



Strengthening the U.S.-Japan Alliance: Pathways for Bridging Law and Policy

**Edited by Nobuhisa Ishizuka,
Masahiro Kurosaki
and Matthew C. Waxman**

Center for Japanese Legal Studies
National Security Law Program
Columbia Law School

Strengthening the U.S.-Japan Alliance

Pathways for Bridging Law and Policy

Edited by
Nobuhisa Ishizuka
Masahiro Kurosaki
and
Matthew C. Waxman

Center for Japanese Legal Studies
National Security Law Program
Columbia Law School

Copyright © 2020 Trustees of Columbia University.
All rights reserved.

Cite as:

Nobuhisa Ishizuka, Masahiro Kurosaki and Matthew C. Waxman (eds.), *Strengthening the U.S.-Japan Alliance: Pathways for Bridging Law and Policy* (Columbia Law School, 2020), available at <https://jls.law.columbia.edu/alliance>

ISBN-13: 978-0-578-71877-4

The images that appear as section dividers throughout this volume are based on prints from the collection of the Metropolitan Museum of Art. We appreciate the museum's generosity in making these images available for use by the public.

Pages 12 & 64: Kobayashi Kiyochika, *Use of Electric Light at the Time of Attack on Bingyang, Korea*, Meiji period (1868–1912). Bequest of William S. Lieberman, 2005. 2007.49.328

Pages 28 & 48: Yamazaki Toshinobu, *Presentation of the Head of Saigo to the Prince Arisogawa*, 1887. Gift of Lincoln Kirstein, 1959. JP3226

Page 76: Tsukioka Yoshitoshi, *Fifty-three Stations of Suehiro: Warrior Looks at Passing Steamship*, ca. 1865. Gift of Lincoln Kirstein, 1959. JP3178

Page 100: Kobayashi Kiyochika, *Illustration of the Great Korean War*, 1882. Gift of Lincoln Kirstein, 1959. JP3310

Pages 116 & 196: Yamazaki Toshinobu, *Commanders Receiving the Emperor's Drinking Cups*, 1886. Gift of Lincoln Kirstein, 1959. JP3251

Page 178: Kobayashi Kiyochika, *Illustration of the Empress Visiting the General Staff Headquarters [to present a tray of bandages]*, 1895. Gift of Lincoln Kirstein, 1959. JP3266

5 Acknowledgements

6 Introduction

PART I: USE OF FORCE IN SELF-DEFENSE

12 The United States and Individual
and Collective Self-Defense in Northeast Asia
Thomas H. Lee, Fordham University

28 Legal Framework of Japan's Self-Defense
with the United States
Masahiro Kurosaki, National Defense Academy of Japan

PART II: DECISION-MAKING PROCESS ON USE OF FORCE

48 Presidential Use of Force in East Asia:
American Constitutional Law and the U.S.-Japan Alliance
Matthew C. Waxman, Columbia University

PART III: THE U.S.-JAPAN ALLIANCE IN LEGAL CONTEXT

64 Japan-U.S. Alliance as a Maritime Alliance and International Law
Hideshi Tokuchi, National Graduate Institute for Policy Studies

76 How the Law of Collective Self-Defense Undermines
the Peace and Security of the Taiwan Strait
Julian G. Ku, Hofstra University

100 Japan's Legal Readiness in the Event of Hostilities
on the Korean Peninsula
Hitoshi Nasu, Exeter University

116 Reconsidering International Law and Cyberspace Operations
Through the Lens of the U.S.-Japan Alliance
Michael J. Adams, Commander (ret.), U.S. Navy

178 Space Deterrence and the Role of the U.S.-Japan Alliance
Kazuto Suzuki, Hokkaido University

196 Toward Meta-Knowledge of Foreign Relations Law in
U.S.-Japan Relations
Ryan Scoville, Marquette University

THE CENTER FOR JAPANESE LEGAL STUDIES AT COLUMBIA LAW SCHOOL

The Center for Japanese Legal Studies at Columbia Law School, aided by the leading collection of Japanese legal materials in the U.S., has actively promoted research on Japanese law for over 40 years. It conducts academic research, scholarly exchanges and programs for students, faculty, scholars and practitioners to enhance understanding of the Japanese legal system.

Nobuhisa Ishizuka is Executive Director of the Center for Japanese Legal Studies and Lecturer in Law at Columbia Law School. He was a graduate research student and is a visiting lecturer at the University of Tokyo. His research interests include international comparative law, East Asian defense and security policy, legal history, and the Japanese constitution. He is a member of the Council on Foreign Relations and a graduate of Columbia College and Columbia Law School, where he was a Senior Editor of the *Columbia Law Review*.

NATIONAL SECURITY LAW PROGRAM AT COLUMBIA LAW SCHOOL

The National Security Law Program focuses on the roles of domestic and international law in national security matters, from the perspective of both lawyers and policymakers. The contours of the dynamic field of national security law are in constant flux, being shaped and reshaped in light of emerging threats, challenges and technologies. The National Security Law Program aims to further academic dialog through partnerships with other centers, programs, universities and think tanks.

ACKNOWLEDGEMENTS

The editors gratefully acknowledge the financial and administrative support of the Weatherhead East Asian Institute at Columbia University, the Center for Japanese Legal Studies at Columbia Law School, the Center for Global Security at the National Defense Academy of Japan, and the Japan Society for the Promotion of Science (JSPS KAKENHI Grant Number 16H03595). Under their auspices, the “Workshop on the U.S.-Japan Alliance and the Power of International Law” was convened on three occasions during the period between 2017–2019 at the School of International and Public Affairs of Columbia University, New York, and the International House of Japan, Tokyo.

The editors would like to acknowledge the contributions of Takako Hikotani, Gerald L. Curtis Associate Professor of Modern Japanese Politics and Foreign Policy, Columbia University. The successful completion of this project would not have been possible without her significant organizational and managerial support.

Special thanks go to Jason Healey, Mira Rapp-Hooper, James Kraska, Adam P. Liff, Masamitsu Nagano, Susumu Nakamura, Shohei Nishimura, Yusuke Saito, Jack L. Snyder, Shinsuke J. Sugiyama, and David A. Welch. Their active engagement in the workshop enriched and inspired our project.

The editors also thank Nika Liora Bederman '22, Peter C.Y. Kim '20, Amanda N. Obi (LL.M.) '20, and Nian Zhan '22 of Columbia Law School for their dedicated editorial support for this project. Grateful acknowledgment is made to Nick Pozek and Daniel James Marcheschi, Jr. of Columbia Law School's Center for Japanese Legal Studies for their very capable administrative support.

Introduction

During the three years leading up to this year's 60th anniversary of the signing of the 1960 U.S.-Japan Security Treaty, a series of workshops were held under the joint sponsorship of Columbia Law School's Center for Japanese Legal Studies and the National Defense Academy of Japan's Center for Global Security. Bringing together experts in international law and political science primarily from the United States and Japan, the workshops examined how differing approaches to use of force and understandings of individual and collective self-defense in the two countries might adversely affect their alliance.

The workshop participants explored the underlying causes of the gap in understanding between the United States and Japan with respect to these issues, and they considered the alliance in the context of each state's interpretation of international law and policy positions regarding its rights and obligations under such law. In doing so, they also examined how the differing approaches could be applied to possible crisis situations of current concern in East Asia, and what that might mean for alliance relations.

Thomas H. Lee starts by articulating the fundamental issues regarding the international law of individual and collective self-defense in "The United States and Individual and Collective Self-Defense in Northeast Asia". He applies them to four Northeast Asia security issues: the North Korean nuclear threat, offensive cyber operations, the status of Taiwan, and Japan-South Korea-China territorial disputes. In doing so, he finds mixed outcomes for support of individual and collective self-defense as justifications for the use of force in each of these areas, if one applies their principles consistently under each scenario.

In "Legal Frameworks on Japan's Self-Defense with the United States," Masahiro Kurosaki explains that, notwithstanding the 2016 policy change in Japan permitting the use of collective self-defense, there still exists a perception gap between Japan and the United States concerning the extent to which Japan is free to exercise such rights. He shows that this divergence arises from Japan's adoption of a narrower view than the United States of the specific

requirements for invoking such rights, and that this view is rooted in case law of the International Court of Justice (ICJ) as well as in its own constitutional constraints.

For framing discussions in this book, on the international law plane, one should first note from Lee's and Kurosaki's arguments that the United States and Japan exhibit contrasting attitudes toward the relationship of the U.N. Charter to customary international law on self-defense. On the one hand, the United States asserts an inherent right of self-defense based on principles of customary law, including a longstanding doctrine of anticipatory self-defense. On the other hand, Japan regards the U.N. Charter as superseding some customary law that the United States continues to embrace.

On the domestic law plane, one needs to consider the constitutional allocation of power for use of force between the executive and legislative branches. In his essay "Presidential Use of Force in East Asia: American Constitutional Law and the U.S.-Japan Alliance," Matthew C. Waxman explains U.S. presidential power and congressional and bureaucratic constraints on such power, placing such issues in the context of military action in East Asia and alliance relations between the United States and Japan. He shows that although the president wields enormous power and discretion to authorize military action, political factors operate to influence presidential decision-making in ways that can affect U.S. use of force and alliance management.

These contrasts on the international and domestic planes could pose significant challenges to the U.S.-Japan alliance, notably at the critical stage of initial reaction to a variety of common threats to both states. To find possible solutions, such challenges need to be addressed in more detail. The next series of essays therefore consider the U.S.-Japan alliance in more specific strategic and legal contexts.

In "Japan-U.S. Alliance as a Maritime Alliance and International Law," Hideshi Tokuchi emphasizes the importance of deterrence for Japan's security, and the role played by the U.S.-Japan alliance and international law to reinforce this imperative. He argues that East Asia must be viewed geographically from a larger Indo-Pacific perspective, and that balance of power in this vast region is only possible through maritime security supported by the alliance. He illustrates how international law considerations interact with the alliance relationship in formulating responses to Chinese activities in the South and East China Seas.

In "Reconsidering International Law and Cyberspace Operations Through the Lens of the U.S.-Japan Alliance," Michael J. Adams considers the U.S. government's new "defend forward" cyber posture as well as Japan's growing ambitions in cyberspace. He outlines the international legal framework applicable to cyber operations as well as gaps therein, including certain contested international law issues such as sovereignty and notice

of countermeasures in the cyber context. He then highlights domestic considerations bearing on the extent to which the allies may share obligations in the cyber domain, and he illustrates through scenarios how the United States and Japan might partner in defensive cyber scenarios.

Julian G. Ku argues that strict adherence to principles limiting the use of force, such as those set forth in the U.N. Charter, could encourage aggression and discourage defensive intervention by states, taking as an example potential hostilities in the Taiwan Strait. In his essay “How the Law of Collective Self-Defense Undermines the Peace and Security of the Taiwan Strait,” he shows how differing conceptions of individual and collective self-defense in the United States and Japan weakens the international legal basis for any intervention by either of them into a China-Taiwan conflict. At the same time, he shows how Taiwan’s status prevents it from invoking such concepts in its own defense.

Hitoshi Nasu elaborates on the legal framework for the U.S.-Japan alliance under international law and Japanese security law in the context of Japan’s possible use of force in the event of outbreak of hostilities on the Korean peninsula. In “Japan’s Legal Readiness in the Event of Hostilities on the Korean Peninsula,” he shows how continuing limitations on the use of force under Japan’s legislative framework will constrain Japan’s options under various scenarios in the event of such hostilities.

Kazuto Suzuki addresses the critical importance of space systems on national security, both from a socio-economic and military standpoint. In his chapter “Space Deterrence and the Role of the U.S.-Japan Alliance,” he demonstrates the multiple ways such assets are vulnerable, and explains why conventional deterrence strategies and the current state of international law are insufficient to address such threats. He argues that the U.S.-Japan alliance can increase the resilience of their space systems by cooperating on early threat detection and enhancing “cross-domain” deterrence.

Finally, in “Toward Meta-Knowledge of Foreign Relations Law in U.S.-Japan Relations,” Ryan Scoville turns attention inward to the operational aspects of the U.S.-Japan alliance, and how deficiencies in knowledge of each other’s foreign relations law can hinder the effective functioning of the alliance. In citing examples showing how knowledge gaps can promote misperceptions between the countries (as well as third parties trying to ascertain their motives), he suggests ways in which such knowledge may be developed to reduce the risk of misunderstanding and miscalculation on both sides and by others.

The U.S.-Japan alliance has been hailed as the “cornerstone” of peace in the Asia-Pacific. Despite policy differences, the alliance relationship in fact has been strengthened and institutionalized over the years, culminating in the Alliance Coordination Mechanism (ACM). That institutionally structured

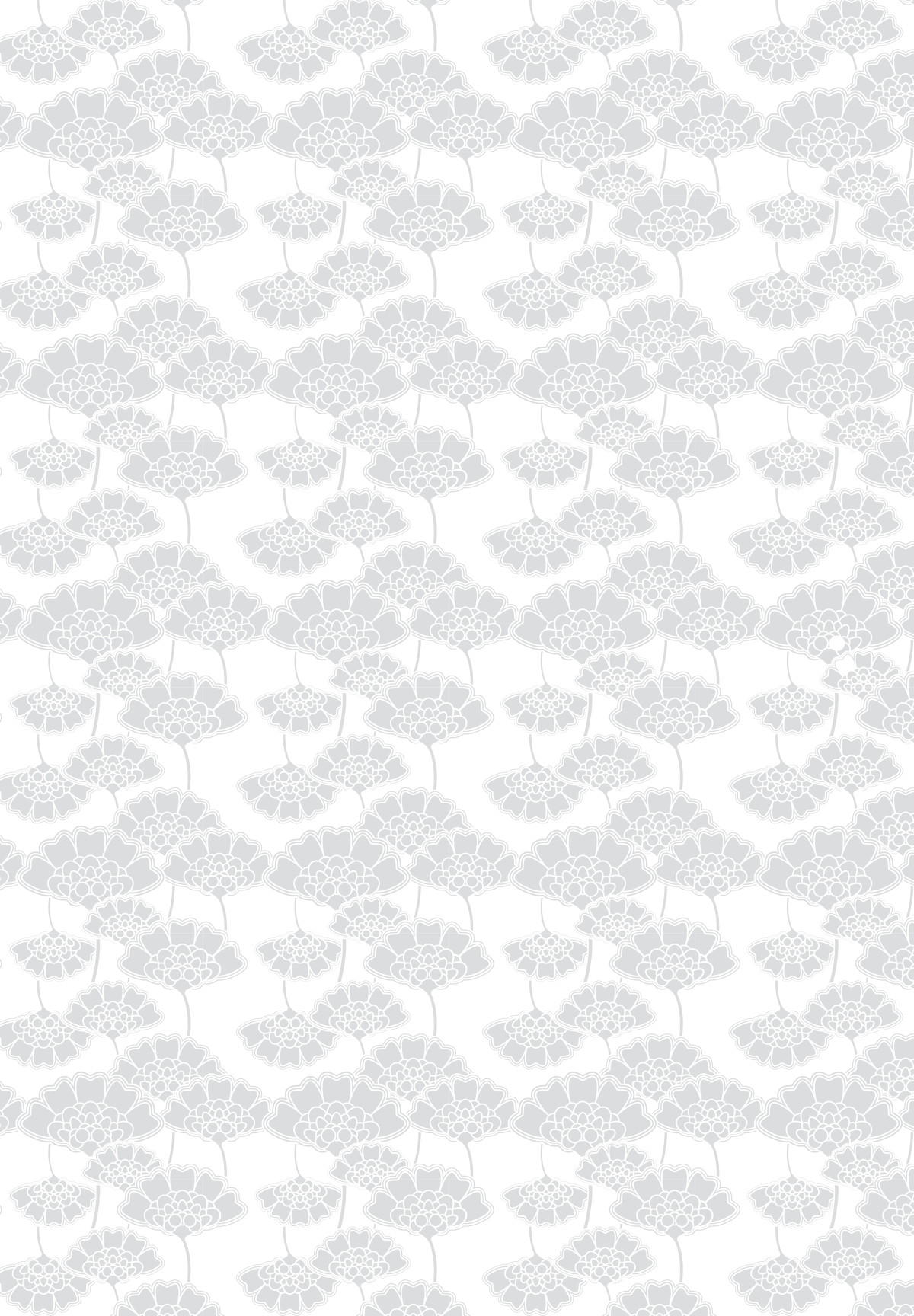
platform, established under the 2015 revised Guidelines for U.S.-Japan Defense Cooperation, aims to respond to the full spectrum of contingencies across the globe in a “seamless, robust, flexible, and effective” manner. As the following essays show, notwithstanding differing approaches to how international law can be used to protect the national security interests of each country, there exist pathways to bridge law and policy to further their common security goals, which should be pursued within the framework of the strengthened ACM.

Nobuhisa Ishizuka

Masahiro Kurosaki

Matthew C. Waxman

June 2020





Use of Force in Self-Defense

PART I



Thomas H. Lee

Fordham University

The
United States
and
Individual
and
Collective
Self-Defense
in
Northeast Asia

Introduction

This essay describes and assesses U.S. positions regarding the international law of individual and collective self-defense with respect to four present-day security imperatives in Northeast Asia:

1. North Korea's possession of nuclear missiles, and the threats they pose to the United States and U.S. allies, namely Japan and South Korea, both of which host significant U.S. bases and troops;
2. Offensive cyber operations against the United States or U.S. nationals in Northeast Asia, by North Korea or China state actors;
3. China, and the threat it poses to Taiwan over which it asserts sovereignty; and
4. Island Disputes:¹
 - Senkaku/Diaoyu islands between Japan and China
 - Dokdo/Takeshima Island between South Korea and Japan

This essay will proceed in two parts. The first part will review the historical background and current status of the international law of grounds for war—*jus ad bellum*. Particular emphasis will be placed on the law of self-defense, both individual and collective. The second part will apply the *jus ad bellum* elaborated in Part One to the four case studies.

Jus Ad Bellum: Self-Defense

Until the twentieth century, there were no multilateral treaties governing *jus ad bellum*, and so customary international law alone regulated the use of armed force. Custom, in turn, was broadly permissive of a sovereign state's right to use armed force in international affairs. In the eighteenth and nineteenth centuries, for example, the state was believed to have the same right to resort to force as

an individual in the state of nature. Henry Wheaton, the first influential U.S. international law writer, put it this way in 1836:

Each State therefore has the right to resort to force as the sole means of reparations for offences caused to it by others, in the same manner as individuals have the right to employ this remedy if they are not subject to the laws of a civil society.”²

Self-defense was one of many legal grounds for war. Instances that might be justified as self-defense today were justified on other legal grounds in the old international legal order. Violation of a treaty was a ground for war. So was another country’s expropriation of the property of a state’s nationals, or failure to pay contract debts owed to its nationals, without any felt necessity to characterize the use of force as self-defense.³ “Humanitarian” military interventions to protect the safety of nationals or third-country nationals such as during the Boxer Uprisings in China at the turn of the twentieth century were also viewed as lawful. Many international lawyers believe the use of force to protect one’s own nationals remains lawful today, but they typically classify it as self-defense, not humanitarian intervention.⁴ This conceptual evolution in characterizing military force to rescue nationals is an example of how dominant self-defense has become as a ground for war in the present day, overshadowing all other grounds.

