, telemetry, and control
UAV	unmanned aerial vehicle
UN	United Nations
UNCLOS	UN Convention on the Law of the Sea

1. Introduction

Scott W. Harold, Ph.D.
Associate Director, Center for Asia Pacific Policy
RAND Corporation

In recent years, national security analysts have noted an alarming rise in the use of so-called gray zone tactics, or actions that are designed to change the status quo through steps that, while consequential, are nonetheless deliberately calculated to remain below the level that would trigger an armed response or that put the burden of escalation on status quo states.[1] China has been one of the leading practitioners of this approach and has built it into a substantial component of Beijing's overall regional political-military strategy, including in both the maritime and cyber domains, with space possibly next.[2] China seeks to shift the regional balance of power in its favor and erode the credibility of U.S. extended deterrence commitments, or the promises that the United States makes that it will deter attacks not only upon itself but also upon its allies, such as Japan, South Korea, or Australia.[3] China is doing this by employing "little blue men" in the form of commercial fishermen and provincial maritime militia forces as proxy cut-

[1] For examples and further discussion, see Michael J. Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict,* Carlisle Barracks, Pa.: U.S. Army War College Press, December 2015. It is important to note that, despite the term, *gray zone* does not refer to a particular physical location; rather, it means a particular ideational space between *white* (wholly peaceful activities) and *black* (truly wartime activities). The gray zone is called that because those who employ such tactics (or, as some authors prefer, *gray zone strategies*) desire to accomplish their goals by means of mixing civilian and military assets, violating norms associated with lawful combatants, and attempting to force status quo powers to fire on paramilitary forces operating under false guises as if they are civilians. In the cyber and space domains—arenas that are inherently less transparent and/or physically remote from ordinary life—states employing gray zone tactics seek to execute attacks with plausible deniability so as to achieve strategic effects without suffering the consequences for their actions.

[2] Denny Roy, "China's Strategy to Undermine the U.S. in Asia: Win in the 'Gray Zone,'" *The National Interest,* September 18, 2015.

[3] *Extended deterrence* refers to the promise by one country to defend an ally and, in so doing, dissuade third countries from attacking that ally (i.e., *deter* other countries from attacking the ally and hence *extend* deterrence to it). Traditionally, countries engage in deterrence in one of two ways: deterrence by denial or deterrence by punishment. *Deterrence by denial* refers to steps taken to frustrate an enemy's attempts to achieve a particular effect; an example could be the use of ballistic missile defenses to intercept and destroy an incoming missile fired by an enemy. Seeing the presence of a dense network of ballistic missile defenses, and seeing them regularly tested under realistic conditions, an enemy might decide that it is undesirable to attempt an attack; the enemy is deterred from attacking by the knowledge that the attack would be denied. *Deterrence by punishment* is premised on possession of the ability to impose unacceptably high post-attack costs on the perpetrator of an attack. In this case, the attacker is credibly informed that s/he would suffer an unacceptably devastating set of consequences (e.g., military, economic, legal, political) if an attack is carried out; to avoid these consequences, the enemy decides not to execute the attack in the first place, even though s/he knows the attack would get through. The enemy is deterred because of the fear of post-attack punishment.

outs and backing them up with maritime law enforcement vessels and over-the-horizon naval forces in the pursuit of its claims to the Senkaku Islands and other features in the maritime domain.[4] Similarly, Chinese cyber warriors target Beijing's political adversaries or enterprises that have valuable information, engaging in clandestine intrusions and attacks through cyberspace that are designed to weaken rival nations, steal their intellectual property, and/or signal to them when they are making China's communist leaders unhappy. Finally, China's military space program and its associated elements have clearly been used for enhancing China's soft power and prestige and for gray zone signaling. China has sought to imply that it intends to use space solely for peaceful purposes, attempting to erode U.S. congressional constraints on space cooperation with China's military-run space program, while at the same time the Chinese People's Liberation Army (PLA) has been demonstrating antisatellite (ASAT) weapons designed to hold at risk or complicate U.S. use of space-based intelligence, surveillance, and reconnaissance (ISR); command, control, and communications; and positioning, navigation, and timing (PNT) architectures critical for deterrence and war-fighting. Due to the very nature of space-based systems and the opaque nature of the medium, China's space assets and cyber capabilities can operate in a highly nontransparent manner where it is potentially possible to carry out gray zone coercion designed to degrade or deny the effectiveness of the space-based assets of the United States or Japan in a deniable fashion over a short or even extended period of time. In summary, across the maritime, cyber, and space domains, China has shown both the willingness and the capacity to employ gray zone tactics and capabilities as part of an overall strategy to challenge the regional status quo.

As a frontline state with territory that China covets (the Senkaku Islands and possibly the broader Ryukyu Chain, up to and including Okinawa[5]), Japan has a clear and compelling interest in understanding how Chinese strategy and tactics in the employment of gray zone coercion unfold across various arenas, most notably the maritime, cyber, and space domains.[6] Given Japan's status as the "cornerstone" of U.S. involvement and presence in the Asia-Pacific, the United States also has a fundamental interest in understanding how to deter and—if necessary—identify, block, defeat, and impose costs on states seeking to change the status quo through the use of gray zone coercion. Recognizing the importance of cooperating to resist attempts to erode the deterrent value of the U.S.-Japan alliance and change the status through gray zone coercion, the United States and Japan announced a decision in April 2015 to issue new guidelines on

[4] Franz Stefan-Gady, "'Little Blue Men': Doing China's Dirty Work in the South China Sea," *The Diplomat*, November 5, 2015; Andrew S. Erickson and Conor M. Kennedy, "China's Maritime Militia: What It Is and How to Deal with It," *Foreign Affairs*, June 23, 2016; Cheng Lai Ki, "The Little Blue Men: China's Maritime Proxy-Warfare Strategy," *Strifeblog*, September 9, 2016; Christopher P. Cavas, "China's Maritime Militia a Growing Concern," *Defense News*, November 21, 2016.

[5] Jane Perlez, "Calls Grow in China to Press Claim for Okinawa," *New York Times*, June 13, 2013.

[6] "Japan to Shoot Down Foreign Drones that Invade Its Airspace," Kyodo, October 20, 2013; Robin Harding, "Japan Scrambles Record Number of Jets as Tensions Rise with China," *Financial Times*, April 13, 2017; "Japan Scrambles Jets over China Drone Flight Near Disputed Islets," *Reuters*, May 20, 2017.

defense cooperation.[7] These new guidelines expanded and deepened military cooperation, extending the focus of the alliance into cyberspace and outer space while also discussing the need to ensure a "seamless" response to adversary actions designed to target gaps in the transition from peacetime to armed conflict. The 2015 guidelines sought to enhance allied coordination and planning by establishing an upgraded Bilateral Planning Mechanism (BPM) and a new Alliance Coordination Mechanism (ACM); the latter is intended to be a standing institution tasked with synchronizing the two sides' reactions to crises.

Understanding that these complex issues lie at the forefront of U.S. policy and alliance management in Asia, as well as Chinese thinking about how to leverage military power and gray zone coercion, the RAND Corporation identified leading U.S. and Japanese experts on maritime, cyber, and space operations and commissioned them to think through the gray zone challenges that the alliance faces from China in these three domains. The authors' papers were presented at a conference held at RAND's headquarters in Santa Monica, California, in March 2017 and are collected here in a conference volume.

As one analysis by RAND experts has shown, Chinese military authors have a particularly ambitious set of policy goals, a well-defined set of strategies designed to achieve these, and a fairly assertive and risk-acceptant concept of national strategy under Xi Jinping that views times of crisis as an opportunity to advance the national interest.[8] Perhaps even more worrisome, PLA experts evince startlingly self-assured beliefs about how finely they can calibrate their control over escalation and how effectively they can employ gray zone tactics to achieve their goals in the maritime, cyber, and space domains, identifying these domains specifically as key areas for power projection and dominance.[9] Indeed, in order to achieve greater ability to project influence in these arenas, the PLA under Xi Jinping has undertaken substantial reforms oriented toward producing greater jointness and directing more resources into the naval and air domains. It has even stood up a new service branch known as the Strategic Support Force to integrate operations in the information (cyberspace), space, and electromagnetic spectrum domains.[10]

In terms of practice, China has put gray zone operations in the maritime domain at the forefront of its efforts to lay claim to the East China Sea and the South China Sea. Lyle Morris, for example, has found that China's use of its fishing fleet, maritime militia, and coast guard and maritime law enforcement forces as "blunt defenders of sovereignty" is driving the East Asian

[7] James J. Przystup, *The U.S.-Japan Alliance: Review of the Guidelines for Defense Cooperation*, Washington, D.C.: National Defense University Press, Institute for Strategic Studies Strategic Perspectives, No. 18, March 2015.

[8] Timothy R. Heath, Kristen Gunness, and Cortez A. Cooper, III, *The PLA and China's Rejuvenation: National Security and Military Strategies, Deterrence Concepts, and Combat Capabilities*, Santa Monica, Calif.: RAND Corporation, RR-1402-OSD, 2016.

[9] Burgess Laird, *War Control: Chinese Writings on the Control of Escalation in Crisis and Conflict*, Washington, D.C.: Center for a New American Security, 2017.

[10] Joel Wuthnow and Philip C. Saunders, *Chinese Military Reforms in the Age of Xi Jinping: Drivers, Challenges and Implications*, Washington, D.C.: National Defense University Institute for National Strategic Studies, 2017.

region toward greater employment of coast guards for "presence competition" and constabulary missions, rather than for such traditional missions as search and rescue at sea.[11] Similarly, China has relied heavily on gray zone tactics and forces operating under unclear relationships of command and control, as Ross Babbage has shown in his recent study of China's "adventurism" in the South China Sea.[12]

Recognizing that, based on Chinese writings, capabilities developments, and the nature of the domains themselves, the gray zone challenges China poses to the U.S.-Japan alliance are probably greatest in the maritime, cyber, and space domains, we therefore identified these as the core focus of our research.[13] In considering how to respond to the challenges that China's gray zone tactics pose for the alliance in these domains, we asked such questions as:

- What roles do land forces and conventional military capabilities play in reinforcing overall deterrence and dissuading gray zone coercion in the maritime domain?
- How can the United States and Japan best posture themselves to resist Chinese maritime coercion through denial and cost-imposition strategies?
- What role do U.S. defense leaders see for allies in cyber deterrence, and how can the United States best assist Japan in cyber defense?
- What challenges does Japan face from a legal perspective in defending itself and extending assistance to the United States in the event of a contingency involving cyberspace?
- How do U.S. and Chinese strategists conceive of the relationship between deterrence and outer space, and what implications do the two countries' approaches have for the U.S.-Japan alliance?
- How can Japan best cooperate with the United States to deter and defend key allied assets in space?

Chapter Summaries

In his essay, "Using Land Forces to Deter Maritime Gray Zone Coercion: The Role of the Japan Ground Self-Defense Forces (JGSDF) in the Nansei (Ryukyu) Islands," Yoshiaki Nakagawa (Lieutenant General, JGSDF, retired) of the Japan Forum for Strategic Studies notes that Japan has made significant strides in improving its capacity to use the land to control the sea and to retake lost islands through amphibious operations. He argues, however, that Japan still needs to make many more changes in order to more effectively deter—or, if necessary, defeat—

[11] Lyle J. Morris, "Blunt Defenders of Sovereignty: The Rise of Coast Guards in East and Southeast Asia," *Naval War College Review*, Vol. 70, No. 2, Spring 2017.

[12] Ross Babbage, *Countering China's Adventurism in the South China Sea: Strategy Options for the Trump Administration*, Washington, D.C.: Center for Strategic and Budgetary Assessments, 2016.

[13] The air domain is also an arena in which China has engaged in gray zone coercion, most notably with its declaration of an Air Defense Identification Zone over the East China Sea, as well as with its deployment of drones into the airspace in and around the Senkaku Islands in 2013 and 2017. Thanks to our colleague Brien Alkire of RAND for reminding us not to neglect to include this important point while focusing on the maritime, cyber, and space domains.

any Chinese effort to seize the Senkaku Islands or any of the other Nansei Shoto (Southwest; Ryukyu) Island chain features. Noting the shift from a static defense of the northern island of Hokkaido against a Soviet ground invasion to the development of a "dynamic defense" (later renamed "dynamic joint defense" to emphasize cooperation with the United States) focused on the south and west, Nakagawa sees the JGSDF as evolving in a direction that will better position it to contribute to a defense of Japanese territory from potential Chinese air, naval, missile, and amphibious assault threats. The procurement of a number of key capabilities—including radar for target acquisition and queuing, truck-mounted surface-to-air missile batteries, road-mobile antiship cruise missiles, and the development of a rapidly deployable reaction force focused on amphibious assault and island-retaking operations—has begun to address Japanese vulnerabilities in an area distant from the mainland and proximate to areas where China has increased its operational capabilities and tempo. Nakagawa advocates a focus on creating greater stockpiles of key commodities (food, water, clothing, munitions) in the event of a prolonged conflict; notes the need for exercising logistics under attack; urges the JGSDF and other services to procure longer-range missiles that can close gaps between widely dispersed islands in the Southwest; and encourages the central government to think more about how it would work with local governments to evacuate or provide shelter and support to civilians caught in a conflict zone, since the Japan Self-Defense Forces (JSDF) may not be able to spare the manpower to attempt to evacuate them. Echoing his fellow retired Lieutenant-General Isobe Koichi, who has argued that the Amphibious Operations Brigade (AOB) is not yet where it needs to be to reliably conduct effective amphibious operations (for a number of reasons, including inadequate experience and the challenges of refining a resilient command-and-control infrastructure), Nakagawa argues that more manpower and more attention to this issue are needed.[14] Nonetheless, inasmuch as Japan's initial investment in an amphibious capability represents an obstacle to Chinese ambitions to seize the Southwest Island chain through low-cost operations, the development of the AOB helps deter (and, if necessary, could be used to help defeat) a gray zone challenge or something even more ambitious.

Following Nakagawa's essay, Junichi Fukuda of the Institute for International Policy Studies in Tokyo offers up "A Japanese Perspective on the Role of the U.S.-Japan Alliance in Deterring—or, If Necessary, Defeating—Maritime Gray Zone Coercion." Fukuda's chapter first describes China's tactics in the East and South China seas, then argues that the U.S.-Japan alliance needs to counter Chinese coercion through a dual strategy of denial and long-term cost imposition.[15] Fukuda argues that if the United States and Japan can improve their abilities to deny China its goals through gray zone coercion, they can raise the costs to China of achieving

[14] Lt. Gen. Koichi Isobe, JGSDF (Ret.), "The Amphibious Operations Brigade: The Establishment of the JGSDF Brigade and Its Challenges," *Marine Corps Gazette*, Vol. 101, No. 2, February 2017.

[15] Junichi Fukuda, "Denial and Cost Imposition: Long-Term Strategies for Competition with China," *Asia-Pacific Review*, Vol. 22, No. 1, May 2015.

its ambitions, thereby delaying the resort to conflict and potentially lowering the cost to the allies by diverting Chinese investments into addressing costly challenges rather than developing more-lethal capabilities to use in coercing the allies. In a viewpoint shared with Nakagawa, Fukuda notes that, first and foremost, the allies need to invest in maintaining and expanding their ability to dominate the conventional war-fight as a way to preserve and improve deterrence. After that, investments should be made in Japan's maritime law enforcement capabilities, ensuring that the Japan Coast Guard (JCG) has both the hardware and staffing it needs, as well as the legal authorities and operational experience necessary to handle cleanly the hand-off of an instance of gray zone coercion to the JSDF if it becomes too much for the civilian authorities to handle on their own. In the realm of cost-imposing strategies, Fukuda argues for expanded U.S. and Japanese efforts to bolster allies' and partners' maritime domain awareness, patrol, and law-enforcement capabilities so as to prevent China from cowing regional neighbors, such as the Philippines and Vietnam. He also argues for the use of expanded diplomatic condemnation of China's gray zone coercion attempts. Noting that the use of international legal actions, such as the Philippines pursued at the International Tribunal on the Law of the Sea (ITLOS), and their associated reputational costs may not persuade China to back away from gray zone tactics to change the status quo, Fukuda advocates considering steps that could impose domestic costs on the Chinese Communist Party, potentially including such measures as releasing information on elite leadership corruption, upgrading ties with Taiwan, offering support to separatist groups in China's far west, or pursuing economic sanctions against China. He closes by reminding the reader that the goal of all such efforts is not conflict with China but preventing China from changing the status quo by force or through gray zone coercion: If China were to accept the regional order and choose to work within its terms and norms, the allies would have no reason to challenge China.

Shifting from a focus on maritime gray zone coercion to one on attempts to use force through cyberspace, Major General John Davis (U.S. Army, retired) of Palo Alto Networks offers his thoughts on how the allies can deter—or, if necessary, defeat—attempts to leverage the anonymity of cyberspace in "The U.S.-Japan Alliance and Deterrence in Cyberspace." Davis begins by noting the growing importance of cyberspace for everyday life, commerce, and military operations and pointing out that the upcoming Tokyo 2020 Olympics will present a major target for adversaries interested in damaging or coercing Japan and/or the United States. He then argues that U.S.-Japanese cyber policy should be built around three pillars: a national component (where whole-of-government policies are bolstered and supplemented by whole-of-nation collaboration, including industry support and greater awareness of cybersecurity among the populace), an alliance component, and a deterrence component that seeks to fill gaps between the allies with the goal of ensuring a seamless response to coercion targeting either party. Davis calls on the allies to focus the majority of their efforts on hardening critical infrastructure to reinforce deterrence by denial of threats that could do large-scale damage or lead to death. However, gray zone threats that run below the threshold of an armed attack or act of war can still pose challenges for the allies' security. To defend the allies' interests, Davis argues for a clear understanding of what must be defended, what must be resilient, and what must be amenable to rapid reconstitution. Defending and repairing these systems, as well as defending against insider threats, are tasks that are largely best suited to each nation, though information and intelligence-sharing on threats and best practices are areas where the two sides can profitably cooperate. In terms of deterrence through cost imposition (also referred to as deterrence by punishment), Davis argues for tighter cooperation between the allies in efforts to impose reputational, diplomatic, economic, and legal sanctions against threat actors who might target either nation through cyberspace. He notes that there is much room for Washington and Tokyo to collaborate on building partner capacity for greater cybersecurity with regional partners in Southeast Asia, where vulnerabilities are legion and countries are generally too poor, weak, and inexperienced to build up their cyber defenses on their own. Davis recommends that the United States should train with Japan on cyber operations from time to time; make an explicit declaratory statement that it will reserve the right to respond to attacks on its ally through cyberspace via other means; and occasionally demonstrate an offensive cyber capability for the purposes of reinforcing deterrence. He concludes by calling on the United States and Japan to move toward joint research and development of automated intrusion detection software, which would enhance cybersecurity by accelerating the process of defense, discovery of intrusion, and reacquisition of control over clean systems.

In her contribution "A Japanese Perspective on Deterrence in Cyberspace Gray Zone Contingencies and the Role of the U.S.-Japan Alliance," Keiko Kono of the Japanese Ministry of Defense's National Institute for Defense Studies notes that Japan is still figuring out how its existing legal authorities and institutional responsibilities fit with and condition its ability to prosecute a cyber contingency that appears to be migrating from a criminal action to a gray zone coercion attempt. This is complicated legal territory, especially for a nation that has sought for several decades to nurture a culture of national security that one leading expert has characterized as reflecting "domestic antimilitarism."[16] Kono notes that Japanese policy has been premised on the notion that violent actions rising to the level of a legally defined armed attack could or would only be carried out by nation-states, making it harder for Japan to respond to attacks conducted in cyberspace, where the identity of a perpetrator may be unknown or where command-and-control relationships to state authorities can be hard to discern or prove. When the Chinese "Red Honker Union"—a group of "patriotic hackers" with an ambiguous command-and-control relationship with the Chinese central government that, at a minimum, appears highly sympathetic

[16] On Japan's national security culture and cultures of national security more broadly, see Peter J. Katzenstein, *Cultural Norms and National Security: Police and Military in Post-War Japan*, Ithaca, N.Y.: Cornell University Press, 1996a; and Peter J. Katzenstein, *The Culture of National Security: Norms and Identity in World Politics*, New York: Columbia University Press, 1996b. On the notion that Japan has a culture of "domestic antimilitarism," specifically, and not "pacifism," see Andrew L. Oros, *Normalizing Japan: Politics, Identity, and the Evolution of Security Practice*, Stanford, Calif.: Stanford University Press, 2008; and Andrew L. Oros, *Japan's Security Renaissance: New Policies and Politics for the Twenty-First Century*, New York: Columbia University Press, 2017.

to Beijing's goals—attacked Japanese websites over the Senkakus crisis in 2012, Japan's system was revealed to be poorly prepared to respond to challenges in this new domain. Japan's legal architecture does not mesh well with a circumstance where a malicious nonstate actor could be working at times independently, at other times alongside state adversaries intending Japan harm, and at yet other times at the behest of those adversaries. How the JSDF could be mobilized to respond to an attack that overwhelms civilian police and cyber defense authorities and appears to be directed by a foreign group in collaboration with a foreign state is unclear. Indeed, Japan appears not to have legal authorities in place to permit the JSDF to respond to a gray zone scenario in cyberspace. A JSDF response (or JSDF response together with a U.S. response) would be especially challenging because the JSDF is not supposed to carry out military operations in defense of Japan that would go beyond Japan's territorial boundaries, whereas cyberspace does not have set territorial meaning in most contexts. Kono notes that while denial in cyberspace appears to fit with the Government of Japan (GOJ)'s current policies, the GOJ probably needs to provide additional legal guidance to support JSDF operations aimed at deterrence through punishment in cyberspace, particularly if it seeks to support deterrence through the use of offensive cyber counterstrikes or through allied cyberwarfare. Like Davis, Kono agrees that information-sharing and a shared common operating picture or understanding of an unfolding contingency will be critical for the United States and Japan in the event of a crisis involving cyberspace. She concludes by noting how difficult it is for the allies to deter gray zone coercion in cyberspace, noting that "the lower limits of gray zone coercion may vary by domain, with cyberspace being perhaps the least amenable to JSDF actions aimed at deterrence."

The final two papers turn to an examination of deterring gray zone coercion in outer space, where deniable attacks can be carried out by numerous vectors and with substantial consequences. Efforts to episodically interfere with PNT satellites, communications satellites, ISR satellites, and other assets can be done via cyberspace, ground-based uplinks/downlinks, implanted malware or hardware, directed energy attacks, or kinetic strikes. Attribution is difficult because systems pass through dark patches, experience normal system failure, are struck by space debris, can be hit by solar flares, or can be subject to genuinely accidental impacts from failing systems by other nations' assets, all of which can be used to mask a gray zone attack.

In his essay "Space Deterrence, The U.S.-Japan Alliance, and Asian Security: A U.S. Perspective," Dean Cheng of The Heritage Foundation builds on his previous work on Chinese views of deterrence, laying out key differences between U.S. and Chinese conceptions of deterrence and space.[17] Cheng begins by laying out the key roles that space-based systems play in U.S. military operations, including ISR, meteorology and Earth observation, communications,

[17] See Dean Cheng, "Chinese Views on Deterrence," *Joint Forces Quarterly*, No. 60, Spring 2011; and Dean Cheng, *Prospects for Extended Deterrence in Space and Cyber: The Case of the PRC*, Washington, D.C.: Heritage Foundation, January 21, 2016.

and PNT. Describing space as an essentially “offense-dominant” environment, he lays out the numerous vulnerabilities of space systems, including effects from physical impacts, directed energy weapons, cyberattacks and/or interference with the systems’ ground-based tracking, telemetry, and control centers. He then notes that, whereas U.S. military experts typically describe deterrence as a goal and tend to treat it as defined by efforts aimed at dissuading an adversary from taking a given action or actions, Chinese thinkers, by contrast, tend to treat deterrence as a means by which to achieve their political ends and see it as involving both dissuasion and compellence. With regard to space, Americans see it as both a medium through which military operations can be prosecuted and a potential domain in which deterrence might be possible; by contrast, Chinese authors tend to regard space only as a force-enabling domain that could be targeted to cripple a rival that relies heavily on space systems—but not one in which deterrence could be executed. Cheng also notes that, for China, deterrence in space tends to involve only dissuading adversaries from attacking China’s space assets, whereas space deterrence for the United States involves both dissuading an enemy from attacking U.S. space assets or those of U.S. allies, such as Japan. Cheng notes that Chinese military writers appear to have a fairly clearly defined escalation ladder of steps that they envision taking in a crisis to signal their intent to deter or coerce an opponent via space operations, including displays of military space capabilities; exercises involving military space assets; deployment or augmentation of space weapons; and a range of employment concepts, including space “shock and awe strikes” and “space blockades” of various types. Cheng argues that

> while there may be clashes in space, the actual source of any Sino-American conflict will remain earthbound, most likely stemming from tensions associated with the situation in the East China Sea, the Taiwan Strait, or the South China Sea. This suggests that U.S. and allied decisionmakers (both in Asia and Europe) should be focusing on deterring aggression in general, rather than concentrating primarily on trying to forestall actions in space. Indeed, there is little evidence that Chinese military planners are contemplating a conflict limited to space.

In order to better counter any potential Chinese military operations aimed at undertaking coercion in space (however unlikely), Cheng concludes that the United States and Japan need to substantially deepen their institutional dialogues on space, build a common set of reference terms, and familiarize each other with decisionmaking processes for the employment of military space assets, perhaps by employing gaming and modeling so as to surface each side’s operational expectations and likely moves.

In the final essay in the volume, “A Japanese Perspective on Space Deterrence and the Role of the U.S.-Japan Alliance in Deterrence in Outer Space,” Kazuto Suzuki of Hokkaido University notes the importance of space systems for the United States and Japan, describes the vulnerability of space systems to various forms of attack and disruption (including by natural phenomena), and explores the fit between traditional concepts of deterrence through denial (hardening) and through punishment (attacks on other space systems), noting that neither hardening nor reciprocal attacks on space systems provides a particularly effective or attractive model for deterring attacks on allied space systems. Suzuki argues that

> the U.S.-Japan alliance will need to deter and defeat attacks on critical space-based systems primarily through the employment of cross-domain deterrence . . . [which] will require a combination of terrestrial and space-based intelligence assets to identify the source of hostile attack, at which point the U.S.-Japan alliance will likely need to respond with actions undertaken in other domains to reinforce or restore deterrence against attacks on the allies' space-based systems."

He encourages U.S. and Japanese policymakers to start by building on already-existing information-sharing and space situational awareness (SSA) cooperation efforts to reduce the anonymity of gray zone coercion in space, and he argues that "the time is ripe for defining what constitutes hostile action and what kinds of means should be taken in responding to such threats." In addition to efforts to enhance transparency in space and increase resiliency through rapid reconstitution, hosted payloads, or shared access to national means, the allies can employ coordinated cross-domain deterrence in the form of norm-building, diplomatic condemnation, economic sanctions, legal actions, and even the use of force if all else fails.

The next six chapters are edited versions of the papers that were presented at the conference. The final chapter provides some concluding thoughts.

2. Using Land Forces to Deter Maritime Gray Zone Coercion: The Role of the Japan Ground Self-Defense Forces in the Nansei (Ryukyu) Islands

Yoshiaki Nakagawa
Lieutenant General, JGSDF (retired)
Japan Forum for Strategic Studies

In recent years, three domains of potential military conflict have gained increased attention: the maritime, cyber, and space domains.[1] While these partly overlap with the domains in which traditional land, sea, and air forces are active, it is not appropriate to think they are the same.[2] Discussions about these domains are evidence of a new element appearing in the security and military field that basically stems from the development of science and technology and from changes in human society. These changes are substantially affecting traditional land, sea, and air forces. In order to contribute to deterrence and defense in these domains, Japan's ground forces have developed specialized groups related to cyberspace and outer space: the signal corps and antiaircraft artillery. In the future, it is possible that there may be a major change in which these specialized forces separate from the main army, much as the navy did long ago. In this sense, the challenges that these new domains pose for the land forces can also be seen as great opportunities. In the short term, however, the army will face intense competition over the distribution of resources.

This article will focus on the JGSDF's deterrence posture in the Nansei (Ryukyu) Islands. It will cover the importance of the Nansei Islands to Japan's security and the broader U.S.-Japan alliance; the roles and missions historically played by the Japanese ground forces in effecting deterrence and defense at sea using forces on land; changes in the roles and missions that the JGSDF can play today and in the future, based on a series of important changes to its posture and

[1] Although the focus of this conference was on deterring and defeating gray zone coercion, we started with a look at how conventional land-based forces can constrain the options possessed by adversaries of the U.S.-Japan alliance that might be contemplating coercion. This is deliberate: We are highlighting an attempt to use conventional capabilities to place an upper bound on gray zone coercion and looking at how such capabilities might shape allied and adversary thinking about coercion in gray zone contingencies that fall below the threshold of a legally defined armed attack. We alert the reader to this decision in an effort to avoid confusion that we are starting the volume with a focus on traditional war-fighting; the aim was to highlight the upper bounds and then explore matters below the level of war. Subsequent chapters will also occasionally elide the boundary between capabilities relevant for war and gray zone contingencies because conventional war-fighting capabilities affect escalation concerns and how adversaries think about risk management.

[2] There is a difference between sea domain and maritime domain. *Sea domain* is the field of naval forces and battle, while *maritime domain* is the field of wider activities, such as fishing, resource development, and ecology.

capabilities; some consideration of the limitations or requirements imposed by the posture the JGSDF is preparing; and the implications for the U.S.-Japan alliance.

Background

The importance of land forces in shaping the maritime domain has been rising rapidly since the turn of the century, mainly because of China's aggressive military build-up. China's nontransparent military modernization drive and its aggressive maritime activities are rapidly shifting the regional military balance. China's attempts to change the status quo in the East China Sea and South China Sea are based on an expansive and historically unsupported set of assertions about its rightful territorial claims. These claims, as China has increasingly sought to act upon them, are fueling a substantial growth in the risk of conflict stemming from disagreements, misunderstandings, and miscalculations and have become a very serious source of security concerns for the international community, especially Japan.

One of China's unique interpretations of international law is its claim to "maritime territory." Based on claims that have been rejected by most international legal experts—including, most definitively, in the South China Sea arbitration case decided by the Permanent Court of Arbitration (PCA) at The Hague on July 12, 2016—China has unilaterally sought to exclude neighboring countries and other nations from accessing international waters near China that it claims the right to control. Disturbingly, China's attempts to convert the international high seas into Chinese "territory" appear to be accelerating. Increasingly, Chinese state and nominally private vessels alike intrude into Japanese territorial waters in the East China Sea, infringing on Japanese sovereignty and threatening Japanese security and territorial integrity. At the same time, as a member of an international community with an interest in international law, global norms, and the peaceful settlement of disputes, Japan has a clear normative interest in the South China Sea remaining global commons and not being converted into a "Chinese lake" by coercion.[3]

While its public diplomacy advocates "peaceful development," in practice, China continues to act in an assertive manner. Such behavior is especially obvious in the maritime domain, where China's interests frequently conflict with those of other nations. China's attempts to change the status quo through coercion include dangerous acts that may cause unintended consequences, but Beijing has been unwilling to compromise because it has been making steady progress at changing the status quo through faits accomplis that have thus far failed to trigger sufficiently consequential resistance from the international community.

China is believed to be enhancing its asymmetric military capabilities to deter the military forces of other countries from approaching and advancing into the region surrounding China and

[3] This is in addition to Japan's more direct economic, geostrategic, and military interests in the South China Sea remaining an open body of water not controlled by China.

to stop military activities in the region. These are referred to as antiaccess/area-denial (A2/AD) capabilities, which are intended primarily to provide China with a counter-intervention option that could prevent the military forces of the United States from responding in the event of a conflict between China and one of the U.S. allies and partners that neighbor it, such as Japan, South Korea, Taiwan, or the Philippines. Such capabilities, and China's apparent willingness to employ them, have fueled great concern in Japan.

Another concern is the rapid growth of China's defense budget.[4] China announced that its national defense budget for fiscal year (FY) 2016 was approximately 954.4 billion yuan (about 18.1 billion yen, or roughly US$143 billion). Moreover, China's announced national defense budget has increased rapidly in recent years, recording a roughly 10-percent annual growth rate since the year 2000. The nominal size of China's announced national defense budget is approximately 44 times larger than it was in 1988 and nearly 3.4 times larger than it was in 2006. Meanwhile, over the same time frame, the size of Japan's defense budget has actually decreased slightly.[5] Russia has reduced its deployment of military forces in the vicinity of China, and the two nations resolved their border conflicts in 2004. In the absence of an obvious military threat to China, its buildup of military capabilities suggests to many Japanese observers that Beijing may aim at changing the status quo through intimidation and coercion.

China's strategically relevant activities in recent years have involved significant action by not only its armed forces but also its paramilitary forces or law enforcement; these latter capabilities have been especially active in Japan's surrounding waters and airspace. The number of Chinese naval surface vessels advancing into the Pacific Ocean has increased in recent years, and such incursions continue to be conducted at a high rate. It is likely that, through such operations, China is seeking to improve its deployment capabilities in the open ocean.[6]

In June 2016, a Chinese PLA Navy frigate entered Japan's contiguous zone near the Senkaku Islands. Shortly thereafter, an intelligence-gathering vessel entered Japan's territorial waters near Kuchinoerabu Island and within Japan's contiguous zone north of Kitadaito Island. After that operation, the vessel sailed back south of the Senkaku Islands. Japanese experts are seriously concerned that China is escalating its activities in the waters near Japan in support of its attempt to lay claim to the Senkaku Islands.[7] That is because Chinese vessels that enter Japanese waters

[4] Ministry of Defense of Japan, *The Defense of Japan, 2016*, Tokyo, white paper, 2016, Chapter 2, Section 3.

[5] Data on estimates of China's defense spending and comparisons with that of Japan come from Ministry of Defense of Japan, "China's Defense Budget," infographic, undated-a.

[6] Ministry of Defense of Japan, 2016.

[7] Japan regards the Senkakus as the inherent territory of Japan and denies that either China or Taiwan have standing to dispute this claim. Beijing and Taipei both separately claim the Senkakus as the Diaoyudao/Diaoyutai on behalf of (respectively) the People's Republic of China and the Republic of China (Taiwan). U.S. policy recognizes Japanese administrative control, and the United States has clarified that Article 5 of the U.S.-Japan mutual security treaty applies to the islands, obliging the United States to defend them in the event of an armed attack. Ministry of Foreign Affairs of Japan and U.S. Department of State, Treaty of Mutual Cooperation and Security Between Japan and the United States of America, 1960.

may have the intention of attempting to exert administrative control (or undermine Japanese administrative control) over these waters or to support the claim that the waters are “in dispute.”

In the case of Chinese paramilitary forces (government vessels and aircrafts), their intrusions into Japanese territorial waters and airspace are becoming routine. Armed Chinese government vessels have begun to intrude into Japanese territorial waters and are increasingly larger in size. Japan is concerned that China is continuously building up an operational posture that might be used to intrude into Japanese territorial waters.

In recent years, the number of scrambles by the Japan Air Self-Defense Forces (JASDF) against Chinese aircraft has increased dramatically as well. Recently, PLA Air Force aircraft have also been intensifying their activities near the Senkaku Islands.

The strategic and operational goal of China’s maritime activities is clear: It is to weaken the control of other countries over the islands to which China claims territorial sovereignty while strengthening its own claims through various surveillance activities and the exertion of governmental authority in the sea and airspace surrounding those islands. The activities are an obvious and clear violation of established international law.[8]

Building maritime platforms is another activity China has employed to weaken the control of other countries over their exclusive economic zones (EEZs). China is known to be building 12 new maritime platforms for oil and gas production in addition to deploying four platforms on the Chinese side of the China-Japan median line. Such a siting potentially allows China to siphon away oil and gas from Japan’s side. These Chinese activities should raise—and, in many cases, have raised—security concerns across the region and from the international community as a whole. To counter these threats, Japan has been reviewing and reinforcing its posture in the strategically located Nansei (Ryukyu) Islands. This portion of Japan’s territory is examined in the next section.

The Strategic Importance of the Nansei Islands

Japan has unique maritime geography.[9] Its many islands are located at the eastern edge of the Asian continent and can be seen as constituting chokepoints on the route from China to the Pacific Ocean. Specifically, the Nansei (Ryukyu) Islands are an island chain stretching from Japan’s Kyushu Island in the north down to Taiwan in the south and are the key gateway to the Pacific Ocean for ships coming east from the Chinese coast.

The location of the Nansei Island chain is a very important factor in Japanese strategic calculations: If the islands are well defended against attack, they can play a key role in deterrence and the defense of Japan. In the event of a conflict, Japan could deploy its A2/AD capabilities along the islands and potentially close important egress routes for Chinese air and

[8] Ministry of Defense of Japan, 2016.

[9] Toshi Yoshihara, “Going Anti-Access at Sea,” Center for a New American Security, September 12, 2014.

naval forces, including surface combatants, submarines and aircrafts, seeking to operate in the western Pacific. Having such an ability to limit the areas where the Chinese Navy can operate around the island chain carries many strategic benefits for both Japan and for the U.S. armed forces, including greater operational safety and more-rapid options for deploying combat power to a potential conflict zone. The more effectively Japan can defend the islands, the more actively the United States can conduct offensive operations in theater. Such a division of labor is a key benefit of the U.S.-Japan alliance and a critical factor in actual allied military operations.

The next section explores the Japanese Imperial Army's historical experience using the land to effect deterrence and war-fighting at sea.