The unprecedented scale of death and destruction posed by modern warfare culminating in the two world wars produced a fundamental shift in the international legal regulation of warfare. To be sure, the collective movement to mitigate the human costs of modern war had significant antecedents. For instance, the late nineteenth and early twentieth centuries had witnessed several multilateral law-of-war conventions such as the 1864 Geneva Convention for the Wounded and the Sick, and the 1899 and 1907 Hague Conventions restricting various ends and means of warfare on land and at sea. But the years immediately after World War II ended were the critical period: the four current Geneva Conventions regulating *jus in bello*—the law in war—were open for signatures in 1949. With respect to *jus ad bellum*—the law of grounds for war, the United Nations Charter, adopted at the end of World War II in 1945, framed the flagship statement of the new international legal order. It also laid out a collective security mechanism to keep world peace and to organize collective responses to the sorts of aggression that had started the war.

The text of the UN Charter constrains modern *jus ad bellum* to two grounds. First, Article 42 of the Charter authorizes the Security Council to “take such action by air, sea or land forces as may be necessary to maintain or restore international peace and security,” if non-force measures have been exhausted. Second, Article 51 recognizes an “inherent right of individual or collective self-defense.” A third consensus ground for the use of armed force abroad under international law is with

the consent of the territorial state in which the force occurs. We might call this a rule of customary international law or reason that is implicitly allowed by the UN Charter because Article 2(4) prohibits “threat or use of force against the territorial integrity or political independence of any state,” which would not to apply when the state consents.

Indeed, to understand what “self-defense” entails under the UN Charter, we must look first at this prohibition of armed force in Article 2(4), which states in full:

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.

Article 2(4)’s prohibition on “the threat or use of force” targets aggressive or offensive war “against the territorial integrity or political independence” of another state. Thus, as noted above, use of force with consent is allowed. Presumably, a state could also use armed force defensively, for instance, to repulse an invader beyond one’s own borders or in defense of another country that is invaded, or perhaps to protect crucial strategic resources that may fall into the hands of an aggressor. Article 51, in this view, seems unnecessary, an intuition which is confirmed by the way that provision is written:

Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security.⁵

PREEMPTIVE SELF-DEFENSE

The opening phrase—“Nothing in the present Charter shall impair”—indicates that Article 51 is *guidance* for interpreting every UN Charter provision to preserve the sovereign state’s pre-existing “inherent right” of self-defense. It does not purport to define the right of self-defense. It does not necessarily follow as a matter of interpretation that what Article 51 says about this “inherent right”—specifically its condition of “if an armed attack occurs”—is a limit to the customary international law right of self-defense. Put another way, Article 51—the UN Charter’s only reference to self-defense—does not say “each state has an inherent right of individual or collective self-defense if, and only if, an armed attack occurs against a Member.”

Is it possible, then, that an “armed attack” is not necessary for lawful self-defense, even in the post-UN Charter era? The drafters and original ratifiers of the UN Charter, having just lived through World War II, may have thought, for instance, that it would have been lawful if the Allies had attacked Nazi Germany shortly before

its invasion of Poland, given Hitler's prior record of militarization and documented aggressions, most notably his acquisition of Czechoslovakia. Even those who insist that an "armed attack" is a strict requirement of the right to self-defense typically allow some room for anticipatory self-defense in a hypothetical case where there is incontrovertible evidence that a foreign army is about to invade, such as when tanks are moving to the border, attack jets are taking off, or communications relaying an invasion order are intercepted. Nevertheless, some commentators cite Article 51 for the proposition that "an armed attack" is a *necessary* precondition for the exercise of the right to self-defense, just as some presume that Article 51 is an affirmative statement of the self-defense right rather than interpretive guidance regarding a pre-existing customary international law right.

The United States, however, holds the view that the threat of an imminent armed attack can also justify a resort to force in self-defense under international law. That is to say, although Article 51 refers explicitly to self-defense only in response to an actual armed attack, the United States maintains that international law also includes the right to use force when an armed attack is imminent. This view of the United States is widely known and is also shared by many like-minded states in the international community.

My close reading of Articles 2(4) and 51 of the UN Charter is confirmed by historical context. The provisions were drafted after World War II to put an end to aggressive wars of conquest and expansion such as those waged by Nazi Germany and the Japanese Empire. Article 2(4) prohibits wars for territorial or political gain. It would have been counter-productive to have handicapped states facing future aggressors by taking away their right to defend themselves, individually or collectively. That is the point of Article 51.

Of course, Germany and Japan also justified their wars in part under a very capacious sense of self-defense against hostile neighbors and great powers. And so we know for sure that their pretextual, self-serving invocations of self-defense are not part of the "inherent right to self-defense" that Article 51 safeguards. But neither Article 2(4) nor Article 51, nor any other provision of the UN Charter for that matter, gives clear guidance on the contours of the right to self-defense in the hard cases we confront today, such as the scope of the anticipatory self-defense right against a state like North Korea with nuclear weapons and some evidence of hostile intent to use them. And, as I have discussed above, there is a strong argument that Article 51's "armed attack" precondition is not absolute both as a textual matter and as a practical matter.

Because of this lack of guidance in the UN Charter, customary international law remains the primary source regarding the scope of any right of anticipatory self-defense. The key precedent is an 1842 letter by U.S. Secretary of State Daniel Webster to British minister plenipotentiary Lord Ashburton in negotiations resolving armed clashes along the Canada-United States border. In 1837, British

forces landed on the U.S. side of the Niagara River. They chased off the crew of the S.S. *Caroline*, a ship that Canadian rebels and their U.S. sympathizers were using to ferry weapons into Canada, apparently killing one American crewmember in the process. The British then set the ship afire and sent her over Niagara Falls. The rebels and their American sympathizers retaliated and there were a series of reciprocal raids and skirmishes. In his correspondence with Ashburton years later, Webster cast doubt on the British invocation of anticipatory self-defense to justify their destruction of the *Caroline* that had fueled the border clashes:

While it is admitted that exceptions growing out of the great law of self-defense do exist, those exceptions should be confined to cases in which the necessity of that self-defense is instant, overwhelming, and leaving no choice of means, and no moment for deliberation.⁶

Based on this passage, international lawyers have crafted an “imminence” requirement that is meant to capture Webster’s idea that anticipatory self-defense is only lawful when the need to defend oneself is “instant, overwhelming, and leaving no choice of means, and no moment for deliberation.” The standard as applied to individuals would entail a person who sees an opponent pulling out a gun to shoot first in self-defense. As applied to states, however, the standard is much more difficult to articulate and to apply.

Lawyers who cite the *Caroline* incident often neglect to point out two important facts that careful scrutiny illuminates. First, it is doubtful that *Caroline* was actually a case of anticipatory self-defense. The British use of force was not aimed to prevent a specific, imminent armed attack by Canadian rebels. Rather, the British intervened because the *Caroline* was habitually used to support attacks by the rebels, and the United States government had not taken sufficient actions to prevent such use. As such, the *Caroline* case study is more evocative of modern *jus ad bellum* doctrines of use of force in self-defense where a formally neutral sovereign state is “unable or unwilling” to stop aggressive acts against another state that originate or have significant support within its borders.⁷

Second, Webster did not explicitly conclude that the British had failed to meet his test. He did not assert that their armed incursion on U.S. territory and destruction of the *Caroline* could not be justified as a case where the necessity of armed force in self-defense was “instant, overwhelming, and leaving no choice of means, and no moment for deliberation.” Rather, he acknowledged that the incident had happened five years ago and that the British had made assurances that they intended no disrespect to U.S. sovereignty and admitted the violation of U.S. territory. Consequently, Webster concluded that it was better to consider the matter closed without deciding “whether the facts of the *Caroline* make out a case of such necessity for the purpose of self-defence.”⁸ To be sure, a fair inference from

his stringent formulation of the legal test is that the British acts did not suffice to meet it, but he did not say that. The upshot for today is that however demanding the *Caroline* formula may seem, whether it is satisfied will depend on the facts. Without much attention to these historical details, modern international lawyers typically frame the *Caroline* standard as a gloss on UN Charter Article 51. Recall that the provision states that “[n]othing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations.” As previously noted, the conventional view—shared by the United States— is that the “inherent right” of self-defense applies not only if there is an armed attack against a UN Member but also if there is an *imminent threat of such armed attack*.

COLLECTIVE SELF-DEFENSE

Article 51 refers to an “inherent right” not only of “individual” self-defense but also of “collective” self-defense. The concept of “collective” self-defense has pre-UN Charter antecedents in treaties of alliance and reciprocal assistance. But collective self-defense goes further than that. No treaty is required, although sometimes there is a treaty, such as the NATO Treaty or the Japan-U.S. Security Treaty. The basic idea is that if State A is attacked or under imminent threat of armed attack by State C and requests State B’s assistance, State B can use armed force against State C to come to State A’s assistance, even if State B itself has not been attacked by State C.

The basic idea is simple, but there are many complications. First, what if State A has a broader conception of what constitutes an armed attack or an imminent threat of armed attack than State B but nonetheless requests State B’s military assistance? In other words, may State B use force in *collective* self-defense, even if it were to conclude that it could not use force under the same circumstances (i.e., if it were attacked rather than State A) in *individual* self-defense? Or would such a use of force constitute prohibited aggression from State B’s perspective? Drafting a treaty is one way to help address such difficult questions.

Second, collective security might be used as a pretext. Imagine, for example, that State A really wants to use armed force against State C but has no lawful ground for war against it. But State B is either at war with State C or does have a persuasive legal argument for use of force against State C. State A could use force against State C by approaching State B and asking it to request State A’s assistance as collective self-defense, or even by urging State B to resist State C’s aggression, even if it was initially unwilling to do so.

Third, what if we are talking about unit self-defense, not national self-defense? It is not State A itself that is being attacked by State C, but State A’s ship in international waters. If State A requests State B’s military assistance, is it lawful for State B to use force against State C as a matter of “collective self-defense”? Or is collective self-defense only appropriate if the attack on the unit is tantamount

to an attack on the “territorial integrity” or “political independence” of State A as specified in Article 2(4) of the UN Charter? The conventional view today is that unit self-defense is generally sufficient as a ground for war, but the position opens the potential for pretextual uses and abuses. For example, what if State A puts its units in harm’s way, in the hope of triggering a hostile act by State C and enlisting State B’s military intervention?

Northeast Asia Case Studies

Having described the fundamental rules and key issues regarding the international law of self-defense, let us apply them to four Northeast Asia case studies.

ANTICIPATORY SELF-DEFENSE AND NORTH KOREA’S NUCLEAR WEAPONS

The recent commentary on the international law of anticipatory self-defense and North Korea’s development of nuclear weapons and ballistic missiles has focused on two related factual scenarios. First, would it be lawful for the United States to launch a limited military strike on suspected North Korean nuclear weapons facilities and missile launch sites based on the current state of play in terms of North Korea’s technological capacity and expressions of hostile intent to launch nuclear weapons at U.S. territory? Second, would it be lawful for the United States to launch such a limited military strike as a matter of collective self-defense in response to the North Korean launch of an unarmed missile that splashes down in Japanese waters or in international waters after overflight of Japanese territory and, if so, would Japanese consent be necessary to make it lawful under the U.S.-Japan Security Treaty of 1960? This second issue has been the subject of recent commentary by Professors Hitoshi Nasu and Masahiro Kurosaki, and so I will not address it here.

In terms of the case for the international legality of a U.S. military strike based solely on the threat posed to the United States, we begin by recalling the *Caroline* test (with my caveat articulated above that it originated as an “unable or unwilling” standard, illustrative of the nexus between that standard and anticipatory self-defense). Given the North Korean nuclear missile program’s current status, is the “necessity” of a U.S. military strike “instant, overwhelming, and leaving no choice of means, and no moment for deliberation”?

The single most compelling factor for imminence is the special nature of nuclear ballistic missiles. They can impact within hours and deliver a devastating toll in terms of death and destruction, far beyond the capacity of conventional weapons. As an originalist matter, the drafting history of the UN Charter indicates that it was not drawn up with nuclear weapons in mind, despite (or perhaps because of) the fact that the United States was the only country to possess and to

have used them. Moreover, although it is not public knowledge, it is likely that both the United States and the Soviet Union (now Russia) had for many years classified contingency planning for the preemptive use of nuclear missiles. Presumably, at least for the United States, this included a legal opinion that first use was consistent with relevant international law.

In the wake of 9/11, the George W. Bush administration asserted in its 2002 National Security Strategy Statement that the United States “must adapt the concept of imminent threat to the capabilities and objectives of today’s adversaries.”⁹ The Statement continued that “[t]he greater the threat, the greater is the risk of inaction—and the more compelling the case for taking anticipatory action to defend ourselves, even if uncertainty remains as to the time and place of the enemy’s attack.”¹⁰ The Statement was addressed most directly to the threat of international terrorism and Saddam Hussein’s alleged possession of chemical weapons. At the time, the North Korean long-range missile program was still in an embryonic state; specifically, there were no indications that North Korea had long-range ballistic missiles capable of reaching U.S. territory. North Korean nuclear missiles that can reach the United States seem to present a far greater and direct risk to U.S. national security than al Qaida or Saddam Hussein with chemical weapons.

There are also precedents directly on point that indicate special latitude in assessing imminence when the threat to be balanced is nuclear missiles capable of reaching U.S. territory. In 1962, the United States instituted a “defensive quarantine” by positioning U.S. naval warships to intercept the shipment of nuclear missile parts to Cuba. The United States, at the urging of State Department Legal Adviser Abram Chayes, did not use the word “blockade” to avoid characterization of its actions as a use of force, but it was a distinction without a real difference. Moreover, President John F. Kennedy and his Cabinet strongly considered a “surgical” air strike to take out suspected missile facilities in Cuba. They ultimately ruled out the option primarily on policy grounds, not mainly because of concerns about its international legality. In 1981, Israel launched an air strike on an Iraqi nuclear reactor at Osirak. It alleged that the reactor was producing weapons-grade material for the manufacture of nuclear weapons and expressed a belief that Israel would be a likely future target. As in the case of Cuba, the international community did not reject the claim to a right of anticipatory self-defense out of hand, but rather disputed that the imminence threshold was met on the facts of the case. And, more recently, the Bush administration seriously considered an anticipatory self-defense rationale as its principal ground for the Second Iraq War. The British ultimately persuaded the United States that an argument based on enforcement of pre-existing UN Security Council resolutions provided a sounder international legal basis.

On the other hand, application of the *Caroline* test to the specific facts of the North Korean case today points strongly in the direction of illegality. The North Korean rhetoric about using its nuclear missiles against the United States has been

strident. However, the North Koreans have not taken any direct hostile action against U.S. military forces for four decades. This is particularly significant because the North Koreans have engaged South Korean military forces on numerous occasions during that time, including pitched naval battles in 1999 and 2002, and the sinking of the South Korean corvette *Cheonan* in 2010, with the loss of 46 sailors. North Korea had also forcefully abducted Japanese nationals on multiple occasions in the 1970s and 1980s.

With respect to “choice of means” and the possibility of deliberation, the present North Korean overtures indicate at the very least that diplomacy and a negotiated peace are still available alternative options. Three summit conferences between U.S. President Donald Trump and North Korean leader Kim Jong-un may have yielded no negotiated settlement, but the North Koreans did pause long-range ballistic missile tests for two years. And even the most recent announcements by Kim have left open the possibility of future negotiations. Moreover, according to press reports, North Korea does not have the technology at the present time to mount a nuclear warhead on a long-range ballistic missile and manage successful reentry of the warhead. The lack of current capacity militates against the “instant necessity” for action the *Caroline* test calls for.

Finally, it seems worth considering, as part of the necessary deliberation, the policy prudence and the precedent that would be established. No nuclear state has actually used anticipatory self-defense as a basis for attacking another nuclear state. To be the first to do so seems particularly risky at a time where U.S. power is declining, and other nuclear powers, most notably China, are on the rise.

In sum, the case for an international legal basis for a limited U.S. military strike on North Korea is stronger than some commentators acknowledge given North Korea’s possession of nuclear weapons, development of long-range ballistic missiles, and hostile relations between the two countries. Those who hold the view that such a strike would be illegal emphasize the phrase “if an armed attack occurs” in Article 51 and tend to construe any anticipatory right of self-defense narrowly. In so doing, however, they gloss over gaps in the Charter’s coverage and downplay the importance of customary international law in giving content to the modern *jus ad bellum*, and the potential scope of the anticipatory self-defense ground as against nuclear missiles. But, at the same time, whether premised on possession with hostile intent, or the incidence of unarmed missiles splashing down in Japanese waters or overflight of Japanese territory, the legal case at present is weaker than proponents of military strikes have asserted.¹¹ Diplomacy seems a viable option; and North Korea, for all its rhetoric, has not used armed force against the United States for a very long time, despite its willingness to use force against South Korea in recent decades. Perhaps most important, there is no clear evidence that North Korea has yet achieved the necessary technology to launch a nuclear ballistic missile successfully at the territory of the United States.

USE OF FORCE AS A RESPONSE AGAINST OFFENSIVE CYBER OPERATIONS

The application of the law of war to cyber operations is in great flux at the present time. But the United States and most countries accept that international law applies to cyberspace and there is agreement on some principles. First, cyber operations that cause physical damage that would be considered a use of force if caused solely by traditional means would constitute a use of force prohibited by Article 2(4) of the UN Charter. Second, cyber operations that coercively intervene in the core functions of another state, such as its ability to hold an election—are also prohibited. But beyond that, there seems to be no broad consensus about the relevant rules; for example, there is no consensus on the scope of the non-intervention principle.

Press reports indicate that China and North Korea are two countries with significant offensive cyber capabilities. What would the United States do if one or the other country were to engage in cyber operations that amounted to a use of force, which the United States views as equivalent to an Article 51 “armed attack”, thus triggering the U.S. right of self-defense? In large part, the analysis would track the analytical framework described above with respect to kinetic armed attacks. That assumes, however, that such an attack could be attributed to China or North Korea, which may be difficult in practice. Attribution thus adds an additional wrinkle into the international legal analysis when we are dealing with cyberspace.

Moreover, many current offensive cyber operations typically “hop” between networks and servers in many different countries, making attribution even more difficult. If the United States is the target, press reports indicate that it would be more than likely that at least one “hop” will occur within the United States, implicating U.S. domestic laws like the Foreign Intelligence Surveillance Act that may be more stringent and specific than any applicable international law. Most of the debate in cyber law, however, involves cyber operations that do not rise to the level of a use of force or interference in sovereign functions: what are the international law rules governing these operations? Press reports indicate that the United States has increased its operational tempo in this space, seeking to “defend forward.” It may, accordingly, announce rules to govern this area in the near future.

CHINA AND TAIWAN

The United States has not committed to collective self-defense of Taiwan, although there is some ambiguity on the point. First, the United States has acknowledged the Chinese position that there is only one China and that Taiwan is a part of China. The United States has not actually endorsed the specific proposition that Taiwan is part of China; rather, it has merely confirmed that view as the Chinese position on Taiwan—an artful dodge, but a dodge nonetheless. The United States has also recognized the People’s Republic of China as the only legitimate government of China. At the same time, the United States continues to sell weapons to Taiwan,

despite Chinese protest, which would likely be a violation of international law if Taiwan were actually a part of China. It has also announced its opposition to any non-peaceful unification of Taiwan and the mainland. Moreover, the Taiwan Relations Act of 1979 provides that the United States will consider:

any effort to determine the future of Taiwan by other than peaceful means, including by boycotts or embargoes, a threat to the peace and security of the Western Pacific area and of grave concern to the United States¹²

But that statute is now forty years old, and the United States has not made any similar statements recently. Additionally, the United States has been careful about engaging in military exercises or any active, obvious form of military cooperation with Taiwan that China might perceive as an imminent threat of armed attack.

What would the United States do if China invaded Taiwan or gave clear, incontrovertible evidence of an imminent attack? Are there any international law arguments for the use of force in self-defense, particularly at Taiwan's request? This is not an inconceivable scenario if local elections in Taiwan bring a regime to power that pursues a separatist policy.

First, the United States may send military forces if needed to evacuate U.S. nationals, thousands of whom may be on the island. Although such operations used to be deemed humanitarian intervention, they are now commonly justified as self-defense.

How about the harder question: would the United States invoke collective self-defense if Taiwan requested military assistance in response to a Chinese armed attack? A definitive answer seems impossible to give at the present time. On the one hand, Article 51 of the UN Charter refers to an "armed attack" against "a member of the United Nations," which Taiwan is not. Moreover, U.S. endorsement of the "one China" position coupled with recognition of the PRC as the legitimate government of China combine to suggest that Taiwan cannot claim to be a sovereign state that could make a request for collective self-defense assistance from the United States or qualify to give consent to the use of force under international law. At the same time, Taiwan is a vibrant democracy and by all functional indicators, it is a fully independent sovereign state with exclusive political control over its territory for over seventy years. Consequently, to the extent that consent and the right to collective self-defense are grounded in customary international law and not limited to the strict language of UN Charter Article 51, Taiwan could very reasonably seek to invoke one or the other as grounds, even if it is not formally a member of the United Nations.

In summary, in terms of legal analysis, there may be enough to argue for legality of U.S. military intervention in collective self-defense of Taiwan under customary international law, even though Taiwan is not a "member of the United

Nations” as the UN charter specifies. This does not mean, of course, that the United States would do so, given the current political circumstances.

ISLAND DISPUTES

The two island disputes in Northeast Asia that would seem to present the greatest risk of hostilities are the disputes between South Korea and Japan over Dokdo/Takeshima Island and between China and Japan regarding the Senkaku/Diaoyu islands. South Korea currently exerts administrative control over Dokdo, although Japan asserts “shadow” jurisdiction with an administrative apparatus purporting to extend to the island. Japan currently has administrative control over the Senkaku Islands, although China similarly asserts shadow jurisdiction.

What would the United States do in the event of an armed attack on either of the islands? Both cases would implicate U.S. alliance treaty obligations. Article III of the Mutual Defense Treaty Between the United States and the Republic of Korea¹³ provides that:

Each Party recognizes that an armed attack in the Pacific area on either of the Parties in territories now under their respective administrative control, or hereafter recognized by one of the Parties as lawfully brought under the administrative control of the other, would be dangerous to its own peace and safety and declares that it would act to meet the common danger in accordance with its constitutional processes.

And Article V of the Japan-U.S. Security Treaty provides that:

Each Party recognizes that an armed attack against either Party in the territories under the administration of Japan would be dangerous to its own peace and safety and declares that it would act to meet the common danger in accordance with its constitutional provisions and processes.¹⁴

In the event of a Chinese attack on the Senkaku Islands, Article V of the Japan-U.S. Treaty would seem to apply, since Japan has administrative control. At the same time, the treaty obligation is to “act to meet the common danger in accordance with its constitutional provisions and processes.” Self-defense is not explicitly mentioned, even though it is mentioned in Article V of the NATO Treaty of 1949 which provides that:

The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defense recognized by Article 51 of the Charter of the United Nations, will assist the Party or

Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.¹⁵

The natural conclusion is that if China were to attack the Senkaku Islands, the United States could invoke collective self-defense to use military force to aid Japan in repelling the attack, so long as the use of force was taken “in accordance with” U.S. domestic “constitutional processes.” Article XI of the NATO Treaty provides that the Treaty “shall be ratified and its provisions carried out by the Parties in accordance with their respective constitutional processes.” Consequently, the NATO Treaty also provides that any acts taken in collective self-defense must be consistent with U.S. constitutional processes, and so it appears that the legal analysis would be identical to that under the Japan-U.S. Security Treaty, despite the difference in language between the two treaties.

In the event of a Japanese attack on Dokdo, Article V of the U.S.-ROK Security Treaty would seem to apply, but there are three additional wrinkles not present in the Senkaku Islands scenario. First, that provision refers to territory “lawfully brought under the administrative control of the other.” Accordingly, if the United States were to determine that South Korea did not “lawfully” bring Dokdo under its administrative control, then Article V would not apply. Second, the U.S. promise is to “act to meet the *common danger* in accordance with its constitutional processes.” It is not clear that Japan would pose a “common danger” for the United States since it is also an ally, in contrast to China vis-à-vis the Senkaku Islands. Third, although both U.S. security treaties with Japan and Korea (and the NATO Treaty) authorize use of force in collective self-defense consistent with domestic “constitutional processes,” the operation of the common provision is complicated in the event that South Korea would seek U.S. military assistance as against a Japanese attack on Dokdo. It seems reasonable to presume that U.S. “constitutional processes” would include compliance with the Japan-U.S. Security Treaty because it is a constitutionally ratified treaty of the United States. Although there is no specific provision in that Treaty that explicitly prohibits the United States from attacking Japanese forces in the exercise of collective self-defense authorized by another treaty, it would seem contrary to the object and purpose of the U.S. Japan Treaty. Hence, it is almost certain that the United States would not intervene in a military conflict between Japan and South Korea over Dokdo/Takeshima.

Conclusion

This Essay has sought to provide a summary overview of the diverse issues implicating the international law of self-defense facing the United States in Northeast Asia at the present time. I hope that it provides insight to public international lawyers and policymakers in dealing with these challenges. ■

Thomas H. Lee is the Leitner Family Professor of International Law at Fordham University School of Law. From May 2019 to August 2020, he served as Special Counsel to the General Counsel of the U.S. Department of Defense. The views expressed in this Essay are the author's own and do not reflect the views of the Department of Defense or the U.S. Government.

Professor Lee has also been a Visiting Professor at Columbia Law School (2017–18, 2005–6), Harvard Law School (2012–13), and the University of Virginia School of Law (2007). Before joining Fordham in 2002, Professor Lee clerked for Judge Michael Boudin of the U.S. Court of Appeals for the First Circuit and for Justice David Souter of the U.S. Supreme Court. From 1991 to 1995, he served as a U.S. naval signals intelligence officer deployed at sea in the Western Pacific and Indian Oceans and ashore in Korea and Japan and with the National Security Agency. He received his A.B. (*summa cum laude*), A.M. (Regional Studies—East Asia) and J.D. from Harvard University.

- 1** I will not discuss the Japan-Russia dispute over the southern Kurile Islands, currently in Russian possession ever since they were invaded near the end of World War II. As recent visits of Japanese tourists to the islands illustrate, the Japanese and Russian governments have engaged in diplomacy over the dispute and there appears to be no prospect of a use of force at the present time.
- 2** Henry Wheaton, *Elements of International Law* 274 (Philadelphia, Carey, Lea & Blanchard 1836).
- 3** See Thomas H. Lee, *The Law of War and the Responsibility to Protect Civilians: A Reinterpretation*, 55 *Harv. Int'l L. J.* 251, 266–69 (2014).
- 4** See *id.* at 265–76.
- 5** Article 51 continues: “Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.” U.N. Charter art. 51.
- 6** Letter from Daniel Webster, Sec’y of State, United States, to Lord Ashburton, British Plenipotentiary, United Kingdom (Aug. 6, 1842) in 2 *A Digest of International Law* 412 (John Bassett Moore ed., 1906).
- 7** See Craig Forcece, *Destroying the Caroline: The Frontier Raid that Reshaped the Right to War* (2018).
- 8** *Id.*
- 9** The White House, *The National Security Strategy of the United States of America* (2002), <https://2009-2017.state.gov/documents/organization/63562.pdf>.
- 10** *Id.*
- 11** John Bolton, *The Legal Case for Striking North Korea First*, *Wall St. Journal* (Feb. 28, 2018).
- 12** Taiwan Relations Act, Pub. L. No. 96-8, 93 Stat. 14 (codified at 22 U.S.C. §§ 3301 et seq. (1979)).
- 13** Mutual Defense Treaty Between the United States and the Republic of Korea, S. Kor.-U.S., Oct. 1, 1953, 5 U.S.T. 2368, 256 U.N.T.S. 199 (entered into force Nov. 17, 1954).
- 14** Treaty of Mutual Cooperation and Security between the United States and Japan, Jan 19, 1960, 11 U.S.T. 1632 (entered into force May 19, 1960).
- 15** North Atlantic Treaty, art. 9, Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243.



Masahiro Kurosaki

National Defense
Academy of Japan

Legal Framework of Japan's Self-Defense with the United States

Introduction

The year 2014 was a dramatic turning point in Japanese security policy with the United States. In April, President Barack Obama officially reaffirmed that the United States would maintain its longstanding commitment to defend Japan under the U.S.-Japan Security Treaty, and that such commitment covers the Senkaku Islands.¹ Three months later, the Japanese government led by Prime Minister Shinzo Abe unprecedentedly adopted a cabinet decision to enable Japan to exercise the right of collective self-defense to “strengthen mutual cooperation with the United States.”² In 2015, the revision of the Guidelines for U.S.-Japan Defense Cooperation³ and the adoption of Japan’s new security legislation, which entered into force on March 29, 2016, enabled a more effective and robust implementation of this decision.

All of these actions represent Japan’s strong determination to seek a more equal alliance with the United States and to bring an end to the past unilateral and imbalanced nature of the alliance, under which Japan had merely granted the United States the right to station its troops in Japan in return for its security commitments. However, Japan’s use of force in self-defense is still restrained to a large extent by complicated constraints at both domestic and international legal levels, which could cause serious gaps of perception and understanding between the two countries. It would be preferable for the U.S. government officials to bear in mind these potential gaps to better plan and implement future U.S.-Japan joint operations.

In light of the foregoing circumstance, this paper aims to offer an overview of applicable constraints on Japan’s self-defense under international law and Japanese law. It also sheds light on the question of when, to what extent, and how Japan has become allowed to use force to defend the United States at a legal level in the face of diversifying security threats and a shifting world order. Although Japan also has various options to protect the United States with forcible measures other than the use of force,⁴ this paper confines itself to the issue of Japan’s use of force within the context of international law centered on Article 2(4) of the U.N. Charter.

Self-Defense as a Notion of International Law and the Constitutional Approach

Although the U.N. Charter permits the use of force by its member states when authorized by the Security Council under Chapter VII, the Japanese Constitution limits Japan's use of force to the case of self-defense against armed attack. However, there is no mention of the term "self-defense" in the Constitution, which suggests that the established notion of national self-defense in Japanese law is not independent of that in international law. In the government's view, there is no significant difference in nature between these two distinct bodies of law.⁵ The Constitution's approach to national self-defense acts as a domestic constraint on Japan's exercise of "the inherent right of individual or collective self-defense" as provided in Article 51 of the U.N. Charter.⁶ Therefore, individual and collective self-defense are defined as follows:

It is generally understood that, under international law, "the right to individual self-defense" is the right of a State to repel armed attack against it by using force. "The right to collective self-defense," on the other hand, is the right of a State to repel armed attack against its closely associated foreign State by using force, notwithstanding it is not being attacked directly.

Thus, it is the government's view that both rights should be sharply distinguished by whether or not the purpose is to respond to the attack directed against itself.⁷

When applied to the context of the defense of the United States, the relevant framework of Japan's individual and collective self-defense can be divided into two categories: one is defense within Japanese territory, and the other is defense outside Japanese territory.

The Individual Self-defense Framework: Defending the United States within Japanese Territory

ATTACK ON U.S. ARMED FORCES STATIONED IN JAPAN

As of March 31, 2019, there are 78 U.S. military facilities and sites in Japan.⁸ The use of those facilities and sites by the United States is based on the 1960 Japan-U.S. Security Treaty and Status of Forces Agreement.⁹ Yet, this does not change the fact that they are located within Japanese sovereign territory. As long as they are stationed in Japan, any attack on those areas by a foreign state could be considered as an armed attack on Japanese territory, triggering Japan's right of individual self-defense.¹⁰

JOINT DEFENSE MECHANISM UNDER THE 1960 JAPAN-U.S. SECURITY TREATY

U.S. Armed Forces in Japan rely for their protection not only on concepts of Japan's individual self-defense, but also on the concept of U.S. collective self-defense of "the territories under the administration of Japan," in accordance with Article V of the Japan-U.S. Security Treaty. Yet, the question is what requirements need to be met for the exercise of the right of collective self-defense. The two countries' views are split over whether a declaration of an armed attack and request for assistance by an attacked state are necessary preconditions for an assisting state to exercise a right of collective self-defense. The International Court of Justice (ICJ) in the *Nicaragua* case found that "there is no rule in customary international law permitting another state to exercise the right of collective self-defense on the basis of its own assessment of the situation."¹¹ While Japan has shown a high deference to the ICJ's conclusion and supports its opinion,¹² the United States strongly challenges it.¹³

However, Japan's consistent position has been that the Japan-U.S. Security Treaty only authorizes the United States to use force in collective self-defense when Japan exercises its right of individual self-defense. This is not inconsistent with the customary international law requirements that a victim state first declares an armed attack and requests assistance.¹⁴ Thus, even when protecting U.S. Armed Forces in Japanese territory, Japan must determine the occurrence of an armed attack and issue a request for assistance to the United States through the treaty-based consultation mechanism¹⁵ before the United States may engage in collective self-defense of Japan. Admittedly, there remains the possibility that the United States may alternatively invoke its inherent right of individual self-defense solely to protect its forces in Japan, claiming that it is outside the regulatory scope of the treaty.¹⁶ But the Japanese government would insist on the joint and coordinated determination of armed attack in consultation with one another under Article V of the treaty insofar as they are stationed in Japanese territory. This is why the United States needs to know how Japan interprets the notion of armed attack.

JAPAN'S UNDERSTANDING OF ARMED ATTACK

Importance of an Opponent's Intent

Article 51 of the U.N. Charter stipulates an "armed attack" as the precondition for any state to exercise its right of individual or collective self-defense. The Japanese government has consistently defined an "armed attack" in this context as meaning "an organized, planned use of force against a state."¹⁷ As the term "planned" suggests, it views the hostile intent of an opponent as the most crucial element in determining the occurrence of an armed attack, not the criteria of "scale and effects" applied by the ICJ in its *Nicaragua* decision¹⁸ (however, scale and effects may serve as evidence of intent as was implied by its 2003 *Oil Platform* decision—"specific intention of harm" may be found depending on the gravity of the use of force¹⁹). This view stems from Japan's strict defense-only constitutional policy that it shall not use force for an aggressive

purpose.²⁰ It is unclear whether hostile intent is required for the determination of an armed attack in a strict legal sense, but the government has always referred to the opponent's subjective intent as the key factor in the determination. Such intent is to be evaluated based on "comprehensive assessment of international situation, demonstrated intent of the state using force, and the means and patterns of attack."²¹

Rejection of an Imminent Threat of Armed Attack

In Japan's view, actual harm is not necessary for armed attack to occur as the concept also includes its initiation phase. For example, there is no need to wait until the attack hits the target when a ballistic missile directed at Japan is being fueled.

However, the initiation of armed attack must be distinguished from an imminent threat of armed attack, a notion of anticipatory self-defense which the Japanese government has consistently rejected. In the government's longstanding interpretation of the U.N. Charter, "the mere likelihood or threat of armed attack does not authorize the exercise of the right to self-defense. In other words, neither preemptive strikes nor preventive acts of war are permissible."²² Hence, Japan is unlikely to respond with the use of force until it determines that an armed attack has been, in fact, initiated.

Armed Attack by Non-State Actors

The Japanese government recognizes that acts of violence by non-state actors outside Japan could constitute armed attack,²³ while the ICJ currently appears to be cautious about this concept. The issue arises when Japan is confronted with protecting its citizens abroad in rescue operations, as illustrated by the Israeli "Operation Entebbe" in Uganda in 1976 and the U.S. "Operation Eagle Claw" in the Iran hostage crisis in 1980. The government first seemed to hold a negative opinion on whether any act of violence by a non-state actor against Japanese citizens abroad could constitute an armed attack on Japan.²⁴ However, since the 9/11 attacks, it has maintained that an armed attack on a state may also be conducted by non-state actors, at least "a quasi-state organization." It defines the term as "although not a state *per se*, those who, as an equivalent thereof, may qualify as a party to an international dispute,"²⁵ citing as examples the Taliban²⁶ and the remnants of Saddam Hussein's regime aiming at its resurgence.²⁷ Such cases could partially satisfy statehood requirements—a defined territory; a permanent population; and a government.²⁸

The Collective Self-defense Framework: Defending the United States Outside Japanese Territory

INTERNATIONAL LEGAL CONSTRAINTS

When an armed attack occurs against the United States *outside* Japanese territory, the collective self-defense framework comes into play in Japan's use of force. In contrast to the duty of the United States to defend Japan under the bilateral treaty, currently Japan has no comparable treaty obligation to defend the United States by using force. Yet, it has the inherent right to do so within applicable legal constraints.