The Japanese Imperial Army in the Pacific Theater in World War II

In World War II, the Japanese Imperial Army launched a very small unit (initially just four divisions, consisting of less than 10 percent of the total force) into the operations in the West Pacific islands. The Japanese Imperial Army approached this theater with the reasonable awareness that the main strategic entity in the Pacific Theater was the Japanese Imperial Navy. The diversion of a large Army force to the Pacific Theater was intended as a response to U.S. offensives in that region during the latter part of the war.

The role the Army played was relatively limited. Its main missions were to provide support to maritime and air operations by ensuring the security of the islands on which harbors and runways were located and assisting with the maintenance of these facilities.

Japan's strategy for leveraging its control over the islands of the Pacific was heavily dependent on its ability to resupply these outposts. Protecting maritime supply lines, the main means by which forces deployed on these islands were supplied, made logistics a key vulnerability during the war. For this reason, gaining sea control became a core objective of the Japanese Imperial Navy and the U.S. Navy.

The strategic location of the various islands, as well as their facilities and distance from enemy bases, were important factors in differentiating their values to Japanese military strategy. While some islands could be bypassed by U.S. forces on their way toward the Japanese home islands, others could not and had to be captured and occupied. As a consequence, in various parts of the Pacific Theater, the U.S. and Japanese militaries fought over the islands. If we look at the history of these island battles, the main roles of the ground forces can be summarized as follows:

- providing support to naval forces
- preventing enemy landings from the sea or air
- denying occupation and use of an island
- preparing island-retaking efforts.

Through the emplacement of an appropriately dug-in and well-provisioned defending force, the Japanese Imperial Army determined that it could force its U.S. adversary to expend between three and five times the number of forces Japan had deployed in order to occupy and use the islands.

Today's JGSDF has drawn several lessons from these experiences. If an enemy is attempting to land from the sea or air on an island, for instance, JGSDF units can interfere with such operations, potentially even causing them to fail. Even if the enemy is able to land, JGSDF units will protect major points on the island for as long as possible to deny use to the adversary, potentially foiling the ability to use such facilities in a timely manner to support other enemy aims. If the operations of the Japan Maritime Self-Defense Forces (JMSDF) progress smoothly and an island-retaking operation is carried out, the JGSDF then transitions into the role of a land attack unit.

Globally, only the U.S. Army and the U.S. Marine Corps have extensive combat experience with amphibious assault, especially the preparation for and capture of enemy-occupied territory from the sea. The JGSDF, however, recently moved to establish its own rapid-reaction and amphibious assault forces, and these have been training with the U.S. Marine Corps for the purposes of learning island defense, island recapture, and how to fight to the land from the sea. The JGSDF also recently purchased or procured substantial new capabilities to enable it to better deter conflict in such contingencies as might occur in the Nansei Islands and, if necessary, prosecute such conflicts more effectively.

Controlling the Sea from the Shore: The JGSDF's New Surface-to-Air and Antiship Cruise Missile Capabilities

In recent years, a major advancement in defense technology has been the rapid improvement in the capabilities of ground-launched surface-to-air missiles (SAMs) and antiship cruise missiles (ASCMs), as well as in the capabilities of long-distance sensing. The development of easily operable unmanned aircraft further supports these improvements in capabilities.

During World War II, land forces were effective against vessels and aircraft out to a distance of only a few kilometers. Today, JGSDF troops equipped with SAMs and ASCMs are able to engage and destroy enemy aircraft and ships up to several hundred kilometers away. This reality is equally true for China and is likely a major motivation behind its construction of artificial islands in the South China Sea.

How should we assess the ability of modern ground forces to affect the air and maritime domains? While expert opinion is divided on this overarching question, there is substantial agreement that one key limitation on such forces stems from their need to be resupplied over time. Such resupply constitutes a primary vulnerability to any nation that has positioned its forces on remote islands. By contrast, A2/AD capabilities deployed on a nation's homeland provide it with substantially greater benefits because of the opportunity to leverage interior supply lines. It is substantially more difficult (and outright impossible, in some cases) to completely block a country's resupply activities on its home territory without executing a substantial ground invasion or achieving virtually uncontested air and maritime dominance (and even then, it is still difficult).

Having explored the relevance of ground forces based on islands for shaping air and naval activities, as well as such ground forces' vulnerabilities, we next turn specifically to the threat to the Japanese Nansei Islands.

The Threat to Japan's Nansei Islands

The greatest current risk of maritime gray zone coercion facing Japan would be an attempt by China to seize the Senkaku Islands, which are part of the Nansei Island chain. China reaffirmed its claim to the Senkakus in 1992.[10] Since that time, Chinese aircraft, state vessels, and nominally private fishing boats (sometimes staffed by fishermen or activists who appear to be acting on the orders of the state) have repeatedly intruded into Japanese waters near the islands. Additionally, Chinese scholars are even quoted from time to time in the Chinese state-run media claiming that Okinawa is Chinese territory that was taken by Japan, citing the historical fact that the Ryukyu Kingdom did send tributary offerings to the Qing Dynasty (while ignoring the fact that it also sent such offerings to Japan during the Edo and Meiji periods over 200 years).[11] Such actions are representative of China's overall United Front tactics and the PLA's "three warfare" strategy (psychological warfare, public opinion or media warfare, and legal warfare).[12] More specifically, China's use of civilian maritime law enforcement capabilities, maritime militia, and private-sector actors operating at the behest of the state constitute an archetypal maritime gray zone coercion effort. In employing such actors and capabilities, China seeks to effect changes in the status quo while remaining below the level of provocation that would elicit a strong response from Japan or the U.S.-Japan alliance, an approach some have labeled as leveraging "salami-slicing" tactics because they involve incremental but consequential changes designed to pile up over time.

The next section explores what the JGSDF can do to deter and defeat such Chinese maritime gray zone coercion attempts in the Nansei Islands.

The Posture of the JGSDF in the Nansei Island Chain

In cooperation with the JMSDF and the JCG, the JGSDF is proceeding with the deployment of new troops to counter the threats discussed in the previous section. As described in the 2013

[10] Standing Committee of the Seventh National People's Congress, Law of the People's Republic of China Concerning the Territorial Sea and the Contiguous Zone, February 25, 1992.

[11] See, for example, Perlez, 2013.

[12] United Front (统一战线) tactics are a legacy of the Chinese Communist Party's efforts to divide enemies and fragment the unity of forces aligned against the Party while seeking to neutralize or unify with any forces that can be used by the Party to defeat its most immediate adversary. Such tactics rely heavily on the use of information operations, psychological warfare, and political deception.

National Defense Program Guidelines and the 2014 Mid-Term Defense Program,[13] the JGSDF aims to accomplish the following measures:

- It will revise its Cold War-era focus on the defense of Hokkaido from a northern Russian ground invasion in favor of preparations to deter—or, if necessary, defeat—an air and maritime threat originating from China in the southwest. This involves developing a strategic posture focused on the defense of the Nansei Islands, including the Senkaku Islands, and Kyushu, which is the main base for supporting JGSDF operations in the Nansei Islands.
- It will adjust and improve force posture by building a base and supply facility in the Nansei Islands and deploying three security guard units to sites across the island chain. The guard units will be equipped with SAMs and ASCMs with which to defend themselves. Each guard unit is intended to be sized at around 500 to 800 personnel.
- In the event that islands in the Nansei Island chain are in fact occupied by enemy forces, the JGSDF will deploy its newly formed amphibious troops to retake these islands.
- In addition, the JGSDF has newly established a rapid-reaction regiment that consists of an airlift-capable armored vehicle unit that can easily move between islands.

In addition, the JGSDF already has one airborne brigade and one special operations force group (of battalion size), as well as one transport helicopter unit capable of lifting a regiment-sized unit. The reinforcements regarding the guard units, amphibious troops, and rapid-reaction regiments will be completed around 2023. In FY 2018, the first rapid-reaction regiment and amphibious combat troops will start to be stood up. The JGSDF's current plans for the creation of amphibious capabilities are envisioned as including an amphibious assault brigade. This is a smaller brigade of about 3,400 members. Equipped with amphibious assault vehicles and landing craft, the brigade can transport about 2,000 infantry plus equipment and supplies at any one time relying on its organic lift capabilities alone. With the assistance of a helicopter transport unit, it will be possible to land roughly 600 additional infantry and their equipment and supplies.

The next section explores the limitations on the JGSDF in operating against maritime gray zone coercion or armed conflict in the Nansei Islands.

The Limitations of the Japan Ground Self-Defense Forces

In considering the deployment of the JGSDF to the Nansei Islands, several factors need to be kept in mind. If the demands of responding to the landing of armed fishermen in the Senkaku Islands exceed the abilities of the JCG to respond effectively, the JGSDF will act as a reserve force. In such a situation, JGSDF units will provide the capabilities necessary to arrest or, if necessary, eliminate the invading foreign personnel (whether fishermen, maritime law enforcement personnel, or other paramilitary forces). Should foreign forces seize Japanese

[13] Ministry of Defense of Japan, "National Defense Program Guidelines for FY 2014 and Beyond," provisional translation, December 17, 2013c; Ministry of Defense of Japan, "Medium Term Defense Program (FY2014-FY2018)," provisional translation, December 17, 2013b.

territory, such as the Senkakus, Japan will first turn to its own forces to respond and will draw on the U.S.-Japan alliance only as necessary and appropriate.[14] While it would not be easy, retaking the Senkaku Islands is certainly possible for Japan to accomplish even after an outright invasion. For landings of armed fishermen or other foreign forces in areas other than the Senkaku Islands, Japanese civilian law enforcement personnel, supported if necessary by JGSDF transport helicopter units and amphibious assault brigade units, should be sufficient to mount an effective response.

Given the presence of deployed JGSDF forces, together with the standing up of an amphibious assault brigade, an adversary looking to invade an important area of the Nansei Islands (for example, Miyakojima) must be able to mobilize 3,000–10,000 amphibious troops or more to overcome the advantages of dug-in defenders. The size of the invading units as measured by vessel volume will be about 60,000–200,000 tons, which represents a substantial set of logistical and lift requirements for the invading side. If the deployment of a rapid-reaction regiment to the Nansei Islands can be completed before enemy forces arrive, the level of invading troops required by the adversary will be even greater. Unless the deployed JGSDF units' ASCMs are completely destroyed by the adversary, enemy ships will not be able to pass safely through Miyako Strait or Tokara Channel.[15]

Nonetheless, there are some limitations and challenges facing the JGSDF in deploying to the Nansei Islands. The first is the need to ensure a continuous resupply chain to the embarked forces and the need to securely transport the amphibious assault brigade and reinforcement units. To ensure that it achieves these lifelines and reinforcements, the JGSDF will rely on its brothers and sisters in the JMSDF and the JASDF. In the case of a more substantial and sustained conflict, the JGSDF also might draw on the assistance of the U.S. Navy and U.S. Air Force.

Second, due to the fact that the Nansei Islands are mostly inhabited, the JGSDF will need to be mindful and exercise protection over the civilian population on the islands. This will mean ensuring a ready supply of commodities: While the JGSDF might be able to hold out a long time under difficult conditions, it would probably be extremely difficult for civilians there to endure a long-term blockade that prevented resupply of critical commodities and foodstuffs, and it may prove politically impossible for the GOJ to sustain a war effort if the local population is experiencing unbearable suffering. Assisting the population of such islands in the event of a blockade is beyond the scope of the JGSDF's capabilities. The GOJ and local governments are responsible for civilian life and safety and will need to prepare for such eventualities.

Third, because the amphibious assault brigade is only around 3,400 members in total, it may need to be substantially expanded if the JGSDF wants to retake islands that have been occupied.

[14] Japan's response would be to turn to the JCG first. If the JCG is overwhelmed, the JSDF would be brought in, operating under a Maritime Security Order.

[15] In the author's experience, a modern army division with roughly 15,000 personnel requires around 300,000 tons in vessel volume for sea-lift. Historically, war planners have tended to employ a manpower requirement ratio of between three and five to one (3-5: 1) for offensive forces to overcome dug-in defenders.

Based on historic ratios required for offensive forces to overcome dug-in defenders, the current JGSDF amphibious assault brigade would be estimated to be capable of dislodging and defeating a hostile unit of only about one battalion size (around 600 troops) or less on its own.[16]

Despite the strengths of the Japanese government's current defense plans, there are some problems. The first is the small size of the forces envisioned for garrisoning the relatively remote and vulnerable islands of the Nansei Island chain. At the present planned scale of approximately 500–800 personnel, the JGSDF deployments can function effectively only if Japan retains maritime and air supremacy. However, in the event that maritime and air supremacy are lost to China, Japan's ground forces would need to be much more substantial in order to continue resisting without sister services' support for an extended period. At a minimum, the JGSDF would likely need a force size closer to that of a combined arms brigade (about 2,500 to 3,000 people), or three to four times the size currently envisioned. A larger force of this size would pose greater requirements on the invading units that China would need to prepare, which would have to grow to about 20,000–22,000 personnel. At that size, the invasion forces required would be about half the total size of the PLA's amphibious battle units and would require more than 400,000 tons of lift capacity.[17] At such a size, it would be extremely difficult for the PLA to conduct a surprise attack operation, and the costs and logistical train that transportation of this many units of this size would require would impose a serious burden, potentially deterring attack.

Another problem with the current Japanese defense plans for the Nansei Islands is that they lack the artillery fire support that the JGSDF units and amphibious assault brigade require. At present, these units are only equipped with short-range mortars. This means it is impossible for units 170 kilometers away in Ishigakijima to support any unit that is operating in the Senkaku Islands. Improvements to the integrated operational capabilities of the JGSDF to utilize the firepower of the JMSDF and the JASDF are important. So, too, are procurement of attack helicopters and systems enabling accurate long-distance fire support, including radars, multiple-launch rocket systems, and surface-to-surface missiles.

Finally, the current transport helicopter unit and the planned incorporation of 17 V-22 Ospreys must be expanded because the JGSDF needs to own sufficient means of rapidly transporting its forces across this very wide theater.

The next section looks at Japan's view of the role of the U.S.-Japan alliance in deterring and defeating maritime gray zone coercion in the Nansei Island chain.

[16] Author's estimate based on personal military experience.

[17] Figures in this paragraph are derived from author's estimate based on personal military experience.

The U.S.-Japan Alliance: An Indispensable Partnership for Peace

Through the framework of the U.S.-Japan alliance, the JGSDF, the U.S. Army, and the U.S. Marine Corps have built up exchanges, cooperation, and support for nearly six decades, laying down a firm foundation for the alliance. The U.S. Army does not deploy active combat units in Japan, but the Marine Corps does, including in Okinawa. In addition, both the U.S. Army and the U.S. Marine Corps, through joint exercises and other exchanges, have been helping to train and strengthen the JGSDF's combat capability and improve the allies' joint operational capabilities.

In the future, the JGSDF, given its capability limitations, may need assistance from the U.S. Army and Marine Corps in a number of areas. While the JGSDF has the ability to handle the anticipated ground battle on the Nansei Islands by itself and can deal with the threat of enemy cruise missiles, it does not currently have good options for defending against adversaries' ballistic missile attacks. Also, as previously argued, its ability to retake islands is extremely limited; if not bolstered indigenously through a further expansion of planned force posture improvements, it might require outside assistance in a contingency of anything more than a few hundred opposing forces occupying a Japanese island.

The U.S. Army's force protection capabilities through superior missile defense capabilities of the U.S. Air Force and Marine Corps on Okinawa will likely complement Japan's own missile defense capabilities and contribute to maritime and air supremacy. To bolster the missile defenses of its vulnerable Nansei Islands, Japan should encourage the United States to consider the urgent deployment of Patriot and Terminal High-Altitude Aerial Defense (THAAD) batteries to the Nansei Islands.[18]

As for the U.S. Marines, through regular and realistic joint exercises by U.S. and Japanese amphibious troops, the JGSDF and the Marine Corps can demonstrate to China that even if it is able to temporarily occupy one or more of the Nansei Islands, it will ultimately be ousted. If occupation of the islands should occur, the JGSDF and the U.S. Marine Corps will be thoroughly prepared to carry out an island-retaking operation shoulder-to-shoulder.

Conclusion

With its current capabilities, and in tandem with the Japanese police and the JCG, the JGSDF can deter—or, if necessary, defeat—most Chinese attempts at gray zone coercion in the Nansei (Ryukyu) Islands. Additionally, in response to an outright invasion, the JGSDF can create an environment in which the invading forces have to pay extremely high costs and may fail to

[18] Since the completion of this report, Japan has announced plans to enhance its missile defenses by procuring the Lockheed Martin–produced midcourse interceptor system Aegis Ashore, which employs the Raytheon Standard Missile-3 that Japan has worked on in a codevelopment and production agreement with the United States. See Elizabeth Shim, "Japan to Install Land-Based Missile Defense Aegis Ashore," *UPI*, August 17, 2017. For more on the history of U.S.-Japan missile defense cooperation, see Michael D. Swaine, Rachel M. Swanger, and Takashi Kawakami, *Japan and Ballistic Missile Defense*, Santa Monica, Calif.: RAND Corporation, MR-1374-CAPP, 2001.

achieve their objectives. Yet, due to the difficult character of possible sea-air-land warfare in an environment that is in close proximity to the Japanese residents who live in the Nansei Islands, several challenges would exist for the JGSDF, perhaps foremost among them helping to ensure that it is able to sustain operations and public support in the face of a possible blockade. Considering the current preparation of civil defense in islands, the period of time that the GOJ, including JGSDF, might be able to maintain the full capacity to resist is limited. There are a few things that the U.S.-Japan alliance should do to strengthen its ability to deter and respond to Chinese maritime gray zone coercion attempts and contingencies on the higher end of the conflict ladder.

On the Japanese side, Japan should strengthen its ability to respond independently, practice and prepare for quickly evacuating residents on islands in an imminent conflict situation, and improve civil defense stockpiles of critical commodities. The residents and local government currently maintain about a one-month stockpile of water, foodstuffs, medicines, and other critical items for the preparation of typhoon season. This is probably insufficient for the civil defense in the Nansei Islands. Establishing civil defense national stockpiles is required to augment the private and local government stockpiles. In total, two months' reserve is necessary and practical to manage the situation in accordance with emergency evacuation of the residents.[19] For its part, with its superior national intelligence capabilities, the United States must provide early warning information about the urgency of a situation and cooperate closely with the JASDF and JMSDF to ensure that the allies retain air and maritime supremacy. In particular, the United States has the ability, which Japan does not, to conduct attacks on long-distance strategic targets in China (sea ports of debarkation, air bases, etc.) that would need to be neutralized in a drawn-out or higher-intensity conflict, making U.S. support absolutely necessary in such situations.

Furthermore, in the case of a conflict over one or more of the Nansei Islands, the situation on the islands where conflict is actively ongoing could worsen rapidly because of the interruption of supplies, so the emergency deployment of reinforcement units should be executed as quickly as possible. Full capacity support within two months from the occurrence of the situation is necessary.

A robust Japanese defense posture in the Nansei Islands, backed up by the unmatched power of the U.S.-Japan alliance, will severely complicate any strategic calculations by China that it can seize Japanese territory on the cheap using either gray zone coercion or low-cost conventional military operations. Further strengthening Japanese defenses, continued commitment by the United States to deploy its most advanced defense capabilities to the Asia-Pacific region, and an increasingly operationally well-coordinated U.S.-Japan alliance will have a substantial effect on shaping China's strategic behavior and ensuring the continuation of peace in East Asia.

[19] Estimate of two-month reserves requirement is based on author's personal professional military experience and *in situ* research on Miyakojima Island.

3. A Japanese Perspective on the Role of the U.S.-Japan Alliance in Deterring—or, If Necessary, Defeating—Maritime Gray Zone Coercion

Junichi Fukuda
Visiting Fellow
Institute for International Policy Studies

This paper describes how the U.S.-Japan alliance can deter security challenges from China in the maritime domain that fall below the threshold of a legally defined armed attack. Generally speaking, as long as an adversary's actions do not cross the threshold of armed attack, a determined challenger can incrementally challenge or undermine the existing status quo without escalating the conflict to a level that will provoke an armed response.[1] Such challenges are generally said to fall in the *gray zone* (or are said to employ gray zone tactics) because they are neither genuine peacetime situations nor clear-cut instances of armed conflict.

China is notorious for using such gray zone (sometimes also called *salami-slicing* or *cabbage-leaf*) tactics to advance its interests in the maritime issues of both the East China Sea and the South China Sea. For China, the use of gray zone tactics is beneficial because it enables China to challenge the existing status quo without employing the coercive methods (and provoking U.S. intervention), thus presenting a less-threatening public image. Such approaches permit China to maintain both quantitative and qualitative superiority by leveraging its maritime law enforcement (MLE) capabilities, as well as its civilian fishing fleet, all while keeping the PLA in reserve in case substantial escalation occurs.

Unfortunately, the U.S.-Japan alliance has not developed a sufficiently sophisticated set of tailored deterrence options to deter or defeat such Chinese gray zone tactics.[2] The U.S.-Japan alliance is (or at least, has been) designed to take coordinated action against legally defined instances of armed attack, something that Chinese military strategists understand well and are seeking to exploit. Article 5 of the alliance treaty prescribes the obligation of collective defense in the case of "armed attack against either party in the territories under the administration of Japan."[3] In the absence of an armed attack, Japan and the United States cannot effectively coordinate their actions to counter Chinese gray zone tactics. Additionally, aside from the formal

[1] For a good review of the problem of gray zone challenges, see Mazarr, 2015.

[2] For more on the concept of tailored deterrence, see Brad Roberts, "Tailored Options to Deter North Korea and WMD Threats," *Korean Journal of Defense Analysis*, Vol. 28, No. 1, March 2016.

[3] Ministry of Foreign Affairs of Japan and U.S. Department of State, 1960.

treaty provisions, the alliance similarly lacks an obvious means to enable the kinds of defense cooperation necessary to maintain the status quo in the South China Sea, despite the increasing need to do so.

Although U.S.-Japan peacetime cooperation has been significantly enhanced by the recent revision of the Guidelines for U.S.-Japan defense cooperation (as well as Japan's related reform of its security policies) in 2015, the alliance still has substantial room to adopt further measures designed to frustrate China's gray zone tactics. This chapter explores some possible options or strategies for the alliance focused on deterring—or, if necessary, defeating—China's efforts to pursue gray zone coercion in the maritime domain.

Examples of China's Gray Zone Tactics in the Maritime Domain

As a starting point, it is useful to present an overview of China's maritime gray zone tactics in the East and South China Seas. China started to emphasize its maritime claims in these bodies of water more than 30 years ago. Soon after Deng Xiaoping started the economic reform of China in the late 1970s, Admiral Liu Huaqing advocated the idea of "island chains" as benchmarks for the development of the PLA Navy.[4] As China's economy developed during the 1990s and 2000s, China's maritime interests also expanded. China similarly developed its military and paramilitary capabilities, so that it could take assertive and even forceful actions to protect its maritime interests. In 1992, China enacted the Law of the People's Republic of China on the Territorial Sea and the Contiguous Zone,[5] which included China's claims to sovereignty over the Senkaku Islands and the "nine-dash line" in the South China Sea. After the global financial crisis of 2007–2008, China's leaders appear to have concluded that they were confronting a strategic opportunity to rapidly expand influence in the Asia-Pacific region. Accordingly, from approximately the end of 2008, China's behavior in the East and South China Seas has become much more assertive.

In the East China Sea, for example, China began to pressure Japan on the issue of the Senkaku Islands. The earliest sign of this new, more assertive approach came in the form of the first intrusion by China's official MLE vessels into the territorial seas of the Senkaku Islands in December 2008. Subsequently, in September 2010, China fiercely clashed with Japan after the JCG arrested a drunken Chinese fisherman who twice deliberately rammed JCG vessels patrolling around the Senkaku Islands.[6] In September 2012, after the GOJ decided to acquire the property rights of some of the Senkaku Islands from a private Japanese owner, China

[4] On Chinese views of the Pacific Island "chains," see Andrew S. Erickson and Joel Wuthnow, "Barriers, Springboards, and Benchmarks: China Conceptualizes the Pacific 'Island Chains,'" *China Quarterly*, 2016.

[5] Standing Committee of the Seventh National People's Congress, 1992.

[6] Michael Green, Kathleen Hicks, Zack Cooper, John Schaus, and Jake Douglas, *Countering Coercion in Maritime Asia: The Theory and Practice of Gray Zone Deterrence*, Washington, D.C.: Center for Strategic and International Studies, May 2017, p. 72.

commenced daily intrusions by its official MLE vessels into the territorial seas and contiguous zones around the Senkaku Islands.[7] These intrusions have continued through today. China also moved away from describing its official ties with Japan as a "mutually beneficial relationship based on common strategic interests" and instead moved to unilaterally develop the seabed natural resources located near the line that is geographically equidistant between Japan and China in the East China Sea.[8] These recent actions starkly contrast with Chinese actions before 2008 in regard to its unilateral stance and assertiveness.

According to records kept by the JCG, Chinese official MLE vessels intruded into the territorial sea of the Senkaku Islands 569 times between December 2008 and December 2016, and the number of total intrusions into the contiguous zone during the same period is even larger: 3,497.[9] To make matters worse, China's challenge has been escalating. Despite an improving overall relationship in the wake of the "four areas of common ground" that Tokyo and Beijing agreed upon in November 2014, China has escalated its provocative maritime behavior since that time. For example, PLA Navy vessels intruded into the territorial sea of the Senkaku Islands for the first time in June 2016. Shortly thereafter, in August 2016, China suddenly deployed a large number of fishing and official MLE vessels around the Senkaku Islands. At the time, a total of 15 Chinese MLE vessels entered the contiguous zone around the Senkaku Islands at once, accompanied by 200–300 fishing vessels (some or all of which may have been operated by China's maritime militia). After this incident, China clearly escalated its challenge by increasing the number of MLE vessels that intrude in Japan's territorial seas from an average of three per month to four. Such gradual escalation by China using its MLE vessels is a typical form of Chinese gray zone tactics.

The shifting strategic balance in terms of the number (and quality) of MLE vessels in recent years clearly favors China. According to one GOJ estimate, the number of China's large MLE vessels (ships weighing more than 1,000 tons) has rapidly increased—from 40 in 2012 to 63 in 2014, 120 in 2015, and estimated to reach 135 by 2019.[10] The number of Japan's vessels of the

[7] Certain parts of the Senkaku Islands (Uotsuri, Kitakojima, and Minamikojima Islands) had been previously owned by the private owner in Japan. In April 2012, then-Tokyo governor Shintaro Ishihara declared that the Government of Tokyo would buy these islands from their private owner. Ishihara intended to build facilities on the islands in order to strengthen Japan's claims of sovereignty. However, this prospect alarmed the Noda administration because the construction of such facilities without proper diplomatic consideration would severely damage the relationship with China. To avoid this possible conflict, the GOJ decided to obtain the property rights of these islands from the private owner, precluding their purchase by the Government of Tokyo. The property rights of the acquired islands were then transferred to the GOJ on September 11, 2012. See Green et. al., 2017, pp. 124–147.

[8] In June 2008, Japan and China agreed to cooperate on the development of natural resources in the East China Sea. After that, China started to develop the natural resources unilaterally, in violation of this agreement, on the China side of the geographical equidistant line. Since the EEZ and the continental shelf in the East China Sea have not been delimited yet, Japan has protested this unilateral development by China.

[9] Ministry of Foreign Affairs of Japan, "Trends in Chinese Government and Other Vessels in the Waters Surrounding the Senkaku Islands, and Japan's Response," web page, November 2, 2016.

[10] Cabinet Secretariat, "Policy on Strengthening Coast Security System" (in Japanese), December 21, 2016, p. 17.

same size was 54 in 2014, was 62 in 2015, and is expected to be 65 in 2019.[11] Obviously, Japan will be outpaced by China in such an "arms race" of MLE capabilities. China seems inclined to intensify its gray zone tactics in accordance with this favorable strategic trend.

China has also been employing gray zone tactics in the South China Sea. Although China's "nine-dash line" claim dates back to the Republic of China's promulgation of a map with this claim in 1947, China renewed its claims in its submission to the Commission on the Limits of the Continental Shelf in May 2009.[12] This Chinese action prompted counteractions from the United States and other regional states in regard to the interpretation of international maritime law and the freedom of navigation in the South China Sea in July 2010. In particular, China's interpretation of the United Nations Convention on the Law of the Sea (UNCLOS) was regarded as different from the ordinary interpretation of other states in regard to the freedom of navigation of other states' naval vessels within China's claimed EEZ.[13] China's insistence on its self-proclaimed "nine-dash line," coupled with its interpretation of UNCLOS as restraining the freedom of navigation of other states' military vessels in their claimed EEZ waters, sparked fears of tension in the South China Sea.

Subsequently, China used gray zone tactics to take over Scarborough Shoal from the Philippines in 2012. China's MLE vessels were dispatched to the Shoal when a Filipino naval vessel seized Chinese fishing boats operating near the Shoal. The vessels of the two states confronted each other from April to July 2012 at the Shoal. China used various tactics to pressure the Philippines to back down, including cyberattacks, imposition of strict regulations on its import of bananas, suspension of tours to the Philippines, and a unilateral ban on fishing in the South China Sea, among other steps. These tactics were components of China's overall gray zone strategy to expand its control over key portions of the South China Sea. Ultimately, the Philippines backed down and withdrew its vessels from the Shoal, which has been occupied by China ever since.

Another major example of China's gray zone tactics is China's large-scale land reclamation in the Spratly Islands.[14] From 2014, China reclaimed large areas of the features in the Spratly

[11] Cabinet Secretariat, 2016.

[12] Division for Ocean Affairs and the Law of the Sea, Commission on the Limits of the Continental Shelf, Outer Limits of the Continental Shelf Beyond 200 Nautical Miles from the Baselines: Submissions to the Commission: Submission by the People's Republic of China, New York, United Nations, May 7, 2009.

[13] In particular, China claims that foreign military activities can be regulated within the coastal state's EEZ, while the United States and other states claim such authority cannot be extended beyond the coastal state's territorial seas. Therefore, the United States maintains that U.S. military activities within China's EEZ are not prohibited by UNCLOS. However, China claims there is no sort of "military freedom of navigation" in the coastal states' EEZs. See Ronald O'Rourke, *Maritime Territorial and Exclusive Economic Zone (EEZ) Disputes Involving China: Issues for Congress*, Washington, D.C.: Congressional Research Service, June 6, 2017.

[14] In this regard, I categorize China's land reclamation in the South China Sea as a maritime gray zone challenge because it is intended to change the status quo (both the legal interpretation of international maritime law under the UNCLOS and the strategic balance of power in the region) by unilateral means without crossing the threshold of a legally defined armed attack. Constructing artificial islands unilaterally in an area under dispute is regarded as

Islands that it occupies, despite widespread international criticism. By the second half of 2015, China had almost completed reclamation activities across the seven features it controls. Among these features, the most important efforts were made at Fiery Cross Reef, Subi Reef, and Mischief Reef. China has established large-scale military outposts, which include 3,000-meter runways and associated infrastructure, such as harbors, hangars, radars, power-generation facilities, and even close-in weapon systems and antiaircraft guns. China is widely believed to be considering announcement of an Air Defense Identification Zone in the South China Sea (as it did in the East China Sea in November 2013).[15] Despite the invalidation of China's "nine-dash line" claims by the award of PCA in July 2016,[16] China seems to have accomplished its strategic objectives by (almost) completing the reclamation and militarization of these features and outposts.

In both the East China Sea and the South China Sea, China has used gray zone tactics to incrementally challenge the existing status quo. Unfortunately, so far, the surrounding states, including Japan and the United States, have failed to stop it. Without crossing the threshold of a legally defined armed attack, China has carefully but steadily probed the acceptable limits of its rivals and successfully changed the status quo more to China's own favor. This is why it is important for Japan and the United States to focus on the issue of gray zone challenges.

China's Gray Zone Tactics as an Issue of Deterrence and Escalation Control

China's maritime gray zone tactics are incrementally challenging the existing status quo. To defend the status quo, the United States, Japan, and other states need to confront China by taking appropriate countermeasures, which means first deterring gray zone coercion if possible and then controlling escalation if deterrence efforts fail. This section describes the core elements of the concepts of deterrence and escalation control and lays out how they contribute to the notion of a long-term competitive strategy.

unlawful and further aggravates tensions with other claimants, in addition to violating China's commitments to the Association of Southeast Asian Nations (ASEAN) under a 2002 declaration. (See ASEAN, Declaration on the Conduct of Parties in the South China Sea, Phnom Penh, Cambodia, November 4, 2002.) Harming the maritime environment violates China's obligation to protect the ecosystem of the South China Sea, and China's reclamation effort clearly challenges the legal interpretation of international maritime law. Regarding the strategic balance of power in the region, China's construction of military facilities on the reclaimed features is also a problem. China promised not to militarize the features at the U.S.-China summit in September 2015 but has nonetheless proceeded to construct military facilities that can be used both in peacetime and wartime and are clearly intended to change the strategic balance of power in the region.

[15] For example, Chinese Vice Foreign Minister Liu Zhenmin stated on July 13, 2016, that Beijing could declare an Air Defense Identification Zone over the South China Sea if it felt threatened. "Beijing Says It Could Declare ADIZ over South China Sea," *Japan Times,* July 13, 2016.

[16] Permanent Court of Arbitration, "PCA Press Release: The South China Sea Arbitration (The Republic of the Philippines v. The People's Republic of China)," July 12, 2016.

First of all, *deterrence* is defined as "deliberate attempts to manipulate the behavior of others through conditional threats."[17] A challenger—in this case, China—seeks to undercut the status quo by employing coercive methods to make the situation more preferable to itself. The defender attempts to block it by employing counteractions to the challenger. Generally, a number of conditions must be satisfied to make deterrence successful.[18] First, the challenger must be rational. Second, the defender must credibly signal its intention to deter the challenger. Third, deterrence must be accompanied by a corresponding "assurance" that if the opponent refrains from undertaking a particular action, then punishment will be averted; another way to put this is that any attempt at deterrence must be conditional, with the target state ultimately having to choose whether to risk the possibility of the threatened punishment.

However, focusing on the concept of deterrence alone is not enough. Stopping China's challenge requires a continuous effort from peacetime to wartime, and the U.S.-Japan alliance needs to be able to present China with unacceptable costs at all levels of escalation and in a continuous, seamless manner if the allies wish to deter Chinese coercion attempts. This requirement puts the focus on the concept of "escalation control." Herman Kahn, a famous strategist of the 1960s and 1970s, simply defined *escalation* as "competition in risk-taking."[19] A nation might have many motivations to escalate a conflict. But a nation also has motivations to control escalation. Avoidance of unintended risk and subsequent loss of strategic interest is a primary concern for nations in a conflict. Thus, if *deterrence* aims to prevent a conflict from occurring, *escalation control* refers to attempts by the parties to a conflict to seek the ability to limit further increases in the costs and violence associated with conflict that has already commenced.

Traditionally, the argument of escalation control was debated in the context of nuclear limited war.[20] Today, the U.S.-Japan alliance needs to focus more on gray zone challenges that stay below the level of a legally defined armed attack. At the same time, however, a possible escalation to the level of an outright armed attack must also be considered. China is likely to back up its MLE capabilities with the PLA, so it is important to think through issues of escalation control across instances of both gray zone coercion and armed attack contingencies.

Figure 3.1 is a simple illustration of this interconnection. The vertical axis shows a degree of challenge from which China can select. The horizontal axis shows a passage of time. At the middle of the vertical axis, there is a threshold for challenges that rise above and sink below the

[17] Lawrence Freedman, *Deterrence*, Malden, Mass.: Polity Press, 2004, p. 6.

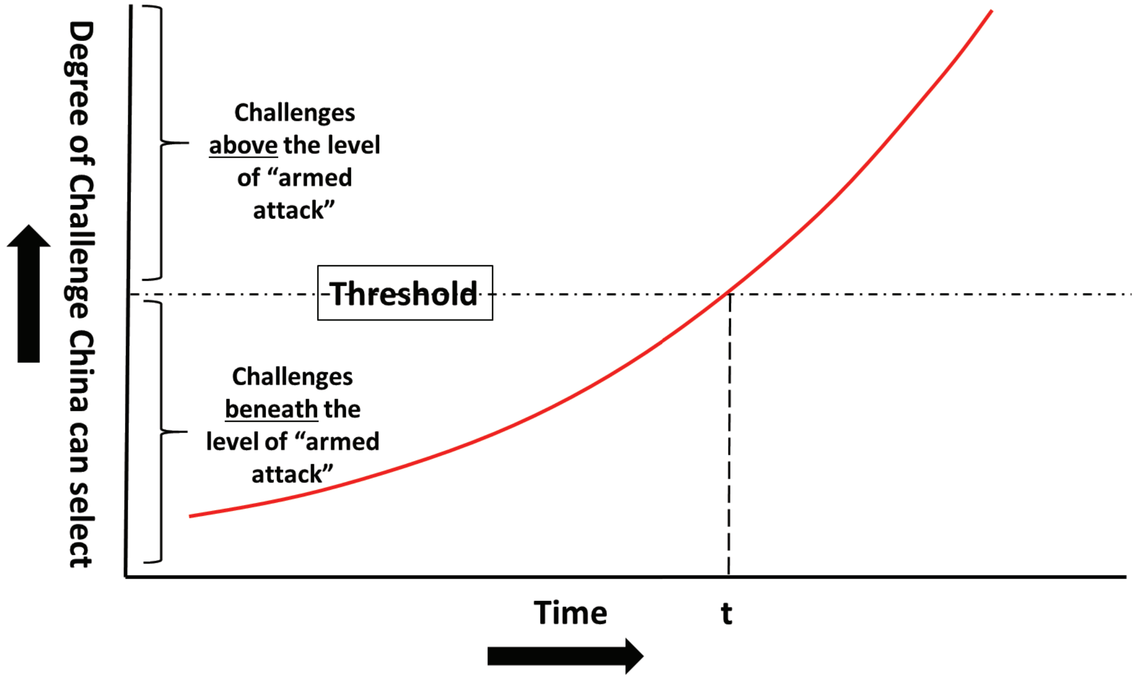
[18] For general arguments on deterrence, see Thomas C. Shelling, *Arms and Influence*, New Haven, Conn.: Yale University Press, 1966.

[19] Herman Kahn, *On Escalation: Metaphors and Scenarios*, New York: Frederick A. Praeger, 1965, p. 3.

[20] The credibility problem of the "massive retaliation" doctrine of the Eisenhower administration led to debates over the concept of "limited" nuclear war in the late 1950s and later to the debate over the "flexible response" strategy. Henry A. Kissinger, *Nuclear Weapons and Foreign Policy*, New York: Harper and Brothers, 1957; Lawrence Freedman, *The Evolution of Nuclear Strategy,* 3rd ed., New York: Palgrave MacMillan, 2003, pp. 89–113.

level of a legally defined armed attack (i.e., gray zone challenges). Since China is expanding its "comprehensive national power" relative to the region, the coercive toolkit from which China can select policy options is expanding over time.[21]

Figure 3.1. Links Between China's Gray Zone Tactics and Armed Attack Challenges


Degree of Challenge China can select
Challenges above the level of "armed attack"
Threshold
Challenges beneath the level of "armed attack"
Time
t

NOTE: Author's conceptualization.

So far, China has kept its challenges below the level of an armed attack. China appears not to be confident enough in its ability to manage the consequences of a conflict were it to escalate to the level of an armed clash with the United States and Japan. Such a conflict could lead to China's political and military defeat, and for this reason, it has chosen to adopt gray zone challenges as the means of undermining the status quo.

[21] Of course, there are some fundamental assumptions in Figures 3.1 and 3.2. China is assumed to be a revisionist power and continuously increasing its relative strength in the region. China's growth rate of coercive power is assumed to be higher than that of Japan and the United States, and thus the curve of the line bends upward over time as China's advantages over the United States and Japan permit it to select higher-order military challenges (i.e., time is assumed to be on China's side). Japan and the United States are assumed to be status-quo powers and not to make any compromise with China in the future. Therefore, the fundamental relationship with China is assumed to be conflictual. If these assumptions are incorrect, the argument turns out differently. If China becomes a status-quo power in the future, then the fundamental source of conflict will dissipate. Even if China remains a revisionist power but its growth stagnates, then the degree of China's challenge also will be lessened. Moreover, if Japan and the United States compromise with China, then China may lessen the degree of challenge, at least temporarily. Every outcome will depend on the assumptions.

However, if China's comprehensive national power continues to grow as time passes, this situation will likely change. The relative growth of China's economic and military power, especially if coupled with a declining commitment of U.S. forces in the Asia-Pacific region, may lead China to have greater confidence in its ability to challenge the status quo through force without suffering unacceptable consequences. China could eventually gain enough confidence that it might feel free to alter the status quo by executing an armed attack, something it has already done in the past in the cases of the Paracel Islands in 1974 and the Spratly Islands in 1988.

Many factors might shape China's thinking about such matters. First, China might become confident that the PLA has acquired the capability to deny U.S. forces access to the region through the employment of a robust suite of A2/AD capabilities, including ballistic and cruise missiles, sea mines, submarines and advanced surface ships, fighters and bombers, cyberwarfare, electronic warfare, and ASAT assets. Second, China might reach the conclusion—correctly or not—that the United States will not intervene in any conflict with China because of problems associated with U.S. domestic politics and a growing reluctance on the part of the American people to continue paying the costs to support U.S. military commitments in the Asia-Pacific region.

Regardless of what factors might shape such a change, it is important to recognize the interconnection between the gray zone and armed-attack challenges, two of which are particularly worth noting. First, in order to prevent escalation in the level of armed conflict, the U.S.-Japan alliance needs to maintain military superiority (both conventional and nuclear). Second, even if the allies succeed in preventing armed conflict, they will still face the possibility of increasingly intense gray zone challenges from China. Indeed, such gray zone challenges may become even more frequent; it is possible that the stability at the higher end of the escalation ladder (above the threshold of armed attack) may have a counterintuitive effect on the lower ends of escalation (below the threshold of armed attack), leading a determined challenger like China to resort to gray zone coercion out of frustration with its inability to do more above the threshold. This is an application to the gray zone phenomenon of a concept derived from studies of the links between the nuclear and conventional realms typically described as the "stability-instability paradox."[22]

Thus, Japan and the United States must strengthen two different sets of capabilities at the same time. First, the nations have to strengthen their military capabilities in order to prevent tensions from escalating to the level of armed conflict. However, maintaining escalation dominance above the level of armed conflict is not enough. Second, the nations must strengthen

[22] This paradox refers to a counterintuitive situation that a risk of escalation at the lower end of a conflict increases because of stability at the higher end. It was traditionally argued in the context of nuclear deterrence. For example, stability at the strategic (nuclear) level may lead to instability at the conventional (or lower) level. See Glenn Snyder, "The Balance of Power and the Balance of Terror," in Paul Seabury, ed., *The Balance of Power*, San Francisco, Calif.: Chandler, 1965.

their capabilities to respond to China's gray zone challenges. As long as Japan and the United States maintain escalation dominance at higher ends of the escalation ladder but appear incapable of responding effectively to challenges below that threshold, China will be incentivized to put more efforts into gray zone challenges that are designed to undercut the status quo at its roots. This makes it necessary for Japan and the United States to have the capacity to respond both to China's possible armed attack and to China's gray zone challenges at the same time.

Countering China's Challenges Through a Competitive Strategy

The argument in the previous section suggested that the U.S.-Japan alliance needs to strengthen its conventional and nuclear military capabilities, especially counter-A2/AD capabilities, in order to confine China's challenge below the level of an armed attack. In this respect, having a credible military deterrence posture is essential for Japan and the United States. However, deterring only an armed attack from China may not stabilize the situation. The allies also need capabilities and counters to China's gray zone challenges because China will likely intensify its efforts at gray zone coercion. This section and the next one explore countermeasures to China's challenges through the use of a competitive strategy.

The idea of competitive strategies has attracted substantial attention in recent years among strategists in the United States and its Asian allies, including Japan.[23] Broadly defined, a *competitive strategy* is a long-term strategy by which a state aims to gain an advantage over its challengers. The idea was used by the United States to counter the challenges from the Soviet Union during the 1970s and 1980s. The same idea seems applicable to the current situation in maritime Asia in the contexts of both gray zone coercion and armed attacks by China.

Properly understood, a competitive strategy is composed of several components, including efforts at denial, cost-imposition, attacking the enemy's strategy, and attacking the enemy's political system.[24] A *denial* strategy is primarily a military (or coercive) concept that mainly deals with the issues of actual conflict, whereas a *cost-imposing* strategy is mainly employed during peacetime, although it does not exclude the application in militarized situations.

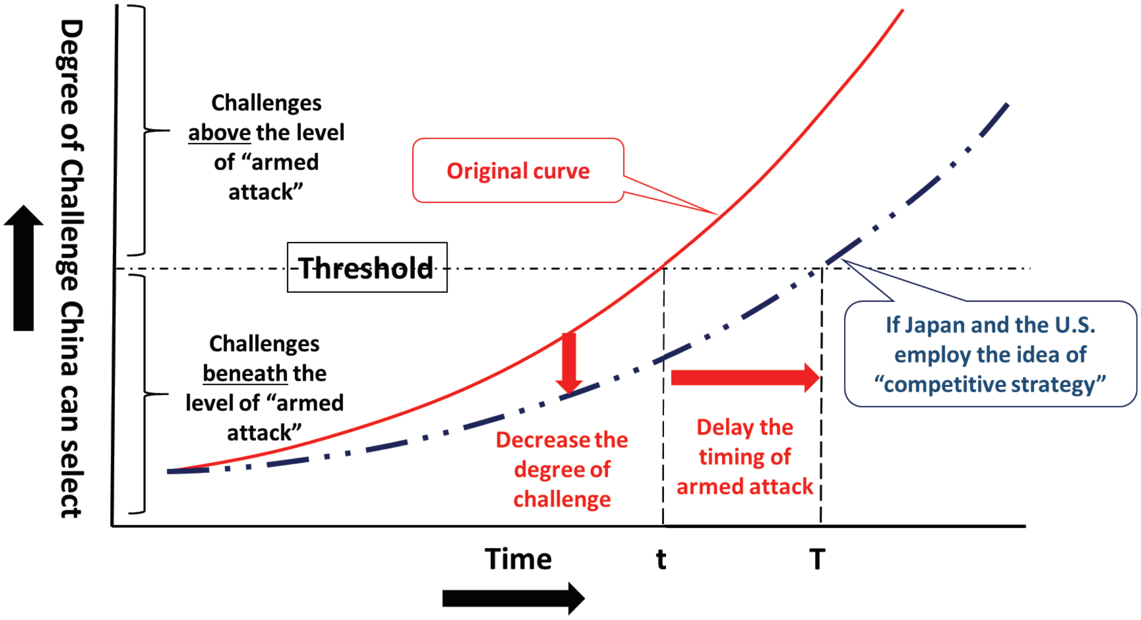
Figure 3.2 illustrates the notional effects of a successful competitive strategy if employed by Japan and the United States against China; when effectively utilized, the original curve of Figure 3.1 will move downward and to the right (i.e., later in time). This means China would be less confident about challenging the status quo through armed conflict and would be incentivized to avoid escalation for a substantially longer period. Assuming that this model is correct, it is

[23] See Thomas G. Mahnken, ed., *Competitive Strategies for the 21st Century: Theory, History, and Practice*, Palo Alto, Calif.: Stanford University Press, 2012; and Thomas G. Mahnken, *Cost-Imposing Strategies: A Brief Primer,* Washington, D.C.: Center for a New American Security, November 2014. Regarding the specific applications to the challenges from China by Japan's perspective, see Fukuda, 2015.

[24] Bradford Lee, "Strategic Interaction: Theory and History for Practitioners," in Mahnken, 2012.

strongly advisable for Japan and the United States to employ the concept of a competitive strategy to confine China's challenge below the threshold of armed attack as long as possible.

Figure 3.2. Modeling the Effects of a Successful U.S.-Japan Competitive Strategy on China's Choices to Initiate Gray Zone Coercion or Armed Conflict


Degree of Challenge China can select
Challenges above the level of "armed attack"
Original curve
Threshold
Challenges beneath the level of "armed attack"
If Japan and the U.S. employ the idea of "competitive strategy"
Decrease the degree of challenge
Delay the timing of armed attack
Time
t
T

NOTE: Author's conceptualization.

However, it is also important to recognize that a competitive strategy may only delay the timing of armed attack from China. Absent a change in Chinese decisionmakers' end goals and given enough time to grow its national power, China may eventually reach a point where it either successfully erodes the foundations of the allies' deterrent posture or amasses enough power to absorb the losses that the allies threaten to impose. For this reason, Japan and the United States need to continue modernizing their military capabilities, operational concepts, and diplomatic postures while also developing ways to defeat lower-level coercion in maritime gray zone contingencies.

Specific Countermeasures to China's Gray Zone Tactics

It is absolutely necessary for Japan and the United States to prepare for armed conflict with China. However, it is also necessary to respond to China's increasing use of gray zone tactics. How should the allies respond to these challenges within the framework of a competitive strategy?

First of all, the concept of a denial strategy suggests that the United States and Japan need capabilities to block China's assertive actions on maritime issues. As demonstrated in the previous section, China uses its MLE capabilities to challenge the existing status quo. Therefore, Tokyo and Washington first need to build up their own MLE and naval capabilities to counter China's activities, especially those in the East China Sea. Japan has already invested a large amount of money to increase the numbers of its MLE vessels and JCG personnel. From FY 2012 to FY 2015, the JCG procured ten new PL (patrol vessel large) vessels in the 1,000+-ton class. Coupled with two existing PLH (patrol vessel large with helicopter) vessels (3,000+-ton class), these vessels formed a unit exclusively dedicated to coping with the situation in the Senkaku Islands. The overall size of the JCG has also expanded: As noted earlier, the number of MLE vessels weighing more than 1,000 tons has increased from 54 in 2014 to 62 in 2015 and is expected to rise to 65 in 2019.[25] In addition, the JCG's budget has increased: In FY 2012, the JCG had only ¥177.96 billion (US$1.58 billion); in FY 2016, it was expanded to ¥187.75 billion (US$1.67 billion); and for FY 2017, the JCG requested ¥204.59 billion (US$1.82 billion).[26] In accordance with this expansion, the number of personnel has also grown. In FY 2010, the JCG had only 12,636 personnel; by FY 2016, that number had climbed by nearly 1,000 to 13,626, and the JCG has requested permission to further increase hiring to 13,744 in FY 2017.[27]

Progress of these efforts is the main priority for Japan to cope with China's gray zone tactics. Japan should invest more money and resources to enhance its own MLE capabilities. Nevertheless, it is important to recognize that this effort alone cannot overturn the basic structure of Japan's relationship with China. Even with this expansion in personnel and budget, Japan's MLE capabilities will soon be quantitatively (and possibly qualitatively) inferior to that of China. Japan's increase in the number of MLE vessels only slows the growth in Chinese Coast Guard overmatch; it does not reverse that trend—China also built additional vessels during the same period. Building up Japan's MLE capabilities is only a first step to offset the superiority of China; such efforts must be supplemented by other initiatives.

Second, Japan needs to construct a seamless framework for cooperation between the JCG and the JMSDF. Sooner or later, Japan may face a situation where it needs to send JMSDF units to supplement the activities of the JCG in the course of dealing with an instance of maritime gray zone coercion initiated by China. This does not necessarily mean that Japan will enter into an armed conflict with China. Japan has legal frameworks for maritime security operations (MSOs) or public security operations (PSOs) that enable the JMSDF to act as a security unit to support JCG activities without crossing the threshold of an armed response (under which Japan would invoke the exercise of the individual right of self-defense).[28] Still, Japan should enhance the

[25] See the previous discussion of private ownership of the Senkaku Islands.

[26] Japan Coast Guard, "Outline of the Decision on the Budget Related to the Japan Coast Guard" (*Kaijo Hoancho Kankei Yosan Kettei Gaiyou*) (in Japanese), December 2011; December 2015; December 2016.

[27] Japan Coast Guard, "Outline of the Assessment of the FY2017 Fixed Number of Personnel Request" (*Heisei 29 nendo Teiin Youkyuu Satei no Gaiyou*) (in Japanese), 2017, p. 2.

[28] The MSO is the legal framework that allows the JSDF units to support the activities of the JCG to protect the public safety of maritime areas surrounding Japan (as stipulated in the Self-Defense Forces Act's Article 82). An

interoperability of the JCG and JMSDF and reform its procedures so as to accelerate the issuance of MSO or PSO orders.

These reforms are more easily said than done, of course. In practice, it will be extremely difficult to construct a truly seamless framework of cooperation between the JCG and the JMSDF because the roles and cultures of the Ministry of Land, Infrastructure and Transportation, which oversees the JCG, and the Ministry of Defense, which oversees the JSDF, are fundamentally different in Japan. For example, the role of the JCG is strictly separated from the role of such military organizations as the JSDF under the law establishing the JCG as an agency of the Ministry of Land, Infrastructure and Transportation. Although Article 80 of the Self-Defense Forces Act recognizes that the Ministry of Defense is supposed to control the activities of JCG units in the case of defense operations or PSOs,[29] Article 25 of the Japan Coast Guard Act prohibits the JCG from functioning as a military organization.[30] A literal reading of this would imply that JCG units will be allowed to carry out policing activities as if they were still operating in peacetime even though the situation is one of actual armed conflict. The clear separation of roles and functions between JCG and JMSDF units will likely hamper the effective coordination between them unless additional work is done to align the two organizations' understandings of possible contingencies and their roles in responding to these more closely.

Formulating an appropriate legal framework is also difficult. In 2015, the Abe administration enacted the new security legislation, which allows Japan to exercise the limited right of collective self-defense. At the same time, there were challenges to the administration's effort to develop an appropriate legal framework to seamlessly connect the activities of the JCG and the JMSDF. In the end, no new legal enactment regarding countermeasures to gray zone challenges was promulgated, only a cabinet decision designed to accelerate procedures for issuing MSO and PSO. The risk of inadvertent escalation resulting from early intervention by JMSDF units was also considered.[31] The limited progress on this issue suggests how difficult it is to achieve a truly seamless framework of cooperation between the JCG and the JMSDF. Nevertheless, Japan will likely need to make continued progress in this area if it wants to counter China's gray zone challenges.

MSO has been ordered three times in the past (in March 1999, in November 2004, and in January 2009). The PSO is the framework that allows JSDF units to support the activities of normal police agencies and the JCG to protect the public safety of Japan (as stipulated in the Self-Defense Forces Act's articles 78 and 81). To date, a PSO has never been ordered in Japan. While a PSO can theoretically be ordered in the circumstances of a maritime gray zone situation and gives wider legal authority to JSDF units to use weapons, the framework of the MSO is more likely to be used because the MSO is procedurally easier to initiate. Government of Japan, Self-Defense Forces Act, Law No. 165, 1954.

[29] Government of Japan, 1954.

[30] Government of Japan, Japan Coast Guard Act, Law No. 28, 1948.

[31] Intervention by JMSDF units under the framework of an MSO or a PSO does not indicate Japan's intention to escalate the situation; rather, it is simply the augmentation of the JCG's capability to manage the situation without crossing the threshold of an armed attack. However, China may not view this in the same way. Chinese policymakers and military officials may consider intervention by the JMSDF as a clear sign of escalation on Japan's side and may decide to send PLA Navy units to protect China's MLE vessels.

Third, Japan and the United States need to leverage the alliance framework to counter China's gray zone tactics. The recent revision of the Guidelines for U.S.-Japan Defense Cooperation has critical importance in this respect.[32] For example, the establishment of an ACM was an important development in the history of the alliance. Previously, the coordination mechanism was activated only after a contingency actually occurred; the ACM establishes a standing, permanent mechanism that enables Japan and the United States to coordinate policies even before a contingency occurs. This allows the alliance to counter any situation that may require an alliance response, including China's gray zone tactics. Another important development was an introduction of the concept of *Flexible Deterrent Options* (FDOs), which are defined as "preplanned, deterrence-oriented actions carefully tailored to send the right signal and influence an adversary's actions."[33] Examples of FDOs include increasing the readiness posture of forces already in place, initiating or increasing show-of-force actions, increasing training and exercise activities, and deploying forces into or near the potential operational area. In essence, FDOs allow Japan and the United States to respond as an alliance even when a given or prospective challenge remains below the threshold of a legally defined armed attack (i.e., when the challenge remains in the gray zone). By combining the ACM and FDOs, Japan and the United States can counter China's gray zone tactics more effectively.

However, it is important to note that these efforts were only initiated in April 2015 and are still being worked through. Before the revision of the Guidelines for defense cooperation, Japan and the United States did not even have options for bilateral planning of operations for the defense of the Senkaku Islands. Over the years, the alliance has been less enthusiastic about proceeding in this area. The revised Guidelines finally committed the two sides to "develop and update" their bilateral planning capabilities.[34] Japan and the United States cannot effectively coordinate their policies for counteracting Chinese gray zone coercion without the proper development of a bilateral mechanism for planning for armed conflict. Therefore, while the direction is positive, progress on the alliance cooperation and its overall deterrent effects should not be overrated at this early stage; Japan and the United States still need some time to fully develop the coordination of policies aimed at countering China's gray zone coercion.

Aside from these important innovations in the alliance, it is also important for Japan and the United States to utilize the network of U.S. alliances in the Asia-Pacific region. Enhanced trilateral cooperation with third countries, such as Australia or South Korea, is highly desirable. Regionwide cooperation among U.S. allies and partners and the U.S.-Japan alliance to counter China's gray zone tactics could include sustained ISR operations and improved maritime domain awareness; promotion of information exchanges and diplomatic coordination; and potentially

[32] U.S. Department of Defense and Government of Japan, Guidelines for U.S.-Japan Defense Cooperation, April 27, 2015.

[33] U.S. Joint Chiefs of Staff, *Joint Operation Planning*, Joint Publication 5-0, August 11, 2011, p. E-1.

[34] U.S. Department of Defense and Government of Japan, 2015.

joint patrols and exercises in international waters, especially those in the South and East China Seas. Although the JCG and JMSDF do not currently have enough vessels to take part in joint patrol operations in the South China Sea, Japan and the United States need to prepare future options to utilize the latent capabilities of alliance networks in the Asia-Pacific region.[35]

Fourth, in order to stop or delay unilateral changes to the status quo initiated by China in the South China Sea, Japan and the United States need to help regional states build up their MLE capabilities.[36] This effort is important because it will reinforce deterrence through denial, preventing China from changing the status quo on the cheap. The allies have already made significant efforts to achieve this objective. For example, Japan has taken steps to provide ten MLE vessels to the Philippines and six used MLE vessels to Vietnam. It has also committed to provide two large MLE vessels to the Philippines, six new MLE vessels to Vietnam, and two used large MLE vessels to Malaysia and decided to lend five JMSDF TC-90 training aircraft to the Philippines. The United States has provided three *Hamilton*-class (3,000+ ton) cutters to the Philippines and committed a large amount of financial support to the ASEAN states to enhance their MLE capabilities, including through the U.S. Department of Defense's Maritime Security Initiative. These capacity-building efforts are not limited to the provision of hardware; development among partner states has also been supported for software capabilities, including education and training and construction of information-sharing networks.

Of course, these efforts have the same limitations in the South China Sea as they did in the case of the East China Sea. Even though Japan and the United States are building up the region's MLE capabilities, the gap between China and Southeast Asian states is too great to be meaningfully filled in. The diplomatic stances of the ASEAN states are also a source of concern. Some states maintain firm stances against China's gray zone tactics, but others are gradually being pulled toward a posture of indifference to Chinese actions or even support for China's positions because of China's economic influence on their well-being. Enhancing regional MLE capabilities is not a perfect solution for the maritime security problems in the region; it can only be one piece of an overall broader strategy. Nevertheless, such efforts are important for enhancing regional confidence in the face of assertiveness by China. Without such efforts, regional states are becoming less confident in their capabilities to protect their territories and maritime interests and eventually could choose to bandwagon with China in the hope of avoiding diplomatic isolation or to win economic assistance from China.

[35] Of course, there is a certain limitation in these efforts as well. These efforts might not be enough to counter China's behaviors.

[36] On the growing role of coast guards in the Asia-Pacific, see Morris, 2017. On U.S. and Japanese efforts to support the further development of Southeast Asian partner nations' maritime domain awareness and MLE capabilities, see Scott W. Harold, Martin C. Libicki, Motohiro Tsuchiya, Yurie Ito, Roger Cliff, Ken Jimbo, and Yuki Tatsumi, *The U.S.–Japan Alliance Series: Strengthening Strategic Cooperation,* Santa Monica, Calif: RAND Corporation, CF-351-GOJ, 2016, especially Chapters 5 and 6.

Fifth, it is not enough to focus only on denial—Japan and the United States also need to focus on the concept of cost-imposition. Here, the allies have many potential options that could be used to impose disproportionately large costs on China if that nation challenges the status quo.

Generally speaking, there are at least three types of "cost-imposing" strategies. First, the allies could seek to impose costs on China's international reputation. Employing such an approach, Japan and the United States could attempt to isolate China by emphasizing Beijing's violation of important international laws, rules, and norms. Japan and the United States (and certain regional states, including the Philippines) have already attempted this approach and achieved an impressive result in the July 2016 decision of the PCA, which denied almost all of China's claims in the South China Sea. The United States has also continued "freedom of navigation" operations in the South China Sea aimed at countering the excessive claims of maritime rights by other states, including China. In international meetings, such as the ASEAN Regional Forum, the ASEAN Defense Ministers' Ministerial＋, the East Asia Summit, and other bilateral and multilateral meetings, Japan and the United States have emphasized the importance of protecting international law and the freedom of navigation on the high seas and in international waters. These efforts have had some positive effects in stigmatizing China's behavior and should therefore be continued as part of an overall cost-imposing strategy.

Nevertheless, the allies should not harbor excessive expectations for this approach; on its own, it is unlikely to substantially change China's strategic behavior. So far, despite the heavy reputational costs its unlawful positions and behaviors have incurred, China has not changed its assertive posture in the South China Sea. Indeed, Beijing simply denounced the PCA award as a "useless scrap of paper" and continued to reclaim large areas in the Spratly Islands.[37] China still maintains its expansive "nine-dash line" claim and its interpretation that UNCLOS permits coastal states to block the military activities of other states in EEZ waters. China also maintains that it has the right to employ "defensive emergency measures" in its unilaterally declared Air Defense Identification Zone in the East China Sea. Although coordinated pressure maintained over a substantial period of time has paid off in some cases, such as the efforts of Japan and the United States in pressing China to accept the Code for Unplanned Encounters at Sea in 2014, China does not appear to have been persuaded to change its overall approach as a consequence of the reputational costs its actions have incurred to date; this might be because these costs have not been large enough to change China's strategic calculus. Thus, while the allies need to continue their efforts to impose diplomatic costs on China, they should be realistic about what this can accomplish in the absence of employment of other policy tools.

Separately, the allies could strive to impose costs on China's domestic political system, pursuing actions designed to damage the domestic legitimacy of China's Communist Party. For example, Japan and the United States could disclose intelligence materials that give evidence of

[37] Camila Domonoske, "Chinese Official on Tribunal Ruling: 'It's Nothing but a Scrap of Paper,'" NPR, July 13, 2016.

corruption among party leadership. Since Xi Jinping is currently engaging in a wide-scale anticorruption campaign, the disclosure of evidence of corruption among his own supporting faction or even his family would be a severe blow to his leadership and personal authority. Such evidence could be used to warn China not to transgress the allies' red lines. Another option might be to upgrade—or threaten to upgrade—diplomatic relations with Taiwan if China attempts to undermine the status quo. A further option would be to direct support to one or more of China's repressed ethnic minority groups, such as the Tibetan or Uighur communities, in an effort to complicate China's domestic control.

Of course, directly challenging the domestic legitimacy of China's Communist Party is a qualitatively different step from the other cost-imposing measures the allies might consider. It carries the risk of inadvertent escalation because it involves China's core interests. Given the risks of this approach, domestic cost-imposition is perhaps most similar to the idea of deterrence by punishment under nuclear deterrence. Such steps could lead to a possible escalation of conflict (even above the threshold of armed conflict) with China. They may be most effective as bargaining techniques to extract concessions but could also damage the fundamental relationship between Japan and China, or the United States and China, and should therefore be considered only as a last-ditch effort to counter China's gray zone tactics.

Lastly, the allies could impose costs on China's economic interests—for example, through economic sanctions. Although Japan and the United States have not put direct economic sanctions on China over its gray zone activities, the United States is considering imposing sanctions on Chinese companies that breach the United Nations (UN) sanctions on North Korea, which are designed to stop that country's nuclear weapon development. Japan and the United States could explore developing a similar approach to sanction China in the event it intensifies its maritime gray zone challenges. Additionally, Japan and the United States could attempt to counter China's gray zone tactics by intentionally manipulating their trade, financial, or economic interactions in a way that damages China's economic interests. Such an approach has been employed by China in past conflicts, such as when Beijing blocked exports of rare earth elements to Japan in the wake of the 2010 Senkaku boat collision incident, or its blocking of banana imports from the Philippines in the wake of tensions over Scarborough Shoal in 2012. China is also using economic coercion tactics against South Korea to pressure Seoul to reverse its approval for the deployment of a THAAD missile battery on the Korean Peninsula. Furthermore, Japan and the United States can enhance their abilities to block China's sea lines of communications during a conflict as a way to tacitly pressure China not to take certain kinds of revisionist behaviors.

However, economic cost-imposition strategies are a double-edged sword: The allies would need to be prepared to endure economic pain if such methods are employed. Additionally, there are a number of hurdles to using these means to pressure China; some may violate World Trade Organization rules; others might be regarded as illegitimate by international society, as well as of questionable legitimacy or legality in the eyes of affected domestic actors in both countries. It is also highly likely that China would retaliate to such actions through reciprocal economic sanctions, which could hurt key actors in Japan and the United States. There is no guarantee that the allies can impose larger costs on China than China can impose on them; China may exhibit relative strength in such an economic conflict, and the allies might eventually be forced to compromise with China.

In short, each element of a cost-imposing strategy has its own problems and limitations: Diplomatic cost-imposition may not be powerful enough to force China to give up its revisionist behavior; domestic cost-imposition may be too escalatory; and economic cost-imposition may be too costly to the allies. None is obviously suited to achieve the desired outcome. Still, doing nothing is not an option either—China appears intent on eroding overall deterrence and changing the regional order through gray zone coercion. Therefore, the allies will probably need to accept greater risks than they would prefer in order to stop China's gray zone challenges. Further consideration of the options outlined here, as well as any others that might be identified by Tokyo and Washington, is merited.

Conclusion

This paper has described the policy options that Japan and the United States face in seeking to counter China's maritime gray zone challenges. It has reviewed examples of China's gray zone tactics and described China's tactics as an issue of deterrence and escalation control. It has also introduced the idea of a competitive strategy designed to counter China's challenges and explained specific counteractions that might be taken in response to China's gray zone coercion. In conclusion, it is worth emphasizing that countering China's maritime gray zone challenge is not an easy task. China's relative strength in the region is growing; thus, the level of challenge that China can choose to select is increasing. China's challenges have remained below the threshold of a legally defined armed attack so far because of the military superiority of Japan and the United States. But if the allies fail to sustain military capabilities sufficient to deter Chinese aggression, China will eventually face powerful incentives to challenge the status quo through force. Therefore, it is absolutely necessary for Japan and the United States to sustain enough military capability to deter China and confine its challenges below the threshold of armed attack in the first place.

Even if the allies succeed in achieving this objective, they will still face growing pressures from China's gray zone challenges. By adopting the idea of a competitive strategy, Japan and the United States can put downward pressure on the level of China's challenges and delay the transition from gray zone coercion to armed attack. Doing so will probably require the allies to endure a long period of Chinese gray zone challenges. China appears to want to change the status quo by using its superior MLE capabilities. As long as China's challenge remains below the threshold of a legally defined armed attack, the allies cannot respond with the exercise of individual or collective self-defense. Considering the rapid growth of China's MLE capabilities, sustaining escalation dominance in a situation of maritime gray zone coercion is no easy task for Japan and the United States.

Although this paper introduces some options or strategies to counter China's gray zone tactics, these options present challenges. Japan and the United States may not be able to increase their MLE capabilities enough to counter China's challenges, and developing a seamless framework of cooperation between MLE and naval capabilities may prove difficult. Tokyo and Washington may not be able to fully utilize the potential of the alliance and partner networks in the region. Capacity-building efforts for states surrounding the South China Sea may not be enough to stop China's assertive behaviors in the region, and many of the cost-imposing options discussed here may not prove attractive, sufficiently impactful, or even possible to execute. Considering the pressure China can bring to bear, there is no guarantee that the U.S.-Japan alliance can successfully deter China's incremental but steady gray zone coercion.

While the allies should guard against wishful thinking, they must also defend against defeatist thinking as well. They might be able to deter China's gray zone coercion if they take the following actions:

- Increase their defense budgets, adjust spending to reflect prioritizing capabilities that will help deter—or, if necessary, defeat—Chinese aggression, and maintain military superiority.
- Adopt competitive strategies for both gray zone and armed attack challenges.
- Increase Japanese MLE capabilities substantially.
- Develop a truly seamless framework for cooperation between MLE and naval capabilities.
- Utilize the full potential of the U.S.-Japan alliance and regional alliance networks and partnerships.
- Increase joint efforts aimed at capacity-building for the states surrounding the South China Sea.
- Develop a menu of cost-imposing policy options to adopt if China continues to escalate its maritime gray zone coercion, including steps focused on damaging China's diplomatic, domestic, or economic interests in response to Chinese aggression.

Finally, it is important to remember that the allies' objective is not a competition with China per se. A competition with China is just a means by which to achieve the strategic objective of preventing China from changing the status quo through coercion. If China abandons its revisionist behavior and starts respecting the status quo, the allies can pursue other policies, including assurance aimed at convincing China that it can live with the existing international order. The allies must also be sensitive to the rate of China's economic growth and its domestic politics, because these will affect its coercive capabilities and assertive behavior, influencing the degree of challenge China can select. Careful analysis of China's capabilities and intentions will be necessary to craft an effective allied strategy for tailored deterrence and assertive engagement.[38]

[38] See Dennis Blair, *Assertive Engagement: An Updated U.S.-Japan Strategy for China,* Washington, D.C.: Sasakawa Peace Foundation USA, 2015.

4. The U.S.-Japan Alliance and Deterrence in Cyberspace

John A. Davis
Major General, U.S. Army (retired)
Vice President and Chief Security Officer (Federal)
Palo Alto Networks

This paper uses the framework of the Barack Obama administration's cyber deterrence policy to offer recommendations that apply to the U.S.-Japan alliance and, in particular, the issue of deterrence in cyberspace.[1]

As background, I should disclose that I was personally involved in the development of the Obama administration's cyber deterrence policy. I served as the acting Deputy Assistant Secretary of Defense for Cyber Policy from 2014 until my retirement from the U.S. Army in 2015. During that period, my office in the Pentagon had primary responsibility for addressing a requirement in the 2014 National Defense Authorization Act for the development of an administration policy for cyber deterrence. The basic cyber deterrence framework reportedly approved by the Obama administration originated under my supervision and was drafted by my Director of Plans at the time, Michael Sulmeyer.[2] How, or even whether, this policy will be positioned within the Donald Trump administration remains to be seen. However, since I have seen nothing to indicate a different policy from the Trump White House, I will assume the previous policy is still in place as a useful framework and can serve as a model for the U.S.-Japan alliance.

I will begin this chapter by proposing that deterrence in cyberspace is essential, unique, and complex. I will then explain how these three characteristics shaped the Obama administration's cyber deterrence policy in general, before outlining its strategic tenets and elements. The paper notes that cyberspace is an attractive domain for those who wish to employ gray zone operations due to the nature of the online world and the difficulty in attributing cyber attacks to specific actors in it. Finally, the paper provides recommendations for the United States and Japan to deter cyber attacks, including those conducted in the context of gray zone operations.[3]

[1] This chapter was completed prior to the articulation of a Trump administration cyber policy and therefore presents the legacy Obama administration cyber policy as both a useful reference and a likely continuing influence on overall U.S. cyber policy going forward.

[2] Michael Sulmeyer, *Report on Cyber Deterrence Policy*, Washington, D.C.: Office of the Secretary of Defense, December 2015.

[3] Like Chapter 2, this chapter focuses in large part on conventional deterrence in cyberspace while also noting that the cyberspace domain is itself extremely friendly to gray zone coercion attempts, primarily due to the multiple vulnerable points that networked systems present and the substantial anonymity and attribution challenges associated with the online world. Gray zone considerations are explored here and more specifically in Chapter 5.

Why Deterrence Is an Essential Component in an Effective Strategy to Deal with Cyber Threats

Deterrence in cyberspace is essential. In its opening statement, the Obama administration's cyber deterrence policy states, "In a globally connected world, cybersecurity is one of the most serious national security concerns that the U.S. and its allies face in the 21st century."[4]

The increasing list of media headlines about cyber breaches and attacks, and the increasing consequences resulting from the theft of personal information and intellectual property, loss of economic advantage and political process legitimacy, and disruption or destruction of critical infrastructure and vital services that could lead to injury and even death make cybersecurity a significant issue of public safety, as well as national and economic security.

A growing number of senior officials in the international intelligence and national security communities, as well as leaders in businesses and boardrooms across global industry, have come to the conclusion that cyber threats are exploding at an alarming rate and more must be done to manage the associated risks. This problem is not going away, and a strategy to deal with this threat that relies solely on playing static defense and building higher digital walls will not be adequate. Development of a more robust, comprehensive strategy has become essential and must include a deterrence component.

Specific to the U.S.-Japan alliance, ensuring the security of the 2020 Tokyo Olympics' information environment provides a specific event emphasizing the essential nature of an effective cyber threat deterrence policy, in addition to the more general rationale described earlier.

Why Deterrence in Cyberspace Is Uniquely Challenging and Analogies to Other Forms of Deterrence in More-Traditional Environments Are Inadequate

It may be tempting to think that deterrence in cyberspace has many analogies in other dimensions of international governmental interaction. Nuclear deterrence is often used as an example. However, cyberspace is a unique environment that defies comparisons. The components, characteristics, and participants involved make cyberspace such an unusual model that conventional deterrence strategies all begin to fall short when simply overlaid on the cyberspace environment.

The focus on what might be termed "regular" cyberspace deterrence and gray zone deterrence in cyberspace was a deliberate approach intended to highlight both aspects and how they interact; it also happens to reflect to some extent how the U.S. and Japanese chapter authors actually conceive of their nations' primary concerns in cyberspace.

[4] Sulmeyer, 2015, p. 2.