As already discussed, the Japanese government supports the ICJ's *Nicaragua* decision, finding that the declaration of an armed attack and request for assistance by an attacked state are necessary preconditions for Japan to engage in collective self-defense. However, even if Japan has met these international legal constraints, domestic legal requirements further constrain its ability to engage in collective self-defense operations, which limits its exercise of international legal rights.

CONSTITUTIONAL CONSTRAINTS

Japan's Approach to Collective Self-Defense: An Expanded Version of Individual Self-Defense?

The Japanese Constitution had formerly been understood as prohibiting under all circumstances the exercise of the international legal right of collective self-defense. The government's view had long been that the war-renouncing clause (Article 9) of the Constitution²⁹ permitted only the use of "minimum necessary force" in self-defense of Japan for the protection of its nationals' "right to life, liberty, and the pursuit of happiness" (Article 13). Hence, the right of collective self-defense of other states, although granted under Article 51 of the U.N. Charter, would be considered as exceeding this constitutional limitation.³⁰

The constitutional ban on collective self-defense was lifted by a Cabinet decision in 2014,³¹ which led to a dramatic and groundbreaking shift in Japan's official position. It was made possible not by revising the Constitution, but by reinterpreting the "minimum necessary force" principle under Article 9, leaving the sanctified war renunciation language untouched. However, even the 2014 Cabinet decision has not changed "the basic logic of the interpretation of Article 9 of the Constitution" since its first formulation in 1972, because "[i]n certain situations, the aforementioned "use of force" permitted under the Constitution is, under international law, based on

*the right of collective self-defense.*³² Due to the retention of the “minimum necessary force” principle, Japan’s collective self-defense of other states must be strictly associated with the defense of Japan and the protection of its citizens’ “right to life, liberty, and the pursuit of happiness.”³³

In this sense, Japan’s doctrine of collective self-defense does not permit the pure defense of another state. It reflects Japan’s firm belief that defending the United States and other partner states must be closely related to the survival of Japan and its people in a significant changing security environment at both regional and global levels. This idea underlies the following three constitutional requirements for the exercise of collective self-defense.

Existential Crisis Situation (Survival-Threatening Situation)

First, to qualify for collective self-defense, a situation must pose an existential crisis to Japan. Article 2 of the Armed Attack and Existential Crisis Situations Law, modified in 2015, defines the standard as “an armed attack against a foreign state that is in a close relationship with Japan occurs, and, as a result, threatens Japan’s survival and poses a clear danger to fundamentally overturn its nationals’ right to life, liberty, and pursuit of happiness.” The foreign state, including one having no diplomatic relations with Japan,³⁴ is expected to be “a country which shares a common interest in responding to an armed attack from outside as a common danger and expresses the intention to do so jointly with Japan.”³⁵ This requirement is intended to ensure consistency with the “basic logic of the interpretation of Article 9”—i.e., that Japan’s use of force is constitutional solely when it is exercised for the purpose of protecting its citizens’ right to live in peace.

The Japanese government further explains that an existential crisis could include “a situation in which a clear danger of the occurrence of an armed attack [on Japan] is imminent” or “the tense situation in which an armed attack [on Japan] is anticipated.”³⁶ Examples include armed attack against U.S. vessels transporting Japanese nationals³⁷; armed attack against U.S. warships conducting ballistic missile surveillance in the vicinity of Japan³⁸; or armed attack against Guam,³⁹ where the U.S. military bases critical for Japan’s security in East Asia are located. The legislation also allows for exceptional cases in which an attack is neither imminent nor anticipated but could still constitute an existential crisis.⁴⁰ A blockade of the Strait of Hormuz, a critical energy lifeline to Japan, was one cited example.⁴¹

Furthermore, the Japanese government has expressed its view on cyber armed attacks.⁴² It has made clear that not only “a cyberattack carried out as part of an armed attack,”⁴³ but even a “cyber-only attack”⁴⁴ could constitute an armed attack and trigger an existential crisis within the meaning of the doctrine.⁴⁵

Whether an existential crisis exists shall be determined “in an objective and reasonable manner”⁴⁶ based on a comprehensive assessment of all information available to the Japanese Cabinet (a decision which will be subject to prior or subsequent approval of the legislature, depending on the circumstances).⁴⁷ Such a complicated and multi-layered approach to a situational determination would require institutionalized facilitating procedures between an assisting state and an attacked state. To enable Japan to practically engage in collective self-defense with the United States, the two countries have established a joint defense mechanism called the “Alliance Coordination Mechanism” (ACM)⁴⁸ based on the Japan-U.S. Guidelines. As this suggests, Japan’s collective self-defense is tailored and limited to the defense of the United States, Japan’s only ally. It is worth noting that this would not include a request to assist in anticipatory self-defense against an imminent threat of armed attack; as already discussed, Japan has rejected that doctrine as a matter of international law.

Necessity to Ensure Japan’s Survival and Protect its People

Even if an existential crisis exists, a second condition must be met: there must be no other appropriate means available to repel the armed attack on Japan’s ally, to ensure Japan’s survival, and/or to protect the Japanese people. This condition is less controversial than other requirements and has not been a source of substantive debate. But it should be distinguished from the necessity requirement under international law that non-use of force be insufficient—it does not go so far as to require that force be the only available response to an armed attack. Under Japan’s constitutional constraints, satisfaction of this element of the doctrine must be judged from the viewpoint of whether the use of force is required to ensure Japan’s survival and protect its people.

Minimum Necessary Force and Geographical Limitations

Third, Japan is constitutionally authorized to use force only to the minimum extent necessary to achieve the foregoing purpose.⁴⁹ This condition concerns the “means, forms and degree” of Japan’s self-defense under the Constitution and must be assessed together with the two other constitutional requirements. It is entirely distinct from “the proportionality requirement for the exercise of the right of self-defense under international law that permits a self-defense operation comparable in degree to an ongoing armed attack from an opponent.”⁵⁰ Therefore, geographical limitations on overseas deployment of Japan’s Self-Defense Force (SDF) are particularly relevant in determining whether this condition is satisfied.

The government’s position has been that Japan’s use of force in any territory of another state exceeds the minimum-force restriction, even if such

state consents. It has emphasized that this stance will continue to apply to the new policy on collective self-defense.⁵¹

Nevertheless, the government has suggested two possible exceptions to this limitation. The first one is minesweeping in the Strait of Hormuz. Such an operation could be conducted in the sovereign territory of Oman or Iran,⁵² but it would fall within the constitutionally permissible scope of minimum necessary force because it secures safe navigation for vessels.⁵³ In addition, a surgical missile strike on an enemy base overseas could be lawful if the alternative would be “boots on the ground.” However, the government emphasizes that this latter exception is theoretical, because Japan lacks the capabilities, such as suppression of enemy air defenses and long-range missile systems, to carry out such an attack.⁵⁴ Thus, minesweeping by Japan’s SDF in the Strait of Hormuz is “the only exception”⁵⁵ in practice.

It should be noted that the third requirement does not limit Japan’s use of force in collective self-defense in areas with no sovereign control, because of its link to the territorial sovereignty of other states. Therefore, the primary operating domains of Japan’s collective self-defense of the United States could be on the high seas and, depending on future circumstances, in cyberspace and in outer space.⁵⁶

Conclusion

Japan has the inherent right to use force in individual or collective self-defense under international law. While Japan’s individual self-defense covers the U.S. Armed Forces and their military bases stationed in Japanese territory, its exercise of collective self-defense also plays a significant role in the defense of the United States outside its territory. To make these frameworks operational, Japan and the United States have established a close bilateral coordination mechanism to enable both countries to jointly exercise its rights of self-defense in a feasible way. Given the background of lifting the ban on Japan’s ability to exercise collective self-defense, the current framework is uniquely tailored to the joint defense of the United States.

That said, the United States needs to understand that there exists a significant potential gap between the two countries in their legal approaches to the exercise of self-defense. This is most evident in the interpretations of armed attack and the requirements for the exercise of the right of collective self-defense under international law. Furthermore, Japanese constitutional constraints limit and complicate Japan’s engagement in collective self-defense with the United States. A more workable and legally consistent basis for the Japan-U.S. alliance requires constant legal dialogue between Japanese and

U.S. government officials. Such dialogue should aim at narrowing or closing the potential gaps in the relevant legal interpretations applied to various specific circumstances. ■

Masahiro Kurosaki is an Associate Professor of International Law and the Director of the Study of Law, Security and Military Operations at the National Defense Academy of Japan's Ministry of Defense. In this capacity, he has also been active as a legal adviser to the Ministry of Foreign Affairs of Japan sometimes representing the Japanese government in diplomatic negotiations on international human rights and humanitarian law. He has published a range of articles and book chapters on the law of international security, the law of armed conflict, international criminal law, and Japanese security laws, which include: "Toward the Special Computer Law of Targeting: 'Fully Autonomous' Weapons Systems and the Proportionality Test," in Claus Kress and Robert Lawless (eds.), *Necessity and Proportionality in International Peace and Security Law* (Oxford University Press, 2020 forthcoming). "The 'Bloody Nose' Strategy, Self-Defense and International Law: A View from Japan," *Lawfare*, February 15, 2018; "The Fight against Impunity for Core International Crimes: Reflections on the Contribution of Networked Experts to a Regime of Aggravated State Responsibility," Holly Cullen, Joanna Harrington, and Catherin Renshaw (eds.), *Experts, Networks and International Law* (Cambridge University Press, 2017). The opinions expressed here are solely those of the author and do not necessarily represent the position of the Japanese government or the Ministry of Defense of Japan.

- 1 The White House, Joint Press Conference with President Obama and Prime Minister Abe of Japan (2014), <https://obamawhitehouse.archives.gov/the-press-office/2014/04/24/joint-press-conference-president-obama-and-prime-minister-abe-japan> ("And let me reiterate that our treaty commitment to Japan's security is absolute, and Article 5 covers all territories under Japan's administration, including the Senkaku Islands."). This reaffirmation was also succeeded to the Trump administration. The White House, Joint Statement from President Donald J. Trump and Prime Minister Shinzo Abe (2017), <https://www.whitehouse.gov/briefings-statements/joint-statement-president-donald-j-trump-prime-minister-shinzo-abe/> ("The two leaders affirmed that Article V of the U.S.-Japan Treaty of Mutual Cooperation and Security covers the Senkaku Islands. They oppose any unilateral action that seeks to undermine Japan's administration of these islands."); Ministry of Foreign Affairs of Japan, Prime Minister Abe Receives a Courtesy Call from U.S. Defense Secretary Mattis (2017), https://www.mofa.go.jp/na/st/page3e_000644.html ("Secretary Mattis stated that the Senkaku Islands are in the territories under the administration of Japan, and are within the scope that is covered by Article 5 of the Japan-U.S. Security Treaty. Secretary Mattis also made clear that the U.S. opposes any unilateral action that seeks to undermine Japan's administration of the Senkaku Islands.").
- 2 Cabinet Secretariat of Japan, Cabinet Decision on Development of Seamless Security Legislation to Ensure Japan's Survival and Protect its People 2 (2014) [hereinafter Cabinet Decision], http://www.cas.go.jp/jp/gaiyou/jimu/pdf/anpohosei_eng.pdf.
- 3 Ministry of Foreign Affairs of Japan, The Guidelines for Japan-U.S. Defense Cooperation (2015), <http://www.mofa.go.jp/files/000078188.pdf>.
- 4 See, e.g., Tomohiro Mikanagi & Hirohito Ogi, The Japanese Views on Legal Issues Related to Security, 59 Japanese Y.B. Int'l L. 360, 369–71 (2016).
- 5 In answering the question of whether the right to self-defense under the Japan's Constitution is "exactly the same" with that under international law, the government simply observed that they were "the same, at least in nature," or "at the conceptual level." Takatsuji Masami Naikaku-hōseikyōkuchōkan Tōben (高辻正巳内閣法制局長官答弁) [Answer by Takatsuji Masami, Dir.-Gen. of the Cabinet Legislation Bureau], Dai 61-kai Kokkai Sangiin Yosai Kaigi-roku dai 21-gō (第61回国会参議院予算委員会議録第21号) [Proceedings of the 61st Diet House of Councillors Budget Comm. No.21], at 15 (1969), available at <http://kokkai.ndl.go.jp/SENTAKU/sangi-in/061/1380/06103311380021.pdf#page=15>.
- 6 Yamada Takio Gaimushō daijin kanbō sanjikan Tōben (山田滝雄外務省大臣官房参事官答弁) [Answer by Yamada Takio, Counselor, Ministry of Foreign Affairs], Dai 186-kai Kokkai Shūgiin Naikaku iin Kaigi-roku dai 19-gō (第186回国会衆議院内閣委員会議録第19号) [Proceedings of the 186th Diet H.R. Cabinet Comm. No. 19], at 37 (2014), available at <http://kokkai.ndl.go.jp/SENTAKU/syugin/186/0002/18605230002019.pdf#page=37>.
- 7 Shūgiin giin Itō Eisei-kun Teishutsu Naikaku Hōsei-kyoku no Kengen to Jiei-ken ni tsuite no Kaishaku ni Kansuru Shitsumon ni Taisuru Tōben-sho (衆議院議員伊藤英成君提出内閣法制局の権限と自衛権についての解釈に関する質問に対する答弁書) [Reply to Questions Regarding Interpretation of Authority and Self-Defense Rights by Mr. Eisei Ito, Member, H.R.], Naikaku Shū-shitsu 156 dai 119-gō (内閣衆質156第119号) [Cabinet H.R. Reply 156, No. 119] (2003), available at http://www.shugiin.go.jp/internet/itdb_shitsumon.nsf/html/shitsumon/b156119.htm.
- 8 See Japan Ministry of Def., Zainichibeigun shisetsu kuiki (senyō shisetsu) menseki (在日米軍施設・区域(専用施設)面積) [U.S. Military Facility Area (Designated Facilities) in Japan] (2019), https://www.mod.go.jp/j/approach/zaibeigun/us_sisetsu/pdf/menseki_h310331.pdf (last updated Mar. 31, 2019).

9 Article 2(1)(a) of the Japan-U.S. Status of Forces Agreement reads: “The United States is granted, under Article VI of the Treaty of Mutual Cooperation and Security, the use of facilities and areas in Japan. Agreements as to specific facilities and areas shall be concluded by the two Governments through the Joint Committee provided for in Article XXV of this Agreement. ‘Facilities and areas’ include existing furnishings, equipment and fixtures necessary to the operation of such facilities and areas.” U.S.-Japan Status of Forces Agreement, Japan-U.S., Jan. 19, 1960, 11 U.S.T. 1652, T.I.A.S. No. 4510.

10 Kishida Fumio Gaimu Daijin Tōben (岸田文雄外務大臣答弁) [Answer by Minister for Foreign Affairs Fumio Kishida], Dai 186-kai Kokkai Shūgiin Anzen Hoshō iinkai gaimu iinkai rengō shinsa Kaigi-roku dai 1-gō (第186回国会衆議院安全保障委員会外務委員会連合審査会議録第1号) [Proceedings of the 186th Diet H.R. Sec. Comm. No. 1], at 22 (2014), available at <http://kokkai.ndl.go.jp/SEN-TAKU/syuguiin/186/0285/18606020285001.pdf#page=22>. In addition to the individual self-defense option, when there is a possibility of large-scale terrorist attacks—not amounting to armed attacks—on U.S. military facilities and sites in Japan and there is a recognized necessity to prevent damage to them, Japan may order the Self-Defense Force (SDF) to conduct “guarding operations” in a manner other than the use of force. See Jietaiho [Self Defense Forces Law], Law No. 165 of 1954 (Japan) [hereinafter SDF Act], art. 84bis.

11 Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ¶ 195 (June 27) [hereinafter Nicaragua Case], available at <https://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf#page=94>.

12 Akiba Takeo Gaimushō Kokusai-hō Kyokuchō Tōben (秋葉剛男外務省国際法局長答弁) [Answer by Takeo Akiba, Dir., Int’l Law Bureau, Ministry of Foreign Affairs], Dai 189-kai Kokkai Sangiin wagakuni oyobi Kokusai shakai no Heiwa Anzen Hōsei ni kansuru Tokubetsu iinkai Kaigi-roku dai 15-gō (第189回国会参議院我が国及び国際社会の平和安全法制に関する特別委員会会議録第15号) [Proceedings of the 189th Diet House of Councillors Spec. Comm. Meeting on Peace and Security Laws of Japan and the International Community No. 15], at 22 (2015), available at <http://kokkai.ndl.go.jp/SEN-TAKU/sangiin/189/0192/18909020192015.pdf#page=21>.

13 Office of Gen. Counsel, U.S. Dep’t of Def., Law of War Manual 49 (2016) (“Collective self-defense of a State must proceed with that State’s consent, although this consent need not necessarily be expressed in the form of an explicit request.”).

14 In the context of the scenario of a North Korean missile attack on the Japanese territory, see Masahiro Kurosaki, *The ‘Bloody Nose’ Strategy, Self-Defense and International Law: A View from Japan*, Lawfare (Feb. 15, 2018), <https://www.lawfareblog.com/bloody-nose-strategy-self-defense-and-international-law-view-japan>.

15 Article IV of the Treaty reads: “The Parties will consult together from time to time regarding the implementation of this Treaty, and, at the request of either Party, whenever the security of Japan or international peace and security in the Far East is threatened.” Treaty of Mutual Cooperation and Security Between the United States of America and Japan, Japan-U.S., art. IV, Jan. 19, 1960, 11 U.S.T. 1632, T.I.A.S. No. 4509. The consultation mechanism is centered on the Japan-U.S. Security Consultative Committee (“2+2”). See *Japan-U.S. Security Consultative Committee*, Ministry of Foreign Affairs of Japan, <https://www.mofa.go.jp/region/n-america/us/security/scc/index.html> (last visited Dec. 8, 2019).

16 See, e.g., Charlie Dunlap, *The “Bloody Nose” Strategy Debate: Why it’s More Complicated than Some Think*, Lawfire (Jan. 24, 2018), <https://sites.duke.edu/lawfire/2018/01/24/the-bloody-nose-strategy-debate-why-its-more-complicated-than-some-think/>.

17 Shūgiin giin Kaneda Seiichi-kun teishutsu Sensō, Funsō, Buryoku no Kōshi-tō no chigai ni kansuru shitsumon ni taisuru Tōben-sho (衆議院議員金田誠一君提出「戦争」「紛争」「武力の行使」等の違いに関する質問に対する答弁書) [Reply to Questions Regarding Differences in War, Conflict, Exercise of Force, etc., by Mr. Seiichi Kaneda, Member, H.R.], Naikaku Shū-shitsu 153 dai 27-gō (内閣衆質153第27号) [Cabinet H.R. Reply 153, No. 27] (2002), available at http://www.shugiin.go.jp/internet/itdb_shitsumon.nsf/html/shitsumon/b153027.htm.