The Obama administration cyber deterrence policy states, “cyber deterrence in the Information Age is substantially different from Cold War–era concepts intended to deter the use of weapons of mass destruction.”[5] There are numerous reasons for this assessment.

First, there is a distinct difference between the main participants. Using the nuclear deterrence example, there was a small number of nation-states possessing nuclear weapons and allied to either the United States or the Soviet Union in a bipolar international system. This nuclear example is a stark contrast with the explosion of highly capable state, nonstate, and hybrid entities (such as state connections to front companies, research organizations, and criminal entities) that have the capability, expertise, and intent to conduct cyber activities that could be—or, in some cases, already are—resulting in significant national and economic security concerns and public safety consequences for the United States and its allies.

Additionally, many cyber capabilities are “dual- or multiple-use” and can therefore simultaneously enable a wide variety of both beneficial and harmful effects. Dual- and multiple-use examples complicate attempts to control or deter their use, especially given the nonstate participant factor, because nonstate entities are involved in both beneficial (e.g., penetration testing, “red teaming,” research and development) and nefarious (e.g., criminal, sabotage of legitimate policies, intimidation, terrorism) activities.

Traditional deterrence concepts and strategies tend to focus on the interaction between states, but the cyberspace environment brings more nonstate and hybrid mixtures of state and nonstate actors and organizations than ever. One reason for this is the continuous increase in computing power at ever decreasing costs (from the use of automation, cloud capabilities, and a marketplace of trading and information-sharing). This means that cyber capabilities are increasingly developed and purchased with fewer resources. It also means that their use results in increasingly broad operational outcomes at relatively low risk because of the difficulty in attributing cyber-related actions to specific actors and organizations.

Why an Effective Cyber Deterrence Policy Is Complex, and Therefore Must Be Comprehensive and Multifaceted

According to the Obama administration cyber deterrence policy, “Cyberspace also has distinctive characteristics—including its global and interconnected nature, largely private ownership, potential for anonymity, and low barriers to entry for those who wish to cause damage—that pose challenges for deterrence that are different in kind and scope than deterrence in more traditional areas.”[6]

[5] Sulmeyer, 2015, p. 4.

[6] Sulmeyer, 2015.

Due to the unique nature of cyberspace, the layers that compose its environment often overlap in a blurry mixture of complexity that make conventional distinctions confusing. These layers include

- geographic (physical location of networks and infrastructure, and applicable national laws, rules, regulations, and political implications)
- network (virtual connectivity and infrastructure)
- component and device (physical infrastructure)
- online identity (persona)
- actual identity (actors and organizations).

Additionally, actions in the cyberspace environment can occur on a global scale at the instantaneous speed of the network. These complex characteristics have significant implications for decisionmaking, responses, and policies (including deterrence) and can confound conventional models of deterrence.

The discussion so far illustrates why deterrence in cyberspace is essential and why one cannot simply overlay a traditional deterrence model on top of the unique and complex cyberspace issue. An effective cyberspace deterrence policy requires a robust, comprehensive, and multidisciplinary approach as a basic strategy. There are no “silver bullets,” and there must be a wide range of both components and participants in order for a strategy of deterrence in cyberspace to be effective.

An effective cyberspace deterrence concept must account for the complexities associated with a situation in which the nature of an adversary’s actions, or even who the adversary is, can be unclear. The gray zone of the cyberspace environment complicates attribution, and the nature of an incident is rarely clear at the outset of, or sometimes throughout, an event. Therefore, deterrence is often difficult, requiring cross-domain linkages, denial, cost imposition (or punishment), patience, and creativity.[7]

Next, I will outline the national strategic framework of the Obama administration’s cyber deterrence policy and provide recommendations for how to apply this framework to the U.S.-Japan alliance going forward.

Applying the Administration Strategic Framework to the U.S.-Japan Alliance

Because of the aforementioned factors, the national strategic framework adopts a broad concept of deterrence in a whole-of-government approach that uses all instruments of national power (diplomatic, information, military, economic, intelligence, and law enforcement). Further, the framework recognizes the unique nature of the cyberspace environment and its reliance on both industry and citizenry. The framework includes public-private partnerships to improve

[7] Summarized from an exchange of ideas with Scott W. Harold of RAND.

cybersecurity for both public and private sectors in addition to the U.S. public. This is sometimes referred to as a *whole-of-nation* effort.

As applied to the U.S.-Japan alliance, my recommendation is to expand that basic strategic framework using three steps:

- First, each nation must account for its internal interests, culture, values, priorities, and resources in a national component of joint policy (as exemplified in the Obama administration cyber deterrence policy for the United States described in this paper).
- Second, a natural extension of the strategic framework should be a combined effort to determine where there is overlap between the independent national components. Common issues can be reinforced in the development of an alliance component of the joint policy. This alliance component would contain common objectives, priorities, implementation measures, and measures for monitoring effectiveness and progress.
- Third, there may be gaps that need to be addressed in the context of the overall alliance that are not covered simply by determining where there is overlap between the two independent national components. These gaps should be addressed and integrated into the alliance component of the joint cyber deterrence policy.

For additional context on how to approach the development of a joint strategic framework, each of these three steps should be viewed as a natural progression. The process should begin with individual whole-of-government efforts. Next, the process should develop and integrate individual whole-of-nation efforts, including public-private partnerships with the industries and citizenry of both countries independently. Finally, by natural extension, the last step would result in a comprehensive joint whole-of-alliance cyber deterrence policy between the United States and Japan, including an action plan for implementation and assessment of effectiveness.

Applying the Obama Administration's Cyber Deterrence Policy to the U.S.-Japan Alliance

The Obama administration's cyber deterrence policy included the following elements:

- a description of what types of activities the policy seeks to deter
- deterrence by denial
- deterrence by cost imposition
- activities that support deterrence.

I will briefly outline the main ideas stemming from each of these basic elements before offering recommendations about how they might be applied in the context of cyberspace deterrence supporting the U.S.-Japan alliance.

A Description of What Types of Activities the Policy Seeks to Deter

The first aspect of the administration policy describes the types of activities the policy seeks to deter. In general, the types of threats the administration was most concerned about and designed its policy to deter were malicious cyber activities that could cause wide-scale disruption, destruction, loss of life, and significant economic consequences for the United States and its interests. This includes national-level threats to core values, such as privacy and freedom of expression.

As applied to the U.S.-Japan alliance, this is a sound approach in defining what to deter. My recommendation is to adopt the general framework for this element in a joint alliance cyber deterrence policy. In fact, the 2015 U.S.-Japan Defense Guidelines set precedence for this kind of policy by explicitly extending the alliance's focus to dealing with threats in cyberspace.[8] The policy should seek to ensure a seamless transition in deterrence and response to threats that emerge from peacetime to gray zone scenarios and all the way into wartime contingencies, as described in the guidelines. The framework already described correctly focuses on the things that matter most, provides the flexibility to adapt to an environment that can change rapidly and dramatically, creates the ambiguity required to preserve flexibility in a national and/or alliance response, and stops short of declaring specific thresholds in order to discourage malicious cyber activity that does not rise to those levels. However, I would also recommend a few adjustments and additions to the general framework for this component.

First, the recent malicious cyber activities the U.S. government attributed to Russia that attempted to influence the U.S. presidential election process is perhaps one example of too much ambiguity within the current policy as written. Another potential example of emerging malicious cyber activity of concern is the exploding Ransomware threat. This is a significant threat in both the Asia-Pacific region and the United States. As more devices become connected to the cyber environment as a result of the "Internet of Things" phenomenon, including devices associated with critical infrastructure and even life-sustaining medical functions, this represents a risk of potentially catastrophic consequence. The alliance should consider its stance on these potentially destabilizing malicious cyber activities and incorporate the results into a joint cyber deterrence policy.

Next, although geography matters differently in cyberspace than in the conventional domains, it still does matter. It matters where various cyber threat actors and organizations are located because this can affect response decisions no matter whether the response uses a cyber capability or any of the other instruments of national power. It also matters in terms of the physical location of potentially hijacked network component or device layer infrastructure or control channel communications used by a cyber threat actor or organization. Besides the generic categories of cyber threats and malicious cyber activities listed in the Obama administration policy, there are some specifics that are unique to the Asia-Pacific region and likely impact the U.S.-Japan alliance directly. These specifics about emerging malicious cyber activities of concern and cyber threat actors and organizations unique to or prevalent within the Asia-Pacific region might therefore be incorporated in a joint alliance cyber deterrence policy.

[8] U.S. Department of Defense and Government of Japan, 2015.

Deterrence by Denial: Defense, Resiliency, and Reconstitution

The second element in the Obama administration cyber deterrence policy is the general category of deterrence by denial. This category is about efforts to persuade adversaries that any attempt to conduct the type of malicious cyber activities the policy seeks to deter are not worth the effort expended. This is due to the combination of strong defenses, architecturally resilient systems that can "take a punch" without significant consequence, and the ability to recover quickly from attacks and other disruptions of consequence that successfully penetrate defenses and overwhelm resiliency. Therefore, the three main functions critical to this element are defense, resiliency, and reconstitution.

There are several subordinate concepts that contribute to the overall effectiveness of the deterrence-by-denial element. In the application of these subordinate concepts, as well as the overall element itself, to the U.S.-Japan alliance, my recommendations focus most of the efforts on the internal dynamics of each national component of the joint alliance policy for cyber deterrence. In other words, deterrence by denial is most effectively applied through the internally focused efforts of each nation independently—with a few exceptions.

First, I will explain what the subordinate concepts in the deterrence-by-denial element mean and why most of them are best applied as independent national efforts. Then, I will describe how the U.S.-Japan alliance should work together to reinforce or improve these independent national efforts. Finally, I will explain why a joint effort in the main function of reconstitution should be considered.

Identification of What Is Important to Defend, What Should Be Resilient, and What Must Be Capable of Rapid Reconstitution

The first subordinate concept under the deterrence-by-denial element is about identifying and protecting critical infrastructure. This concept is a practical result of the saying "an attempt to be strong everywhere results in being strong nowhere." The concept uses a risk-based approach to identify critical infrastructure where a cyber threat event could reasonably result in large-scale, significant consequences affecting public safety, economic viability, or national security.

In applying this subordinate concept to the U.S.-Japan alliance, my recommendation is that each nation do so as an independent effort.

First, there are cultural, economic, legal, political, military, and historical differences between the nations that affect a determination of what is and is not critical. Additionally, this concept requires the strong participation of each of the private-sector entities that own, operate, control, and maintain systems, networks, endpoint devices, and data within most, if not all, critical infrastructure sectors of each nation.

The mechanisms for managing the ways that public and private sectors are organized and controlled are unique to each nation. This dictates a tailored, independent approach within each nation. This is the case for the United States under Executive Order 13636, which requires the U.S. Department of Homeland Security to consult with the owners and operators representing all 16 of the U.S. critical infrastructure sectors, as well as sector-specific agencies, sector coordinating councils, government coordinating councils, independent regulatory agencies, and subject-matter experts.[9]

While it would simply be too complicated to attempt a joint alliance effort for this concept, each nation sharing the results of what it considers critical with the other is certainly recommended. This may illuminate some gaps that can be addressed in the subsequent joint alliance policy development process.

Bolstering Government Network Defenses

This subordinate concept contributes to the element of deterrence by denial. It spans the main functions of defense, resilience, and reconstitution and holds U.S. government agencies accountable for achieving a cybersecurity standard of excellence. It also serves to set the example for other public- and private-sector organizations, as well as the U.S. public in general, to emulate.

Everything about this concept is applicable to both the United States and Japan. But because of the differences cited earlier, my recommendation is to initially approach this concept as an independent effort within each nation. This allows for effective designation of responsibilities, efficient application of resources, and accountability for progress that is likely unique for each nation's governmental structure and processes.

Though initially done independently, the sharing of the independently applied results during subsequent joint alliance policy development is advisable and may indicate gaps or lessons beneficial to the joint effort.[10]

Defending Against Insider Threats

Recent cases involving the unauthorized disclosure of classified information, most notably the Bradley Manning-WikiLeaks and Edward Snowden events, have resulted in extremely serious consequences for the national security of the United States. The U.S. response to these kinds of insider threat events has been to leverage executive action to organize and establish procedures for safeguarding classified information vital to U.S. national security, and to reduce insider threats through the use of technical safeguards and standards.

[9] Barack Obama, "Executive Order: Improving Critical Infrastructure Cybersecurity," Washington, D.C., White House, February 12, 2013.

[10] Additional options, all of which would require thorough discussion, review, and legal approval prior to implementation, could include assistance with reconstitution during a crisis or joint exercises during peacetime to help identify weaknesses that need fixing.

Again, while it applies equally to both the United States and Japan, this is another example of a concept best employed within the legislative, executive, and legal frameworks of each nation independently. While the two nations should initially develop such policies independently, my recommendation is that they then share results and lessons, to the extent allowable, during subsequent joint alliance policy development.

Sharing Cyber Threat Information and Intelligence

Cyber threat information-sharing is one of the most powerful subordinate concepts within the deterrence-by-denial element of the previous administration's cyber deterrence policy. As a result, there has been a significant amount of development, investment, expansion, and progress over the past few years in the United States in building up the architectures and channels for exchanging information with allies and partners on cybersecurity threats (including some positive results from last year's U.S.-Japan alliance conference regarding information-sharing[11]). Under existing executive authorities and a new law enacted at the end of 2015, the United States has lowered both perceived and real barriers to cyber threat information-sharing. Enhancements and expansion of this concept across the United States now include sharing both within and across the public and private sectors.

Information-sharing is a powerful tool in deterring and defeating attacks because shared situational awareness of cyber threats and indicators of malicious cyber activity enables the cybersecurity community to more quickly and effectively address vulnerabilities before they can be fully exploited. It also remains a sensitive issue because of privacy and civil liberty issues, and liability issues linger despite improvements resulting from recent legislative action to reduce this concern.

Applying this subordinate concept to the U.S.-Japan alliance warrants an exception to the more general recommendation about keeping the deterrence-by-denial efforts primarily independent at a national level. Effective cyber threat information and intelligence-sharing requires a nuanced approach when taken in the context of the U.S.-Japan alliance.

The laws, regulations, privacy and civil liberties concerns, and liability issues unique to each nation require a degree of independent effort to support the best interests of each partner in the alliance. However, cyber threats do not stop at national borders, and there should be an extension of information- and intelligence-sharing between the United States and Japan.

My recommendation is to expand cyber threat information-sharing between the United States and Japan in several ways. Doing so more effectively requires the two countries to take advantage of some important lessons the United States has learned as a result of its experiences over the past several years. These lessons include clarifying the type of information to be shared, developing a standardized method for sharing this information, and employing an automated

[11] Harold et al., 2016.

platform to not only share the information in real time but also deploy the resulting security controls to the appropriate elements of each network enterprise to stop threats in real time.

First, there should be agreement on exactly what information to share. This is important because there has been a tendency by some information-sharing detractors to conflate cyber threat information with the highly contentious information- and intelligence-sharing associated with countering terrorism and related surveillance and encryption issues. Make no mistake, this is a false narrative. In cybersecurity, security does not compete with or detract from privacy or civil liberties; rather, security ensures them both.

Cyber threat information-sharing is not associated with personally identifiable information (PII), protected health information (PHI), intellectual property (IP), or personal or corporate content of communications. It is associated with cyber threat actors and organizations, the malicious code and techniques they use, the information infrastructure transmission and collection points and communication control channels they use and where these elements are located, the techniques that they execute on endpoint devices to hijack their intended functions, and the general categories of cyber threat targets. This is the type of information that should be acceptable within privacy and civil liberty parameters.

Next, the sharing of information must progress from the traditional methods of manual (passing information on spreadsheets and pdf files) and ad hoc (literally hundreds of varying formats with confusing and inconsistent fields of information) transfer. Effective sharing requires a streamlined procedure that is standardized (a single recognized and accepted standard for information fields about the threat) and automated (through the employment of a platform that automatically translates the standardized threat information into the security controls that are also automatically pushed out to the appropriate elements of the network to mitigate the threat). There is simply no other way to outmaneuver modern cyber threats because they increasingly employ automation, routinely trade cheap capabilities, and effectively use information-sharing procedures of their own.

My recommendation is for the United States and Japan to employ a staged progression of cyber threat information-sharing that provides for the simultaneous movement of both independent and shared steps, based on where progress can be achieved. Continuous and close coordination is required. This recommendation is not without complexities because of such issues as addressing individual privacy rights, corporate liability, and reputational costs for cyber breach reporting, with differing standards, regulations, and even laws in each country. However, the payoff is enormous in effectiveness against cyber threats if successful sharing can be achieved.

Promoting Best Practices Through the National Institute of Standards and Technology Cybersecurity Framework

The final subordinate concept in the Obama administration's deterrence-by-denial approach is about promoting best practices through the National Institute of Standards and Technology (NIST) Framework. This is a template of globally recognized standards and practices to help organizations, regardless of whether they are public or private, to better understand, communicate, and manage their cyber risks.

The NIST Framework consists of five parts:

1. identify (critical networks, systems, and information that must be defended, resilient, and able to recover quickly)
2. protect (said critical elements through a proactive, prevention-first mindset and strategy)
3. detect (threats of significance to the critical elements, whether the threats are cyber related or not)
4. respond (effectively to any events that compromise protection and prevention measures)
5. recover (minimizing the operational consequences of any event).

This framework was developed in full partnership between the U.S. public and private sectors. As a result, its adoption and implementation has been successful across the various sectors of U.S. industry and government organizations. Thus, this is the most adaptable subordinate concept for a joint effort within U.S.-Japan alliance cyber deterrence policy development.

My recommendation is that the United States and Japan should each plan and implement the NIST Framework on their own but then synchronize their efforts for a mutually reinforcing outcome. There is no reason to separate national efforts for this concept, and a joint effort would result in synergy across the combined national outcomes for defense, resiliency, and reconstitution. This recommendation is consistent with the 2015 U.S.-Japan Defense Guidelines and would significantly contribute to deterrence by making adversary expenditure of effort in malicious cyber activities more difficult.

The Function of Reconstitution as a Joint Alliance Opportunity for Deterrence

My last recommendation in applying the deterrence-by-denial element to the U.S.-Japan alliance pertains to reconstitution. While most of my previous recommendations in applying the deterrence-by-denial elements focused on independent national efforts with a few adjustments and exceptions, reconstitution is one function that I believe can be a significant joint effort.

If a malicious cyber event were capable of breaching either nation's independent defenses and overwhelm either nation's independent resilience, any potential adversary that clearly understood that the United States and Japan had established a mutual agreement to quickly bring the required expertise, manpower, capabilities, and resources to bear in order to accelerate an effective reconstitution effort might question whether the attempted malicious cyber event was worth the effort. This could be a very helpful dynamic in contributing to deterrence, and the alliance should consider incorporating this concept as part of the broader Humanitarian Assistance/Disaster Relief function already in place.

Deterrence by Cost Imposition and Its Relationship to Deterrence by Denial

The third element in the Obama administration cyber deterrence policy is the general category of deterrence by cost imposition, sometimes referred to as deterrence by punishment. This consists of measures that include the threat, as well as the actual employment, of actions that result in undesirable costs for any potential or active adversary considering or conducting attacks or other malicious cyber activities against the United States—and, as it applies to this discussion, the U.S.-Japan alliance.

According to the Obama administration's policy, the measures associated with this element

> take advantage of the United States Government's ability and willingness to respond to cyber attacks through all necessary means, as appropriate and consistent with applicable international law. Such measures include, but are not limited to, pursuing law enforcement measures, sanctioning malicious cyber actors, conducting offensive and defensive cyber operations, projecting power through air, land, sea, and space, and, after exhausting all available options, to use military force.[12]

It is important to understand the relationship between this and the previous element of deterrence by denial, especially when considering the use of offensive cyber operations as a deterrence measure. In my experience, the more a nation (or alliance) is dependent on the cyberspace environment and is vulnerable to the malicious cyber activities that it seeks to deter, the less realistic it becomes to employ a symmetric option (conducting offensive cyber operations) to deter cyber attacks. This can be a counterproductive approach resulting in a cycle of escalation. Said best by James N. Miller, Under Secretary of Defense for Policy, when I served as his senior military cyber adviser during 2012–2014, "It's not wise to throw a match if you're covered in gasoline."[13]

In fact, the cure can be worse than the illness when applying any of the other noncyber and more asymmetric options unless there is a strong deterrence-by-denial posture in place. These options include:

- deterrence by cost-imposition options (economic, law enforcement, and "traditional" military instruments of power)
- activities that support deterrence (diplomatic, informational, and intelligence instruments of power).

[12] Sulmeyer, 2015.

[13] Personal communication with author.

Therefore, it is important to realize that the failure of a nation or alliance to prioritize deterrence by denial (using defense, resilience, and reconstitution) will limit, and, in some cases, eliminate, options to deter through cost imposition or other activities that support deterrence. These components are irrevocably tangled, and an effective policy about deterrence in cyberspace should acknowledge and account for this interrelationship.

Applying Economic Deterrence-by-Cost-Imposition Options to the U.S.-Japan Alliance

The Obama administration policy states,

> Economic tools may offer options for imposing costs on malicious cyber actors and deterring certain cyber threats, particularly from adversaries who seek to undermine U.S. economic security by illicitly obtaining trade secrets, including intellectual property, or controlled technology. When appropriate and warranted, the Administration will pursue actions to impose economic costs on the malicious cyber actors responsible for such activity, including when such activity constitutes a violation of international trade rules or the rules of the World Trade Organization.[14]

This is a deterrence by cost imposition measure that has long been used by the United States in other international policy challenges and is now similarly being applied to the challenge of cyber threats of significant consequence.

The policy document then provides an example of employing this option following the North Korean destructive and coercive attack on Sony Pictures Entertainment in 2014, which was intended to harm a U.S. business and suppress free speech. In this case, the United States imposed financial sanctions on specified North Korean cyber actors. More broadly, it also authorized sanctions on individuals and organizations that had a role in supporting or enabling those whose cyber activities contributed to a significant threat to U.S. national security, foreign policy, economic health, or financial stability.

In applying this measure to the U.S.-Japan alliance, my recommendation is that, where possible, the United States and Japan should consider reinforcing each other's economic sanctions when the cyber threat or malicious cyber activity falls under the category of activities the joint alliance policy seeks to deter. Recognizing that independent national determinations must be made on a case-by-case basis before a joint sanctioning effort can proceed, the demonstration of resolve in the application of a joint sanction would likely magnify the undesirable consequences on an adversary and contribute to deterrence of the threat.

[14] Sulmeyer, 2015, p. 11.

Applying Law Enforcement Deterrence-by-Cost-Imposition Options to the U.S.-Japan Alliance

The Obama administration policy states, “Law enforcement can also be an effective deterrent to cyber threats both through denial (e.g., taking down a criminal botnet that could be used in an attack) or cost imposition (e.g., arresting the perpetrators of cyber attacks).”[15] The law enforcement options include two main categories of action:

- investigating, prosecuting, and disrupting malicious cyber activity
- building international capacity to combat cyber crime.

I will provide more detail about each category, offer some recent examples of how these law enforcement options have been employed, and then offer my recommendations about how to best apply them to the U.S.-Japan alliance.

The first category is imposing direct costs on both malicious cyber threat actors and organizations, as well as the states that protect or provide support to them, by opening investigations and prosecuting those responsible. The U.S. indictment of five uniformed members of China’s PLA in 2014 for hacking six U.S. industry victim entities serves as a recent example. These types of law enforcement actions demonstrate that there are consequences for conducting malicious cyber activities and can contribute to deterrence through the imposition of costs. Additionally, several of my former U.S. government colleagues have privately expressed the belief that the indictments of these Chinese military members played a significant role in the ultimate outcome of the Obama-Xi agreement in September 2015. This demonstrates an effective deterrent by impacting foreign policy decisionmaking and agreement to limit certain types of malicious cyber activity, such as theft of intellectual property for profit as outlined in the Obama-Xi agreement.

In applying law enforcement options to the U.S.-Japan alliance, separate national legal frameworks will necessitate independent efforts by each country. However, I have two recommendations for applying these options within the alliance framework. First, the alliance cyber deterrence policy and implementation procedures should include the agreement to routinely share lessons (both positive and negative) about instances of the use of law enforcement tools as they apply to cyber threats and malicious cyber activities that the two nations seek to deter. Second, there are opportunities for the two nations to work together on law enforcement investigations, prosecutions, and disruptions through either the establishment of a bilateral agreement and structure or through existing international law enforcement mechanisms, such as Interpol. This leads to the next category of law enforcement action, building international capacity to combat cyber crime.

This second category of law enforcement action is obviously something that can be incorporated into the U.S.-Japan alliance policy for deterrence in cyberspace quite easily.

[15] Sulmeyer, 2015.

Recognizing that cyber threats and malicious cyber activities rarely respect geographic national borders, the problem is clearly an international law enforcement issue, and it is in every responsible nation's interest to cooperate on these matters.

Not all nations have the capabilities or capacity to combat cyber crime effectively. Therefore, the United States regularly assists other countries in building the capacity to investigate, prosecute, and disrupt cyber crime. One example in which the United States and Japan have already successfully engaged in an international law enforcement capacity-building effort is the Budapest Convention on Cybercrime, which became effective in 2004 and has more than 50 state signatories as of 2016, including the United States and Japan. The United States is already working with Japan to encourage more countries to sign up and use the Convention's structure as a basis for capacity-building.

According to the previous administration's cyber deterrence policy, there are three key concepts within the Budapest Convention's framework: ensuring law enforcement agencies have the authorities and tools to investigate cyber crime and to deal with electronic evidence, enacting substantive cyber crime laws, and using mechanisms like the 24/7 Network on High Tech Crime to ensure effective and timely international cooperation.

My recommendation is that the United States and Japan should use the development and implementation of their alliance policy for deterrence in cyberspace as an opportunity to set an example of international leadership and jointly advocate an increase in membership in the Budapest Convention and in the 24/7 Network. Taking the joint lead on the world stage in promoting international law enforcement cooperation and capacity-building would contribute to deterring those who might constitute a significant threat not just to the national and economic security of the alliance, but much of the world.

Applying the Building of Capabilities to Defend the Nation in Cyberspace to the U.S-Japan Alliance

The Obama administration's cyber deterrence policy states,

> The United States Government's first preference is to use network defense, law enforcement measures, economic actions, and diplomacy to defend against, to deter, and to deescalate cyber incidents. When defense and deterrence efforts are insufficient, however, the United States Government must have the capability and capacity to defend the nation in cyberspace. The United States Government will be prepared, if directed by the President, to use all necessary means, including military, to respond to a cyber attack on the nation.[16]

In support of this policy, the U.S. military has been building organizational structure, skills and expertise, capabilities, and procedures to defend the nation in cyberspace since the establishment of U.S. Cyber Command and its Army, Navy, Air Force, Marine Corps, and other

[16] Sulmeyer, 2015, p. 13.

defense agency and joint military command components in 2010. By doing so, the U.S. military is creating credible and reliable options for the President to use in deterring potential or active adversaries from employing malicious cyber activities of significant consequence to the nation.

Although most of the U.S. military cyber structure is prioritized for deterrence by denial (through the functions of defense, resilience, and reconstitution), some forces are designed for conducting offensive cyber operations. In applying this deterrence-by-cost-imposition option to the U.S.-Japan alliance, I have several recommendations.

First, though not a part of this option per se, the development of U.S. cyber forces for defense, protection, resilience, and reconstitution can and already does play a role in supporting the alliance. This is through joint training, education, exercises, and even operations that involve cooperation among the U.S. forces stationed in Japan, the cyber defense teams supporting them, and the JSDF. As mentioned previously, deterrence by denial inherently affects options to impose costs, and defensive military cooperation is a critical component of the alliance. This defensive cooperation should include the functions of adversary emulation (or "red teaming"), cybersecurity readiness posture evaluation, and cybersecurity training and assistance with such issues as resilience, recovery, and even active "hunting" for adversary activity on military networks where appropriate.

The offensive cyber forces in the U.S. military are designed primarily for integrating cyber capabilities alongside the more traditional air, land, and maritime forces and capabilities in the context of responding to threats to the national security of the United States or its vital interests via military operations approved by the President. These are called Cyber Combat Mission Forces and they are integrated into the contingency and operations plans for each of the Unified Combatant Commands of the Defense Department. Therefore, there are Cyber Combat Mission Forces integrated into the plans (and operations, when approved) of U.S. Pacific Command, including support to U.S. Forces Japan.

Given this arrangement, I have two recommendations for how to apply these offensive cost-imposing options to the U.S.-Japan alliance. Before providing those recommendations, it is important to note that, within the context of alliance policy, I cannot envision using these offensive forces in the near term in a combined U.S.-Japan organizational structure. This is due mainly to sensitivities regarding the intelligence and technical capabilities associated with these specialized cyber forces, as well as the current strict adherence to a U.S.-only risk management and approval process with significant policy, operational, technical, and legal oversight mechanisms.[17] However, this does not preclude some degree of cooperation, especially as it may be useful as a deterrent.

My first recommendation is to publicly declare in the alliance policy as a measure of resolve that the United States reserves the right to employ these offensive military capabilities in

[17] Japanese legal restrictions, political sensibilities, and capabilities constraints would obviously also play a role in constraining or shaping the range of cooperative policy options. These are discussed more extensively in Chapter 5.

response to situations where network defense and law enforcement actions are insufficient and there is an assessed cyber threat or ongoing cyber actions impacting the national security, economic viability, or public safety of the alliance. The United States would obviously retain decisionmaking authority for the conduct of any offensive cyber operation, but the United States and Japan would share in the assessment of the consequences of malicious cyber activities and the threat actors and organizations responsible.

The first recommendation is about declaring the will to respond, if required. My second recommendation is about demonstrating the capability to do so, and this is not easy for a number of reasons peculiar to the cyber environment. Transparency about capabilities that originated in the darkness and the anonymity of underground communities that do not like exposure (the world of espionage, criminal activity, and political activism, for example), the legitimate need for protecting sensitive technical capabilities and methods, and the unique and dynamic nature of the cyberspace environment all make models for projecting traditional power in a demonstration of resolve and deterrence look much easier than doing so in cyberspace. What is the cyber equivalent of parking an aircraft carrier within sight of some adversary's coast? Any public demonstration that exposes a technical offensive cyber capability will "burn" that capability for any further use, so this must be factored into that decision. However, there are ways to demonstrate offensive cyber capabilities within certain parameters.

Options could include the public demonstration of a technical capability that has already been exposed, limiting public exposure in the demonstration to the military force and its people or skills, limiting public exposure in the demonstration to the effects of the operation rather than the technical capability that caused it, or any combination. The key to an effective deterrent effect is to demonstrate that the United States has credible options to impose costs on potential or active adversaries using offensive military cyber capabilities, and a policy to use them if necessary to defend the alliance. Because of both legal and cultural sensitivities, the United States and Japan should explore these options within the context of how Article 9 of Japan's Constitution applies to this concept.[18]

Applying Activities That Support Deterrence in the U.S.-Japan Alliance

The final element of the previous administration's cyber deterrence policy involves activities that support deterrence. These include some approaches already discussed, such as:

- bringing a whole-of-government and whole-of-nation approach to cyber incident response and national-level events (and as a natural progression, a whole-of-alliance approach within the cyber deterrence policy strategic framework)
- bolstering international engagement to improve collective defenses, foster law enforcement cooperation, and standardize capabilities required to combat cyber crime

[18] Constitution of Japan, promulgated on November 3, 1946, in effect on May 3, 1947. Article 9 refers to a renunciation of war.

- using the diplomatic instrument of power to create consensus regarding appropriate joint (or separate, but reinforcing) responses for malicious cyber activities of significant consequence
- leveraging the informational instrument of power to promote a nuanced and graduated declaratory policy and employing strategic communications to reinforce resolve while retaining ambiguity about response and consequence thresholds that discourage preemption or malicious cyber activities below any announced trigger.

There are a few additional activities mentioned in the Obama administration's policy that are worth noting, as they might also be applied to the U.S.-Japan alliance. These include further developing intelligence capabilities that improve the ability to attribute and act against malicious cyber activities, establishing peacetime norms of responsible behavior in cyberspace as part of international engagement, and conducting research and development to reverse the existing malicious attacker's advantage over the defense. My recommendations for each of these activities focus more on the role that the private sectors of each country can play in the alliance than on either government's role.

While there is an existing support relationship between the United States and Japan in intelligence-sharing that can be improved upon for cyber threats, my recommendation is to expand and empower the role that industry can play in cyber threat information- and intelligence-sharing. Exposure of the identity of malicious cyber actors and organizations, their capabilities, and their playbooks has been a key factor in changing their behaviors, including by reinforcing U.S. deterrence.

Examples include the public exposure of the Chinese and North Korean organizations and individuals identified earlier, but this was also a factor in the 2016 exposure of the Iranian actors and organizations involved in the distributed denial of service attacks against the U.S. financial sector and the infrastructure of a dam in New York. Most recently, identification and exposure of Russian intelligence and military actors and organizations and their malicious cyber activities associated with the 2016 U.S. election campaign continue to play a prominent role in U.S. government economic sanctions, diplomatic expulsions, and likely covert action directed against Russia. The surprising aspect of these events is that private-sector cybersecurity companies played a prominent role in every one of these exposures, either working with the U.S. government or separately.

What was once perhaps the sole purview of government intelligence agencies is now becoming more and more a function of the private sector as well. Government intelligence capabilities probably cannot do everything that is required to deal with the explosion of cyber threats. The United States and Japan should therefore build on the growing private-sector industry cyber threat intelligence-gathering and -sharing efforts and plan around how to leverage the private sector in alliance policy and implementation planning.

Regarding the activity of establishing peacetime norms of responsible state behavior in cyberspace, there is certainly room for the United States and Japan to work together within the alliance framework toward greater international acceptance of the idea that states should

- not conduct or knowingly support online activity that intentionally damages critical infrastructure or otherwise impairs the use of critical infrastructure to provide services to the public
- not conduct or knowingly support activity intended to prevent national computer security incident response teams from responding to cyber incidents
- not conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantage to its companies or commercial actors
- cooperate, in a manner consistent with its domestic law and international obligations, with requests for assistance from other states in investigating cyber crimes, collecting electronic evidence, and mitigating malicious cyber activity emanating from its territory.[19]

However, norms of responsible behavior in cyberspace should not be limited to governmental interaction because the vast majority of the cyberspace environment is owned, operated, and maintained by private industry.

Therefore, my recommendation is that the U.S.-Japan alliance should set an example of inclusion with the private sectors of both nations and encourage the development of complementary industry norms that can be showcased for the rest of the international community. Industry has keen interest in helping to shape contentious issues impacting such norms as the free flow of information across borders, mandatory insertion of "backdoors" into information technology products, the use of information security concerns as a pretext for trade restrictions, and even the right of businesses to "hack back," just to name a few.

My final recommendation for inclusion in the U.S.-Japan alliance policy for deterrence in cyberspace builds on the Obama administration's goals for research and development. The administration's policy stated, "The Administration seeks to shape the future of cybersecurity through a comprehensive plan and investment strategy to develop the tools, techniques, and national workforce necessary to continue to improve the resilience of U.S. computers, networks, and critical infrastructure and provide new technological options for deterring malicious cyber activities."[20]

From my recent industry experience, I know that one of the biggest challenges in reducing the attacker's advantage over the defender is about reversing three trends, and industry can lead the way in this effort. In my experience, the United States and Japan currently suffer significantly within their public and private sectors from a broad focus on each of the three legacy trends that follow. Therefore, reversing these legacy trends can greatly reduce cyber threats by increasing the cost of doing business, which can contribute to deterrence.

First, we must move away from legacy technology that is primarily focused on detection of and response to a cyber threat after an event and toward next-generation technology that is

[19] Sulmeyer, 2015, p. 13.

[20] Sulmeyer, 2015, p. 18.

focused on protecting our critical networks, systems, and information through a prevention-first mindset.

Next, we must move away from a legacy strategy of adding more and more-independent point solutions within our critical networks and systems. Point products are not designed to communicate with one another and look at only one specific portion of a cyber threat life cycle. Success requires an integrated platform approach that is organically built to look at the complete set of cyber threat life cycle threat indicators as a whole. This approach not only provides an alert when there is an actual threat (instead of the false positive "avalanche" from the independent point solution model, which focuses on isolated threat indicators in the absence of context) but also automatically pushes the required security controls out to the network enterprise to fix the vulnerability before there is widespread consequence. This reduces complexity, the need for more equipment and people, and ultimately the cost of effective cybersecurity.

Finally, reversing the first two trends is only possible by moving away from a legacy reliance on human decisionmaking and manual action and toward the use of automation. Automation is the key to successfully outmaneuvering a sophisticated and growing cyber threat. It is the only way to reverse the dynamic that is currently providing cyber threats the ability to leverage polymorphic malicious code to exponentially increase the number of attacks at decreasing costs. By turning this threat attack trend around, it is possible to return a better advantage to the defender.

The United States and Japan should establish joint operational requirements in their alliance policy oriented at leveraging the private industries of both countries. Then they should charge these industries with assisting both governments in reversing the three legacy trends listed to establish a more effective foundation for deterrence in cyberspace.

Conclusion

The strategic framework and elements of the Obama administration's cyber deterrence policy provide useful guideposts for the United States and Japan to apply in the development of an alliance policy for deterrence in the cyber gray zone. In this zone, events can blur the distinction between peacetime and armed conflict due to the fuzziness of what is happening and who is doing it. The framework recognizes that deterrence in cyberspace is essential, unique, and complex. Therefore, an effective strategy must involve a multipronged, multicomponent, and multiparticipant effort.