18 Nicaragua Case, *supra* note 11, ¶ 195.

19 Case Concerning Oil Platforms (Iran v. U.S.), Judgement, 2003 I.C.J. Rep. 161, ¶ 64 (Nov. 6), available at <https://www.icj-cij.org/files/case-related/90/090-20031106-JUD-01-00-EN.pdf#page=35>.

20 In contrast, the issue of hostile intent usually comes into play on the force-user side in international legal debates. See, e.g., 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)?*, 108 Am. J. Int’l L. 159, 209 (2014) (“[W]henver a state deliberately uses (potentially) lethal force within its own territory—including its territorial sea and its airspace—against military or police units of another state acting in their official capacity, such action amounts to the interstate use of force in the sense of Article 2(4). . . . By the same token, any incursion that would have warranted deliberate recourse to lethal force (primarily because it demonstrates a manifest hostile intent) arguably constitutes a use of force in the sense of Article 2(4) (irrespective of the actual response of the territorial state). . . . [A]ny deliberate projection of lethal force onto the territory of another state . . . will normally trigger Article 2(4).”).

21 Inada Tomomi Bōei Daijin Tōben (稲田朋美防衛大臣答弁) [Answer by Minister of Def. Tomomi Inada], Dai 193-kai Sangiin Gaikō Bōei iinkai Kaigi-roku dai 18-gō (第193回参議院外交防衛委員会議録第18号) [Proceedings of the 193rd House of Councillors Foreign Affairs Def. Comm. No. 18], at 5 (2017), available at <http://kokkai.ndl.go.jp/SENTAKU/sangiin/193/0059/19305160059018.pdf#page=5>; Noroda Yoshinori Bōeichō Chōkan (野呂田芳成防衛庁長官) [Yoshinori Noroda, Sec’y of Def.], Dai 145-kai Kokkai Shūgiin Anzen Hoshō iin Kaigi-roku dai 3-gō (第145回国会衆議院安全保障委員会議録第3号) [Proceedings of the 145th Diet H.R. Sec. Comm. No. 3], at 5 (1999), available at <http://kokkai.ndl.go.jp/SENTAKU/syugin/145/0015/14503030015003.pdf#page=5>.

22 Yamagami Shingo Gaimu Daijin Kanbō Shingi-kan Tōben (山上信吾外務大臣官房審議官答弁) [Answer by Shingo Yamagami, Deputy Sec’y for Foreign Affairs], Dai 189-kai Kokkai Sangiin Gaikō Bōei iinkai Kaigi-roku dai 4-gō (第189回国会参議院外交防衛委員会議録第4号) [Proceedings of the 189th Diet House of Councillors Foreign Affairs Def. Comm. No. 4], at 14 (2015), available at <http://kokkai.ndl.go.jp/SENTAKU/sangiin/189/0059/18903260059004.pdf#page=14>; Kishida Fumio Gaimu Daijin Tōben (岸田文雄外務大臣答弁) [Answer by Minister for Foreign Affairs Fumio Kishida], Dai 189-kai Kokkai Shūgiin wagakuni oyobi Kokusai shakai no Heiwa Anzen Hōsei ni kansuru Tokubetsu iinkai Kaigi-roku dai 3-gō (第189回国会衆議院我が国及び国際社会の平和安全法制に関する特別委員会議録第3号) [Proceedings of the 189th Diet H.R. Spec. Comm. Meeting on Peace and Security Laws of Japan and the International Community No. 3], at 13 (2015), available at <http://kokkai.ndl.go.jp/SENTAKU/syugin/189/0298/18905270298003.pdf#page=13>; Saito Akira Bōei fuku Daijin ken Naikaku-fu fuku Daijin Tōben (左藤章防衛副大臣兼内閣府副大臣答弁) [Akira Saito, Deputy Minister of Def. & Vice Cabinet Minister], Dai 189-kai Kokkai Shūgiin Gaimu iin Kaigi-roku dai 12-gō (第189回国会衆議院外務委員会議録第12号) [Proceedings

of the 189th Diet H.R. Comm. on Foreign Affairs No. 12], at 5 (2015), available at <http://kokkai.ndl.go.jp/SENTAKU/syugin/189/0005/18905220005012.pdf#page=5>; Shūgiin giin Nagatsuma Akira-kun teishutsu Shūdantekijieikenkōshi Yōnin-tō kansuru shitsumon ni taisuru Tōben-sho (衆議院議員長妻昭君提出集団の自衛権行使容認等に関する質問に対する答弁書) [Reply to Questions Regarding the Approval of the Right to Exercise Collective Self-Defense, etc., by Mr. Akira Nagatsuma, Member, H.R.], Naikaku Shū-shitsu 189 dai 333-gō (内閣衆質189第333号) [Cabinet H.R. Reply 189, No. 333] (2015), available at http://www.shugiin.go.jp/internet/itdb_shitsumon.nsf/html/shitsumon/b189333.htm; Togo Kazuhiko Gaimushō Jōyaku Kyokuchō Tōben (東郷和彦外務省条約局長答弁) [Answer by Togo Kazuhiko, Dir.-Gen. of the Treaty Bureau, Minister of Foreign Affairs], Dai 145-kai Kokkai Shūgiin yosan iin Kaigi-roku dai 14-gō (第145回国会衆議院予算委員会議録第14号) [Proceedings of the 145th Diet H.R. Budget Comm. No. 14], at 43 (1999), available at <http://kokkai.ndl.go.jp/SENTAKU/syugin/145/0018/14502160018014.pdf#page=43>.

23 Kishida Fumio Gaimu Daijin Tōben (岸田文雄外務大臣答弁) [Answer by Foreign Minister Fumio Kishida], Dai 187-kai Kokkai Shūgiin Anzen Hoshō iin Kaigi-roku dai 2-gō (第187回国会衆議院安全保障委員会議録第2号) [Proceedings of the 187th Diet H.R. Sec. Comm. No. 2], at 6 (2014), available at <http://kokkai.ndl.go.jp/SENTAKU/syugin/187/0015/18710140015002.pdf#page=6>.

24 Even if the act in question is irrelevant to its qualification as an armed attack, the government view is that it does not necessarily foreclose the possibility of exercising the inherent right of self-defense to rescue nationals under general international law as distinct from the U.N. Charter. Date Muneaki Gaimushō Jōyaku Kyokuchō Tōben (伊達宗起外務省条約局長答弁) [Answer by Muneaki Date, Dir.-Gen. of the Treaty Bureau, Minister of Foreign Affairs], Dai 91-kai Kokkai Shūgiin Anzen Hoshō tokubetsu iin Kaigi-roku dai 2-gō (第91回国会衆議院安全保障特別委員

会議録第2号) [Proceedings of the 91st Diet H.R. Sec. Spec. Comm. No. 2], at 33 (1980), available at <http://kokkai.ndl.go.jp/SENTAKU/syugin/091/0770/09104260770002.pdf#page=33>; Komatsu Ichiro Gaimushō Jōyaku-kyoku Hōki Kachō Tōben (小松一郎外務省条約局法規課長答弁) [Answer by Ichiro Komatsu, Dir. Gen., Law Bureau, Ministry of Foreign Affairs], Dai 120-kai Kokkai Shūgiin Anzen Hoshō tokubetsu iin Kaigi-roku dai 5-gō (第120回国会衆議院安全保障特別委員会議録第5号) [Proceedings of the 120th Diet H.R. Sec. Spec. Comm. No. 5], at 21 (1991), available at <http://kokkai.ndl.go.jp/SENTAKU/syugin/120/0770/12003130770005.pdf#page=21>. See also *Summary records of the meetings of the fifty-second session*, [2000] 2 Y.B. Int'l L. Comm'n 218–20, U.N. Doc. A/CN.4/SER.A/2000/Add.1 (Part 1).

25 Shūgiin giin Ogata Rintarō-kun teishutsu Kuni ni Junzuru Shoshiki ni kansuru shitsumon ni taisuru Tōben-sho (衆議院議員緒方林太郎君提出『国に準ずる組織』に関する質問に対する答弁書) [Reply to Questions Regarding “Organizing According to the Country” by Mr. Rintaro Ogata, Member, H.R.], Naikaku Shū-shitsu 193 dai 148-gō (内閣衆質193第148号) [Cabinet H.R. Reply 193, No. 148] (2017), available at http://www.shugiin.go.jp/internet/itdb_shitsumon.nsf/html/shitsumon/b193148.htm.

26 Ishiba Shigeru Bōeichō Chōkan Tōben (石破茂防衛庁長官答弁) [Answer by Shigeru Ishiba, Sec’y of Def.], Dai 156-kai Kokkai Sangiin Buryoku Kōgeki jitai e no Taisho ni kansuru tokubetsu iinkai Kaigi-roku dai 11-gō (第156回国会参議院武力攻撃事態への対処に関する特別委員会会議録第11号) [Proceedings of the 156th Diet House of Councillors Spec. Comm. on Coping with Armed Attack Situations No. 11], at 23 (2003), available at <http://kokkai.ndl.go.jp/SENTAKU/sangin/156/0074/15606040074011.pdf#page=23>.

27 Dai 156-kai kokkai shūgiin iraku jindō fukkō shien narabini kokusai terorizumu no bōei oyobi wagakuni no kyōryoku shien katsudō-tō ni kansuru tokubetsu iin Kaigi-roku dai 7-gō (第156回国会衆議院イラク人道復興支援並びに国際テロリズムの防衛及び我が国

の協力支援活動等に関する特別委員会議録第7号) [Proceedings of the 156th Diet H.R. Spec. Comm. Meeting on Iraq Humanitarian Reconstruction Support, International Terrorism Defense, Japan's Cooperation Support, etc., No. 7] (2003), available at <http://kokkai.ndl.go.jp/SENTAKU/syugin/156/0132/15607020132007.pdf#page=4>.

28 Ishiba Shigeru Bōei Daijin Tōben (石破茂防衛大臣答弁) [Answer by Def. Minister Shigeru Ishiba], Dai 169-kai Kokkai Shūgiin Anzen Hoshō iin Kaigi-roku dai 6-gō (第169回国会衆議院安全保障委員会議録第6号) [Proceedings of the 169th Diet H.R. Sec. Comm. No. 6], at 2 (2008), available at <http://kokkai.ndl.go.jp/SENTAKU/syugin/169/0015/16904250015006.pdf#page=2>.

29 Article 9 of the Constitution reads: “[a] spiring sincerely to an international peace based on justice and order, the Japanese people forever renounce war as a sovereign right of the nation and the threat or use of force as means of settling international disputes. . . In order to accomplish the aim of the preceding paragraph, land, sea, and air forces, as well as other war potential, will never be maintained. The right of belligerency of the state will not be recognized.” *Nihonkoku Kenpō* [Kenpō] [Constitution], ch. II, art. 9 (Japan).

30 Shūdantekijieiken to Kenpō to no kankei ni kansuru Seifu Shiryō (集団的自衛権と憲法との関係に関する政府資料) [Gov't Materials on the Relationship between Collective Self-Def. Rights & Constitution], Shōwa 47-nen 10 tsuki 14-nichi Sangiin kessan iinkai teishutsu shiryō (昭和47年10月14日参議院決算委員会提出資料) [Materials Submitted to the House of Councillors Fin. Results Comm. on Oct. 14, 1972] (1972), available at <http://www.kantei.go.jp/jp/singi/anzenhosyou2/dai4/siryou.pdf#page=9>; Shūgiin giin Inaba Seiichi-kun teishutsu Kenpō, Kokusai-hō to Shūdantekijieiken ni kansuru shitsumon ni taisuru Tōben-sho (衆議院議員稲葉誠一君提出「憲法、国際法と集団的自衛権」に関する質問に対する答弁書) [Reply to Questions on Constitution, Int'l Law & Collective Self-Def. by Mr. Seiichi Inaba, Member, H.R.], Naikaku Shū-shitsu 94 dai 32-go (内閣衆質94第32号) [Cabinet H.R.

Reply 94, No. 32] (1981), available at http://www.shugiin.go.jp/internet/itdb_shitsumona.nsf/html/shitsumon/b094032.htm.

31 Cabinet Decision, *supra* note 17, at 8.

32 *Id.* at 6–7, ¶ 1–2 (emphasis added).

33 Some might argue that this constitutional approach to collective self-defense is, or should be, better understood as an expanded version of Japan's individual self-defense, and that such an understanding is inconsistent with the ICJ's view that collective self-defense is the defense of the victim state by the assisting state irrespective of their relationship. For this matter, see, e.g., Stanimir A. Alexandrov, *Self-Defense against the Use of Force in International Law* 228 (1996). Yet, it is also true that there have been diverging views among experts as to the nature of collective self-defense, see, e.g., Derek W. Bowett, *Self-Defense in International Law* 200–07 (1958); Derek W. Bowett, *Collective Self-Defense under the Charter of the United Nations*, 32 *Brit. Y.B. Int'l L.* 130, 132–39 (1955–1956), and that Japan's approach could be in harmony with traditional scholarly views. In fact, in his dissenting opinion in the ICJ's *Nicaragua* case, Judge Jennings rejected the concept of collective self-defense as “vicarious defence by champions” and observed that “[t]he assisting State surely must, by going to the victim State's assistance, be also, and in addition to other requirements, in some measure defending itself. There should even in ‘collective self-defence’ be some real element of self.” *Nicaragua Case*, *supra* note 11, at 545.

34 Kishida Fumio Gaimu Daijin Tōben (岸田文雄外務大臣答弁) [Answer by Foreign Minister Fumio Kishida], Dai 189-kai Kokkai Shūgiin wagakuni oyobi Kokusai shakai no Heiwa Anzen Hōsei ni kansuru Tokubetsu iinkai Kaigi-roku dai 10-gō (第189回国会衆議院我が国及び国際社会の平和安全法制に関する特別委員会議録第10号) [Proceedings of the 189th Diet H.R. Spec. Comm. Meeting on Peace and Security Laws of Japan and the International Community No. 10], at 29 (2015), available at [42 Strengthening the U.S.-Japan Alliance](http://kokkai.ndl.go.jp/SEN-</p></div><div data-bbox=)

TAKU/syugiin/189/0298/18906150298010.pdf#page=29.

35 Sangiin giin Mizuno Kenichi-kun teishutsu Sonritsu kiki jitai ni kansuru shitsumon ni taisuru Tōben-sho (参議院議員水野賢一君提出存立危機事態に関する質問に対する答弁書) [Reply to Questions Regarding Existential Crisis by Mr. Kenichi Mizuno, Member, House of Councillors], Naikaku San-shitsu 189 dai 202-gō (内閣参質189第202号) [Cabinet House of Councillors Answer 189, No. 202] (2015), available at <http://www.sangiin.go.jp/japanese/joho1/kousei/syuisyo/189/touh/t189202.htm>; Shūgiin giin Okada Katsuya-kun teishutsu Shūdantekijijieken no Kōshi o Yōnin suru Kenpō kaishaku no Henkō-tō ni kansuru shitsumon ni taisuru Tōben-sho (衆議院議員岡田克也君提出集団的自衛権の行使を容認する憲法解釈の変更等に関する質問に対する答弁書) [Reply to Questions Regarding Changes in the Interpretation of the Constitution allowing the Exercise of Collective Self-Defense by Mr. Katsuya Okada, Member, H.R.], Naikaku Shū-shitsu 188 dai 1-gō (内閣衆質188第1号) [Cabinet H.R. Reply 188, No. 1] (2015), available at http://www.shugiin.go.jp/internet/itdb_shitsumon.nsf/html/shitsumon/b188001.htm.

36 See Buryoku kōgeki jitai-tō oyobi sonritsu kiki jitai ni okeru wagakuni no heiwa to dokuritsu narabini kuni oyobi kokumin no anzen no kakuho ni kansuru hōritsu [Armed Attack and Existential Crisis Situations Law], Law No. 79 of 2003 (Japan), arts. 2(2)–(3).

37 Abe Shinzo Naikakusōri Daijin Tōben (安倍晋三内閣総理大臣答弁) [Answer by Prime Minister Shinzo Abe], Dai 189-kai Kokkai Sangiin Kaigi-roku dai 34-gō (第189回国会参議院会議録第34号) [Proceedings of the 189th Diet No. 34], at 6 (2015), available at <http://kokkai.ndl.go.jp/SENTAKU/sangiin/189/0001/18907270001034.pdf#page=6>. In fact, the Japanese government recognizes that even an attack on a merchant vessel could constitute an armed attack on the flag state: “[W]hen a private or government ship or an aircraft of its nationality is attacked on the high seas, as a matter of international law, a State is in principle in a position to

repel the attack as the exercise of the right of individual self-defense.” Answer by Ichiro Komatsu, *supra* note 24, at 21, translated in Mikanagi & Ogi, *supra* note 4, at 369.

38 Nakatani Gen Bōei Daijin Tōben (中谷元防衛大臣答弁) [Reply by Def. Minister Nakatani], Dai 190-kai Kokkai Sangiin Gaikō Bōei iinkai Kaigi-roku dai 5-gō (第190回国会参議院外交防衛委員会会議録第5号) [Proceedings of the 190th Diet House of Councillors Foreign Affairs Def. Comm. No. 5], at 7 (2016), available at <http://kokkai.ndl.go.jp/SENTAKU/sangiin/190/0059/19003170059005.pdf#page=7>.

39 Onodera Itsunori Bōei Daijin Tōben (小野寺五典防衛大臣答弁) [Answer by Def. Minister Itsunori Onodera], Dai 193-kai Kokkai Shūgiin Anzen Hoshō iin Kaigi-roku dai 9-gō (第193回国会衆議院安全保障委員会会議録第9号) [Proceedings of the 193rd Diet H.R. Sec. Comm. No. 9], at 11 (2017), available at <http://kokkai.ndl.go.jp/SENTAKU/syugiin/193/0015/19308100015009.pdf#page=11>.

40 Wagakuni oyobi kokusai shakai no heiwa oyobi anzen no kakuho ni shisuru tame no jietai-hō-tō no ichibu o kaisei suru hōritsu-an oyobi kokusai heiwa kyōdō taisho jitai ni saishite wagakuni ga jissai suru sho gaikoku no guntai-tō ni taisuru kyōryoku shien katsu dō-tō ni kansuru hōritsu-an ni taisuru futai ketsugi (我が国及び国際社会の平和及び安全の確保に資するための自衛隊法等の一部を改正する法律案及び国際平和共同対処事態に際して我が国が実施する諸外国の軍隊等に対する協力支援活動等に関する法律案に対する附帯決議) [A Bill to Revise Part of the Self-Defense Forces Act, etc., to Contribute to Ensuring Peace and Security of Japan and the International Community, and Cooperation Support Activities for Foreign Troops, etc., Implemented by Japan in the Event of a Joint International Peace Treaty] (2015), available at http://www.sangiin.go.jp/japanese/gianjoho/ketsugi/189/f429_091701.pdf#page=2.

41 Answer by Prime Minister Shinzo Abe, *supra* note 37, at 7.

42 As a member of the Group of Seven (G7), Japan joined the declaration on cyber-security in 2016. Ministry of Foreign Affairs of Japan, G7 Principles and Actions on Cyber 1 (2016), <http://www.mofa.go.jp/mofaj/files/000160279.pdf> ("We affirm that under some circumstances, cyber activities could amount to the use of force or an armed attack within the meaning of the United Nations Charter and customary international law. We also recognize that states may exercise their inherent right of individual or collective self-defense as recognized in Article 51 of the United Nations Charter and in accordance with international law, including international humanitarian law, in response to an armed attack through cyberspace.").

43 Sangiin giin Okubo Tsutomu-kun teishutsu Saibā Kōgeki o Buryoku Kōgeki jitai to nin-tei suru tame no yōkenni kansuru shitsumon ni taisuru Tōben-sho (参議院議員大久保勉君提出サイバー攻撃を武力攻撃事態と認定するための要件に関する質問に対する答弁書) [Reply to Questions Regarding Requirements for Certifying a Cyber Attack as an Armed Attack Situation by Mr. Tsutomu Okubo, Member, House of Councillors], Naikaku San-shitsu 189 dai 221-gō (内閣参質189第221号) [Cabinet House of Councillors Answer 189, No. 221] (2015), available at <http://www.sangiin.go.jp/japanese/joho1/kousei/syuisyo/189/touh/t189221.htm>.

44 Abe Shinzo Naikakusōri Daijin Tōben oyobi Iwaya Takeshi Bōei Daijin Tōben (安倍晋三内閣総理大臣答弁及び岩屋毅防衛大臣答弁) [Answer by Prime Minister Shinzo Abe & Def. Minister Takeshi Iwaya], Dai 198-kai Kokkai Shūgiin Honkaigi-roku dai 24-gō (第198回国会衆議院本会議録第24号) [Proceedings of the 198th Diet H.R. Sess. No. 24], at 13, 15 (2019), available at <http://kokkai.ndl.go.jp/SENTAKU/syugin/198/0001/19805160001024.pdf#page=13>.

45 Nakatani Moto Bōei Daijin Tōben (中谷元防衛大臣答弁) [Reply by Former Def. Minister Nakatani], Dai 189-kai Kokkai Sangiin wagakuni oyobi Kokusai shakai no Heiwa Anzen Hōsei ni kansuru Tokubetsu iinkai Kaigi-roku dai 9-gō (第189回国会参

議院我が国及び国際社会の平和安全法制に関する特別委員会会議録第9号) [Proceedings of the 189th Diet House of Councillors Spec. Comm. Meeting on Peace and Security Laws of Japan and the International Community No. 9], at 15 (2015), available at <http://kokkai.ndl.go.jp/SENTAKU/sangiin/189/0192/18908110192009.pdf#page=15>.

46 Answer by Prime Minister Shinzo Abe, *supra* note 37, at 7.

47 Armed Attack and Existential Crisis Situations Law, *supra* note 36, art. 9(4)(6)(7); Resolution Supplement to the Peace and Security Bills, *supra* note 40, ¶ 2. The resolution requires the government to obtain prior approval of the Diet unless the existential crisis situation/the survival-threatening situation simultaneously amounts to the armed attack on Japan, and in case of emergency. See also Cabinet Decision, *supra* note 2, at 7–8, ¶ 3.

48 See Ministry of Def. of Japan, *Diplomatic Bluebook* 2018, ch. 3-2(2)A, available at <https://www.mofa.go.jp/policy/other/bluebook/2018/html/chapter3/c030102.html>.

49 Yokohata Yusuke Naikaku-hōseikyō-kuchōkan Tōben (横畠裕介内閣法制局長官答弁) [Answer by Yusuke Yokohama, Cabinet Sec'y Gen.], Dai 189-kai Kokkai Shūgiin wagakuni oyobi Kokusai shakai no Heiwa Anzen Hōsei ni kansuru Tokubetsu iinkai dai 4-gō (第189回国会衆議院我が国及び国際社会の平和安全法制に関する特別委員会第4号) [Proceedings of the 189th Diet H.R. Spec. Comm. Meeting on Peace and Security Laws of Japan and the International Community No. 4], at 5 (2015), available at <http://kokkai.ndl.go.jp/SENTAKU/syugin/189/0298/18905280298004.pdf#page=5>.

50 *Id.*

51 Sangiin giin Mizuno Kenichi-kun teishutsu kobetsu-teki jie-i-ken no chiri-teki yōken nado ni kansuru shitsumon ni taisuru Tōben-sho (参議院議員水野賢一君提出個別的自衛権の地理的要件などに関する質問に対する答弁書) [Reply to Questions Regarding Geographical Requirements of the Individual Right to Self-Defense by Mr. Kenichi Mizuno,

Member, House of Councillors], Naikaku San-shitsu 189 dai 201-gō (内閣参質189第201号) [Cabinet House of Councillors Answer 189, No. 201] (2015), available at <http://www.sangiin.go.jp/japanese/joho1/kousei/syuisyo/189/touh/t189201.htm>.

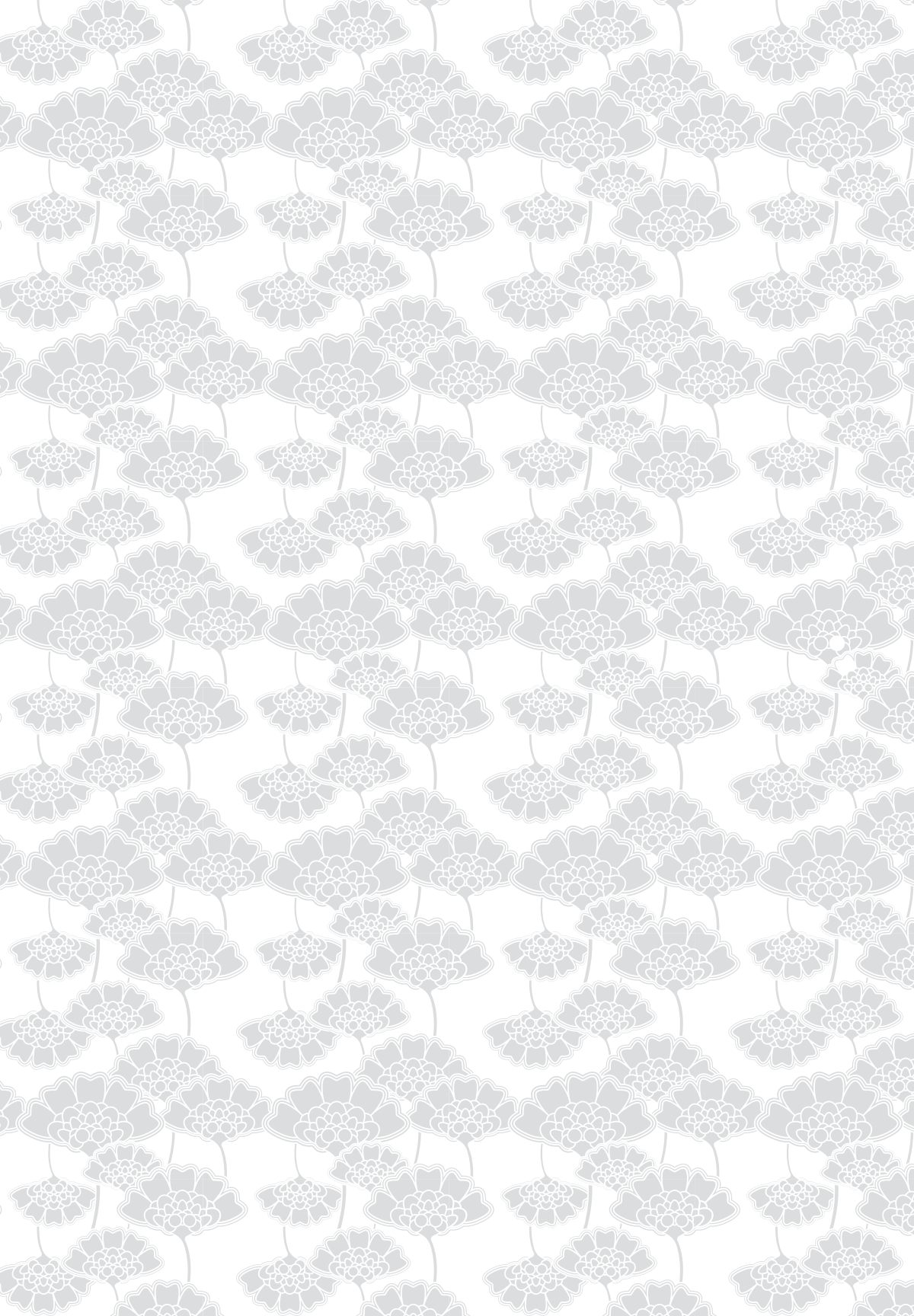
52 Shūgiin giin Tsujimoto Kiyomi-kun teishutsu Shūdantekijieiken no kōshi to hōfuku kōgeki ni kansuru shitsumon ni taisuru Tōben-sho (衆議院議員辻元清美君提出集団的自衛権の行使と報復攻撃に関する質問に対する答弁書) [Reply to Questions Regarding the Exercise of Collective Self-Defense and Retaliation Attacks by Kiyomi Tsujimoto, Member, H.R.], Naikaku Shū-shitsu 186 dai 271-gō (内閣衆質186第271号) [Cabinet H.R. Reply 186, No. 271] (2014), available at http://www.shugiin.go.jp/internet/itdb_shitsumon.nsf/html/shitsumon/b186271.htm.

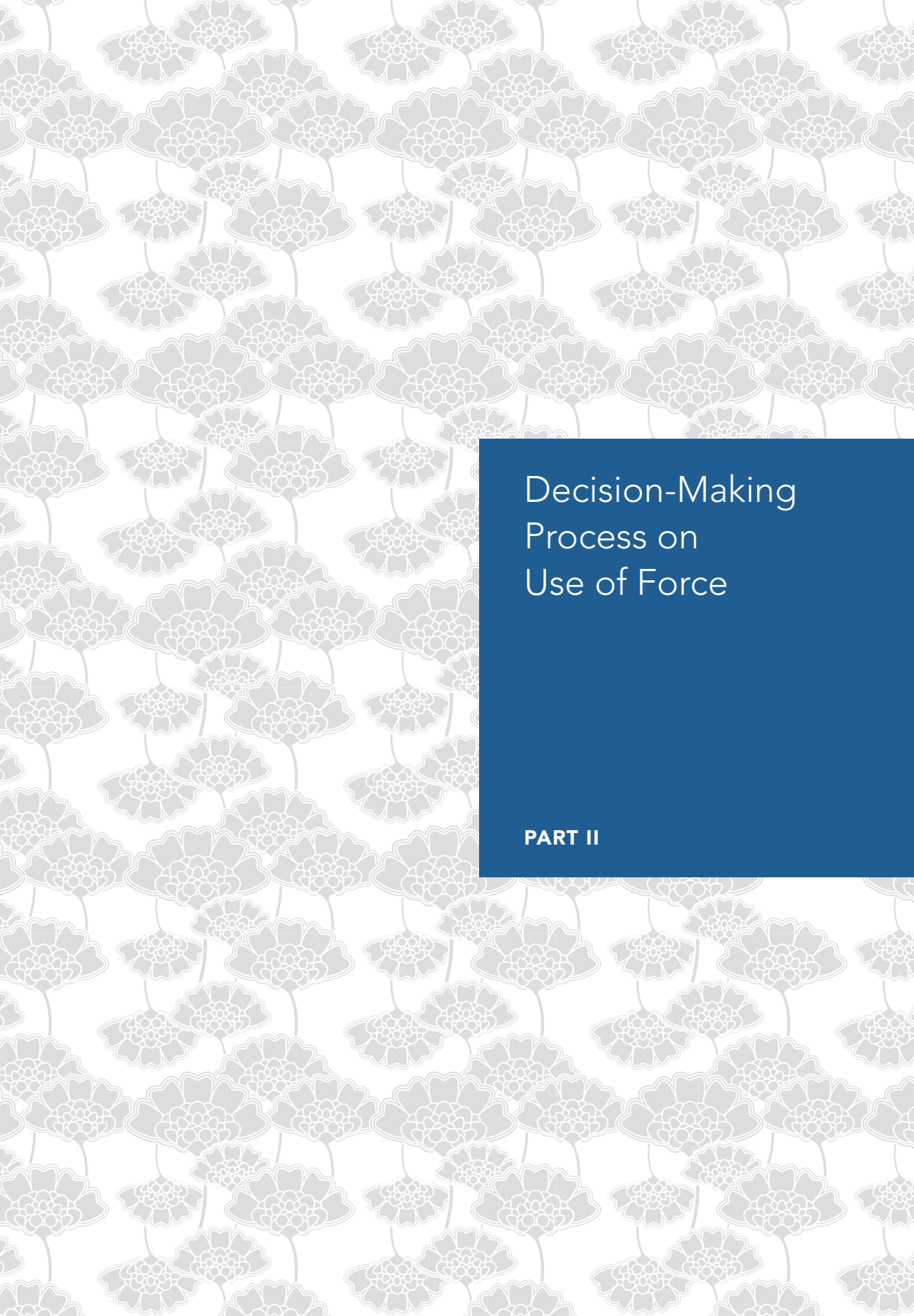
53 Sangiin giin Haku Shinkun-kun teishutsu gaikoku no ryōiki ni okeru buryoku no kōshi ni kansuru shitsumon ni taisuru Tōben-sho (参議院議員白眞勲君提出外国の領域における武力の行使に関する質問に対する答弁書) [Reply to Questions Regarding Use of Force in Foreign Territories by Mr. Shinkun Haku, Member, House of Councillors], Naikaku San-shitsu 190 dai 105-gō (内閣参質190第105号) [Cabinet House of Councillors Answer 190 No. 105] (2016), available at <http://www.sangiin.go.jp/japanese/joho1/kousei/syuisyo/190/touh/t190105.htm>.

54 Abe Shinzo Naikakusōri Daijin Tōben (安倍晋三内閣総理大臣答弁) [Answer by Prime Minister Shinzo Abe], Dai 189-kai Kokkai Sangiin wagakuni oyobi Kokusai shakai no Heiwa Anzen Hōsei ni kansuru Tokubetsu iinkai Kaigi-roku dai 11-gō (第189回国会参議院我が国及び国際社会の平和安全法制に関する特別委員会会議録第11号) [Proceedings of the 189th Diet House of Councilors Spec. Comm. Meeting on Peace and Security Laws of Japan and the International Community No. 11], at 9 (2015), available at <http://kokkai.ndl.go.jp/SENTAKU/sangiin/189/0192/18908210192011.pdf#page=9>.

55 Kishida Fumio Gaimu Daijin Tōben (岸田文雄外務大臣答弁) [Answer by Foreign Minister Fumio Kishida], Dai 189-kai Kokkai Sangiin wagakuni oyobi Kokusai shakai no Heiwa Anzen Hōsei ni kansuru Tokubetsu iinkai Kaigi-roku dai 10-gō (第189回国会参議院我が国及び国際社会の平和安全法制に関する特別委員会会議録第10号) [Proceedings of the 189th Diet House of Councilors Spec. Comm. Meeting on Peace and Security Laws of Japan and the International Community No. 10], at 17 (2015), available at <http://kokkai.ndl.go.jp/SENTAKU/sangiin/189/0192/18908190192010.pdf#page=17>.

56 See Masahiro Kurosaki, Japan's Evolving Position on the Use of Force in Collective Self-Defense, *Lawfare* (Aug. 23, 2018), <https://www.lawfareblog.com/japans-evolving-position-use-force-collective-self-defense>. It was also reported that the Japanese Defense Minister recognized the applicability of the right of collective self-defense to outer space for the purpose of the defense of foreign partners, such as the United States and the European Union. Uchū demo Shūdantekijieiken Bōei-shō ga Kenkai (宇宙でも集団的自衛権 防衛相が見解) [Collective Self-Defense Right in Space: Views by the Defense Minister], *Nikkei* (Oct. 16, 2019), <https://www.nikkei.com/article/DGXMZO51064430W9A011C1000000>.





Decision-Making Process on Use of Force

PART II



Matthew C. Waxman

Columbia Law School

Presidential Use of Force in East Asia

*American
Constitutional
Law and the
U.S.-Japan
Alliance*

Introduction

The U.S. Constitution's allocation of military authority has adapted over time to major shifts in American power and grand strategy. This paper explains, with a focus on U.S. military actions in East Asia and possible scenarios of special joint concern to the United States and Japan, that the president in practice wields tremendous power and discretion in using military force. Although formal, legal checks on the president's use of force rarely come into play, Congress nevertheless retains some political power to influence presidential decision-making. The president's powers are also constrained by interagency processes within the executive branch, and alliance relations often feed into those processes.

This paper is mostly focused on U.S. domestic law issues. It also touches, however, on a few key questions of international law, especially as they relate to presidential power to interpret international law and to possible crisis scenarios of current concern.

The Constitutional Framework

Drafted in the late 18th century, the U.S. Constitution divided responsibility for military affairs between Congress and the president, providing several checks on presidential uses of force. The Constitution vests “executive power” in the president and designates him “commander in chief” of military forces. But it assigns to Congress responsibility for creating, maintaining, and funding those military forces, and gives Congress the power to “[d]eclare war.” The constitutional framers generally wanted to give the president unified, tactical control over military forces, but they wanted Congress to retain primary control over decisions to go to war. The framers were also sensitive to political opposition to large, standing military forces,

which many Americans associated at the time with repression and a proclivity toward war.

Even from the start, this division of constitutional authority left ambiguous whether and under what circumstances the president could unilaterally engage in military activities. Although early presidents were usually hesitant to use much military force without explicit congressional backing—particularly since standing U.S. military forces were small and the president therefore relied on Congress to provide continuing financial support for them—over time a practice accumulated of unilateral presidential deployments and limited uses of military force short of all-out war in the absence of legislative prohibitions.