The components of this type of comprehensive strategy provide a sound approach for the United States and Japan. These components involve a careful description of what activities the policy seeks to deter, focus only on issues of significant consequence in the joint view of the alliance, and provide enough flexibility for the inevitable dramatic and rapid changes in the cyberspace environment. The elements also account for the reinforcing dynamic between deterrence by denial, deterrence by cost imposition (or punishment), and activities that support deterrence. Some of these are best done independently by each nation, while others should be done in varying degrees of coordination and synchronization. Finally, in undertaking activities that support deterrence, there is an enormous opportunity for private industry's participation in support of each nation's independent efforts, as well as the overall alliance.

Looking to the future, the United States and Japan should consider the concept of encouraging the formation of an allied cybersecurity cooperation in a regional, multilateral setting. This might encourage participation from South Korea, Australia, India, and other Asia-Pacific countries with compatible goals and challenged by common threats in the cyberspace environment.[21]

Because of the varying cultures, values, political systems, policies, objectives, priorities, and available resources involved in such a wide-ranging effort, I recommend an approach similar to that outlined for the United States and Japan. This would include the sequencing of independent national efforts along with other coordinated joint efforts to make progress manageable. Most importantly, I believe that the same basic strategic framework and elements as described in this paper would serve as a useful model for a broader allied security cooperation for the region.

[21] Summarized from an exchange of ideas with Scott W. Harold of RAND.

5. A Japanese Perspective on Deterrence in Cyberspace Gray Zone Contingencies and the Role of the Japan-U.S. Alliance

Keiko Kono, Ph.D. [1]
National Institute for Defense Studies
Ministry of Defense, Japan

In recent years, Japanese analysts have developed a new conceptual framework to describe situations where an adversary seeks to coerce Japan during peacetime with a set of military and nonmilitary actions that challenge the status quo while remaining below the threshold that would permit the invocation of the Treaty of Mutual Cooperation and Security Between Japan and the United States of America.[2] Such situations, which lie between *white*, or peacetime, environments and *black*, or wartime, situations are called *gray zone contingencies*. The government of Japan, adopting this line of analysis, has described a gray zone situation affecting Japan as one involving an infringement of the rights of Japan that does not amount to an armed attack. These include situations that are neither purely peaceful nor armed conflict contingencies and that derive from conflicting assertions between states over territory, sovereignty, or maritime economic interests.[3]

The GOJ has listed four types of gray zone situations. These include:

- an unlawful landing on a remote island by an armed group
- noninnocent passage by foreign warships in Japanese territorial or internal waters
- violence against Japanese private ships on high seas
- violence against U.S. and other states' forces acting in preparation for defense of Japan.[4]

[1] The views expressed herein are my own and do not necessarily represent those of the National Institute for Defense Studies or the Japanese Ministry of Defense.

[2] The Treaty of Mutual Cooperation and Security between Japan and the United States of America, signed on January 19, 1960, took effect on June 23, 1960. Ministry of Foreign Affairs of Japan and U.S. Department of State, 1960.

[3] "Cabinet Decision on Development of Seamless Security Legislation to Ensure Japan's Survival and Protect Its People," Prime Minister of Japan and His Cabinet, July 1, 2014, pp. 2–3; Ministry of Defense of Japan, 2016, p. 2.

[4] An addition of Article 95(2) to the Self-Defense Forces Act (Act No. 165 of June 9, 1954, as amended), by the Law Concerning Partial Amendments to the Self-Defense Forces Law and Other Existing Laws for Ensuring the Peace and Security of Japan and the International Community (the Legislation for Peace and Security), which was approved by the Diet in September 19, 2015, and came into effect in March 29, 2016. See Government of Japan, "Japan's Legislation for Peace and Security: Seamless Responses for Peace and Security of Japan and the International Community," Japanese Ministry of Foreign Affairs, March 2016. As the case of violence against the U.S. forces is not an infringement of the rights of Japan in a strict sense, a question has been raised on the legal basis for using weapons for the purpose of protection of U.S. and other forces by JSDF units. See Kentaro Wani, "The Concept of 'Unit Self-Defense' in International Law" (*Kokusaihō ni okeru 'unit self-defense' no hōtekiseishitsu to*

The term "gray zone" first appeared in official Japanese documents in 2013, but the concept is not new to Japan; the government has simply highlighted it so as to clarify its perception of a growing risk in light of more-assertive claims by some neighboring states.[5] This paper starts by sorting out various types of gray zone situations and their legal implications. The next section discusses some possible operational issues related to cyberspace gray zone scenarios involving Japan. The last section explores the feasibility of deterrence and the role of the Japan-U.S. alliance.

Considerations Related to Gray Zone Situations in Cyberspace Involving Japan

In its simplest form, the gray zone concept amounts to a use of force provided in Article 2(4) of the UN Charter.[6] According to the case law records of the International Court of Justice (ICJ), an armed attack is understood to be the gravest form of the use of force but is also merely a subset of the use of force as an overarching category of state action.[7] The criteria for determining both an "armed attack" and an instance of the "use of force" were formulated by the ICJ and are defined by the "scale and effects" of the operation, although, beyond this, the definition remains underdetermined.[8] One view on the latter issue that is prevalent within academic circles is that all deliberate forcible acts by states fall within the scope of the application of Article 2(4) of the UN Charter.[9] However, this is not the view that the GOJ has adopted, especially when the government assigns various missions to the JSDF. Table 5.1 shows the GOJ's view on the spectrum of operations between peacetime and an armed attack situation (also referred to as wartime) and scope of the gray zone situations.

igi), *Osaka Law Review (Handai hōgaku)* (in Japanese), Vol. 295, 2015; and Yuichiro Hitoshi, "Some Problems of Japan's New Legislation for Peace and Security from the Viewpoint of Unit Self-Defense: Implication and Limitation of JSDF's Protection of Foreign Armed Forces" (*Unit self-defense kara mita shin-anpohōsei no ronten*) (in Japanese), *The Reference*, No. 783, April 2016.

[5] Committee on Defense Posture Review, *Defense Posture Review Interim Report*, Japan Ministry of Defense, July 26, 2013; National Security Council, "National Security Strategy," Cabinet Secretariat, December 17, 2013; Ministry of Defense of Japan, 2013c.

[6] Chapter I, Article 2(4) reads: "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." United Nations, Charter of the United Nations and Statute of the International Court of Justice, San Francisco, Calif., 1945.

[7] International Court of Justice, *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)*, June 27, 1986, p. 101, para. 191.

[8] International Court of Justice, 1986, p. 103, para. 195.

[9] Tom Ruys, "The Meaning of 'Force' and the Boundaries of the Jus ad Bellum: Are 'Minimal' Uses of Force Excluded from UN Charter Article 2(4)?" *American Journal of International Law*, Vol. 108, No. 2, 2014.

Table 5.1. The Japanese Government's View of the Peacetime-to-Wartime Spectrum and the Scope of Gray Zone Contingencies

Category of Situations	Legal Basis in the Self Defense Forces Act
A: Armed Attack • JSDF in the lead *Japan-U.S. mutual security treaty Article 5 most likely to be invoked*	• Art.76: Defense Operation
B-1: Gray Zone (1) Use of Force • JSDF involved in support of Japanese civilian law enforcement agencies • More grave form of coercive/destructive • activities by a state (includes actions by nonstate actors attributable to a state) *Article 5 could be invoked*	• Art. 78: PSO by Order • Art. 82: MSO
B-2: Gray Zone (2) Actions Not Amounting to Use of Force • Japanese civilian law enforcement in the lead • JSDF on stand-by to support if civilian law enforcement incapable of managing situation • Less grave form of coercive/destructive activities by a state or coercive/destructive activities performed by nonstate actors not attributable to a state *Article 5 less likely to be invoked*	• Art. 78: PSO by Order • Art. 82: MSO
C: Peacetime: • Japanese civilian law enforcement in the lead *Article 5 not invoked*	Self-Defense Forces Act does not apply

SOURCE: Author's elaboration based on classification and definition of an armed attack, use of force, and gray zone situations used by the GOJ in various sources, including the Self-Defense Forces Act. Government of Japan, 1954. See, also, Ministry of Foreign Affairs of Japan and U.S. Department of State, 1960.

Regarding Situation A in Table 5.1, the GOJ defines the criteria constituting an armed attack as requiring an organized and systematic use of force against Japan.[10] In the case of an armed attack, Article 5 of the Japan-U.S. mutual security treaty can be invoked. And regarding the concept of a use of force such as that described in Situation B-1, the GOJ defines it as an act of combat by a state as part of an international armed conflict.[11] The concept of a gray zone use of force as described in B-1 is also defined in the Ministry of Defense's white papers as an act of combat, generally carried out by "a state or quasi-state organization" actor, and regarded as amounting to the use of force during an instance of international armed conflict.

[10] This definition is in sharp contrast to the U.S. government's position that "the inherent right of self-defense potentially applies against *any* illegal use of force." Harold Hongju Koh, "International Law in Cyberspace," *Harvard International Law Journal Online*, Vol. 54, 2012, p. 7.

[11] The government has clarified that, in its view, the meaning of "use of force" in Article 2(4) of the UN Charter, Article 1 of the Japan-U.S. mutual security treaty, and Article 9 of the Constitution of Japan are all the same. Comment No. 27 by the Government of Japan to a Question by House of Representatives (Lower House) Member Seiichi Kaneda on "The Difference Among 'War,' and 'Dispute,' and 'Use of Force,' etc." at the 153rd session of the Diet (Extraordinary session of 2001), Cabinet Decision (in Japanese), February 5, 2002.

But such a use of force does not constitute the lowest limit of the gray zone. The Ministry of Defense white paper suggests that the GOJ does not consider certain coercive or forcible acts by the JSDF conducted against “a state or quasi-state organization” as a use of force under the UN Charter. According to its formulation, certain forcible measures under Article 36 (self-defense) and Article 37 (averting present danger) of the Penal Code[12] are defined as a passive and limited use of weapons, not constituting a use of force.[13] Accordingly, it is possible that a B-2 gray zone situation, composed of a less grave form of forcible activity, falls below the threshold of a use of force. An offender in a B-2-type situation could be a state or nonstate group.

The GOJ has traditionally premised its defense and national security policies on the notion that an incident of the use of force in international relations is only possible between states; violent activities by foreign nonstate actors are generally not recognized as instances of the use of force under Japanese government policy unless they are attributable to a foreign government.[14] Regarding coercive acts by a state, these may or may not constitute a use of force, depending on the gravity of the incident. For example, in the incident of illumination of a fire-control radar by a Chinese warship that occurred in 2013, then–Defense Minister Satoshi Morimoto stated that it could amount to a use or threat of force under the UN Charter depending on the overall circumstances at the time.[15]

The next relevant question is how, if a gray zone incident does occur, could the GOJ deal with it? Relevant international agreements and other rules of international law imply that states have certain rights and responsibilities when they are facing a gray zone incident.

First, states have a right to make individual military responses to unlawful acts, even if that preceding act does not constitute an armed attack.[16] These are known as countermeasures to internationally wrongful acts under Article 22 of the UN International Law Commission’s Articles on State Responsibility.[17] Accordingly, a response to a gray zone situation could be justified on the condition that it meets the requirements for legal exercise, even if the GOJ’s

[12] Government of Japan, Penal Code, Law No. 45, as amended, April 24, 1907.

[13] Ministry of Defense of Japan, 2016, pp. 416–417.

[14] It is a natural consequence that derives from the definition of a use of force by the GOJ. As noted earlier in the chapter, the GOJ focuses on “a state or quasi-state organization” as an actor capable of exercising the use of force. Nonstate actors have been excluded from the scope of application in terms of legal personality. To take a hypothetical example, a military provocation by local armed groups operating out of another state and the responsive defensive measures by a JSDF unit would not constitute a use of force.

[15] Ministry of Defense of Japan, “Press Conference by the Defense Minister,” transcript, February 8, 2013a.

[16] Terry D. Gill, “Non-Intervention in the Cyber Conflict,” in Katharina Ziolkowski, ed., *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy*, Tallinn, Estonia: NATO NATO Cooperative Cyber Defence Centre of Excellence, 2012, pp. 230–232, 236–237.

[17] James Crawford, *The International Law Commission’s Articles on States Responsibility: Introduction, Text and Commentaries,* Cambridge, UK: Cambridge University Press, 2002.

response measures could infringe on the rights of another state, such as the sovereign immunity of an offending state or flag state jurisdiction.[18]

Second, the GOJ has recognized its primary responsibility to respond to "serious cyber incidents that affect the security of Japan" under the Japan-U.S. Revised Defense Guidelines, suggesting that the government is increasingly viewing cyber gray zone coercion as a subset of the broader universe of gray zone challenges that it has the responsibility and authority to address.[19] The document does not refer to gray zone situations specifically but notes "the two governments will take measures to ensure Japan's . . . security in all phases, seamlessly, from peacetime to contingencies, including situations when an armed attack against Japan is not involved."[20]

In terms of the legal basis for responding to a gray zone incident, there are several articles in the Japan Self-Defense Forces Act that apply. For example, both Article 78 (on PSOs by order)[21] and Article 82 (on MSOs)[22] could be invoked to dispatch JSDF units in the event of an illegal landing on a remote island by an armed group. These measures are sometimes described as reflecting a "minor self-defense right," but that description has nothing to do with the right of self-defense provided in Article 51 of the UN Charter. Even those who apply this description know well that these measures are actually law enforcement activities. For the purpose of drawing a distinction between the two phenomena, the use of force by the JSDF in time of peace (all cases other than an armed attack situation) is usually described as a law enforcement measure involving the use of weapons, while the use of force undertaken in time of an armed attack is described as a use of force.[23] For this reason, even though the JSDF may be compelled to use its weapons or other equipment in a gray zone situation, it is not presumed to be using force in accordance with the meaning of the UN Charter.

[18] Crawford, 2002, Part III, Chapter II.

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

[20] Ministry of Defense of Japan, 2015, p. 4.

[21] A PSO by order is initiated when an indirect aggression or other emergency occurs and the law enforcement authorities are not able to address it. There have not been cases where this provision was invoked.

[22] An MSO was invoked for the first time when two North Korean spy vessels disguised as Japanese fishing boats entered the territorial sea off the Noto Peninsula in 1999. Ministry of Defense of Japan, *Defense of Japan 1999,* annual white paper, Tokyo: Urban Connections, 1999, pp. 208–214; National Police Agency, "Terrorism by the Democratic People's Republic of Korea (North Korea)," *Focus*, Vol. 271, 2006, p. 18. See also Ministry of Defense of Japan, 2016, pp. 414–415, Reference 24: Main Operations of the Self-Defense Forces.

[23] For those who take the former view, the government's proposition is not persuasive at all. They argue that "the use of weapons" by the JSDF amounts to a use of force under international law, when it is conducted in international relations. See Masahiko Asada, "Japan and the Right of Individual Self-Defense" (*Nihon to jieiken: kobetsutekijieiken wo tyu-shin ni*), in Japanese Society of International Law, ed., *National Security* (in Japanese), Tokyo: Sanseidō, 2001, p. 51.

Considerations Related to Cyberspace Gray Zone Contingencies Involving Japan

Japanese experts believe a cyber attack might be conducted against the country, either separately or in tandem with other actions undertaken during a broader gray zone situation.[24] Indeed, cyber attacks against Japanese government and private companies have already been undertaken, with one of the most wide-scale examples having occurred in 2012. The Chinese hacker group "Honker Union" called for cyberattacks against Japan in retaliation for the purchase of the Senkaku Islands by the GOJ from a private Japanese owner. In postings to the Chinese microblog *YY Chat*, the hacker group discussed its plan to attack Japanese websites, distributed information about attack vectors and software vulnerabilities, and congratulated itself on successfully striking Japan via cyberspace. It also claimed Chinese ownership over Uotsuri-shima of the Senkaku Islands and boasted about having awakened the patriotic spirit of Chinese youth.[25] While it is unclear whether Honker Union is indeed a purely private group, there are numerous hacker groups in China and many of these groups are believed to be working, at least on an "as-needed" basis, at the behest of the Beijing government. In the future, if China attempts to use gray zone coercion again, it is likely that cyber attacks will be a part of its overall coercive approach.

Separately, current Japanese policy distinguishes two discrete types of cyber attacks in the context of a large-scale cyber attack: cyber armed attacks and cyber terrorism.[26] The concept of "cyber gray zone attacks" will be added to the list in the future. According to the GOJ's annual plan on cybersecurity in 2016, Tokyo defines a *large-scale cyber attack* as a national emergency that has caused, or is likely to cause, material damage to the lives, bodies, or property of Japanese citizens.[27] It describes an example of a cyber attack resulting in a death or injury of citizens and breakdown in the functioning of critical infrastructure.[28] By contrast, cyber crime is

[24] Hiroshi Ito, *The Fifth Battlefield: Threat of Cyber Warfare* (*Dai go no senjō: Saiba-sen no kyōi*) (in Japanese), Tokyo: Bungeishunju, 2012; Motohiro Tsuchiya, *Cyber Terrorism: Japan, the U.S. vs. China* (*Saiba-tero; Japan, the U.S. vs. China*) (in Japanese), Bungeishunju, 2012. According to Tsuchiya, a combination of cyber and conventional attacks is highly likely to be employed in a future war.

[25] National Police Agency, ed., "Cyber Attack Situation," *Focus* (in Japanese), Vol. 282, 2013, p. 35; Public Security Intelligence Agency of Japan, *Annual Report 2012: Review and Prospects of Internal and External Situations,* 2013, p. 47; Laura Saporito and James A. Lewis, *Cyber Incidents Attributed to China*, Washington, D.C.: Center for Strategic and International Studies, 2013.

[26] A classification of national emergencies by the Japanese government makes explicit reference to both an armed conflict and cyber terrorism. These are described on the Japan Cabinet Secretariat website. Cabinet Secretariat, "Main Classifications of Emergency Situations" (in Japanese), undated.

[27] Japan Cybersecurity Strategic Headquarters, "Cyber Security Annual Plan 2016" (in Japanese), National Center of Incident Readiness and Strategy for Cybersecurity, August 31, 2016, p. 18. The definition of the "large-scale cyberattack" derives from the concept of "an emergency" in Government of Japan, Cabinet Law, Law No. 5 as amended, Article 15 (2), January 22, 1947.

[28] Japan Cybersecurity Strategic Headquarters, 2016, p. 34.

not generally considered to rise to the level of a national emergency because it does not result in sufficiently widespread or high-impact consequences. The Japanese government classifies each type of large-scale cyber attack in relation to its effects on the physical domain, as well as its gravity, the identity of the perpetrator, and other relevant circumstances (see Table 5.2).

Table 5.2. Classification of Large-Scale Cyber Attacks

	State or Quasi-State Actor(s)	Nonstate Actor(s)	Gravity
A: Armed Attack	○	○	Cyber Armed Attack
B-1: Gray Zone (1) : *Coercive Act Amounting to Use of Force*	○		Cyber Gray Zone
B-2: Gray Zone (2) : *Coercive Act Not Amounting to Use of Force*	○	○	
C: Peace Time: Cyber Crime	○	○	Cyber Terrorism

SOURCE: Author's elaboration based on Japan Cybersecurity Strategic Headquarters, 2016; Cabinet Secretariat, undated.

In the light of recent state practices, the GOJ has developed its view on the right of self-defense, by which it would see a nonstate actor as the perpetrator of an armed attack if the attack were comparable to an armed attack by a foreign state because of its scale and effects.[29] On the other hand, if the perpetrator of a cyber attack not amounting to an armed attack is a nonstate actor and the government is not able to confirm any attribution to a foreign state, there is a high possibility that the incident will be dealt with by the police in the same manner as an ordinary cyber crime. Yet as a prerequisite for dealing with a cyber attack, the threshold of a cyber armed attack is a pending issue among many countries. The question of how existing international law can be applied to cyber activities has been discussed in the UN Group of Government Experts (GGE) on cybersecurity. And, as a member of the cyber GGE, Japan has been active in trying to shape the norms and rules that apply to online activities.[30]

[29] Fumio Kishida, remarks at the Committee on National Security of the House of Representatives (Lower House) at the 187th session of the Diet (Extraordinary session of 2014), *Report of the Committee on National Security of the House of Representatives* (in Japanese), No. 2, 2014.

[30] See the GOJ's response to UN General Assembly Resolution 70/237. United Nations General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security*, Report of the Secretary-General, U.N. Doc. A/71/172, July 19, 2016, pp. 11–12.

When it comes to cyber terrorism, no specific provision in Japanese domestic law provides a clear definition of the characteristic traits of this phenomenon, but we can find a practical definition in various documents, such as the *White Paper on Police 2012* and statements at the Diet by senior officials from the National Police Agency. According to these sources, *cyber terrorism* is defined as "an electronic attack on the core systems of a critical infrastructure, or serious failure in the core system of a critical infrastructure that is highly probable to have been caused by an electronic attack."[31] The National Police Agency is designated as the lead agency in responding to instances of cyber terrorism.

With reference to critical infrastructure, there has not been a uniform definition in international agreements, but in official documents, such as *The Basic Policy of Critical Information Infrastructure Protection,* the GOJ designates it as the following 13 sectors: information and communication systems, finance, aviation, railways, electricity, gas, government/administrative services, medical, water, logistics, chemical, credit card services, and the petroleum industry.[32] The *White Paper on Police 2012* states that, to date, Japan has not experienced any significant damage as a result of cyber terrorism targeting the nation's critical infrastructure.[33]

On the other hand, the Japanese government has not mentioned cyber attack issues in the context of the gray zone situation; no policies or guidelines to deal with such scenarios appear to exist in official government documents. The GOJ does not seem to be excluding the possibility of cyber gray zone situations in the future, however—it may simply not yet have thought through these issues fully within the context of a gray zone contingency framework. Additionally, the four kinds of gray zone scenarios described may just be examples that do not exhaust the universe of possible contingencies, and the government's response may be inferred through reasoning by analogy.

For example, with regard to an unlawful landing on a remote island by an armed group, if the JCG and the National Police Agency were incapable of responding effectively, the JSDF could be called upon to conduct a PSO by order under Article 78 of the JSDF Act, as noted. That article applies to a situation in which the law enforcement authorities are not capable of suppressing violence and maintaining public security through their own efforts. Assuming that the same requirements would be applied to an instance of gray zone coercion in cyberspace, the JSDF could be mobilized to respond under the same authorities.

[31] *Cyber terrorism* is mentioned in the context of cyber attack and should not be confused with electronic warfare. National Police Agency, *White Paper on Police 2012*, digest edition, 2012, p. 30; Information Security Policy Council, *Information Security 2012*, No. 19, July 4, 2012, p. 20.

[32] Information Security Policy Council, *The Basic Policy of Critical Information Infrastructure Protection*, 3rd ed., May 19, 2014, updated by the Japan Cybersecurity Strategic Headquarters, May 25, 2015, p. 9.

[33] National Police Agency, 2012, p. 30.

According to official Japanese documents, the government is tackling the issue of a possible large-scale cyber attack through the following approaches.[34] First, the Cabinet Secretariat is organizing an initial response exercise to be conducted in collaboration with other ministries and private-sector actors. Second, the government has set up the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) within the Cabinet Secretariat for the purpose of supervising the information networks of the government. The NISC has been assigned the following three tasks: performing continuous 24-hour network monitoring, conducting cybersecurity audits, and engaging in investigations in serious incidents. The NISC is considered "the leading organization of [the GOJ] for cybersecurity issues."[35] But its responsibilities are limited in scope, covering only the central government bodies, incorporated administrative agencies, and designated corporations, such as special corporations and authorized corporations.[36] Other private-sector actors are not under the supervision of the NISC. The NISC also is not authorized to conduct a criminal investigation, nor can it respond to large-scale cyber attacks that do not fall within its jurisdiction.

In 2014, the Ministry of Defense established a "cyber defense group" under the Command, Control, Communications, and Computer Systems Command of the Joint Staff Office. As the NISC is responsible for 24-hour monitoring of the communications and network systems of all central government agencies (including the Ministry of Defense), it should detect the initial signs of a cyber attack through sensors set up at the entry points of central government agency network systems. Therefore, if a malicious file is sent to the Ministry of Defense from outside of Japan and sensitive information flows out to overseas destinations designated by criminal groups, the NISC will be able to detect the security breach and notify the Ministry of Defense of the incident. On the other hand, the Ministry of Defense is operating a pair of unique information systems inside the ministry at all times called the Defense Information Infrastructure and Central Command System. These systems monitor all communications by JSDF members and Ministry of Defense employees around the clock. The Ministry is responsible for the protection of its own systems and networks. Not surprisingly, the Ministry's Cyber Defense Group only responds to cyber threats carried on the JSDF's own network system. Some Japanese misunderstand the missions to be undertaken by the Cyber Defense Group, arguing that it should also protect civilian network systems. The JSDF, however, is not allowed to take any measures unless provided with the legal authority to do so via domestic legislation. Moreover, its core mission is to ensure the secure command and control over the JSDF networks, and this is appropriately its

[34] Government of Japan, "Cybersecurity Strategy," Cabinet decision, September 4, 2015; Japan Cybersecurity Strategic Headquarters, 2016.

[35] Yasuhiko Taniwaki, "Cybersecurity Strategy in Japan," presentation at the Sasakawa Peace Foundation USA's Third Annual Security Forum: American and Japanese Interests and the Future of the Alliance, May 6, 2016.

[36] The NISC has expanded its authority after a cyber incident of the Japan Pension Service occurred in 2015 and has brought some special corporations—such as the Pension Service—under its supervisory control. See Motohiro Tsuchiya, "Japan-U.S. Cooperation in Cybersecurity," in Harold et al., 2016.

highest priority. A media report last year revealed that the Ministry of Defense was victimized by a sophisticated cyber attack that might have compromised the Defense Information Infrastructure system.[37]

In addition, several issues would need to be addressed for the JSDF to assume new missions in the cyber domain. The GOJ has adopted a so-called positive list scheme in its legal system, which means that government agencies—such as the police, the JSDF, or any other government organizations—always need permission to take action. In the absence of such authorization based on legal authority, any operation would constitute a violation of discipline, at a minimum, and in the worst case would represent a criminal act, even if it appeared justified due to time pressures in an emergency situation. Indeed, compared with other government organizations, such as the National Police Agency, a much higher threshold is applied to the JSDF because their missions have always been controversial in Japan in the post–World War II era. Japan is also still grappling with the question of the scope of the use of weapons in cyberspace operations. At present, the very concept of "use of force" in cyberspace is still unclear.[38]

A separate question is the geographical scope of cyber measures permitted in response to gray zone contingencies. According to the traditional interpretation of the Japanese government, Article 9 of the Constitution of Japan does not generally permit JSDF units to be dispatched to a foreign state with the aim of using force, even in the event of an armed attack on Japan.[39] This is because such steps would exceed the requirements the Constitution and related legislation have established for the legal exercise of the right of self-defense, which permit the JSDF to respond only up to the minimum necessary level of force for the purposes of self-defense.

The government will need to consider whether such standards are relevant or useful for responding to gray zone contingencies involving cyberspace or whether a response measure can be executed against the source of an attack within an offending state, especially if this is the only option left. The government must also consider whether a response can be made against nonstate actors, such as private hacker groups that are operating out of another state that may lack the capacity or the will to take action against the group (or may even be encouraging or controlling it).

If a cyber incident cannot be imputed to a state but foreign authorities are incapable of responding or refuse to assist in investigating and arresting the suspected perpetrators of a cyber attack (for whatever reason), the government would face a significant challenge. Given that the Japanese government is inclined to attach great value to the obligation to respect the sovereignty and territorial integrity of other states in peacetime, it is highly likely that it would be cautious

[37] "Defense Ministry, SDF Networks Hacked; State Actor Suspected," *Japan Times*, November 28, 2016.

[38] See Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of The NATO Cooperative Cyber Defence Centre of Excellence*, Cambridge, United Kingdom: Cambridge University Press, 2013, p. 48.

[39] See Constitution of Japan, 1947.

about the prospect of using force to respond to a coercive act originating overseas in a cyberspace gray zone contingency.

Deterrence and the Role of the Japan-U.S. Alliance

With regard to deterrence, especially deterrence by punishment, possession of offensive cyber capabilities could be an effective option. However, the Japanese government has numerous hurdles to overcome before it could develop an approach based on this deterrence model. Such a development would have to be reviewed in light of the current framework regulating JSDF operations. At a minimum, cyber intelligence operations would be a necessary condition for deterrence. Some experts in Japan claim that if the JSDF engages in hacking into the network systems of a foreign government for the purposes of collecting intelligence, such operations would be tantamount to a crime of "unauthorized computer access" under Article 2(4) of the Act on the Prohibition of Unauthorized Computer Access.[40] According to this argument, all that Japan can do under existing legislation is engage in open-source intelligence collection operations.[41]

In contrast, while deterrence by denial presents fewer legal hurdles, it is difficult to achieve in practice because Japan relies heavily on information technology systems and there are a very large number of points of vulnerability, many of which lie outside of the control of the government and in the hands of private-sector actors. Thus, while raising the resiliency of network systems is a necessary component of an overall cyber deterrence posture for Japan, it is insufficient in the absence of additional steps.

In light of these considerations, the government might need to examine whether its current technical means, legal authorities, and deterrent strategy are sufficient to prevent a destructive cyber attack. Technically, shutting down all internet traffic to and from Japan might be an attractive option, a capability that was demonstrated in Estonia when that nation came under cyber assault by the Russian Federation in 2007. Legally, the right to the secrecy of correspondence guaranteed by Article 21 of the Japanese Constitution also needs to be closely scrutinized in light of the requirements of national security in the cyber age.

With regard to the role of the U.S.-Japan alliance in cyber gray zone situations, both states will be able to cooperate on a more reciprocal basis if the GOJ adopts some of the solutions proposed here, such as adopting offensive cyber capabilities, implementing cyber intelligence operations, and raising the resilience of network systems. As a prerequisite to deepening

[40] Government of Japan, Act on Prohibition of Unauthorized Computer Access, Law No. 128, August 13, 1999. In addition to the description above, Professor Fumiaki Yamazaki also claims that if the JSDF engages in the development of cyber weapons, it may commit a crime of electromagnetic records giving unauthorized commands (developing a computer virus) under Article 168 of the Penal Code (Government of Japan,1907). Fumiaki Yamazaki, "Challenges and Proposal for Cyber Security in Japan" (*Nihon no saiba-sekyuriti no kadai to teigen*) (in Japanese), NEC Corp. website, August 30, 2013.

[41] The argument does not touch upon usual signals intelligence operations, such as detecting electromagnetic waves.

cooperation on cyberspace deterrence measures, the GOJ must explain when and how an instance of gray zone coercion might occur in cyberspace. Additionally, both the United States and Japan would need to develop a shared understanding of the specific character of an incident were one to occur.[42] There is no doubt that Japan will have to assume the primary responsibility to act in a gray zone incident targeting Japan via cyberspace, but there may be room for cooperation with the United States aimed at preventing an escalation to full-scale warfare.

Conclusion

This chapter has discussed several issues associated with possible cyber gray zone contingencies that could arise in Japan in the future. With regard to an upper limit of the gray zone, the GOJ recognizes that "cyber activities could amount to . . . an armed attack," and it has reserved the option to invoke its right to self-defense in responding to such scenarios.[43] On the other hand, it is far less clear where the lower limit of gray zone coercion lies in cyberspace. The government's description suggests that it would involve coercion that the police cannot address effectively, yet it is unclear which criteria are used to determine when an incident exceeds the capacity of the police to respond. Moreover, if the government's goal is just to repel an attack (as might be implied by the notion of an "exclusively defense-oriented defense policy"), and if it is not interested in striking back at the source of an attack, the government may believe that offensive cyber capabilities exceed the required minimum response capabilities.[44] In that case, the government is less likely to assign any response mission to the JSDF.

In short, the lower limits of gray zone coercion may vary by domain, with cyberspace being perhaps the least amenable to JSDF actions aimed at deterrence; the threshold in the cyber domain might be higher than in maritime gray zone contingencies, for example. Therefore, when the government articulates its policy and guidance on the role of the JSDF in responding to gray zone situations in cyberspace, it will need to tackle complicated questions, such as how to define cyberspace gray zone situations, which organizations are tasked with responding to them, at what point responsibility shifts in the course of an unfolding instance of gray zone coercion in cyberspace, and how the lead agencies are permitted to respond.

[42] Development of such shared understandings could be facilitated through intelligence cooperation and information-sharing between the United States and Japan.

[43] "G7 Principles and Actions on Cyber," adopted at the G-7 Ise-Shima Summit on May 27, 2016, Ministry of Foreign Affairs of Japan website, undated.

[44] This policy belongs to the GOJ's basic policies on national defense. See Ministry of Defense of Japan, "Fundamental Concepts of National Defense: Basics of Defense Policy," undated-b.

6. Space Deterrence, the U.S.-Japan Alliance, and Asian Security: A U.S. Perspective

Dean Cheng
Senior Research Fellow
The Heritage Foundation

Since the beginning of the Space Age 60 years ago, outer space has played an increasingly central role in international security. The strategic high ground of space has afforded visibility into states that had previously been "a riddle wrapped in a mystery inside an enigma." It is this increased transparency that allowed the United States and Soviet Union to engage in arms control agreements and détente with some degree of confidence. Over the past quarter-century, space has moved from providing strategic intelligence to becoming a central part of the basic approach to modern U.S. war-fighting, as well as the approaches of a number of other advanced militaries. Space-based systems have enabled widely separated forces to coordinate their activities and engage at previously inconceivable ranges. Consequently, just as space operations are increasingly essential for modern warfare, they are also becoming a major factor in deterrence calculations. This applies not only to "basic deterrence" situations (where the United States seeks to deter aggression against itself) but also "extended deterrence" situations (where the United States strives to deter aggression against key allies, such as Japan).

With space deterrence increasingly important to the United States and its allies, this chapter will explore the following questions:

- How does the United States conceive of space deterrence?
- What threats does the United States perceive to its space assets?
- How does China, widely regarded as one of the greatest potential rivals to the United States in space, view the question of space war and space deterrence?[1]
- What do the answers to these questions suggest about the value of the U.S.-Japan alliance for meeting the challenges that the United States faces in deterring attacks on its own and allied space systems?[2]

[1] This chapter focuses first on the United States and China as the two major actors in space and national security in the Asia-Pacific, then turns to a discussion of the role of Japan and the U.S.-Japan alliance.

[2] As with Chapter 2 and Chapter 4, this chapter focuses a bit more heavily on traditional space missions and deterrence while also touching on gray zone issues, while Chapter 7 deals with gray zone scenarios a bit more fully. As noted, space, as a domain, is inherently quite gray because attribution of actor and intent is extremely difficult, much like in cyberspace. Thus, general discussions of deterrence in space necessarily touch, to some extent, on deterrence of gray zone operations in space.

Space Missions and Western Pacific Security

The tactical role of space systems rose to public prominence as a component of U.S. warfighting in the first Gulf War (Operations Desert Shield and Desert Storm), as images of munitions using space-derived guidance information precisely hitting their targets were projected around the world. At the same time, products of ISR platforms, which had previously been highly classified as part of "national technical means," were now revealed to both operating forces and the global audience. In subsequent wars in the Balkans, Afghanistan, and Iraq, the ubiquity of space systems in modern military operations was underscored.

Given the distances encompassed within the Asia-Pacific theater, now extending even to the Indian Ocean as part of the "Indo-Pacific," space-based systems play a central and growing role in coordinating forces and creating a common situational picture. This reliance on space is especially great for U.S. forces, because they are typically conducting expeditionary operations far from the U.S. homeland. Consequently, space capabilities will likely play an outsized role in key mission areas in future conflicts between technologically enabled militaries; space assets will play a critical role in such areas as ISR, meteorology, communications, PNT, and SSA. These are explored in turn.

Intelligence, Surveillance, and Reconnaissance

ISR functions are perhaps the most widely recognized uses for satellites. The notion of spy satellites capable of maintaining watch over much of the globe has been popularized in print and film almost since the dawn of the Space Age. In fact, many of the earliest satellites were intelligence-gathering systems (even if not publicized as such). Several of the earliest U.S. satellites were part of the CORONA program of electro-optical surveillance satellites. Similarly, some of the first Soviet satellites were reconnaissance platforms (i.e., the Zenit series, which began deployment in 1961).

The range of information that ISR systems now collect has greatly expanded over the intervening half-century. While there are still imaging satellites, they not only operate in the visible light part of the spectrum but also in other bands. Synthetic aperture radars (SARs), for example, provide radar imaging through clouds and fog. Other types of intelligence gathered by space-based systems include signals intelligence about various states' communications systems, electronic intelligence about various states' radars and other electronic systems, and detection of missile launches and nuclear detonations.

Of particular importance for the United States is missile early warning. The United States has long relied on space-based systems to detect missile launches, providing the President and other key military and civilian leaders with warning of possible attack on the United States. Since the first Gulf War, space-based systems have also been employed for countering tactical missile launches. Patriot, THAAD, and Aegis ballistic missile defense functions depend on space-based systems for cueing. Russia has also devoted substantial effort to detecting missile launches from space. Interestingly, the Chinese PLA has not pursued space-based missile early warning. As of 2017, China had not officially deployed such a system, although there are reports that it may deploy one or more such satellites in the near future.

Both China and the United States field an array of ISR systems, including electro-optical imaging satellites, SAR satellites, and intelligence collection satellites.

Meteorology and Earth Observation

An important subset of imaging satellites involves Earth observation satellites. These provide a variety of data about the Earth and its environment. Some measure the Earth's magnetic and gravitational fields; others monitor changes in ground cover due to changes in the season. Still others observe Earth's atmosphere, including changing weather patterns. While these satellites are mainly serving civilian functions, their information is also often incorporated into maps and other military information databases.

Indeed, accurate, timely meteorological information is essential for successful air and maritime operations. The Allies succeeded on D-Day in part because they had access to more-complete meteorological information and could better predict weather conditions over the English Channel on June 6, 1944. Similarly, U.S. forces were able to operate amid sandstorms and other adverse weather conditions during Operation Enduring Freedom (the 2003 invasion of Iraq) because of U.S. access to meteorological and ISR satellites. Such systems will be at least as central in supporting operations in the western Pacific should a conflict break out there in coming years.

Both the United States and China currently deploy an array of meteorological satellites at both low-Earth orbit and geosynchronous orbit.

Communications

Among the most important roles for space is the provision of communications support. The distances involved in operating U.S. military forces in and around the western Pacific, South China Sea, and Indian Ocean place a premium on space systems to provide globe-spanning communications. In peacetime, much of the bandwidth for both voice and data transmissions are shouldered by the network of submarine cables.[3] These, however, may not survive intact in time of conflict; at the same time, satellite communications are the only means of providing real-time long-range communications at the requisite data rates for ships at sea and for unmanned aerial vehicles (UAVs). Both submarine cables and satellite communications are likely to be threatened in the event of conflict.

This reliance on space architectures for communications and other critical deterrence and war-fighting support and enabling functions poses a particular challenge because of the

[3] Douglas Main, "Undersea Cables Transport 99 Percent of International Data," *Newsweek*, April 2, 2015.

asymmetry of geography. In the event of a military contingency in the Indo-Pacific, U.S. forces must be prepared to operate far from U.S. shores, and potentially even at substantial distances from key bases, such as Guam, which is three steaming days from the Philippines and the South China Sea.[4] By contrast, the homelands of such potential adversaries as China and the Democratic People's Republic of Korea are already in theater. These nations not only possess interior lines but can employ a variety of communications methods, including fiber optic land lines, cell phones, microwave, and radio. Many of these capabilities are protected behind their own borders.

Both China and the United States have communications satellites at geosynchronous orbit. China's Beidou navigation satellite system also has the ability to transmit text messages. Both nations can also access commercial communications satellites.

Position, Navigation, and Timing

Another vital system is the constellation of PNT satellites, such as the U.S. Global Positioning System (GPS) network and the Chinese Beidou network. These satellites allow very precise location determination, including at sea. This precision, in turn, allows for not only better coordination of various forces and activities (by knowing where both friendly and adversary forces are located) but also better weapon accuracy (by very precisely determining both the launch and aim points). Even if a weapon is not guided by GPS signals, knowing precisely where the weapon's starting point is can contribute substantially to improved accuracy.

PNT systems, however, not only are useful for providing precise locations on the trackless oceans but play a vital part in other activities. Many frequency-hopping, spread-spectrum radio systems, including military ones, employ the timing function of satellites (with their global coverage) to synchronize their frequency shifts. Electronic intelligence and identification-friend-or-foe systems also rely on the precise timing signals from such systems as GPS to operate.[5]

Space Situational Awareness

While the various space-based systems provide vital information support, SSA is central to coordinating their activities, ensuring safety of flight, and maintaining awareness of potential threats. According to the U.S. military, SSA "involves characterizing as completely as necessary the space capabilities operating within the terrestrial environment and the space domain."[6] SSA spans a range of activities, including space surveillance; maintaining a clear picture of the status of U.S. and other nations' satellite systems; and monitoring of the space environment, including space weather and unidentified space objects. Good SSA can not only provide satellite operators

[4] Robley Blandford, *Pacific Dilemma: Basing, Access, and Forward Deployment,* Newport, R.I.: Naval War College, 1996, p. 14.

[5] John R. Vig, "Accurate Clocks and Their Applications," Princeton ACM, November 2011.

[6] U.S. Joint Chiefs of Staff, *Space Operations*, Washington, D.C.: Government Printing Office, JP 3-14, May 2013.

with early warning of possible collisions or space weather problems but, in the event of conflict, could play a central role in both offensive and defensive space operations. Methods of SSA include the use of radar, telescopes, and various intelligence sources, as well as space-based systems.

The United States particularly benefits from its network of alliances and bases to provide it with a global SSA network, supplemented increasingly by such space-based systems as the Geosynchronous Space Situational Awareness Program, which can provide characterization of other satellites. The United States has access to some of the best SSA data and regularly provides information about the overall space situation to other spacefaring states, including China.[7]

Challenges Facing the Space Operating Environment

Space power—i.e., the ability to exploit space in support of national goals—is not only a matter of placing satellites in orbit. Those satellites must have a supporting infrastructure if they are to provide information in a timely, sustained manner. This includes mission control facilities, such as tracking, telemetry, and control (TT&C) stations, and data links for controlling the satellites. Without these, orbiting platforms could not conduct their missions of collecting and relaying data. The ability to employ space power requires all three elements (terrestrial facilities, orbiting satellites, and the connecting data links) to function properly.

The successful operation of space systems is challenged by their fundamental fragility. Although they are designed to operate in the harsh environment of outer space, which involves exposure to wide temperature variations and massive amounts of radiation in their day-to-day operations, satellites remain vulnerable to a variety of other phenomena. Major spikes in radiation, whether due to solar flares or being struck by an electromagnetic pulse, can cripple satellite electronics. They also remain susceptible to physical damage from collisions with other items in space, including micrometeorites, debris, and kinetic kill vehicles. Indeed, even if the central "bus" of a satellite could be armored or otherwise protected, the communications antennae and solar panels would necessarily remain exposed.

Space systems, moreover, are susceptible to deliberate interference and "soft kill" techniques, such as laser dazzling and radio frequency jamming. As important, space services can be interfered with terrestrially; PNT receivers, for example, can have their signals disrupted by ground-based jammers. Iran has been known to jam satellite television signals. Such measures may be reversible, with temporary effects. They can therefore be hard to distinguish from problems with normal satellite operations, or the vagaries of space weather. This allows an attacker to potentially mask at least some efforts to degrade a satellite's operations, and it makes space an inherently gray zone–friendly environment, where adversaries can undertake actions that degrade U.S. or allied capabilities or change the status quo, possibly without their actions being easily attributed.

[7] Ankit Panda, "U.S. Air Force to Share Space Data Directly with China," *The Diplomat*, December 9, 2014.

Exacerbating the physical vulnerability of satellites is the nature of orbital mechanics. Satellites follow highly predictable paths, making them easier to target. Altering those paths can be accomplished only at the cost of fuel, which in turn affects their lifespans (and which can also affect their ability to fulfill their main missions). Changes in the orbital plane (as opposed to their velocity within the same orbit) are especially exorbitant in terms of fuel expenditure.

The rest of the space infrastructure is similarly vulnerable. Most space launch and mission control sites, for example, are very large complexes, with control centers, communications arrays, and fuel storage facilities that are often "soft" targets. Due to the complexity and expense, nations can generally afford only a handful of such sites. Damaging one or two can therefore have an outsized impact on a nation's ability to sustain space operations.

Tying the terrestrial and orbiting components together are the data links of the TT&C networks. Like any other communications network, these are potentially liable to disruption by cyber activities. Furthermore, the data that the satellites gather or transmit can also be intercepted, spoofed, interfered with, or otherwise attacked.

Compared with the variety of threats that confront space systems, the ability to protect satellites and their supporting infrastructure is much more limited. Perhaps most widely applied are means of countering adversary efforts to jam and dazzle, including spread-spectrum and frequency-hopping communications techniques and filters to counter laser dazzling. Hardening or armoring satellites have more-limited benefits; solar panels are hard to protect. To date, no nation is known to have successfully installed active defense systems for satellites. A point defense gun or missile system would require its own sensors, and the attendant weight and power requirements would come at the cost of the mission payload. Satellites can engage in avoidance maneuvers (including in the course of normal operations to prevent an accidental collision), but only for a limited period before their fuel is exhausted. And the attendant information systems are almost certainly high-priority targets for adversary hackers and information warfare forces.

China, the United States, and Japan all labor under broadly the same set of physical constraints. China, however, has a space industrial base that is composed of state-owned enterprises, so its ability to purchase satellites and launch vehicles is less affected by considerations of profitability (though not wholly insulated from that consideration). Japan and the United States rely on their respective private sectors to build satellites and launch systems, which means fewer redundancies in the interest of greater cost efficiencies.

This set of considerations highlights the challenges confronting efforts at space deterrence in an "offense dominant" environment. Deterring an adversary requires affecting its cost-benefit calculation. But in an offense-dominant world, the attacker is more likely to benefit by striking first. This troubling incentive structure is exacerbated by the combination of many potential targets and varied forms of threats, as well as a widespread belief that the United States is substantially more dependent on space to fight in the Indo-Pacific theater and in the manner to which U.S. forces have become accustomed.

Space Deterrence: The U.S. View

For the United States, space deterrence is a pressing concern, given its heavy reliance on space systems. U.S. concepts of deterrence focus on the combination of actual capability and willingness to employ that capability in persuading an adversary not to do something—i.e., dissuasion. As Alexander George and Richard Smoke wrote in 1974, deterrence "in its most general form . . . [is] simply the persuasion of one's opponent that the costs and/or risks of a given course of action he might take outweigh its benefits."[8] Deterrence is typically seen by U.S. decisionmakers as a goal. There is nothing in this formulation that presupposes deterrence as being dissuasive rather than coercive, but deterrence in the Western conception is almost wholly associated with the idea of dissuasion.

Official U.S. policy seems to be focused on two different but related forms of activities that contribute to the overall goal of deterrence. One is to deter an adversary from acting against U.S. interests through a variety of means, including space systems and activities, but also nuclear and conventional operations. That is, the United States seeks to deter an adversary through space (and other) means. At the same time, U.S. policy also seeks to deter an adversary from acting against U.S. space systems. That is, the United States seeks to deter an adversary in space.

To these ends, the United States pursues a four-pronged strategy, as reflected in an array of U.S. government strategic documents, including the National Security Space Strategy, the National Space Policy, the U.S. National Security Strategy, and the U.S. National Military Strategy.[9]

1. Support the development of norms of space conduct. The U.S. Department of Defense recognizes, however, the limitations of expecting norms to constrain adversaries. Instead, the expectation is that the creation of norms will allow easier identification of bad actors by noting when they step beyond acceptable bounds.
2. Build coalitions to support collective security in space. The view is that, by creating coalitions, an aggressor will be deterred because it will likely face an array of adversaries, rather than just one. There is also the belief that forming a coalition will create synergies in capabilities and capacity, making for a more robust posture, which will also exert a deterrent effect.
3. Enhance resilience, so that an adversary's efforts will be frustrated. Resilience is an aspect of space mission assurance, along with reconstitution and defensive operations. Resilience may employ a variety of techniques, including protection, distribution, diversification, disaggregation, proliferation, and deception. This approach embodies the idea of deterrence by denial. It is hoped that any potential adversary will conclude that efforts to attack U.S. space systems will not generate sufficient benefit to make them worthwhile.

[8] Alexander George and Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice*, New York: Columbia University Press, 1974, p. 11.

[9] U.S. Department of Defense, "DOD Deterrence Strategy for Deterrence in Space," fact sheet, 2011.

4. Be prepared to respond to an adversary's attacks. The U.S. response to an attack on its space assets is not necessarily limited to symmetric responses against the adversary's space capabilities: Attacks against the enemy's homeland; ground, air, and naval forces; or information networks are all possible options. Such U.S. retaliatory actions could also entail economic, diplomatic, legal, or other nonmilitary actions.

This set of goals arguably parallels U.S. deterrent policies in the nuclear, cyber, and conventional arenas. This includes the ability to deter an adversary through a combination of soft and hard power, to forge coalitions that will threaten an adversary with an expanded conflict should war break out, and to undertake both deterrence by denial (i.e., denying any benefit from aggression) and deterrence by punishment (i.e., imposing consequences in the event of aggression).

It is not clear, however, how successful this approach to space deterrence actually is. Analysts in the PLA, for example, have written extensively about U.S. reliance on space systems and appear to regard this dependency as a weakness that China needs to be prepared to exploit in the event of a conflict between the two countries. For example, one Chinese military analysis noted that:

- In the 1991 Gulf War, the United States used 52 military satellites.
- In the 1999 Kosovo conflict, the United States and the North Atlantic Treaty Organization (NATO) used 86 satellites.
- In the 2003 Iraq war, U.S. and United Kingdom forces used more than 100 satellites.[10]

For the 2003 Iraq war, another Chinese article estimates that the United States relied on satellites for 95 percent of reconnaissance and surveillance information, 90 percent of military communications, 100 percent of navigation and positioning, and 10 percent of meteorological and weather forecasting.[11]

Insofar as U.S. conventional capabilities are reliant on space for their effectiveness, a successful effort to disrupt, deny, degrade, or destroy America's ability to access space would significantly erode the U.S. military's ability to use force to punish the attacker. For the United States, credibly threatening to punish an adversary for attacking its space systems itself requires being able to exploit space.

At the same time, there has been a blurring of nuclear and conventional roles for space systems. During the Cold War, missile early warning satellites were almost entirely a strategic asset, providing warning of an attack on the U.S. and Soviet homelands. Satellite communications, too, were of only limited utility for conventional operations. In more recent years, however, many of these systems have assumed more of a dual function. During the first

[10] Zhang Yuwu, "Informationalized Warfare Will Make Seizing the Aerospace Technology 'High Ground' a Vital Factor," *PLA Daily*, March 30, 2005.

[11] Wang Yao and Shi Chunming, "Regarding 'Space Information Warfare,'" *China National Defense Newspaper*, June 12, 2003.

Gulf War, for example, missile early warning satellites provided cueing for tactical missile defense systems, such as Patriot, against medium-range ballistic missiles, such as Iraqi Scuds. Similarly, communications satellites are now employed for tactical activities, as well as strategic ones. This confluence opens the door to attacks against such space systems, not as part of a strategic attack, but in response to tactical and operational-level imperatives.

Recognizing this conundrum, the United States has undertaken various steps to reduce its reliance on space by diversifying information sources and striving to incorporate redundant means into weapons and operational planning. During NATO's Operation Allied Force in the Balkans in the 1990s, it was reported that some U.S. munitions, such as the AGM-130, employed both GPS and inertial navigation systems.[12] These measures have gained added urgency in recent years, with additional research into miniaturizing and integrating both systems in the face of widespread development of GPS jammers.[13] The U.S. Naval Academy, meanwhile, has reinstituted training in celestial navigation, after dropping it in 2006.[14]

The Challenge of Extended Deterrence in Space

If U.S. efforts at effecting deterrence in space are complicated, the situation is even more difficult when considering the relationship between space and *extended* deterrence. The parallels between the space deterrence situation and past nuclear and conventional deterrent efforts, imperfect at best when focused on basic deterrence, are arguably even less relevant when trying to extend deterrence to U.S. allies, such as Japan.

This is partly because today's security environment is more complex than that during the Cold War (which provides the framework for most U.S. deterrence thinking). For most of the period between 1947 and 1991, the situation was largely marked by a bipolar balance, where the two major players created somewhat symmetrical blocs of allies, friends, and client states. Consequently, there was a relatively unchallenging environment for symmetric responses and signaling. As important, there was a perceived continuum of security that spanned conventional and nuclear thinking, linking the use of force in the former to the potential for escalation into the latter. It is within this context that "extended deterrence" took shape.

Today's world, however, is much more multipolar, so that most states—including, increasingly, the United States—have to consider more than just a single highest-priority contingency. Consequently, signaling is also more difficult, especially because there is no symmetry of relations and alliance networks since most potential U.S. adversaries do not have

[12] Carlo Kopp, "Breaking Serbia: The Allied Force Campaign," Airpower Australia, August 1999.

[13] John Keller, "DARPA Seeks to Wean Smart Weapons Off GPS with Hybrid Inertial Navigation System-on-a-Chip," *Military & Aerospace Electronics*, April 18, 2012; Joe Gould, "Guided-Bomb Makers Anticipate GPS Jammers," *Defense News*, May 31, 2015.

[14] Andrea Peterson, "Why Naval Academy Students Are Learning to Sail by the Stars for the First Time in a Decade," *Washington Post*, February 17, 2016.

formal treaty alliances or commitments. Additionally, because attacks on space assets are a relatively new and poorly understood phenomenon in terms of how they fit within more-conventional forms of armed attack, the extent to which the United States is obligated to respond to an attack on an ally's space systems is unclear. Unlike an attack on an ally's territory or traditional military forces, an attack on an ally's space system may constitute another example of "gray zone" conflict, one that does not fall cleanly into either a peacetime accident or criminal action or a wartime act of armed conflict. Still, the United States has noted that it "will employ a variety of measures to help assure the use of space for all responsible parties, and, consistent with the inherent right of self-defense, deter others from interference and attack, defend our space systems and contribute to the defense of allied space systems, and, if deterrence fails, defeat efforts to attack them."[15]

This is especially the case because of the range of potential actions against allied space systems, which complicates efforts at extended deterrence. What would be the proper response to an adversary dazzling or jamming an ally's satellite systems, even assuming attribution could be rapidly made? Was the use of a laser against a satellite an attempt at interference, or simply an attempt to measure its distance? Barring sustained jamming and dazzling, any response will also suffer from a lag time. It is not clear what a symmetric response would be for a third party (i.e., the one providing extended deterrence) on behalf of its supported partner. To use a hypothetical example involving the U.S.-Japan alliance and China, should the United States jam or dazzle a Chinese satellite in response to Chinese jamming or dazzling actions against a Japanese space system? If so, at what point? As soon as they occur? Even if they lasted only during one or two orbits? Or only if they cause permanent damage? And is the United States obliged to respond immediately, or only if Japan indicates that it cannot effectively respond militarily for some reason? In such a case, is the most appropriate response a U.S. military response, or should the expectation be that Japan employ deterrence by punishment in some other domain (such as diplomatic or economic sanctions) rather than turning to the United States to strike back on its behalf?

A final complication stems from the asymmetric alliance relationships that characterize the United States and China. During the Cold War, both the United States and the Soviet Union had allies and commitments outside their national territories. Consequently, there were at least some parallels in terms of understanding extended deterrence. In the case of China, however, Beijing does not have any real allies that it is clearly and credibly committed to defending. (Although China and North Korea are, at least on paper, linked by their 1961 Mutual Defense Treaty, many observers doubt that this commitment is truly binding on either side.) For Beijing, neither Pakistan nor North Korea, the closest analogues, are really comparable to the U.S. relationship with Japan.

[15] Office of the President of the United States, *The National Space Policy of the United States*, Washington, D.C., 2010.

As a result, China does not face the problem of extending deterrence; it is defending itself but it is not attempting to defend allies. Indeed, it would be more accurate to say that China is not focused on engaging in extended deterrence, but on countering extended deterrence. Along its periphery, China does not directly confront the United States; it is seeking to deter and coerce U.S. friends and allies. This creates substantially different asymmetric concerns between China and the United States. Where Washington is engaged in extended deterrence in support of allies, Beijing is concerned about direct deterrence—i.e., direct threats to China.

Space Deterrence: The Chinese View

This situation of incongruent strategic circumstances is further exacerbated by divergent views on deterrence itself. Based on the writings of its leading military thinkers, it seems clear that China has a very different perspective on deterrence in general, as well as space deterrence specifically.[16] For the United States, the very act of deterring an opponent, or multiple opponents, from acting in certain ways is seen as serving U.S. interests. In the Chinese view, deterrence is a means rather than an end. This is because the Chinese concept of *weishe* (威慑), which is typically translated as "deterrence," embodies both "dissuasion" and what Western analysts would regard as "coercion." Coercion, in turn, is typically in the service of some other goal—one does not simply coerce an adversary, one coerces an adversary to get it to do something that one wants. Thus, the Chinese would employ *weishe* as the means, whether dissuasive or coercive, to persuade an opponent to follow a course of action that accords with larger Chinese strategic objectives.

Within such a framework, Chinese military thinkers are not necessarily interested so much in deterrence in the space environment, but rather in the use of space (and other means) to *effect* deterrence, including coercion. Thus, in Chinese writings, space operations are characterized as contributing to an effort to achieve overall goals, whether in conjunction with conventional and/or nuclear operations or on their own; either through *weishe* (i.e., dissuasion and coercion) or in actual combat. There is little discussion of deterring actions occurring in space, which is consistent with the broader Chinese tendency to discuss deterrence in terms of employing various means (including nuclear and information) in order to achieve certain dissuasive or coercive goals.

These fundamental differences in perspective and definition make comparisons of U.S. and Chinese approaches to even basic deterrence approaches difficult. For the Chinese, for example, actual use of space weapons is the highest rung of what they appear to view as an "escalation ladder" of deterrent actions. This would seem to be a radically different perspective from the United States, where weapon use is rarely considered part of deterrence.

[16] See, for example, Academy of Military Science Military Strategy Research Office (China), *The Science of Military Strategy*, Beijing: Military Science Publishing House, 2013.

This divergence holds dangerous implications in event of a crisis. China may employ weapons (e.g., ASAT systems) in order to dissuade or coerce an adversary, but adversaries may see this action as initiating larger hostilities. It should be noted that U.S. Congressman Adam Schiff, the ranking Democrat on the U.S. House of Representatives Permanent Select Committee on Intelligence, has stated that even a cyber attack on a U.S. satellite could be considered an act of war; a physical attack is even more likely to be interpreted that way.[17] Conversely, efforts to find "offramps" by an adversary may be interpreted by the Chinese as fear of further Chinese actions rather than an effort to de-escalate.

Comparisons are further complicated by the nature of many of the tensions that could lead to conflict between the United States and China. From the Chinese view, few of these disputes are rooted in space issues. Whether it is China's attempt to lay claim to the Senkakus, the issue of Taiwan, or the South China Sea, Beijing sees the main sources of tensions as challenges to Chinese sovereignty claims that are described as "core interests." Thus, China is seeking to engage in *weishe* (whether dissuasion or coercion) over territorial concerns, to which the United States is not a party. Beijing appears to (or, at a minimum, wants to appear to) perceive these concerns as defensive and preserving the status quo (i.e., its territorial integrity and sovereignty), which casts a different light again on the objectives being served by *weishe*. Deterring threats to one's own immediate territory typically embodies greater commitment and resolve.

Chinese Views of Space Deterrence

A review of PLA writings on space deterrence (*kongjian weishe*; 空间威慑) highlights additional divergences between Western and Chinese perspectives.[18] Space deterrence is characterized by the PLA as the use of space forces and capabilities to deter or coerce an opponent, preventing the outbreak of conflict, or limiting its extent of conflict should one occur.[19] By displaying one's own space capabilities and demonstrating determination and will, the PLA hopes to induce doubt and fear so that an opponent will either abandon its goals or limit the scale, intensity, and types of operations that China sees as harmful to its interests. It is important to note that PLA conceptions of space deterrence are not aimed solely, or even necessarily, at deterring actions in space, but rather in conjunction with nuclear, conventional, and informational deterrence capabilities and activities, aimed at influencing an opponent's overall perceptions and activities.

[17] Colin Clark, "Cyber Attack on Satellite Could Be Act of War: HPSCI Ranking," *Breaking Defense*, June 10, 2016.

[18] This section is drawn from Jiang Lianju, *Space Operations Teaching Materials*, Beijing: Military Science Publishing House, 2013; and Chang Xianqi, *Military Astronautics*, 2nd ed., Beijing: National Defense Industries Press, 2005.

[19] Jiang, 2013, p. 126.

PLA teaching materials suggest that there is a perceived hierarchy of space deterrence actions, somewhat akin to an "escalation ladder," involving displays of space forces and weapons, military space exercises, deployment or augmentation of space forces, and ultimately employment of space weapons. It is noteworthy that official U.S. writings do not seem to provide a comparable hierarchy of measures.

Displays of space forces and weapons (*kongjian liliang xianshi*; 空间力量显示) occur in peacetime or at the onset of a crisis. The goal is to warn an opponent in hopes of dissuading escalation of a crisis or the pursuit of courses of action that will lead to conflict. Such displays involve the use of various forms of media to highlight one's space forces and are ideally complemented by political and diplomatic gestures and actions, such as inviting foreign military attachés to attend weapon tests and demonstrations.

Military space exercises (*kongjian junshi yanxi*; 空间军事演习) are undertaken as a crisis escalates, if displays of space forces and weapons are insufficient to compel an opponent to alter course. These exercises can involve actual forces or computer simulations and are intended to demonstrate one's capabilities but also military preparations and readiness. At the same time, such exercises will also improve one's military space force readiness. Examples include ballistic missile defense tests, ASAT unit tests, exercises demonstrating space strike (*kongjian tuji*; 空间突击) capabilities, and displays of real-time and near-real-time information support from space systems.

Space force deployments (*kongjian liliang bushu*; 空间力量部署) are seen as a significant escalation of space deterrent efforts. These are used when one concludes that an opponent is engaged in preparations for war and involve the rapid adjustment of space force deployments. As with military space exercises, this measure is not only intended to deter an opponent but also, should deterrence fail, seen as improving one's own preparations for combat. Such deployments, which may involve moving assets that are already in orbit and/or reinforcing current assets with additional platforms and systems, are intended to create local superiority of forces so that an opponent will clearly be in an inferior position. It may also involve the recall of certain space assets (e.g., space shuttles), either to preserve them from enemy action or to allow them to prepare for new missions. This may be akin to the evacuation of dependents from a region in crisis, as a signal of imminent conflict.

"**Space shock and awe strikes"** (*kongjian zhenshe daji*; 空间震慑打击) is the Chinese term for the final step of space deterrence. If the three previous, less-violent deterrent measures are insufficient, then the PLA suggests engaging in punitive strikes to warn an opponent that one is prepared for full-blown, comprehensive conflict in defense of the nation. Such strikes are seen as the highest and final technique (*zuigao xingshi he zui hou shouduan*; 最高形式和最后手段) in seeking to deter and dissuade an opponent. Employing a combination of hard-kill and soft-kill methods, one would attack an opponent's physical space infrastructure and data links. Success is defined as opposing decisionmakers being psychologically shaken and hopefully ceasing their activities. If the effort fails, an opponent’s forces will nonetheless have suffered some damage and losses, which will help ensure victory in the course of open conflict.

Chinese Views on Space Blockades

While space deterrent activities are intended to coerce or dissuade, Chinese writings on the imposition of space blockades gives some indications of PLA thinking about potential “gray zone” activities in space.[20] PLA conceptions of space blockades involve the use of space-based and/or terrestrial forces to prevent an opponent from entering space, and from gathering or transmitting information through space, without necessarily directly attacking the adversary’s space infrastructure. Chinese writings reveal that PLA analysts are considering several different varieties of space blockade activities.

One is to *blockade terrestrial space facilities*, including launch sites, TT&C sites, and mission control centers. This includes blocking access to these facilities, such as by disrupting road and rail connections. In addition, they can be disrupted through computer and information network interference. At a more extreme level, one can use kinetic means (e.g., special forces, missiles) to prevent the facilities’ normal operation.

Another method is the *obstruction of launch windows*. If one can delay a launch, whether through interfering with a launch vehicle’s onboard systems or otherwise disrupting the schedule, then a satellite may not be able to reach its proper orbit. In the past, some U.S. space launches have been delayed because fishing and pleasure boats were present down-range.[21] This alternative also includes the possibility of a boost-phase intercept of a space launch vehicle.

A more threatening approach is to *obstruct orbits*. This can include actually destroying satellites that are in orbit or simply obstructing orbits, such as by creating clouds of space debris or deploying space mines. By threatening the destruction of adversary satellites (without necessarily doing so), one might limit the function of those satellites (e.g., by limiting their maneuvers). The risk, however, is that any such step might lead to damage to third-party space systems, which in turn could lead to strategic consequences. Therefore, Chinese authors tend to view this approach to imposing a space blockade as demanding very high levels of precise control; extremely detailed SSA; and highly focused, limited deployment.

Finally, one can impose *an information blockade*. By interfering with and disrupting an opponent’s data links between terrestrial control stations and the satellite, one can effectively neutralize an orbiting satellite by hijacking the satellite’s control systems or preventing ground control from issuing instructions. Alternatively, one can interfere with the data that the satellite is transmitting—i.e., rather than tampering with the satellite’s controls, one can contaminate or block the data that it is gathering or transmitting. A third form of information blockade involves

[20] This section is drawn from Jiang, 2013, pp. 132–137.

[21] “Atlas 3 Scrubbed to Tuesday,” *Space Daily*, May 21, 2000; Jessica Orwig, “A Rocket Launch Was Delayed Monday Because of a Boat,” *Business Insider*, October 28, 2014.

"dazzling" a satellite, which means using low-powered, directed-energy weapons against sensors or other systems. In each case, the intent is to effect a "mission kill," whereby the satellite cannot perform its functions but is not necessarily destroyed.

Space and Deterrence in the Western Pacific: Implications for the United States

For the United States and China, each is the other's most challenging potential adversary in the western Pacific, and hence a major focus of their respective political, diplomatic, and military activities has been dissuading the other from challenging key security concerns. The space domain has been steadily rising in importance in this regard. Given the very different extent to which each side relies on space, as well as the diverging demands of alliances, the potential for deterring conflict in space is increasingly challenging.

But while there may be clashes in space, the actual source of any Sino-American conflict will remain earthbound, most likely stemming from tensions associated with the situation in the East China Sea, the Taiwan Strait, or the South China Sea. This suggests that U.S. and allied decisionmakers (both in Asia and Europe) should be focusing on deterring aggression in general, rather than concentrating primarily on trying to forestall actions in space. Indeed, there is little evidence that Chinese military planners are contemplating a conflict limited to space. While there may be actions against space systems, Chinese writings suggest that they would either be limited in nature, as part of a signaling and coercive effort, or else would be integrated with broader terrestrial military operations.

This would suggest that current U.S. strategy can be effective in at least limiting the success of any Chinese effort at degrading and denying space to the United States and its allies. Enhancing resilience of space-based systems—including through hosted payloads, deployment of on-orbit spares, and increased ability to rapidly replace space systems—will likely affect the Chinese calculus for undertaking action against space-based systems. At the same time, efforts must be made to improve the resilience of the terrestrial components of space-based systems' architectures. Proliferating ground control links (as is under way with the GPS constellation), establishing additional mission control facilities, and moving away from a handful of fixed launch sites (e.g., through sea-based space launch options) all need to be taken into consideration as part of a solution to complicating adversary targeting and thereby bolstering deterrence through denial. The growing array of nongovernmental space players, including space launch (e.g., SpaceX, Blue Horizons) and remote sensing (e.g., GeoEye, Digital Globe), may provide additional resiliency because they can augment governmental assets and capabilities. This has long been the case in the area of satellite communications, with such firms as Intelsat and Inmarsat providing the bulk of global satellite communications services.

Decreasing reliance on space-based systems might also make attacks on them less inviting—or at least reduce the impact should they occur. GPS has proven marvelously versatile, with myriad new applications and uses for both the location and timing functions, but it is also a potential single-point failure. Returning to training U.S. sailors in the art of celestial navigation and other similar steps can be employed to maintain at least a minimal level of effectiveness, but no more than that. Such steps cannot replace the timing function on which so many systems depend. Similarly, communications satellites are vital for the operation of many UAVs, relaying commands and data. Interference with those constellations would therefore affect the viability of many UAV operations. Future weapon developments should therefore incorporate nonspace means, including high-altitude air-breathing systems and near-space capabilities, into their initial design.

Beyond technical fixes, there is also the need to build and expand international coalitions, improve intra-alliance interoperability and data-sharing, and generally strengthen alliance relationships. These may have a deterrent effect on Beijing or other actors who might target the United States or Japan in space. They also could improve the ability to counter such actors should deterrence fail.

For such steps to succeed, however, the scale and depth of U.S. space cooperation with key Pacific allies, especially Japan, must be expanded. Unlike the NATO relationship, U.S. alliances with Asian nations have not been tested by recent real-world combat experience. Japanese and South Korean combat forces did not participate in Operations Desert Shield and Desert Storm, the Balkan conflicts, the war in Afghanistan, or the 2003 invasion of Iraq. This makes assessing current modalities of cooperation on space issues extremely difficult.

For Japan, in particular, substantially expanded cooperation on space deterrence may pose significant challenges. Japan’s national security space establishment is still in its infancy. The Basic Space Law was only passed in 2008, and there have been reorganizations of the national security space establishment since then. The chain of command and lines of responsibility for such vital aspects as space situational awareness are not yet fully settled. The roles of the National Space Policy Secretariat, Japanese Ministry of Defense, and Japanese Aerospace Exploration Agency (JAXA) are not necessarily well understood by their American counterparts at U.S. Pacific Command, U.S. Strategic Command, and U.S. Air Force Space Command.

It is also unclear how the United States can integrate space cooperation with Japan with its long-standing relations with other key allies, ranging from South Korea (with whom Japan has tense political relations at present) to NATO. Space is a new venue for cooperation between the U.S. and Japanese militaries. Information that can be shared with, for example, NATO allies (where there are long-standing mechanisms) may not be easily shared with Japan, and vice versa. Similarly, information shared by some key U.S. allies with the United States might be restricted from dissemination to Japan, and vice versa. Yet, SSA data cannot be easily compartmented if it is to be fully exploited.

To remedy this, senior U.S. and allied Japanese space decisionmakers, including both military officers and civilians, need to engage in more regular dialogues. Space cannot simply be one of many agenda items; it needs dedicated forums and consistent, continuous engagement.

This should begin by establishing terms of reference, so that all sides are speaking from a common starting point.

As rapidly as possible, efforts to deepen cooperation on deterrence in space need to progress to the cooperative establishment of common rules of engagement and mutual familiarization with space policy decisionmaking. This should include cross-posting of military officers, as well as exchanges of mid-level officials.[22] Given the speed with which events occur in space (where the kill chain may last only seconds or minutes), the ability to respond promptly is vital. One possible means of accelerating this process may be to conduct joint space-oriented planning, exercises, and war games. Joint interactions would introduce both individuals and offices on both sides to each other, while providing additional context for space decisionmaking that would not necessarily be afforded by extended briefing sessions.

Conclusion

For the United States, China, and Japan, the ability to access information derived from or transmitted through space systems while denying an adversary that same capability is of growing importance. For all three states, there is a recognition that the struggle for "space superiority" or "space dominance" will be a decisive part of future conflicts. It will also be a vital means of effecting deterrence; the side that cannot readily access space will be at a major disadvantage and is likely to be deterred. Terrestrial security will increasingly depend on the ability to access outer space.

[22] For some time to come, such cross-posting could face challenges because of the legal and constitutional constraints on Japanese use of force, even within the U.S.-Japan alliance framework; such cross-posting may be best conceived of as a possible longer-term goal to be considered should regional security trends continue to deteriorate, leading to growing flexibility and loosening of the limitations on Japanese military activities. On the constraints facing Japan in security cooperation even with the United States, see Jeffrey W. Hornung, *Modeling a Stronger U.S.-Japan Alliance: Assessing U.S. Alliance Structures*, Washington, D.C.: Center for Strategic and International Studies, November 2015; and Jeffrey W. Hornung and Mike M. Mochizuki, "Japan: Still an Exceptional Ally," *Washington Quarterly*, Vol. 39, No. 1, Spring 2016.

7. A Japanese Perspective on Space Deterrence and the Role of the U.S.-Japan Alliance and Deterrence in Outer Space

Kazuto Suzuki, Ph.D.
Professor of International Politics
Public Policy School of Hokkaido University

Space systems are inseparable from today's socioeconomic activities and security. Many commercial and private airliners use GPS signals, financial institutions will be in chaos if there are no precision timing signals from space, drones cannot be flown without communication through space, disasters will be much more difficult if we do not have satellite images, and so on. Space systems have become central to how advanced modern societies function.

Space systems are also critically important for national security. Modern warfare relies on data collected by reconnaissance satellites, navigation and positioning information provided by GPS systems, and communications over long distance via telecommunication satellites. In short, the C4ISR (command, control, communications, computers, intelligence, surveillance, and reconnaissance) networks that lie at the heart of modern, silicon-enabled warfare depend heavily on space.

This means that degrading or destroying the space capabilities of an enemy country can potentially cripple its ability to continue to undertake all but the most basic military operations. The more a country depends on space systems, the more vulnerable it will be. This is the situation of many countries, including both the United States and China. In a situation of conflict, attacking an adversary's vulnerabilities and causing maximum damage to an opponent's fielded forces and supporting economic infrastructure are the most effective ways to gain superiority and potentially force an end to the fight. Space systems, therefore, are a prime target.

Having established the importance of space-based systems to both modern life and modern combat operations, how can the security of such space systems be defended? Traditionally, military strategists have sought to prevent attacks on vulnerable systems through deterrence, or a mix of hardening and resiliency to convince the adversary that its actions will fail to achieve the desired effect at an acceptable cost, plus threats of punishment designed to persuade others to refrain from taking actions that may cause harm by credibly vowing to hurt them in unacceptable ways if they do carry out an attack. These traditional notions of deterrence do not work well in outer space, however, due to the different physical characteristics of the space environment, as well as differences in various actors' dependencies on space systems. Attacks on space systems cannot be deterred by retaliating against an adversary's space systems if the adversary does not depend on space assets to any substantial degree.