During the first half of the 19th century, for example, presidents authorized punitive raids and shows of military force in Sumatra and Pacific islands, typically to protect American commercial interests. In the 1850s, the president ordered Commodore Matthew Perry to lead a Navy squadron on a diplomatic mission, using a show of military force, to open trade and other relations with Japan. On several occasions during that decade, presidents sent small military forces to defend U.S. interests in China, and likewise in Korea during the decades that followed. In 1900, the president dispatched about 5,000 troops to China, as part of a multinational expeditionary force responding to the “Boxer Rebellion.”¹ Especially after the United States gained territories in Asia following the Spanish-American War—one of only five declared wars in American history, though many other military operations have been authorized by Congress—presidents frequently directed armed forces to intervene in that region to protect American interests.

As Louis Henkin explains in his treatise of U.S. foreign relations law:

By repeated exercise without successful opposition, Presidents have established their authority to send troops abroad, probably beyond effective challenge, where Congress is silent, but the constitutional foundations and the constitutional limits of that authority remain in dispute.²

Nevertheless, through the first half of the 20th century, it was still widely agreed that, except in cases of repelling an attack against the United States, only Congress could take the nation to full-blown war (as opposed to much more limited uses of military force, even if they involved some combat).

Post-World War II Presidential Powers

Several interrelated factors in the years immediately following World War II combined to dramatically increase the president's power to use military force. These factors include more expansive constitutional theory regarding presidential powers, the formation of mutual defense treaties, and the establishment of a permanent, large-scale military force.

First, presidents during most of the Cold War asserted very broad prerogatives to use even relatively large-scale force without congressional authorization. Executive branch lawyers adopted an expansive view of presidential foreign relations and military powers, and Congress largely acquiesced. The Korean War, which was never expressly authorized by Congress but lasted more than three years and cost the lives of over 33,000 U.S. troops, stands out as a turning point. It marked the largest unilateral military action abroad by a president to date and was justified by vigorous and expansive executive branch claims of constitutional power.³ As Arthur Schlesinger describes the ascendancy of an "imperial presidency" at that time:

The menace of unexpected crisis hung over the world, demanding, it was supposed, the concentration within government of the means of instant decision and response. All this, reinforcing the intellectual doubt about democratic control of foreign relations, appeared to argue more strongly than ever for the centralization of foreign policy in the Presidency.⁴

Since the Korean War, successive presidential administrations have asserted that the president, by virtue of his power to manage foreign relations and his role as commander in chief, has broad authority to initiate military operations that he deems to be in the national interest. The Justice Department has acknowledged in recent years that some large-scale military operations might be of such size, intensity, and nature as to constitutionally require congressional authorization. This point could be important in legal debates about possible military action against North Korea, given the likely large magnitude of such action, but, as explained below, that legal threshold may not in practice be of much consequence.⁵

Second, the United States concluded a set of defense pacts around the world, including with allies in the Asia-Pacific region, and these alliances contributed to a growth of presidential powers. These pacts included the Philippines (1952), Australia and New Zealand (1952), the Republic of Korea (1954), the Southeast Asia Treaty Organization (1954), the Republic of China (1955), and Japan (1960). In the Japan case, the security treaty provides that:

Each Party recognizes that an armed attack against either Party in the territories under the administration of Japan would be dangerous to its own peace and safety and declares that it would act to meet the common danger in accordance with its constitutional provisions and processes. Any such armed attack and all measures taken as a result thereof shall be immediately reported to the Security Council of the United Nations in accordance with the provisions of Article 51 of the Charter. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security.⁶

Defense pacts turned the traditional American aversion to “entangling alliances” on its head; whereas for most of its history, American strategic thinking rested on the idea that the alliances might draw the United States into unnecessary wars, post-war thinking rested on the idea that alliances were necessary to prevent wars that would engulf the United States. These defense pacts meant that presidents could, in effect, rely on a pre-commitment of public support for military action to defend these allies. Presidents also justified expansive unilateral power to use force on the need to preserve the credibility of American security guarantees. Bilateral and regional security treaties generally contain a provision specifying that mutual defense will take place in accordance with each party’s own constitutional processes. This allowed the executive and legislative branches to paper over differences about constitutional prerogatives during ratification, but in practice the executive branch has asserted authority to invoke these provisions unilaterally. In other words, whereas one might think of international law as a likely constraint on executive branch discretion to use force, presidents have repeatedly used multilateral or regional security agreements as a basis for defending broader executive power with regard to military force.⁷ As Mira Rapp-Hooper and I recently wrote:

Some of the president’s constitutional powers relevant to alliances—such as the power to direct military operations in war and to appoint ambassadors (subject to Senate confirmation)—have always been clear. Starting in the early Cold War, though, the centrality of alliances to U.S. foreign policy contributed to the vast accumulation of additional presidential powers—some of them delegated by Congress and others established through executive branch practice over time. After nearly 70 years, presidential authority over U.S. security guarantees now appears to be almost entirely unilateral.⁸

A third major factor contributing to presidential powers to use force was that the United States maintained large, standing military forces after World War II, and the permanence of these forces diminished constraints on presidential power to

use them. Throughout most of its history, the United States had maintained very small or modest peacetime military forces. It mobilized wartime military forces to meet crises, and then it quickly demobilized them post war. With the advent of the Cold War, however, the United States never demobilized to the extent it had in the past. Large numbers of U.S. troops have for decades been stationed on bases in, for example, Japan and South Korea, in addition to a major U.S. naval presence in the Pacific at all times. Especially when combined with a nuclear arsenal, this large-scale standing military power guarantees that a president, as commander in chief, has had permanently-ready forces at his disposal.

As a result of these and other factors, from the early Cold War onward the president has had wide latitude with regard to initiating force, and Congress has often played a reactive, sometimes even passive, role. For the purposes of this paper, one notable counter-example, in which the president showed significant deference to Congress, was President Dwight Eisenhower's approach toward Taiwan (then Formosa) in 1955. In threatening to use force—possibly including nuclear weapons—to defend Nationalist China-controlled islands against aggression by Communist-China, Eisenhower sought and obtained explicit congressional approval to use whatever military means he deemed necessary. Even in seeking congressional approval, however, Eisenhower asserted that he had independent constitutional power to take some military measures anyway, and this case of seeking congressional approval for military intervention in advance stands out as more an exception than the norm.⁹ More typically, in the Vietnam War, for example, presidents slowly escalated U.S. military involvement before requesting and receiving very broad congressional authorization (in the Gulf of Tonkin Resolution) to use military force to defend U.S. and allied interests in Southeast Asia. As public opposition to the war grew, Congress found it difficult to resist presidential requests for additional funds. Eventually, that opposition reached the point that Congress passed or threatened to pass legislative restrictions on the conduct of the war, pushing President Nixon to wind it down.¹⁰

Following the Vietnam War, Congress tried to adjust the balance of power among the political branches by enacting, over President Nixon's veto, the 1973 War Powers Resolution.¹¹ Its stated purpose was to defend the constitutional framers' original constitutional vision: that the "collective judgment of both the Congress and the president will apply to the introduction of United States Armed Forces into hostilities, or into situations where imminent involvement in hostilities is clearly indicated by the circumstances, and to the continued use of such forces in hostilities or in such situations."¹² The War Powers Resolution stipulates that if the president sends U.S. forces into combat, he must withdraw them within 60 days unless Congress declares war or expressly authorizes the president to use force. Over time that law has been watered down in several ways, however, and Congress

has not proven willing to enforce it strictly by further exercising its legislative powers.¹³

In practice, the president thus has broad unilateral discretion to engage U.S. military forces in hostilities abroad. Examples in the Asia-Pacific region since the Vietnam War include action to retake the captured merchant vessel *Mayaguez*, deployments to the Philippines during the 1989 coup attempt, and contribution to UN efforts to restore peace in East Timor.

Although this paper has mostly focused on U.S. domestic law related to use of force, another quick note about international law is important here and relates directly to these observations about presidential power: the president has wide latitude, domestically, in interpreting international law constraints on force, such as self-defense, and the provisions of security treaties (though usually that interpretive power is delegated to subordinate officers and exercised through interagency processes). Moreover, and as explained further below, the United States has adopted broader interpretations than most states, including close allies like Japan, of self-defense rights under Article 51 of the UN Charter.¹⁴ These include a broader understanding of anticipatory self-defense (though its scope is still a matter of ongoing internal debate) and the view that any use of force—even a small one—against the United States under Article 2(4) could also constitute an “armed attack” triggering self-defense rights. Interpreting these international legal constraints on force is left to the president, with Congress playing little if any formal role and courts regarding international legal issues of force as non-justiciable.

It is, in sum, generally understood that from the Korean War onward, the president has exercised vast unilateral powers to use military force. The sheer scope of this presidential authority to use force obviously contrasts sharply with Japanese government decision-making about force. Moreover, whereas Japan’s approach is generally premised on clear lines of what is or is not permitted in advance, the U.S. approach is premised on the idea that security contingencies are unpredictable, and it is better therefore to vest the government with substantial discretion as new issues arise.

Politics, Process, and Diplomacy of Presidential Decisions to Use Force

In some ways, the standard account of a post-WWII imperial presidency often actually *understates* the president’s power. That is because the actual deployment of forces into hostile situations is only one way in which he can use force. More often, the president wields the threat of force to deter or coerce certain conduct by others. With regard to East Asia, for example, the credible threat of U.S. military

force is a significant element of U.S. strategy for deterring Chinese and North Korean aggression, as well as reassuring other Asian powers of U.S. protection, to avert a destabilizing arms race.¹⁵ This includes explicit or implicit threats of force in response to specific crises or contingencies, such as during diplomatic confrontations with North Korea, in addition to more routine displays of force, such as free navigation exercises in the South China Sea. As I have argued:

Decisions to go to war or to send military forces into hostilities are immensely and uniquely consequential, so it is no surprise that debates about constitutional war powers occupy so much attention. But one of the most common and important ways that the United States uses its military power is by threatening war or force—to coerce, to deter, to bargain, to reassure—and the constitutional dimensions of that activity have received almost no scrutiny or even theoretical investigation.¹⁶

There are no formal legal checks on the president's power to threaten force and, given the size of the standing U.S. military arsenal, that power to threaten force is immense.

There are, however, significant political checks on the president's discretion to use military force, and these checks also affect how the president wields threats of force. As Jack Goldsmith and I have argued:

The United States has a long history of presidential military initiative borne of responsibility and opportunity, and congressional acquiescence borne of irresponsibility and collective action hurdles. This historical pattern of executive unilateralism has not meant that the president is unchecked. It has simply meant that the checks were political, not legal, and were imposed by the threat of congressional retaliation if the president's initiatives go terribly wrong, and by the U.S. public through electoral accountability.¹⁷

In recent years there has been a wave of political science scholarship substantiating these checks.

Douglas Kriner, for example, argues that although there has been much literature devoted to claims of an imperial presidency, Congress exerts significant influence over the use of force. Congressional politics affect both the frequency with which presidents use force abroad and the probability with which they respond militarily to crises. There are many ways in which Congress influences presidential uses of force, and presidents anticipate congressional reactions, such as introduction of legislation to authorize or curtail a use of force; congressional oversight hearings; and public debate over military policymaking.¹⁸ Congressional action or inaction also sends signals about domestic resolve to foreign parties—including adversaries and allies—thereby affecting the president's calculus regarding force.¹⁹

In their study of congressional efforts to constrain presidential war powers during the post-World War II era, William Howell and Jon Pevehouse “discover considerable evidence that checks and balances, though diminished, persist.”²⁰ Although they concede the president’s unilateral powers are very substantial, they argue that, under certain conditions, the congressional checks are constraining. Moves by members of Congress to introduce bills, pass resolutions, hold hearings, and make public declarations can increase political costs for presidents, and even sometimes impose legal limits on force.²¹ Like Kriner, they also find that congressional opposition to military force reduces the president’s ability to signal resolve to allies and influence public opinion.²²

Besides congressional political checks, internal process within the U.S. executive branch exerts significant influence on presidential use of force. The same post-World War II period in which constitutional practice shifted toward unilateral presidential power also included the creation and institutionalization of formal interagency deliberative processes for national security and crisis decision-making. The 1947 National Security Act created the modern Department of Defense, Central Intelligence Agency, and National Security Council (NSC). Although the NSC has evolved, and the details of its composition and organization vary from presidential administration to administration, it helps structure deliberation on possible uses of force to ensure participation of key departments and agencies, as well as the president’s principal military advisers.²³

It is also through these interagency processes that the executive branch interprets international law in this area. The recently published Department of Defense Law of War manual describes the process this way:

Jus ad bellum issues might raise questions of national policy that, in the Executive Branch, would be decided by the President. In U.S. practice, legal advice provided to national-level principal officials on such issues generally would need to be addressed through interagency discussions coordinated by the legal adviser to the National Security Council, including consultation and coordination among senior counsel of relevant U.S. departments and agencies.²⁴

Alliance relationships also influence presidential uses of force and are among the considerations that inform executive branch deliberations. On the one hand, a general approach to defense planning that emphasizes military primacy has meant that the United States has great flexibility in wielding its armed might.²⁵ Moreover, the U.S. executive branch can make decisions on the use of force more quickly and dexterously than can allies with more cumbersome approval processes or, as in the case of Japan, stricter restrictions on what military forces can or cannot be called upon to do.

On the other hand, coalition building and maintenance is often an important strategic and political concern, constraining U.S. military actions or threats of military force. Military-to-military ties mean that allies' interests will also generally exert constant, even if sometimes subtle or indirect, influence on executive branch deliberations through the departments involved in maintaining and exercising those relationships. This is a ripe area for further research, especially with regard to how different alliance relationships and structures feed into U.S. decision-making processes, particularly during crises.

North Korea and Taiwan Strait Tensions

Recent tensions and negotiations over North Korea's nuclear weapons development, as well as concerns about China's ambitions toward Taiwan, help illustrate many of the issues discussed above.

As to North Korea, although each of the previous three presidents has reportedly considered military strikes against North Korea's nuclear capabilities, president Trump was initially, and prior to his summits with Kim Jong Un, much more open about the possibility of such action than his predecessors. Some members of Congress publicly questioned or pushed back against Trump's bellicosity, including suggesting that he lacks constitutional authority to take actions without congressional authorization, but Congress as a body showed little willingness or capacity to apply more than informal and diffuse political pressure against a possible rush to war.²⁶

As to the international law dimensions of the North Korea situation, the Trump administration has been publicly reticent.²⁷ At a 2017 Senate hearing, the Secretaries of Defense and State confirmed under questioning that the United States lacked international legal authority to strike North Korea absent an "imminent threat," but they declined to clarify how they interpreted that standard in the North Korea context.²⁸ President Trump's advisors had—again, prior to the presidential summit meetings between the American and North Korean leaders—emphasized that the window is closing for action before North Korea develops the capability to attack the continental United States with nuclear weapons. It seems likely that the current U.S. administration interprets "imminence" significantly more broadly than its East-Asian allies, especially Japan.

Besides the prospect of actual military intervention abroad, the North Korea situation also illustrates related presidential powers for managing alliances that can have signaling effects. As commander in chief who can deploy forces abroad, the president can also withdraw them. President Trump has hinted at his interest in bringing U.S. troops home from South Korea, though Congress recently passed a statute limiting his ability to do so (and the constitutionality of that restriction is uncertain). The president can also cancel or downgrade military exercises, as President Trump has done with U.S.-South Korean military exercises as part of his

diplomacy toward the peninsula.²⁹

The Taiwan Strait is another hotspot that highlights the vast scope of presidential powers, and especially the wide latitude presidents have to engage in demonstrative shows of force. Ever since the United States normalized relations with China in the 1970s, Congress has generally taken a hard line in favor of defending Taiwan, so there has not been much political or legislative constraint from Congress on strong executive action. In 1995, for example, after China engaged in missile tests and other actions to intimidate Taiwan, President Clinton ordered additional naval forces to the Taiwan area and sent some of them through the Taiwan Strait. The Trump administration has also used naval deployments to reinforce and signal American commitments to prevent Chinese military actions against Taiwan (as well as China's assertions of control in areas of the South China Sea). As with South Korean military exercises, displays of force like this can reassure and bolster defense of partners, but they can also provoke escalatory responses. Such moves are almost exclusively within the president's discretion, at least in the absence of direct legislative restrictions to the contrary.

Conclusion

However the U.S. constitutional system was originally intended to constrain formally the president's military authority, the modern president in practice wields tremendous power and discretion to initiate military operations. The system has adapted over time to major shifts in American power and grand strategy. Although formal, legal checks on the president's use of force rarely come into play, Congress nevertheless retains some political power to influence presidential decision-making, and internal bureaucratic processes also constrain presidential action. ■

Matthew C. Waxman is the Liviu Librescu Professor of Law and the faculty chair of the National Security Law Program at Columbia Law School.