This chapter argues that, in order to protect the key space-based assets that the United States and Japan rely on for both peaceful purposes and deterrence and war-fighting, the United States and Japan need to develop a strategy for cross-domain deterrence situated within the context of the alliance relationship. Because of the vulnerabilities of space systems, defending space assets from possible hostile attack is neither easy nor cost-efficient. To make matters more complicated, deterrence in space is also extremely difficult. Thus, with both direct defense and deterrence complicated by the nature of the space environment, it is the central contention of this chapter that the U.S.-Japan alliance will need to deter and defeat attacks on critical space-based systems, primarily through the employment of cross-domain deterrence. In other words, such deterrence will require a combination of terrestrial and space-based intelligence assets to identify the source of hostile attack, at which point the U.S.-Japan alliance will likely need to respond with actions undertaken in other domains to reinforce or restore deterrence against attacks on the allies' space-based systems. In short, achieving deterrence in space will require actions undertaken on the ground and in cyberspace.

As a starting point, close cooperation and information-sharing between the United States and Japan is of the utmost importance. Monitoring space activities through SSA and sharing SSA data play a crucial role in identifying impending or ongoing hostile action(s) in space, and planning and coordination for responding to such hostile action are extremely important. At this moment, there is an ongoing discussion about the coordination of SSA between the allies, but, to date, this discussion has not been focused on the issue of planning for each country's reaction and anticipated retaliatory steps in the event of an attack on either of the allies' space-based systems. This chapter argues that the time is ripe for defining what constitutes hostile action and what kinds of means should be taken in responding to such threats.

Traditionally, space systems have been developed and funded by national governments. Each state has its own objectives to develop space systems for its military and civilian purposes. The United States has developed full operational capabilities in space as the leader of the West and provided such services as civilian GPS signals to the entire world. Meanwhile, Japan has developed space capabilities for purely civilian purposes. In 1969, the Diet adopted a resolution that prohibited the Ministry of Defense (then Japan Defense Agency) and the JSDF from developing, owning, operating, or using any space systems. This prohibition continued until 1985, when the JSDF was allowed to use satellite communications for joint naval exercises with the United States for the first time but still only permitted to use services derived from space; the prohibition on development, ownership, and operation of space assets continued. In 1998, when a North Korean missile flew over Japan, Japanese policymakers realized that Japan's lack of satellites for intelligence-gathering purposes prevented the country from predicting the launch of North Korean missiles and would need to be addressed. However, as the Diet was not able muster the votes to override the previous resolution of 1969, the GOJ instead chose to designate the Cabinet Intelligence and Research Office as the agency responsible for operating information-gathering satellites. It was only in 2008, when the Basic Space Law was passed, that the Diet reinterpreted the 1969 Resolution and defined Japanese space activities as permissible for contributing to national and international security.

Thus, Japanese contributions of military space system capabilities within the alliance are very limited. However, given the recent green light for investing in military satellite systems through the Basic Space Law, the legal constraints on developing space systems for military purposes and for the benefit of the alliance have come down somewhat. Although Japanese space systems are strategic assets, they are not directly engaged in military combat; they merely support it. Those who support the Diet Resolution of 1969 argue that space should remain restricted to peaceful activities for promoting science and technology, but for most observers this represents a difference over relative priorities and their opposition is not rooted in pacifist or antiwar sentiment.

Space is a typical example of dual-use technology. Such capabilities as the debris removal system developed by JAXA are intended to be civilian technologies but can also be used against hostile satellites. Legally speaking, such technology can be transferred to the Ministry of Defense and used for military purposes, but there is no such plan to use this technology for taking out an adversary's space assets. Policymakers, as well as those who are in both JAXA and the Ministry of Defense, are still trying to figure out what role space systems can play in the national defense structure because it has developed without space for so many years (except satellite communications). Thus, when the Basic Space Law was established, it was SSA that Ministry of Defense focused on because it was the primary issue to contribute to the U.S.-Japan alliance.

Vulnerabilities in Space

Space assets are vulnerable. They are designed to be light in order to reduce the weight for effective launch, and they are therefore largely undefended by any sort of protective armor. In addition, because space assets in Earth orbit are traveling very fast (approximately 17,700 miles per hour), any collision can produce devastating effects. These are delicate machines carrying large numbers of electronic parts that are exposed to solar flares and electromagnetic pulses. Although they are not stationary, their orbits can be easily detected and predicted and therefore targeted without much difficulty. Additionally, there is no place to hide in space; because of the physics of the space environment, space-based assets are extremely vulnerable. There are very few ways to improve their resilience other than hardening, duplication, or reconstitution (all of which are extremely costly and/or time-consuming and none of which does anything to make the actually targeted platform any more difficult to attack or capable of surviving an adversary's assault).

Further complicating matters is the fact that space assets are vulnerable to unintentional and intentional incidents. The largest threat to space assets is actually collision with space debris. There are about 20,000 known pieces of space debris larger than 10 centimeters in diameter in orbit (about 3,000 of these were created by a Chinese ASAT weapon test in 2007), and an estimated 500,000 debris items smaller than that. The Joint Space Operations Center under the U.S. Department of Defense monitors the movement of orbital debris and issues warnings to satellite operators to avoid collisions. Supporting and further improving this SSA mission is an important contribution that the U.S.-Japan alliance can make for not only Japan and the United States but also all satellite-operating nations.

Solar flares and geomagnetic activities are another source of unintentional threats to space assets. High-energy showers of radiation, such as those that occur during solar flares, can affect the electronic systems onboard satellites; they can also affect the accuracy of GPS signals. There is little that can be done to avoid the impact of solar flares, but some space weather forecasts may provide early warning so that the operators can turn off their machines and thereby reduce the impact on sensitive systems.

Unintentional threats, such as space debris and solar flares, have been the primary threats to space activities from the beginning of human activities in space. More recently, however, a growing threat to space-based assets comes from intentional, hostile activities directed toward them.

Antisatellite Attack

Because space assets are highly vulnerable and play a vital role in U.S. combat operations, there is a strong incentive for any militarily advanced nation that is confronting the prospect of conflict with the United States to attempt to attack the space capabilities of the United States and any allies that may be supporting it, such as Japan. Attacks on space assets can be more appealing to adversaries because such attacks are not as easily visible to terrestrially based observers as, for example, aerial bombardment or missile attacks on ground targets would be; in addition, any casualties caused would largely be indirect results of systems knocked offline rather than deaths caused directly by the attacker. Furthermore, there is likely to be an attribution problem in most attacks on space-based assets. The only way to know whether space assets are under attack is through the collection and monitoring of data based on radar and optical SSA monitoring. But in many cases, it would be difficult to identify who carried out the attack and how it was executed because the nature of the monitoring systems makes it almost impossible to monitor space assets all the time. Satellites travel around the globe in 90 minutes. SSA radars and telescopes remain in one place on the surface of the Earth and can therefore only see a part of the satellite's circumnavigatory movement. There are a substantial number of blind spots, and a sophisticated adversary could take hostile action in those areas without the United States or Japan noticing. While there are mathematical methods to analyze the trajectory of space objects as a way to deduce the most likely perpetrators of any given attack, it would nonetheless be difficult, if not impossible, in many cases to capture definitive proof of the exact moment when the attack took place, as well as the identity of the actor who perpetrated it.

The ASAT weapon test conducted by China in 2007 was a good example of a country demonstrating its ability to take action against the space assets of other countries, possibly in the hopes that this would deter other countries from engaging in conflict with China. The 2007 ASAT test was a wakeup call for all spacefaring nations that space is vulnerable and assets in space can be easy targets if a conflict takes place. It also reminded observers that space is a vital domain for national security and that attacks aimed at degrading national space capabilities would significantly erode war-fighting capability.

The 2007 ASAT test also taught China a number of lessons. The test created thousands of new pieces of space debris that pose a risk of harm to China's own space assets. Since China is in the process of modernizing its own military forces, its reliance on space assets is increasing. Of course, the number of operational Chinese satellites, including both civilian and military satellites, totals just 178, whereas the United States operates more than 540 satellites of all types. Still, the creation of additional space debris places China's space-based assets at just as much risk as those of other nations.

Also, because of the international condemnation of its ASAT test and the consequential creation of a large debris field, China recognized the impact of the test. Immediately after the test, the UN Committee on the Peaceful Uses of Outer Space adopted Debris Mitigation Guidelines that call for avoiding the intentional creation of long-term debris fields in orbit. The European Union took the initiative to establish an International Code of Conduct in Outer Space, which prohibits attacks on space assets and invokes the inherent rights of states to self-defense, implying that attacks on space assets are to be considered as acts of war and conferring upon states the right to retaliate against such attacks. Although the negotiation of the International Code of Conduct has been stalled by strong opposition from China and Russia, who proposed a Treaty on the Prevention of the Placement of Weapons in Outer Space and of the Threat or Use of Force Against Outer Space Objects as an alternative, China has, at a minimum, had to deal with international criticism toward its kinetic ASAT test.

Nonkinetic ASAT: Cyber Attack on Space Systems

While the Chinese ASAT test in 2007 helpfully called attention to the fact that kinetic ASAT capabilities pose a threat to the space capabilities of other countries, it also convinced many observers that the cost of attacking other nations' systems in this way was too high in terms of both diplomatic fallout and potential debris fields that do not subsequently distinguish between the space assets of the victim or the attacker in later years. Thus, nonkinetic methods, or what could be referred to as gray zone operations in space, are now seen by many observers as likely to be more attractive methods for attacking an opponent's space assets because they are more covert and less likely to produce unwanted side effects, such as a debris field. One way of attacking an adversary's satellites without creating debris is via cyber attack. Cyber attacks can be done both on satellites (i.e., by taking over control of the satellite) and through satellites (i.e., by taking over the communication networks and hacking the network). A number of studies have been conducted to improve cyber defenses and protect networks.[1] However, the number of studies on how to defend against a cyber attack on a satellite is much smaller.[2] For military and civilian operators, the network is much more valuable than the satellite itself, so it is understandable that attention is paid to the cyber attack on the network as a whole. However, protecting satellite control is equally important for protecting assets from adversaries.

Obviously, military space systems pay more attention to these vulnerabilities. However, increases in the military use of commercial satellite telecommunications, which are not as resilient as military systems, may increase the vulnerability of military operations. Further, civilian critical infrastructure—such as air traffic control, train control, or control over the electricity grid—also relies on the use of commercial satellites. These can be soft targets for adversaries to attack. In addition to the vulnerabilities of commercial and civilian satellites, global networks of ground stations can also be targets of attack. Satellite telemetry datalinks need to have global network access across different jurisdictions, and sometimes security arrangements for these stations can be complicated or patchwork, exhibiting uneven integrity. Commercial and civil satellite communications involve lots of confidential transactions, including non–command-and-control military communications, and the security of these ground stations can be at risk from cyber attacks or possible physical attacks.

It is well-known that the radio frequency for satellite communications is limited. Traditionally, the radio frequency bands were arranged through the world radio communication conferences at the International Telecommunications Union, but the increase in the number of commercial and private satellites put huge pressure on the distribution of this scarce resource. Some operators, particularly small satellite operators, are now using less-secure frequencies. These frequencies are open to anyone; therefore, it is easy to detect and hack if malign actors want to take over those satellites. Furthermore, the cost for upgrading security from cyber attack would discourage small satellite operators from taking appropriate measures to harden themselves against this threat. The cost of encrypting command, tracking, and telemetry data and the cost of securing ground stations would put additional financial pressure on commercial ventures. There is no regulatory mechanism to force these types of operators to improve their security against cyber attack.

[1] For example, see Tarek Saadawi and Louis H. Jordan, Jr., eds., *Cyber Infrastructure Protection*, Carlisle, Pa.: U.S. Army War College, May 2011; Tarek Saadawi, Louis H. Jordan, Jr., and Vincent Boudreau, eds., *Cyber Infrastructure Protection*, Vol. II, Carlisle, Pa.: U.S. Army War College, May 2013; Tarek Saadawi and John D. Colwell, Jr., eds., *Cyber Infrastructure Protection,* Vol. III, Carlisle, Pa.: U.S. Army War College, June 2017; U.S. Department of Defense, *The DOD Cyber Strategy*, Washington, D.C., April 2015; and Cabinet Office, *The UK Cyber Security Strategy: Report on Progress and Forward Plans*, London, December 2014.

[2] David Livingstone and Patricia Lewis, *Space, the Final Frontier for Cybersecurity?* London: Chatham House, September 2016. Other, older studies include U.S. General Accounting Office, *Critical Infrastructure Protection: Commercial Satellite Security Should Be More Fully Addressed*, Washington, D.C., GAO-02-781, August 2002.

Another gray zone method of attacking satellite systems is the spoofing of telemetry data. Spoofing is a technique to provide false information about a satellite's location, position, and health (in this case, its mechanical condition). It can be done by either hacking satellite frequencies or providing false signals to ground station networks. If satellite operators receive false information, they will likely try to change the satellite's orbit to maintain continuous service. However, if an actor with malicious intent calculates the post-spoofing maneuvers carefully, it can direct the satellite onto a collision course with another satellite. It would be hard to detect spoofing unless the false data received show extreme abnormality from the original data.

Nonkinetic, Noncyber ASAT

Apart from cyber attacks on satellites, there are several other gray zone methods for attacking adversaries' satellite capabilities without using kinetic forces. Jamming space-based or terrestrial receivers of satellite signals by overwhelming them with energy is one way to interfere with space-based communication, GPS signals, and radio frequency sensors. In 2013, for example, North Korea directed a very strong radio frequency signal toward South Korea to disrupt GPS signals. This mass-scale jamming caused huge confusion for air traffic and other vital socioeconomic infrastructures. This incident took place using only local terrestrial means, so the effect was geographically quite limited, but if it had been done using assets on orbit, the effect might have been larger in scale. Jamming of GPS signals or other radio telecommunications can be done with very simple and commercially available tools. They are mostly available for local jamming (i.e., within a range of 500 meters), but with more power to the devices, they can affect much wider areas.

Spoofing of satellite signals is another method of nonkinetic attack on space systems. As in the case of spoofing satellite telemetry data, one can insert false signals with the same frequency onto the receiving devices. The receiver would identify the false information provided by the spoofer as genuine data from the satellite and act upon it accordingly. For example, if false signals from civilian GPS (military-code GPS is highly encrypted) are inserted into unmanned vehicles, then an attacker can easily disrupt traffic or operations of these vehicles.

Another method of nonkinetic attack on satellites is *dazzling*, the use of narrowly focused beams of energy, such as lasers or other types of light, to temporarily or permanently blind satellites. There are some reports that lasers have already been used against European civilian and military Earth observation satellites. U.S. military authorities have commented that they too have experienced dazzling attacks for some time. While these attacks, to date, have not caused permanent damage to satellites, if more powerful laser devices are used in the future, they can burn out satellites' sensors permanently.

A final gray zone method of attacking satellites is through the use of rendezvous and docking technologies. With sufficient sophistication and thrust control, a hostile satellite can approach a target satellite and use electronic or kinetic forces to undertake an attack directly or in close proximity to the target. China, for example, is known to have been testing satellites that can deploy robotic arms to grab, smash, or otherwise interfere with orbiting satellites. Such an approach can reduce the creation of space debris substantially or even entirely eliminate the creation of such debris. Other measures include the use of co-orbital satellites to deliver small explosive packages that would detonate on or near the targeted satellite. One drawback of these methods is that, because such attacks require time to synchronize the attacking satellite's orbit with that of its target, it is difficult for hostile actors to carry out such attacks without being detected, making it harder to preserve anonymity. The United States and its allies are rapidly developing the capacity to monitor the movements of satellites and space debris through SSA, which detects any satellite or debris that approaches existing space assets. With a more complete picture of what is in the space domain, it becomes more difficult for an attacking nation to avoid attribution when using these kinds of methods to perpetrate an attack.

Deterrence in Space?

In order to prevent kinetic, cyber, and nonkinetic/noncyber attacks on space assets, nations need to develop a space deterrence strategy. However, as discussed in the preceding paragraphs, deterrence in space is quite different from other conventional or nuclear deterrence strategies.

First, it is impossible to develop a space deterrence strategy based on territorial occupation and geographical targeting. Space is mostly a vast, empty domain where nothing stays in one place physically. Traditionally, the concept of deterrence was developed based on the geopolitical placement of forces and marked with the defense of territory. However, such a concept of geopolitics does not work in space. Objects in orbit are high-speed, high-velocity objects moving in a vacuum. States can claim sovereignty over space objects, like vessels on the high seas, but they cannot occupy territory or even claim rights to specific orbital trajectories. The Bogota Declaration—declared by countries on the equator (Colombia, Ecuador, Congo, Indonesia, Kenya, Uganda, and Zaire)—categorized geostationary orbit as a natural resource, not a region of space. These countries sought to claim that sovereign airspace does not have a limit and that therefore they should have absolute control over geostationary orbit—36,000 kilometers above the equator—as a natural resource. However, none of these countries has the ability to exercise control over such "sovereign space." In case of a space station, a state can occupy a certain limited space in orbit, but this is, again, analogous to a vessel operating on the high seas. Thus, any deterrence strategy has to be based on the nongeopolitical nature of space.

Second, tit-for-tat deterrence is unlikely to be an effective strategy because of the asymmetric nature of space dependency. If one country heavily depends on space assets (such as the United States) while another is less dependent (such as North Korea), then an attack on the space assets of the country that is more space-dependent would likely be a very effective way to even the odds in a conflict. By contrast, if a country does not depend on space assets for either its economy or its military operations (as is largely the case with North Korea), it would be useless to retaliate against that nation's space assets because they either do not exist or hold very little value to the country. Because countries hold substantially differing attachment to and dependency on space-based assets, deterrence in space cannot simply rely on "in-kind" responses in the way that nuclear deterrence operates.

Third, deterrence by denial is a difficult strategy to pursue in space. The core concept of deterrence by denial is to make it difficult for an adversary to achieve its objective by making a successful attack more difficult and costly to achieve. If one tries to apply a deterrence-by-denial approach in space, one has to deny any attack on space assets. There are many ways to attack space assets, so this is an extremely difficult proposition. For example, a state would need to be able to defend against kinetic ASAT attacks by ground-based missiles, which would require the ability to shoot down any missile targeting a space asset. While not impossible, this is nonetheless extremely difficult, and most nations prefer to reserve their ballistic missile defenses for prevention of attacks on their homelands, not their space assets. Additionally, deterrence by denial would require defending against cyber-based ASAT attacks, meaning a state needs the ability to protect its satellites' command-and-control systems. Again, this is possible, and states already try to prevent such attacks, but it is extremely difficult to guarantee that no cyber intrusions can succeed in seizing control of a satellite. Further complicating matters in pursuit of deterrence by denial, a state would need to defend its satellites against jamming, which requires protecting the satellite's ability to receive and deliver signals through the use of frequency-hopping and encryption. This is also possible but limited by the availability of frequencies and by the cost of implementing such an expensive frequency management system on each and every satellite. To defend against the threat of dazzling, one has to improve the protection of sensors, but this is not technically feasible: There are a variety of measures that can take out sensor capabilities, and to implement countermeasures for all types of attack would compromise the functions of the sensors. Deterrence by denial against rendezvous and docking maneuvers is also difficult because the satellite has no means to reject other space objects' approach unless it has some sort of defense mechanism (such as robot arms or some type of space gun), which adds weight to the satellite. If the approaching objects tried to jam the signals from the satellite, it would face the same difficulty as ground-based jamming. Overall, the cost of attacking a satellite is extremely low, but the cost of denying an attacker success is very high. Thus, although it is important to improve the protection of satellites against kinetic and nonkinetic attacks, it would not be a good strategy to rely only on the strategy of deterrence by denial.

Fourth, there is an attribution problem similar to the one for cybersecurity. Space objects are registered when launched under the Convention on the Registration of Objects Launched into Outer Space (commonly referred to as the Registration Treaty) and catalogued by the U.S. Air Force's Joint Space Operations Center, so if a collision in space occurs, ownership of assets involved in the collision can be determined. However, there will always be some degree of uncertainty over the question of who is responsible for the collision. There may be a natural cause behind the malfunction of the space system, such as a solar flare or geomagnetic activities, or unintentional collision with space debris. Since current SSA efforts can detect space debris only bigger than the size of a softball, there is always a possibility that malfunction occurred due to the collision with smaller space debris. Even if the collision took place between active satellites, one cannot be sure whether the collision was conducted with malign intention or was the unintended consequence of an attempted satellite maneuver. It would be difficult to make a judgment whether to launch retaliatory action under such uncertainties. Given the recent development of "hybrid warfare" strategies by such countries as Russia and China, the recognition and identification of hostile action may be even more difficult because a given adversary may choose to employ such a strategy to exploit the gray zone nature of space.

A Tallinn Manual for Space?

Deterrence in space, therefore, has to be based on something other than conventional deterrence strategies. One can argue that the space security situation looks somewhat similar to that of cybersecurity, where actions can be taken without kinetic forces and with difficulties of attribution, lack of physical protection (such as geographical borders), and other methods of retaliation. In fact, both cyber and space security issues were discussed at the UN by the GGE in the early 2010s.[3]

One achievement that grew out of the international discussions on how to establish norms governing cybersecurity was the *Tallinn Manual on the International Law Applicable to Cyber Warfare*.[4] This document was developed by an international group of experts on international law from NATO countries, so it is rather academic and not legally binding, but it provides certain ideas on how to apply international law in a nonconventional deterrence setting, such as the cyber domain. The *Tallinn Manual* identifies the extent to which national sovereignty may be applied to the disruptive nature of cyber attack, which can be regarded as "armed attacks" during periods of armed conflict, and reaffirms that the inherent rights of self-defense can be applied to these attacks. It defines the means and methods of warfare in retaliation to those cyber attacks with principles of necessity and proportionality. The *Tallinn Manual* is a collection of existing international law on armed conflict, but cyber intrusions are taking place on a daily basis even in the absence of armed conflict. Thus, the international group of experts revised their study and re-published it as the *Tallinn Manual 2.0* in 2017.[5]

[3] United Nations General Assembly, resolution adopted December 2, 2011, A/RES/66/24, December 13, 2011; United Nations General Assembly, resolution adopted December 27, 2013, A/RES/68/243, January 9, 2014; United Nations General Assembly, resolution adopted December 23, 2015, A/RES/70.237, December 30, 2015.

[4] Schmitt, 2013.

[5] Michael N. Schmitt and Liis Vihul, eds., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare*, Cambridge, United Kingdom: Cambridge University Press, 2017.

The *Tallinn Manual 2.0* emphasizes that even in case of an instance of cyber attack and retaliation, the rule of state sovereignty dictates the military action. In short, it argues that retaliation to cyber attacks with force are not legitimate unless they are authorized by the UN Security Council. If a cyber attack is conducted by a nonstate actor, countermeasures can be taken only with the consent of the sovereign state from which the attack was launched, unless there are reasonable grounds to believe that the state government is conspiring with the nonstate actors.

In case of space, there is no equivalent to the *Tallinn Manual*, but a project was launched in 2016 between McGill University and the University of Adelaide to develop a Manual on International Law Applicable to Military Uses of Outer Space.[6] Following the footsteps of not only the *Tallinn Manual* but also the *San Remo Manual on International Law Applicable to Armed Conflict at Sea* and the *Harvard Manual on International Law Applicable to Air and Missile Warfare*,[7] it aims to develop a widely accepted manual clarifying the rules applicable to the military uses of outer space by both state and nonstate actors. The project aims to produce a final volume in three years, so there is not much to discuss yet, but there appears to be a certain understanding that there should be rules and a code of conduct governing retaliatory action in responding to hostile activities against space assets.

Such a manual for the military use of space would certainly contribute to the transparency and predictability of state actions. Although not a legally binding document, it would give some clarity as to what could be expected if a state or nonstate actor tried to attack the space assets of another state. However, it is almost certain that existing international law is far from sufficient to define the new domain of military activities. Thus, the U.S.-Japan alliance, a defense treaty-based partnership between two of the most highly capable states in space, needs to play a defining role in developing international rules to regulate the use of military actions in responding to threats against space assets.

The Role of the U.S.-Japan Alliance in Space Deterrence

Even though deterrence in space may not be as straightforward as nuclear deterrence, there are several things that the U.S.-Japan alliance can do to prevent adversaries from undertaking hostile actions against the two countries' space assets.

First, Japan and the United States can work together to increase transparency of activities in space. Japan has already decided to upgrade its telescope and radar facilities in Okayama

[6] Institute of Air & Space Law, *Manual on International Law Applicable to Military Uses of Outer Space*, Montreal, Canada: McGill University, undated.

[7] Louise Doswald-Beck, ed., *The San Remo Manual on International Law Applicable to Armed Conflict at Sea*, New York: Press Syndicate of the University of Cambridge, 1995; Program on Humanitarian Policy and Conflict Research at Harvard University, *Manual on International Law Applicable to Air and Missile Warfare*, New York: Cambridge University Press, 2013.

prefecture to be able to detect space objects less than 1 meter in diameter (the exact capabilities of the system Japan is preparing to deploy have not been publicly disclosed). Japanese participation in the SSA network is extremely important because the current network does not cover western Pacific and Asian regions. Japanese SSA installations will help cover blind spots, including the spaces above North Korea and China. Although Japanese SSA capabilities do not provide ballistic missile early warning for the purposes of immediately detecting ground-based ASAT missile launches, they should provide sufficient data to determine whether a given ASAT action is attributable to China or North Korea.

Transparency in space activities is obviously the most important element for deterring hostile activities against space assets. Without monitoring space activities through SSA, the cost of ASAT attacks drops off precipitously, making it very attractive for an adversary of the U.S.-Japan alliance to strike at the allies' space assets. The most likely targets for any adversary's attack are the allies' reconnaissance satellites in low-Earth orbit, including Japan's information-gathering satellites, and their satellites in medium-Earth orbit, such as GPS. Effective SSA increases the cost of hostile actions against these systems, particularly kinetic attacks, but does little to prevent nonkinetic activities. Thus, the U.S.-Japan alliance has to work to improve detection of cyber and noncyber ASAT activities. The allies need to share information so as to quickly and accurately identify and attribute such attacks, with the goal of increasing the economic and social costs to any adversary of taking such actions by providing evidence of hostile activities to the international community.

Second, the U.S.-Japan alliance can work to improve the resilience of space systems.[8] Resilience (or mission assurance) is necessary because space assets are both vulnerable and crucial for socioeconomic and security purposes. If the functions of space assets are taken away intentionally or unintentionally, they need to be replaced in as short a period of time as possible by alternative assets. Those alternative assets could be small satellites that can be launched rapidly, but they could also be the assets of allied or friendly countries. The U.S.-Japan alliance would be able to provide ideal alternative assets for each of the two partner nations because the assets of both countries are interoperable and easily replaceable.

Last but not least, the U.S.-Japan alliance implies a deterrence through punishment approach by planning possible actions, including economic sanctions and cyber and/or military retaliation for attacks on the allies' space assets. Although the rules and regulations on how to respond to attacks on space assets are not yet well-defined under international law, the alliance should use the Bilateral Planning Mechanism initiated in the new Defense Guidelines issued in 2015 to prepare for the worst-case scenario and demonstrate its determination to employ appropriate

[8] In the United States, *resilience* is defined as an aspect of mission assurance, along with reconstitution and defensive operations. The Japanese concept of resilience is also a part of mission assurance (*kinou-hosyou*) but does not include defensive operations.

measures to retaliate in case of intentional attacks on allied space assets.[9] Deterrence, by definition, is based on the mutual understanding of what would happen if one takes certain action. The main purpose of deterrence is to persuade adversaries not to take any action to harm the allies' space assets in the first place. As discussed earlier, deterrence by denial and deterrence of attacks on space assets through retaliation in space are not convincing because of physical and technical difficulties. Therefore, the allies should use means other than those in space to threaten punishment and persuade the adversary to abjure such attacks in the first place. In other words, the alliance should prepare and plan for cross-domain deterrence as a means of dissuading its enemies from striking at its space assets. Japan has constraints on its ability to take aggressive actions toward adversaries, but exercising collective self-defense with the United States in joint operations—thanks to the recent amendment of the interpretation of the Japanese constitution's Article 9, plus related collective self-defense-enabling legislation—can be used to reinforce a convincing deterrent posture toward potential adversaries.

Conclusion

There is no doubt that space systems are vital for daily activities and security. But the security of space systems falls far short of the desired level; such systems are fragile and extremely vulnerable to an adversary's first strike. To date, much of the focus on the security of space systems has stemmed from the need to defend against direct assent kinetic attacks, such as the Chinese ASAT test in 2007, but there are many other ways for hostile nations to attack allied satellite capabilities.

It is worth bearing in mind that any satellite in space today can easily be repurposed as a space weapon tomorrow. If command uplinks are hacked and the satellite is taken over by actors with malign intentions, that satellite can be placed in an orbit that will lead it to collide with other satellites. This means that the U.S.-Japan alliance needs to prioritize the cyber integrity not only of the satellites of the United States and Japan but even those of Russia or China: Any satellite, whether it is state-operated or run by a commercial or private entity, a university, or a scientific research group, can have its assets hacked and turned into weapons. Protecting all satellites from cyber attack is an urgent need to achieve the secure and sustainable use of space.

Space debris is only one example of possible consequences that could stem from this lack of security. If a satellite collision creates thousands of pieces of debris, that debris will not only increase the risks to other satellites but also create a situation referred to as the Kessler Syndrome, where new debris collides with older debris and creates even more debris until the orbital environment becomes so contaminated that it is fundamentally unsafe for human usage.[10]

[9] Ministry of Defense of Japan, 2015.

[10] Michelle La Vone, "The Kessler Syndrome: 10 Interesting and Disturbing Facts," *Space Safety Magazine*, September 15, 2014.

In this situation, it would be impossible to use space for the benefit of mankind and socioeconomic welfare, not to mention security.

To prevent such a catastrophic outcome, the U.S.-Japan alliance should prepare for any intentional and unintentional attacks on space assets. To deter adversaries, the allies need to aim at increasing the cost of attacks, with the goal of establishing a global coverage of their SSA capabilities, which are the means of ensuring that any activities in space are monitored and any malicious activities can be detected and attributed. Also, the alliance needs to improve the resilience of space systems to make sure that ASAT attacks do not achieve their objectives. Finally, the alliance should develop a plan to respond to any intentional attacks so that the adversaries can understand that the cost of attacking allied space assets will be exceedingly (and, from their perspective, unacceptably) high. For Japan, the alliance with the United States is the key to protecting its space assets from any hostile attacks; therefore, Tokyo and Washington should work together to develop a joint, cross-domain allied space deterrence strategy.

8. Conclusion: Leveraging the U.S.-Japan Alliance to Deter Gray Zone Coercion in the Maritime, Cyber, and Space Domains

Scott W. Harold, Ph.D.
Associate Director, Center for Asia Pacific Policy
RAND Corporation

As the chapters in this volume demonstrate, the challenges that the United States and Japan face from China's employment of gray zone coercion across multiple domains are real, pressing, and a serious challenge for policymakers (the same would hold true if other countries, such as Russia or North Korea, were to employ such means on a similar scale). A common thread among these challenges is that they involve actors and/or domains that are intended to obfuscate state responsibility for command and control so as to achieve material change in the status quo while enabling a revisionist power to capture gains at the expense of the allies. While a response in kind (i.e., of the same type or in the same domain) is often either difficult or undesirable (as the chapters on cyber and space make clear), this by no means is intended to imply that the allies are bereft of policy options to reinforce deterrence. In many cases, the allies can undertake substantial steps to shape international norms, reduce the incentives and opportunities favoring or empowering gray zone tactics, enhance deterrence through denial, and demonstrate their willingness to retaliate via deterrence through punishment or cost-imposition. This concluding chapter outlines several findings drawn from and inspired by the analyses of the research presented in this report.

First, a common feature across all three domains, as several of the authors note, is the value of normative stigmatization of gray zone coercion. Allies can raise the costs to actors who would employ gray zone coercion in any domain (or multiple domains) by equating such actors with illegal combatants, pirates, privateers, criminals, or terrorists. When revisionists erode the boundaries between civilian and military norms, they imperil the rules that protect all fishermen, all internet users, and all of those who would rely on commercial use of space. If the global commons of the high seas, the internet, or outer space are turned into arenas where actors of unknown provenance can carry out attacks on peaceful status quo powers with impunity, then the order that has supported peace and development will itself be at risk, including the order that has supported China's growth. The United States, as one of the leading powers in the United Nations, and Japan, as the world's preeminent civilian power and leading supporter of international law and organizations, are particularly well-positioned to mobilize global support for stigmatizing gray zone coercion and should move to reinforce these norms, building off the success they have seen in stigmatizing Russian aggression in the Crimea, over the shooting down of Malaysian Airlines Flight 17, and over Moscow's interference in numerous Western countries' democratic elections.

Designation of a state as a user of gray zone coercion could come to be seen as a new category akin to "international armed aggressor" or "state sponsor of terror," potentially with legal and normative implications that might cause national leaders to think twice about employing tools of gray zone coercion in the hopes of changing the status quo on the cheap.

Such an approach, of course, implies the importance of diplomacy and multilateral cooperation that extends far beyond the U.S.-Japan alliance to draw on other U.S. alliances, security partnerships, and cooperative relationships, as well as international organizations to establish a broad coalition to stigmatize those who would employ such gray zone coercive tactics. Numerous recent studies have shown that the Asia-Pacific region may be open to knitting itself together in new and important ways in the security domain, such as would be necessary to accomplish such stigmatization. Key U.S. allies and partners in the region have been moving beyond the "power play" hub-and-spokes model that the United States established in the early Cold War era and may be evolving toward something one study has described as a "power web," or toward what another has characterized as a possible "federated defense" model.[1] A third study has even gone so far as to lay out an "alliance roadmap" designed to achieve a "dynamic balance" for nonallies and other partners that could be encouraged to build cooperation around the core of the networked allies.[2]

Second, the role of intelligence-sharing and the creation of a common operating picture among actors in the maritime domain in East Asia, in the online domain, and in outer space helps reduce the opacity that favors actors who seek to exploit ambiguity in carrying out gray zone coercion. Increasing the transparency and improving the ability of all parties to understand who is who, what assets are where, and who is controlling what dramatically improves the ability to reduce or even eliminate the "grayness" of the gray zone. While this is difficult in many cases, it is not impossible in all cases, and to the extent that it can be done, it calls into doubt an aggressor's ability to achieve gray zone coercion without running unacceptable risks of escalation into the military domain that the aggressor is seeking to avoid. For this reason, investments in intelligence and agreements aimed at enhancing intelligence- and information-sharing emerge as promising arenas for deeper cooperation between the United States and Japan, as well as between the allies and other regional partners, such as South Korea, Taiwan, or the Philippines in the maritime domain or other major cyber or space powers in other domains.

Third, when it comes to deterrence through denial, the allies have a number of options available. Japan can and should acquire additional maritime law enforcement capabilities and

[1] Victor Cha, "Powerplay: Origins of the U.S. Alliance System in Asia," *International Security*, Vol. 34, No. 3, Winter 2009/2010; Patrick Cronin, Richard Fontaine, Zachary M. Hosford, Oriana Skylar Mastro, Ely Ratner, and Alexander Sullivan, *The Emerging Asia Power Web: The Rise of Intra-Asian Security Ties*, Washington, D.C.: Center for a New American Security, 2013; Michael J. Green, Kathleen H. Hicks, and Zack Cooper, *Federated Defense in Asia*, Washington, D.C.: Center for Strategic and International Studies, 2014.

[2] Patrick Cronin, Mira Rapp-Hooper, and Harry Kresja, *Dynamic Balance: An Alliance Requirements Roadmap for the Asia-Pacific Region*, Washington, D.C.: Center for New American Security, 2016.

hire more staff; it can also eliminate any legal and operational seams between the JCG and the JSDF.[3] Together, the United States and Japan can continue to bolster their conventional military posture in the Southwest Island chain; bring in new capabilities, such as those outlined in Chapter 2; and develop additional concepts of operations to close off the option of a low-cost island seizure (for the maritime domain). Although touched on but little in this volume with respect to maritime affairs, the U.S. military (and especially its amphibious assault capabilities, which are particularly useful for combating Chinese conventional A2/AD capabilities[4]) can be leveraged to bolster deterrence by denial through planning, training, and exercising. This can be done by leveraging the BPM and the ACM with the goal of ensuring a seamless, joint, allied response to gray zone contingencies. As the August 2016 intrusion into the waters around the Senkakus has shown, China's fisheries fleet, maritime law enforcement forces, maritime militia, and, behind them all, the PLA stand ready to pose a real and continuing threat to the Southwest Island Chain, including the Senkakus.[5] The allies stood up the BPM and ACM to address exactly this kind of gray zone coercion attempt, and it will be important to learn lessons from that incident and further coordinate, refine, and improve response times and measures to present a more complicated and difficult target to China should it continue to seek to change the status quo through maritime gray zone coercion.

Similarly, the allies can further improve their national public-private cooperation on cyber defenses, encouraging greater "cyber hygiene" among the population and mandating it among all defense and critical infrastructure–related private-sector firms. At the same time, Washington and Tokyo can accelerate information-sharing, participate in joint research and development aimed at further automating detection and defense programs, and expand efforts to stigmatize cyber attacks through the promotion of global norms.[6] They can accelerate vulnerability patching protocols, routinely test their own systems, and even engage in limited testing of each other's capabilities for military operations as a means of trying to find and fix vulnerabilities before they are exploited by an adversary.

In space, while hardening is difficult, deterrence by denial still has a role to play, though like in the cyber and maritime domains, it is but one part of a broader overall strategy to complicate and frustrate adversaries' targeting and efforts to degrade space-based assets or hold them at risk.

[3] On this last concern in particular, see Celine Pajon, "Japan's Coast Guard and Maritime Self-Defense Force in the East China Sea: Can a Black-and-White System Adapt to a Gray-Zone Reality?" *Asia Policy*, No. 23, January 2017.

[4] Grant Newsham, "Exploiting Amphibious Operations to Counter Chinese A2/AD Capabilities," Center for a New American Security, June 13, 2016.

[5] "Japan Protests After Swarm of 230 Chinese Vessels Enter Waters Near Senkakus," Kyodo, August 6, 2016. The nominally private fishing vessels were escorted by at least six Chinese Coast Guard vessels and followed a similar incident the day prior when eight Chinese Coast Guard vessels entered Japanese territorial waters around the Senkakus.

[6] For more on U.S.-Japan cooperation on cyber hygiene, see Harold et al., 2016. For more on strengthening norms as a strategy to shape Chinese behavior in cyberspace, see Scott W. Harold, Martin C. Libicki, and Astrid Stuth Cevallos, *Getting to Yes with China in Cyberspace*, Santa Monica, Calif: RAND Corporation, RR-1335-RC, 2016.

Such hardening requires continued efforts to defend ground-based TT&C facilities, further enhancements to cybersecurity and efforts to harden other means of two-way communications, and improvements to shared or joint SSA. Satellites, owing to the environment in which they operate, probably cannot be truly stealthy in comparison to the background temperature of space (which currently hovers a mere 2.7 degrees Kelvin above absolute zero). Additionally, space systems cannot be hardened sufficiently or made sufficiently mobile and repositionable to absorb or avoid a deliberate kinetic strike. Therefore, satellites and other space assets are best hardened in a limited sense in terms of actions taken on the ground and in the uplinks and downlinks between the space-based assets and their ground-based controllers.

Finally, there are several ways to enforce deterrence by punishment (or deterrence through cost-imposition, as some of the authors prefer to call it), in addition to normative background framing, which is probably unlikely to work in the short to medium term unless bolstered by substantial additional incentives. Such incentives could include the use of legal and economic sanctions to impose costs on state, substate, and private-sector actors who engage in gray zone coercion. Individuals and firms can be listed with Interpol, firms can be delisted from stock exchanges and banned from selling in overseas markets, assets can be frozen, visas can be blocked, and individuals or groups who participate in cyber activities or maritime gray zone coercion could even be cyber stalked. Furthermore, as Fukuda suggests, political and covert or clandestine intelligence activities could be undertaken to impose costs against actors who may mistakenly believe that they can act from a position of sanctuary from reprisal but who actually fear their own people or revelations of their own leaders' corruption; the allies could seek to extend greater support to repressed groups seeking to demand their universal human rights. As a final option, the United States and Japan can always adopt an escalatory framework intended to restore deterrence through an acceptance of higher levels of risk—something a number of U.S.-China watchers have called for—with the aim of restoring deterrence through a willingness to absorb the possibility of a resulting accidental conflict.[7]

In conclusion, while there is no guarantee that the U.S.-Japan alliance can successfully dissuade China or other actors from seeking to engage in gray zone coercion directed against the allies in the maritime, cyber, or space domains, the authors of this volume present a wide array of considerations that will aid policymakers and analysts seeking to understand how best to tailor efforts to deter—or, if necessary, defeat—gray zone coercion. The benefits to the U.S.-Japan relationship, the academic and policy communities, the alliance, and peace and security in the Asia-Pacific from continued engagements (such as those associated with the U.S.-Japan alliance conference series proceedings reported on here) will likely continue to pay dividends for years to come.

[7] Oriana Skylar Mastro, "Why Chinese Assertiveness Is Here to Stay," *Washington Quarterly*, Vol. 37, No. 4, 2014; Robert Blackwill and Ashley J. Tellis, *Revising U.S. Grand Strategy Toward China*, Washington, D.C.: Council on Foreign Relations, 2015; Blair, 2015.

About the Authors

Scott W. Harold is associate director of the Center for Asia Pacific Policy and a political scientist at the RAND Corporation, where he specializes in East Asian security and international affairs. Prior to joining RAND in August 2008, he worked at the Brookings Institution's John L. Thornton China Center from 2006 to 2008. In addition to his work at RAND, Harold is an adjunct professor in the Security Studies Program at Georgetown University's Edmund A. Walsh School of Foreign Service, where he has taught since 2006, and an adjunct associate professor of international affairs at Columbia University.

Dean Cheng is a senior research fellow on Chinese political and security affairs at the Heritage Foundation. He specializes in the study of China's military and foreign policy, particularly its relationship with the rest of Asia and with the United States. Prior to joining Heritage, he worked for 13 years as a senior analyst with Science Applications International Corp., and then with the China Studies division of the Center for Naval Analyses. Before entering the private sector, Cheng worked as an analyst in the International Security and Space Program of the Office of Technology Assessment, a congressionally established agency, where he studied China's defense-industrial complex. He earned a bachelor's degree in politics from Princeton University in 1986 and studied for a doctorate at the Massachusetts Institute of Technology.

Major General John A. Davis *(U.S. Army, retired)* is the vice president and federal chief security officer at Palo Alto Networks. He has more than a decade of senior executive experience across all aspects of cybersecurity while directing organizations in the U.S. national security sector. He now expands cybersecurity initiatives and policy for the international public sector and assists governments and industries around the world in preventing cyber attacks. His experience includes cybersecurity risk management, leadership and team building, strategic planning, and cyber threat technical knowledge.

Junichi Fukuda is a visiting fellow at the Institute for International Policy Studies and the Japan Air Self-Defense Force Staff College. He is also a concurrent lecturer at the Graduate School of Law at Hosei University in Tokyo. He has 20 years of experience studying international relations, international security, and defense issues. Previously, he worked as an analyst in the Intelligence and Analysis Service of the Japanese Ministry of Foreign Affairs, as a research fellow at the Sasakawa Peace Foundation, and as a research fellow at the Institute for International Policy Studies.

Keiko Kono is a senior fellow at the National Institute for Defense Studies (NIDS), the think tank of the Japanese Ministry of Defense. She joined NIDS in 2002 after completing her doctoral degree in law at Sophia University. Her current research focuses on international law and domestic legislation on cybersecurity.

Lieutenant General Yoshiaki Nakagawa ***(Japan Ground Self-Defense Forces, retired)*** joined the JGSDF in 1978 and was commissioned in 1979. He holds a master's degree in nuclear engineering from the Massachusetts Institute of Technology. His commands included a JGSDF tank company and an infantry division. His last assignment was as Commander, JGSDF Research and Development Command. He retired in 2013. He is currently a research associate at the Japan Forum for Strategic Studies in Tokyo.

Kazuto Suzuki is a professor of international politics at the Public Policy School of Hokkaido University, Japan. He graduated from the Department of International Relations, Ritsumeikan University, and received his doctorate from Sussex European Institute, University of Sussex, England. He previously worked as an assistant researcher at the Fondation pour la Recherche Strategique in Paris, France, and as an associate professor at the University of Tsukuba. Suzuki served on the Panel of Experts for the Iranian Sanction Committee under the UN Security Council. He is an expert on space policy, nuclear energy policy, export controls, and nonproliferation. He has contributed to the drafting of the Basic Space Law of Japan and serves as a member of subcommittees on industrial policy and space security policy at the National Space Policy Commission.

References

Academy of Military Science, Military Strategy Research Office (China), *The Science of Military Strategy*, Beijing: Military Science Publishing House, 2013.

Asada, Masahiko, "Japan and the Right of Individual Self-Defense" (*Nihon to jieiken: kobetsutekijieiken wo tyu-shin ni*), in Japanese Society of International Law, ed., *National Security* (in Japanese), Tokyo: Sanseidō, 2001.

ASEAN—*See* Association of Southeast Asian Nations.

Association of Southeast Asian Nations, Declaration on the Conduct of Parties in the South China Sea, Phnom Penh, Cambodia, November 4, 2002.

"Atlas 3 Scrubbed to Tuesday," *Space Daily*, May 21, 2000. As of October 25, 2017: http://www.spacedaily.com/news/eutelsat-00g.html

Babbage, Ross, *Countering China's Adventurism in the South China Sea: Strategy Options for the Trump Administration*, Washington, D.C.: Center for Strategic and Budgetary Assessments, 2016.

"Beijing Says It Could Declare ADIZ over South China Sea," *Japan Times,* July 13, 2016.

Blackwill, Robert, and Ashley J. Tellis, *Revising US Grand Strategy Toward China*, Washington, D.C.: Council on Foreign Relations, 2015.

Blair, Dennis, *Assertive Engagement: An Updated U.S.-Japan Strategy for China,* Washington, D.C.: Sasakawa Peace Foundation USA, 2015.

Blandford, Robley, *Pacific Dilemma: Basing, Access, and Forward Deployment***,** Newport, R.I.: Naval War College, 1996.

"Cabinet Decision on Development of Seamless Security Legislation to Ensure Japan's Survival and Protect Its People," Prime Minister of Japan and His Cabinet, July 1, 2014.

Cabinet Office, *The UK Cyber Security Strategy: Report on Progress and Forward Plans*, London, December 2014.

Cabinet Secretariat, "Main Classifications of Emergency Situations" (in Japanese), undated. As of October 25, 2017:
http://www.cas.go.jp/jp/gaiyou/jimu/pdf/kinkyu.pdf

———, "Policy on Strengthening Coast Security System" (in Japanese), December 21, 2016. As of January 31, 2017:
http://www.kantei.go.jp/jp/singi/kaihotaisei/dai1/siryou.pdf

Cavas, Christopher P., “China’s Maritime Militia a Growing Concern,” *Defense News*, November 21, 2016.

Cha, Victor, “Powerplay: Origins of the U.S. Alliance System in Asia,” *International Security*, Vol. 34, No. 3, Winter 2009/2010, pp. 158–196.

Chang Xianqi, *Military Astronautics*, 2nd ed., Beijing: National Defense Industries Press, 2005.

Cheng, Dean, “Chinese Views on Deterrence,” *Joint Forces Quarterly*, No. 60, Spring 2011, pp. 92–94.

———, *Prospects for Extended Deterrence in Space and Cyber: The Case of the PRC*, Washington, D.C.: Heritage Foundation, January 21, 2016. As of October 25, 2017: http://www.heritage.org/defense/report/prospects-extended-deterrence-space-and-cyber-the-case-the-prc

Cheng Lai Ki, “The Little Blue Men: China’s Maritime Proxy-Warfare Strategy,” *Strifeblog*, September 9, 2016.

Clark, Colin, “Cyber Attack on Satellite Could Be Act of War: HPSCI Ranking,” *Breaking Defense*, June 10, 2016. As of October 25, 2017: http://breakingdefense.com/2016/06/cyber-attack-on-satellite-could-be-act-of-war-hpsci-ranking/?mkt_tok=eyJpIjoiTURabFlUTmhNemswTURWayIsInQiOiJ4dzExcEZuMzJUSWM3TytNa2NZREtmcVNvY1E2Y1l5YWxBRHNQSEV2cjM1eDhkR3c0TElJR0JjN1ZNTVNcL2E5ekNrclJKbEpTXC9uTXlmYldWclZoc01kN1ZUd0J0clQ2d3FpVHB0WFZHWm5FPSJ9

Comment No. 27 by the Government of Japan to a Question by House of Representatives (Lower House) Member Seiichi Kaneda on “The Difference Among ‘War,’ ‘Dispute,’ and ‘Use of Force,’ etc.” at the 153rd session of the Diet (Extraordinary session of 2001), Cabinet Decision (in Japanese), February 5, 2002. As of October 25, 2017: http://www.shugiin.go.jp/internet/itdb_shitsumon.nsf/html/shitsumon/b153027.htm

Committee on Defense Posture Review, *Defense Posture Review Interim Report*, Japan Ministry of Defense, July 26, 2013.

Constitution of Japan, promulgated on November 3, 1946, in effect on May 3, 1947. As of October 25, 2017: http://japan.kantei.go.jp/constitution_and_government_of_japan/constitution_e.html

Crawford, James, *The International Law Commission’s Articles on States Responsibility: Introduction, Text and Commentaries,* Cambridge, UK: Cambridge University Press, 2002.

Cronin, Patrick, Richard Fontaine, Zachary M. Hosford, Oriana Skylar Mastro, Ely Ratner, and Alexander Sullivan, *The Emerging Asia Power Web: The Rise of Intra-Asian Security Ties*, Washington, D.C.: Center for a New American Security, 2013.

Cronin, Patrick, Mira Rapp-Hooper, and Harry Kresja, *Dynamic Balance: An Alliance Requirements Roadmap for the Asia-Pacific Region*, Washington, D.C.: Center for New American Security, 2016.

"Defense Ministry, SDF Networks Hacked; State Actor Suspected," *Japan Times*, November 28, 2016. As of October 25, 2017: https://www.japantimes.co.jp/news/2016/11/28/national/politics-diplomacy/defense-ministry-hit-cyberattack-info-may-accessed/#.Wbiw34vzmbM

Division for Ocean Affairs and the Law of the Sea, Commission on the Limits of the Continental Shelf, Outer Limits of the Continental Shelf Beyond 200 Nautical Miles from the Baselines: Submissions to the Commission: Submission by the People's Republic of China, New York, United Nations, May 7, 2009. As of October 27, 2017: http://www.un.org/depts/los/clcs_new/submissions_files/mysvnm33_09/chn_2009re_mys_vnm_e.pdf

Domonoske, Camila, "Chinese Official on Tribunal Ruling: 'It's Nothing but a Scrap of Paper,'" NPR, July 13, 2016. As of October 26, 2017: http://www.npr.org/sections/thetwo-way/2016/07/13/485814417/chinese-official-on-tribunal-ruling-its-nothing-but-a-scrap-of-paper

Doswald-Beck, Louise, ed., *The San Remo Manual on International Law Applicable to Armed Conflict at Sea*, New York: Press Syndicate of the University of Cambridge, 1995.

Erickson, Andrew S., and Conor M. Kennedy, "China's Maritime Militia: What It Is and How to Deal with It," *Foreign Affairs*, June 23, 2016.

Erickson, Andrew S., and Joel Wuthnow, "Barriers, Springboards, and Benchmarks: China Conceptualizes the Pacific 'Island Chains,'" *China Quarterly*, 2016, pp. 1–22.

Freedman, Lawrence, *The Evolution of Nuclear Strategy,* 3rd ed., New York: Palgrave MacMillan, 2003.

———, *Deterrence*, Malden, Mass.: Polity Press, 2004.

Fukuda, Junichi, "Denial and Cost Imposition: Long-Term Strategies for Competition with China," *Asia-Pacific Review*, Vol. 22, No. 1, May 2015, pp. 46–72.

"G7 Principles and Actions on Cyber," adopted at the G-7 Ise-Shima Summit on May 27, 2016, Ministry of Foreign Affairs of Japan website, undated. As of October 25, 2017: http://www.mofa.go.jp/files/000160279.pdf

George, Alexander, and Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice*, New York: Columbia University Press, 1974.

Gill, Terry D., “Non-Intervention in the Cyber Conflict,” in Katharina Ziolkowski, ed., *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy*, Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2013.

Gould, Joe, “Guided-Bomb Makers Anticipate GPS Jammers,” *Defense News*, May 31, 2015. As of October 26, 2017: http://www.defensenews.com/story/defense/air-space/2015/05/31/guided-bomb-makers-gps-jammers-battlefield-spoof-munitions-laser-jdam/28117951/

Government of Japan, Penal Code, Law No. 45, as amended, April 24, 1907. As of October 26, 2017: http://www.japaneselawtranslation.go.jp/law/detail/?id=1960

———, Cabinet Law, Law No. 5 as amended, Article 15 (2), January 22, 1947.

———, Japan Coast Guard Act, Law No. 28, 1948.

———, Self-Defense Forces Act, Law No. 165, 1954.

———, Act on Prohibition of Unauthorized Computer Access, Law No. 128, August 13, 1999. As of October 26, 2017: http://www.japaneselawtranslation.go.jp/law/detail/?id=2250&vm=04&re=02

———, “Cybersecurity Strategy,” Cabinet decision, September 4, 2015. As of October 26, 2017: https://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf

———, “Japan’s Legislation for Peace and Security: Seamless Responses for Peace and Security of Japan and the International Community,” Japanese Ministry of Foreign Affairs, March 2016. As of October 26, 2017: http://www.mofa.go.jp/files/000143304.pdf

Green, Michael J., Kathleen H. Hicks, and Zack Cooper, *Federated Defense in Asia*, Washington, D.C.: Center for Strategic and International Studies, 2014.

Green, Michael, Kathleen Hicks, Zack Cooper, John Schaus, and Jake Douglas, *Countering Coercion in Maritime Asia: The Theory and Practice of Gray Zone Deterrence*, Washington, D.C.: Center for Strategic and International Studies, May 2017.

Harding, Robin, “Japan Scrambles Record Number of Jets as Tensions Rise with China,” *Financial Times*, April 13, 2017.

Harold, Scott W., Martin C. Libicki, and Astrid Stuth Cevallos, *Getting to Yes with China in Cyberspace*, Santa Monica, Calif: RAND Corporation, RR-1335-RC, 2016. As of October 30, 2017: https://www.rand.org/pubs/research_reports/RR1335.html

Harold, Scott W., Martin C. Libicki, Motohiro Tsuchiya, Yurie Ito, Roger Cliff, Ken Jimbo, and Yuki Tatsumi, *The U.S.-Japan Alliance Conference: Strengthening Strategic Cooperation*, Santa Monica, Calif: RAND Corporation, CF-351-GOJ, 2016. As of October 25, 2017: https://www.rand.org/pubs/conf_proceedings/CF351.html

Heath, Timothy R., Kristen Gunness, and Cortez A. Cooper, *The PLA and China's Rejuvenation: National Security and Military Strategies, Deterrence Concepts, and Combat Capabilities*, Santa Monica, Calif.: RAND Corporation, RR-1402-OSD, 2016. As of October 24, 2017: https://www.rand.org/pubs/research_reports/RR1402.html

Hitoshi, Yuichiro, "Some Problems of Japan's New Legislation for Peace and Security from the Viewpoint of Unit Self-Defense: Implication and Limitation of JSDF's Protection of Foreign Armed Forces" (*Unit self-defense kara mita shin-anpohōsei no ronten*) (in Japanese), *The Reference*, No. 783, April 2016, pp. 5–33. As of October 26, 2017: http://dl.ndl.go.jp/view/download/digidepo_9957297_po_078302.pdf?contentNo=1

Hornung, Jeffrey W., *Modeling a Stronger U.S.-Japan Alliance: Assessing U.S. Alliance Structures*, Washington, D.C.: Center for Strategic and International Studies, November 2015.

Hornung, Jeffrey W., and Mike M. Mochizuki, "Japan: Still an Exceptional Ally," *Washington Quarterly*, Vol. 39, No. 1, Spring 2016, pp. 95–116.

Information Security Policy Council, *Information Security 2012*, No. 19, July 4, 2012.

———, *The Basic Policy of Critical Information Infrastructure Protection*, 3rd ed., May 19, 2014, updated by the Japan Cybersecurity Strategic Headquarters, May 25, 2015.

Institute of Air & Space Law, *Manual on International Law Applicable to Military Uses of Outer Space*, Montreal, Canada: McGill University, undated. As of October 26, 2017: https://www.mcgill.ca/iasl/milamos

International Court of Justice, *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)*, June 27, 1986.

Isobe, Lt. Gen. Koichi, Japan Ground Self Defense Forces (Ret.), "The Amphibious Operations Brigade: The Establishment of the JGSDF Brigade and Its Challenges," *Marine Corps Gazette*, Vol. 101, No. 2, February 2017, pp. 24–29.

Ito, Hiroshi, *The Fifth Battlefield: Threat of Cyber Warfare* (*Dai go no senjō: Saiba-sen no kyōi*) (in Japanese), Tokyo: Bungeishunju, 2012.

Japan Coast Guard, "Outline of the Decision on the Budget Related to the Japan Coast Guard" (*Kaijo Hoancho Kankei Yosan Kettei Gaiyou*) (in Japanese), December 2011.

———, "Outline of the Decision on the Budget Related to the Japan Coast Guard" (*Kaijo Hoancho Kankei Yosan Kettei Gaiyou*) (in Japanese), December 2015.

———, "Outline of the Decision on the Budget Related to the Japan Coast Guard" (*Kaijo Hoancho Kankei Yosan Kettei Gaiyou*) (in Japanese), December 2016.

———, "Outline of the Assessment of the FY 2017 Fixed Number of Personnel Request" (*Heisei 29 nendo Teiin Youkyuu Satei no Gaiyou*) (in Japanese), 2017.

Japan Cybersecurity Strategic Headquarters, "Cyber Security Annual Plan 2016" (in Japanese), National Center of Incident Readiness and Strategy for Cybersecurity, August 31, 2016. As of October 26, 2017:
https://www.nisc.go.jp/active/kihon/pdf/cs2016.pdf

"Japan Protests After Swarm of 230 Chinese Vessels Enter Waters Near Senkakus," Kyodo, August 6, 2016.

"Japan Scrambles Jets over China Drone Flight Near Disputed Islets," Reuters, May 20, 2017.

"Japan to Shoot Down Foreign Drones that Invade Its Airspace," Kyodo, October 20, 2013.

Jiang Lianju, *Space Operations Teaching Materials*, Beijing: Military Science Publishing House, 2013.

Kahn, Herman, *On Escalation: Metaphors and Scenarios*, New York: Frederick A. Praeger, 1965.

Katzenstein, Peter J., *Cultural Norms and National Security: Police and Military in Post-War Japan*, Ithaca, N.Y.: Cornell University Press, 1996a.

———, *The Culture of National Security: Norms and Identity in World Politics*, New York: Columbia University Press, 1996b.

Keller, John, "DARPA Seeks to Wean Smart Weapons Off GPS with Hybrid Inertial Navigation System-on-a-Chip," *Military & Aerospace Electronics*, April 18, 2012. As of October 26, 2017:
http://www.militaryaerospace.com/articles/2012/04/darpa-seeks-to-wean-smart-weapons-off-gps-with-hybrid-inertial-navigation-system-on-a-chip.html

Kishida, Fumio, remarks at the Committee on National Security of the House of Representatives (Lower House) at the 187th session of the Diet (Extraordinary session of 2014), *Report of the Committee on National Security of the House of Representatives* (in Japanese), No. 2, 2014. As of October 26, 2017:
http://kokkai.ndl.go.jp/SENTAKU/syugiin/187/0015/18710140015002a.html

Kissinger, Henry A., *Nuclear Weapons and Foreign Policy*, New York: Harper and Brothers, 1957.

Koh, Harold Hongju, "International Law in Cyberspace," *Harvard International Law Journal Online*, Vol. 54, December 2012, pp. 1–12. As of October 26, 2017: http://www.harvardilj.org/wp-content/uploads/2012/12/Koh-Speech-to-Publish1.pdf

Kopp, Carlo, "Breaking Serbia: The Allied Force Campaign," *Airpower Australia*, August 1999. As of October 26, 2017: http://www.ausairpower.net/oaf-analysis.html

La Vone, Michelle, "The Kessler Syndrome: 10 Interesting and Disturbing Facts," *Space Safety Magazine*, September 15, 2014. As of October 26, 2017: http://www.spacesafetymagazine.com/space-debris/kessler-syndrome/

Laird, Burgess, *War Control: Chinese Writings on the Control of Escalation in Crisis and Conflict*, Washington, D.C.: Center for a New American Security, 2017.

Lee, Bradford, "Strategic Interaction: Theory and History for Practitioners," in Mahnken, 2012, pp. 28–46.

Livingstone, David, and Patricia Lewis, *Space, the Final Frontier for Cybersecurity?* London: Chatham House, September 2016.

Mahnken, Thomas G., ed., *Competitive Strategies for the 21st Century: Theory, History, and Practice*, Palo Alto, Calif.: Stanford University Press, 2012.

———, *Cost-Imposing Strategies: A Brief Primer*, Washington, D.C.: Center for a New American Security, November 2014.

Main, Douglas, "Undersea Cables Transport 99 Percent of International Data," *Newsweek*, April 2, 2015. As of October 26, 2017: http://www.newsweek.com/undersea-cables-transport-99-percent-international-communications-319072

Mastro, Oriana Skylar, "Why Chinese Assertiveness Is Here to Stay," *Washington Quarterly*, Vol. 37, No. 4, 2014, pp. 151–170.

Mazarr, Michael J., *Mastering the Gray Zone: Understanding a Changing Era of Conflict*, Carlisle Barracks, Pa.: U.S. Army War College Press, December 2015.

Ministry of Defense of Japan, "China's Defense Budget," infographic, undated-a. As of October 24, 2017: http://www.mod.go.jp/j/approach/surround/pdf/ch_d-budget_20170406e.pdf

———, "Fundamental Concepts of National Defense: Basics of Defense Policy," undated-b. As of October 26, 2017: http://www.mod.go.jp/e/d_act/d_policy/dp02.html

———, *Defense of Japan 1999,* annual white paper, Tokyo: Urban Connections, 1999.

———, "Press Conference by the Defense Minister," transcript, February 8, 2013a. As of October 26, 2017:
http://www.mod.go.jp/e/press/conference/2013/02/08.html

———, "Medium Term Defense Program (FY2014–FY2018)," provisional translation, December 17, 2013b. As of February 2, 2017:
http://www.mod.go.jp/j/approach/agenda/guideline/2014/pdf/Defense_Program.pdf

———, "National Defense Program Guidelines for FY 2014 and Beyond," provisional translation, December 17, 2013c. As of February 2, 2017:
http://www.mod.go.jp/j/approach/agenda/guideline/2014/pdf/20131217_e.pdf

———, "The Guidelines for Japan-U.S. Defense Cooperation," April 27, 2015. As of October 26, 2017:
http://www.mod.go.jp/e/d_act/anpo/shishin_20150427e.html

———, *Defense of Japan 2016,* annual white paper, Ministry of Defense of Japan, 2016.

Ministry of Foreign Affairs of Japan, "Trends in Chinese Government and Other Vessels in the Waters Surrounding the Senkaku Islands, and Japan's Response," web page, November 2, 2016. As of January 31, 2017:
http://www.mofa.go.jp/region/page23e_000021.html

Ministry of Foreign Affairs of Japan and U.S. Department of State, Treaty of Mutual Cooperation and Security Between Japan and the United States of America, 1960.

Morris, Lyle J., "Blunt Defenders of Sovereignty: The Rise of Coast Guards in East and Southeast Asia," *Naval War College Review*, Vol. 70, No. 2, Spring 2017, pp. 75–112.

National Police Agency, "Terrorism by the Democratic People's Republic of Korea (North Korea)," *Focus*, Vol. 271, 2006. As of October 26, 2017:
https://www.npa.go.jp/archive/keibi/syouten/syouten271/english/pdf/sec04.pdf

———, *White Paper on Police 2012*, digest edition, 2012.

———, "Cyber Attack Situation," *Focus* (in Japanese), Vol. 282, 2013. As of October 26, 2017:
https://www.npa.go.jp/archive/keibi/syouten/syouten282/pdf/15_34-37P.pdf#search='%E8%AD%A6%E5%AF%9F%E5%BA%81+%E3%82%B5%E3%82%A4%E3%83%90%E3%83%BC%E6%94%BB%E6%92%83+%E4%B8%89%E8%8F%B1%E9%87%8D%E5%B7%A5+%E5%AE%87%E5%AE%99

National Security Council, "National Security Strategy," Cabinet Secretariat, December 17, 2013.

Newsham, Grant, "Exploiting Amphibious Operations to Counter Chinese A2/AD Capabilities," Center for a New American Security, June 13, 2016.

Obama, Barack, “Executive Order: Improving Critical Infrastructure Cybersecurity,” Washington, D.C., White House, February 12, 2013.

Office of the President of the United States, *The National Space Policy of the United States*, Washington, D.C., 2010.

Oros, Andrew L., *Normalizing Japan: Politics, Identity, and the Evolution of Security Practice*, Stanford, Calif.: Stanford University Press, 2008.

———, *Japan’s Security Renaissance: New Policies and Politics for the Twenty-First Century*, New York: Columbia University Press, 2017.

O’Rourke, Ronald, *Maritime Territorial and Exclusive Economic Zone (EEZ) Disputes Involving China: Issues for Congress*, Washington, D.C.: Congressional Research Service, June 6, 2017.

Orwig, Jessica, “A Rocket Launch Was Delayed Monday Because of a Boat,” *Business Insider*, October 28, 2014. As of October 26, 2017: http://www.businessinsider.com/why-rocket-launch-delayed-by-a-boat-2014-10

Pajon, Celine, “Japan’s Coast Guard and Maritime Self-Defense Force in the East China Sea: Can a Black-and-White System Adapt to a Gray-Zone Reality?” *Asia Policy*, No. 23, January 2017, pp. 111–130.

Panda, Ankit, “U.S. Air Force to Share Space Data Directly with China,” *The Diplomat*, December 9, 2014.

Perlez, Jane, “Calls Grow in China to Press Claim for Okinawa,” *New York Times*, June 13, 2013.

Permanent Court of Arbitration, “PCA Press Release: The South China Sea Arbitration (The Republic of the Philippines v. The People’s Republic of China),” July 12, 2016. As of October 26, 2017: https://pca-cpa.org/en/news/pca-press-release-the-south-china-sea-arbitration-the-republic-of-the-philippines-v-the-peoples-republic-of-china/

Peterson, Andrea, “Why Naval Academy Students Are Learning to Sail by the Stars for the First Time in a Decade,” *Washington Post*, February 17, 2016. As of October 27, 2017: https://www.washingtonpost.com/news/the-switch/wp/2016/02/17/why-naval-academy-students-are-learning-to-sail-by-the-stars-for-the-first-time-in-a-decade/?utm_term=.c59c5f01de15

Program on Humanitarian Policy and Conflict Research at Harvard University, *Manual on International Law Applicable to Air and Missile Warfare*, New York: Cambridge University Press, 2013.

Przystup, James J., *The U.S.-Japan Alliance: Review of the Guidelines for Defense Cooperation*, Washington, D.C.: National Defense University Press, Institute for Strategic Studies Strategic Perspectives, No. 18, March 2015.

Public Security Intelligence Agency of Japan, *Annual Report 2012: Review and Prospects of Internal and External Situations*, 2013. As of October 27, 2017: http://www.moj.go.jp/content/000112383.pdf

Roberts, Brad, "Tailored Options to Deter North Korea and WMD Threats," *Korean Journal of Defense Analysis*, Vol. 28, No. 1, March 2016, pp. 25–30.

Roy, Denny, "China's Strategy to Undermine the U.S. in Asia: Win in the 'Gray Zone,'" *The National Interest*, September 18, 2015.

Ruys, Tom, "The Meaning of 'Force' and the Boundaries of the Jus ad Bellum: Are 'Minimal' Uses of Force Excluded from UN Charter Article 2(4)?" *American Journal of International Law*, Vol. 108, No. 2, 2014, pp. 159–210.

Saadawi, Tarek, and John D. Colwell, Jr., eds., *Cyber Infrastructure Protection*, Vol. III, Carlisle, Pa.: U.S. Army War College, June 2017.

Saadawi, Tarek, and Louis H. Jordan, Jr., eds., *Cyber Infrastructure Protection*, Carlisle, Pa.: U.S. Army War College, May 2011.

Saadawi, Tarek, Louis H. Jordan, Jr., and Vincent Boudreau, eds., *Cyber Infrastructure Protection*, Vol. II, Carlisle, Pa.: U.S. Army War College, May 2013.

Saporito, Laura, and James A. Lewis, *Cyber Incidents Attributed to China*, Washington, D.C.: Center for Strategic and International Studies, 2013. As of October 27, 2017: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130311_Chinese_hacking.pdf

Schmitt, Michael N., *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of The NATO Cooperative Cyber Defence Centre of Excellence*, Cambridge, United Kingdom: Cambridge University Press, 2013.

Schmitt, Michael N., and Liis Vihul, eds., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare*, Cambridge, United Kingdom: Cambridge University Press, 2017.

Shelling, Thomas C., *Arms and Influence*, New Haven, Conn.: Yale University Press, 1966.

Shim, Elizabeth, "Japan to Install Land-Based Missile Defense Aegis Ashore," UPI, August 17, 2017.

Snyder, Glenn, "The Balance of Power and the Balance of Terror," in Paul Seabury, ed., *The Balance of Power*, San Francisco, Calif.: Chandler, 1965, pp. 196–201.

Standing Committee of the Seventh National People's Congress, Law of the People's Republic of China Concerning the Territorial Sea and the Contiguous Zone, February 25, 1992.

Stefan-Gady, Franz, "'Little Blue Men': Doing China's Dirty Work in the South China Sea," *The Diplomat*, November 5, 2015.

Sulmeyer, Michael, *Report on Cyber Deterrence Policy*, Washington, D.C.: Office of the Secretary of Defense, December 2015. As of October 25, 2017:
http://federalnewsradio.com/wp-content/uploads/2015/12/Report-on-Cyber-Deterrence-Policy-Final.pdf

Swaine, Michael D., Rachel M. Swanger, and Takashi Kawakami, *Japan and Ballistic Missile Defense*, Santa Monica, Calif.: RAND Corporation, MR-1374-CAPP, 2001. As of October 24, 2017:
https://www.rand.org/pubs/monograph_reports/MR1374.html

Taniwaki, Yasuhiko, "Cybersecurity Strategy in Japan," presentation at the Sasakawa Peace Foundation USA's Third Annual Security Forum: American and Japanese Interests and the Future of the Alliance, May 6, 2016. As of October 27, 2017:
https://spfusa.org/event/third-annual-security-forum-american-japanese-interests-future-alliance/

Tsuchiya, Motohiro, *Cyber Terrorism: Japan, The U.S. vs. China* (*Saiba-tero; Japan, The U.S. vs. China*) (in Japanese), Tokyo: Bungeishunju, 2012.

———, "Japan-U.S. Cooperation in Cybersecurity," in Harold et al., 2016, pp. 16–25.

United Nations, Charter of the United Nations and Statute of the International Court of Justice, San Francisco, Calif., 1945.

United Nations General Assembly, resolution adopted December 2, 2011, A/RES/66/24, December 13, 2011.

———, resolution adopted December 27, 2013, A/RES/68/243, January 9, 2014.

———, resolution adopted December 23, 2015, A/RES/70.237, December 30, 2015.

———, *Developments in the Field of Information and Telecommunications in the Context of International Security, Report of the Secretary-General*, U.N. Doc. A/71/172, July 19, 2016. As of October 27, 2017:
http://undocs.org/A/71/172

U.S. Department of Defense, "DOD Deterrence Strategy for Deterrence in Space," fact sheet, 2011. As of October 27, 2017:
http://archive.defense.gov/home/features/2011/0111_nsss/docs/DoD%20Strategy%20for%20Deterrence%20in%20Space.pdf

———, *The DOD Cyber Strategy*, Washington, D.C., April 2015.

U.S. Department of Defense and Government of Japan, Guidelines for U.S.-Japan Defense Cooperation, April 27, 2015. As of October 28, 2017: http://archive.defense.gov/pubs/20150427_--_GUIDELINES_FOR_US-JAPAN_DEFENSE_COOPERATION.pdf

U.S. General Accounting Office, *Critical Infrastructure Protection: Commercial Satellite Security Should Be More Fully Addressed*, Washington, D.C., GAO-02-781, August 2002.

U.S. Joint Chiefs of Staff, *Joint Operation Planning*, Joint Publication 5-0, August 11, 2011.

———, *Space Operations*, Washington, D.C.: Government Printing Office, Joint Publication 3-14, May 2013. As of October 27, 2017: http://www.dtic.mil/doctrine/new_pubs/jp3_14.pdf

Vig, John R., "Accurate Clocks and Their Applications," Princeton ACM, November 2011. As of October 27, 2017: http://princetonacm.acm.org/downloads/AccurateClocksVig.pdf

Wang Yao and Shi Chunming, "Regarding 'Space Information Warfare,'" *China National Defense Newspaper*, June 12, 2003. As of October 27, 2017: http://news.xinhuanet.com/mil/2003-06/12/content_916804.htm

Wani, Kentaro, "The Concept of 'Unit Self-Defense' in International Law" (*Kokusaihō ni okeru 'unit self-defense' no hōtekiseishitsu to igi*), *Osaka Law Review* (*Handai hōgaku*) (in Japanese), Vol. 295, 2015, pp. 25–85.

Wuthnow, Joel, and Philip C. Saunders, *Chinese Military Reforms in the Age of Xi Jinping: Drivers, Challenges and Implications*, Washington, D.C.: National Defense University Institute for National Strategic Studies, 2017.

Yamazaki, Fumiaki, "Challenges and Proposal for Cyber Security in Japan" (*Nihon no saiba-sekyuriti no kadai to teigen*) (in Japanese), NEC Corp. website, August 30, 2013. As of October 27, 2017: https://www.blwisdom.com/linkbusiness/linktime/future/item/8963/8963.html?start=1

Yoshihara, Toshi, "Going Anti-Access at Sea," Center for a New American Security, September 12, 2014.

Zhang Yuwu, "Informationalized Warfare Will Make Seizing the Aerospace Technology 'High Ground' a Vital Factor," *PLA Daily*, March 30, 2005.