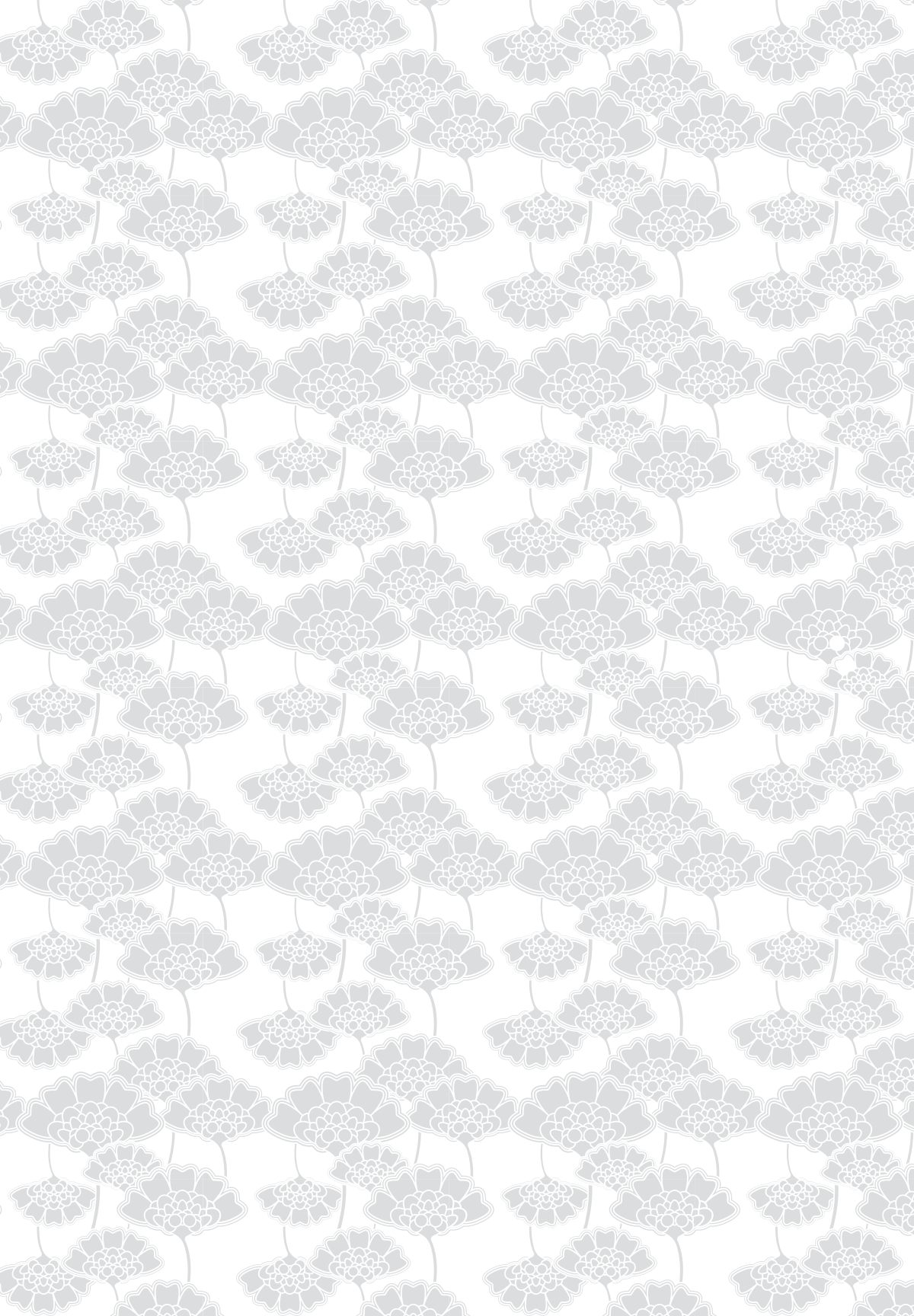
Waxman is an expert in national security law and international law, including issues related to executive power; international human rights and constitutional rights; military force and armed conflict; and terrorism. He clerked for Supreme Court Justice David H. Souter and Judge Joel M. Flaum of the 7th U.S. Circuit Court of Appeals.

Before joining the Law School faculty, he served in senior positions at the State Department, the Department of Defense, and the National Security Council. Waxman was a Fulbright Scholar to the United Kingdom, where he studied international relations and military history. He is a member of the Council on Foreign Relations, where he also serves as Adjunct Senior Fellow for Law and Foreign Policy, and he is the co-chair of the Cybersecurity Center at the Columbia Data Science Institute.

He holds a J.D. from Yale Law School.

- 1** For a compilation of uses of U.S. military force, see Barbara Salazar Torreon, Cong. Research Serv. Report, *Instances of Use of United States Armed Forces Abroad, 1789-2016* (2016).
- 2** Louis Henkin, *Foreign Affairs and the U.S. Constitution* 49 (2d ed. 1996).
- 3** See Stephen M. Griffin, *Long Wars and the Constitution* 11–51 (2013); Arthur M. Schlesinger, Jr., *The Imperial Presidency* 135 (2004).
- 4** Schlesinger, *supra* note 3, at 128.
- 5** See Authority to Use Military Force in Libya, 35 Op. O.L.C. 1 (2011).
- 6** Treaty of Mutual Cooperation and Security Between the United States of America and Japan, Japan-U.S., art. V, Jan. 19, 1960, 11 U.S.T. 1632, T.I.A.S. No. 4509.
- 7** Mira Rapp-Hooper & Matthew C. Waxman, *Presidential Alliance Powers*, 42 Wash. Q. 67 (2019).
- 8** *Id.* at 68.
- 9** See Matthew C. Waxman, *Remembering Eisenhower's Formosa AUMF*, Lawfare Blog (Jan. 29, 2019), <https://www.lawfareblog.com/remembering-eisenhowers-formosa-aumf>.
- 10** See John Hart Ely, *War and Responsibility: Constitutional Lessons of Vietnam and Its Aftermath* 12–46 (1993).
- 11** War Powers Resolution, 50 U.S.C. §§ 1541–1548 (2006).
- 12** *Id.* § 1541(a).
- 13** On Congress's failed effort to correct this with the War Powers Resolution, see Michael J. Glennon, *Constitutional Diplomacy* 87–111 (1990); Jack Goldsmith & Matthew C. Waxman, *The Legal Legacy of Light-Footprint Warfare*, 39 Wash. Q. 7, 13–14 (2016).
- 14** Matthew C. Waxman, *Regulating Resort to Force: Form and Function of the UN Charter*, 24 Eur. J. Int'l L. 151 (2013).
- 15** See Joint Chiefs of Staff, *The National Military Strategy of the United States of America: Redefining America's Military Leadership* 14 (2011); Jane Perlez, *Cancellation of Trip by Obama Plays to Doubts of Asia Allies*, N.Y. Times (Oct. 4, 2013), <https://www.nytimes.com/2013/10/05/world/asia/with-obama-stuck-in-washington-china-leader-has-clear-path-at-asia-conferences.html>.
- 16** Matthew C. Waxman, *The Power to Threaten War*, 123 Yale L.J. 1635 (2014).
- 17** Goldsmith & Waxman, *supra* note 13, at 17.
- 18** Douglas L. Kriner, *After the Rubicon: Congress, Presidents, and the Politics of Waging War* 12 (2010).
- 19** *Id.*
- 20** William G. Howell & Jon C. Pevehouse, *While Dangers Gather: Congressional Checks on Presidential War Powers* 6 (2011).
- 21** *Id.* at 10.
- 22** *Id.* at 32.
- 23** For a comparison discussion of Japanese government decision-making structures, see Adam P. Liff & Andrew S. Erickson, *From Management Crisis to Crisis Management? Japan's Post-2012 Institutional Reforms and Sino-Japanese Crisis (In)stability*, 40 J. Strategic Stud. 604 (2017).
- 24** Dep't of Def., *Law of War Manual* 39–40 (2016).

- 25** Hal Brands, *Choosing Primacy: U.S. Strategy and Global Order at the Dawn of the Post-Cold War Era*, 1 Tex. Nat'l Security Rev. 9 (2018), available at <https://tnsr.org/2018/02/choosing-primacy-u-s-strategy-global-order-dawn-post-cold-war-era-2/>.
- 26** Amber Philips, *Can Congress Stop Trump from Launching a Nuclear Attack on North Korea?*, Wash. Post (Aug. 11, 2017), https://www.washingtonpost.com/news/the-fix/wp/2017/08/11/can-congress-stop-trump-from-launching-a-nuclear-attack-on-north-korea/?utm_term=.41e8fec04d73.
- 27** For a discussion of Japanese government positions on some of these issues, see Masahiro Kurosaki, *The 'Bloody Nose' Strategy, Self-Defense and International Law: A View from Japan*, Lawfare Blog (Feb. 15, 2018), <https://www.lawfareblog.com/bloody-nose-strategy-self-defense-and-international-law-view-japan>.
- 28** Rebecca Kheel, *Mattis, Tillerson: No Authority for Military Action in North Korea Outside 'Imminent Threat'*, The Hill (Oct. 30, 2017), <http://thehill.com/policy/defense/357927-mattis-tillerson-no-authority-for-military-action-in-north-korea-outside>.
- 29** Rapp-Hooper & Waxman, *supra* note 7, at 76.





The U.S.-Japan Alliance in Legal Context

PART III

The background of the cover features a dark blue, monochromatic illustration of a steamship at sea. The ship is positioned in the middle ground, with its smokestack emitting a large, billowing cloud of white smoke. In the foreground, several figures are visible, appearing to be on a beach or a small boat, looking towards the ship. The overall style is reminiscent of a historical or maritime theme. The top of the cover is decorated with a repeating pattern of stylized, light-colored flowers or leaves.

Hideshi Tokuchi

National Graduate
Institute for
Policy Studies

Japan-U.S. Alliance as a Maritime Alliance and International Law

Introduction

Japan is a small and densely populated country in an unstable security environment in Northeast Asia. If Japan were to be invaded and the invading country repelled, the consequence of the war would be disastrous. For Japan, winning the war is not victory. That is why deterrence is the first priority of Japan's national security and defense policy.

However, deterrence is not guaranteed. Deterrence is ineffective if the deterring country does not succeed in communicating its intention correctly, inviting miscalculation on the part of the opponent. Communication between adversaries is not easy even if both of them are rational actors. This is particularly the case because of lack of correct information and difference of values, cultures and political institutions. Miscommunication is to an extent inevitable because of the anarchical nature of the international community. Furthermore, even if communication is successful, deterrence will not necessarily be effective. Once aggression takes place, the status quo ante cannot be restored by reprisal or punishment. So, reprisal or punishment after aggression may not be an effective solution. In addition, deterrence is invisible. All of us know from our experience in our daily life that threats to retaliate may be successful in preventing assault, but it is hard to know whether or not deterrence is working in a specific situation. The effectiveness of deterrence is a serious question in specific circumstances.

This question becomes more serious when a sovereign state has to depend on an alliance to achieve its national security. Deterrence is a tactic that prevents one's opponent from taking action against one's interests. Deterrence to prevent one's opponent from taking action against the interests of a country other than the deterring power is called "extended deterrence". A typical way to ensure extended deterrence is through an alliance.

It is easy to cast doubt on the credibility of the U.S. commitment to come to Japan's aid in the event of an armed attack against Japan; one could ask, "Is

the U.S. willing to risk San Francisco and Los Angeles to defend Tokyo?” This argument sounds plausible. Complete trust cannot be expected, for, after all, allies are independent sovereign states. The answer to this question seemed relatively easy until recently, because of the magnitude of nuclear weapons and because of our experience with the mutual deterrence between the U.S. and the former Soviet Union in the Cold War days. The said question continued to be asked, and we had no reason to doubt the right answer.

However, today we have to think about a more fundamental issue: that of the American president’s view of the alliance. We should recall the remarks Defense Secretary James Mattis made in his resignation letter: “While the U.S. remains the indispensable nation in the world, we cannot protect our interests or serve that role effectively without maintaining strong alliances and showing respect to those allies.”¹ As suggested in the letter, its addressee does not understand the value of U.S. alliances although having allies is a great soft power. Although an alliance is mutual cooperation from which all of its members benefit, the U.S. president does not have a correct view on these points. Mutual cooperation does not necessarily mean that the alliance is symmetrical. A correct understanding of the division of roles and missions between the alliance partners is indispensable for the management of the alliance, as well as for maintaining and showing the robustness of the alliance. From this point of view, U.S. President Donald Trump’s remarks in his press conference in Osaka, Japan on June 29, 2019, in response to the question if he was thinking about withdrawing from the Japan-U.S. Security Treaty is quite problematic.² The question of extended deterrence has to deal with this new and more serious situation. That is the dilemma we confront right now.

Nonetheless, we ought to stop agonizing over this question. We should make a distinction between the words of the president himself and the actions of the U.S. government as a political institution. The distribution of power among the branches of the U.S. government, provided for by the U.S. Constitution, is at work. The Constitution is a guarantor for the U.S. president not to be a dictator. If the dilemma continues, we ought not to lament or criticize the situation, but rather to strengthen the alliance and to make the alliance commitment more effective. There is no alternative solution, as the alliance is the most reliable instrument of power-balancing in the heavily armed and volatile Indo-Pacific region.

Another serious and related question is about the uncertainty concerning the rules-based liberal international order. This order is fragile for a number of reasons. First of all, it is basically a Western idea. It is easily exposed to the question of whether the order has become truly universal even in the post-Cold War era. In addition, the liberal order helps produce diversity of values and of ways of life, both nationally and internationally. It accelerates policy changes, for example, on migration and same-sex marriage. It erodes the stability of societies in which traditional values are dominant, and brings uncertainty and anxiety to the minds

of those who are not accustomed to such an enormous shift. Such uncertainty and anxiety raises doubts about the order. Furthermore, the idea of the rules-based liberal international order reflects the American political system. Not all peoples necessarily like the American flavor, although Masataka Kosaka wrote near the end of the Cold War that if given the right to choose, the public tends to choose Americanism, citing Denis Brogan.³ Though fragile, the rules-based liberal international order contributes to the stability and growth of the world by connecting the actors more closely and making their behavior more predictable; thus its value cannot be underrated.

The question of how to address the challenges to the established rules of the international community is a major issue for Japan and the U.S., as both countries have benefited from the rules-based order for their survival and prosperity. As both countries are maritime nations and as the Indo-Pacific region is a huge maritime area, the task of upholding the international rules to govern the maritime commons should be critically important for the Japan-U.S. Alliance in the coming age. China's maritime expansion in East Asia has caused many problems to the rules-based regional order at sea.

No matter how Japan, the U.S. and other regional countries describe the region—the Asia-Pacific or the Indo-Pacific—the sea cannot be separated. As seagoing officers have kept saying, the sea is one.⁴ As the sea is one, the rule to govern the sea must be one. Otherwise, connectivity of the maritime space cannot be ensured. The importance of maritime transit for mass transportation is incomparable to land and air transit even in this high-tech age. As “Indo-Pacific” literally connects the world's largest and third largest oceans, this term symbolizes the physical fact of the global ocean's unity and the importance of the unity for the region much more explicitly than “Asia-Pacific,” which connects land and sea.

As the alliance is a traditional tool of balance of power, the first priority of the Japan-U.S. Alliance in East Asian (or Indo-Pacific) maritime security is to restore the regional balance of power, particularly at sea. The fact that China is more assertive against neighboring countries' public vessels and fishing boats in the South China Sea than in the East China Sea indicates that difference of the balance of power matters. While Japanese and American military presence in Northeast Asia is robust, there is no permanent presence of the U.S. military in Southeast Asia, and the military capabilities of most of the Southeast Asian countries are very limited. The Japan-U.S. Alliance cooperation to enhance the presence of the alliance in the South China Sea and to extend their helping hands to Southeast Asian developing countries for maritime security capacity building is critically important.

However, a balance of power is just one factor to consider in international security even under the theory of realism. James Mayall is right in stating that international law is the bedrock institution on which the idea of an international

society stands or falls.⁵ Looking back into the interwar period, E.H. Carr stated, “Power is always an essential element of politics,” and “Power is a necessary ingredient of every political order,”⁶ but at the same time he also argued, “If, however, it is utopian to ignore the element of power, it is an unreal kind of realism which ignores the element of morality in any world order.”⁷ Even though morality and law are not the same, Carr’s view on morality can be applied to international law as well because, as he says, no political society can exist without law.⁸

Therefore, the authority of international law must be asserted. The Japan-U.S. Alliance must cover international legal cooperation in order to effectively counter China’s influence operations related to maritime security in East Asia. The Government of Japan stated in the new National Defense Program Guidelines (NDPG) of December 2018, “The Japan-U.S. Alliance plays a significant role for peace, stability and prosperity of not only Japan but also the Indo-Pacific region and the international community.” As the Alliance plays such a role, legal cooperation should be conducted in close coordination with political, diplomatic and military cooperation.

The South China Sea Issue

Japan has a number of reasons to be concerned about the maritime security of the South China Sea. The South China Sea is increasingly important, as it connects the Pacific and Indian oceans, which in total occupy two thirds of the world’s sea surface. China uses maritime law enforcement ships to control access to and from islands and other features in the South China Sea, nonviolently, daring other states to fire the first shot.⁹ In 2012, twelve maritime militia trawlers were netting tons of endangered species at Scarborough Shoal, and when a Philippine vessel boarded two of the trawlers, militiamen onboard radioed for help, and the China Coast Guard (CCG) rode to the rescue. According to Andrew Erickson, the Chinese researcher Zhang Jie of the Chinese Academy of Social Sciences uses the phrase “Scarborough Shoal Model,” an indication of the premeditated tactics China has developed to increase its maritime control. Erickson also points out Zhang’s emphasis of the model being explored vis-à-vis Chinese gray zone incursions in Japan’s waters surrounding the Senkaku Islands.¹⁰ Thus, the issue of the East China Sea, which is directly linked to the security of Japan, is closely connected to the South China Sea disputes.

The South China Sea issue is often discussed in relation to the principle of freedom of navigation. China questions if there is any problem with freedom of navigation in the South China Sea. Liu Xiaoming, China’s ambassador to the UK, wrote, “Amid recent hype about ‘freedom of navigation’ in the South China Sea, the U.S., an outspoken opponent of China’s ‘militarisation’, has been flexing its own

military muscle by sending naval vessels and aircraft carriers to the region.” The ambassador further asserted, “The reality is that more than 100,000 merchant ships pass through these waters every year and none has ever run into any difficulty with freedom of navigation.”¹¹ I strongly wonder if this is a correct message. The international community is questioning whether the Chinese side respects the freedom of navigation in international waters. It appears China is talking about innocent passage through territorial waters, based on their own unilateral and unjustifiable claim of sovereignty. If China insists on its claim of the Nine-Dash Line, this would mean there are almost no international waters left in the South China Sea.

China will repeat the “100,000 ships” assertion again and again if it remains unrefuted. In fact, China’s Defense Minister General Wei Fenghe said in his speech at the Shangri-La Dialogue in 2019, “The current situation in the South China Sea is generally stable and positive. It is attributable to the joint efforts of the countries in the region. However, there are always people trying to make profits by stirring up troubles in the region. ... Who is threatening security and stability in the South China Sea? Over 100,000 ships sail through the South China Sea every year. None has been threatened. The problem, however, is that in recent years some countries outside the region come to the South China Sea to flex muscles in the name of freedom of navigation. The large-scale force projection and offensive operations in the region are the most serious, destabilizing and uncertain factors in the South China Sea.”¹² China’s neighbors are aware of what has really happened in the South China Sea, but those far away from China may not be aware of the reality. Thus, Japan, the U.S. and other countries upholding the rules-based liberal international order at sea should continue to speak up unequivocally and with a single voice against China’s assertion.

With regard to the issue of freedom of navigation, James Kraska and Raul Pedrozo argue, “Chinese defense officials have repeatedly stated that freedom of navigation in the South China Sea is not at risk, and that the United States ‘should stop playing up the issue.’ These assurances are pointless because China interprets freedom of navigation as applying only to civilian or commercial ships.”¹³ They are right, but, as mentioned above, General Wei only said “100,000 ships.” He did not add “merchant,” whether intentionally or not. I assume that both Ambassador Liu and General Wei used the term “freedom of navigation” not as a legal term, but merely to express the peacetime situation in an imprecise way.

Incidentally, China has recently grown more silent about its claim of the Nine-Dash Line. Presumably it is because of the international community’s efforts to unite against the Chinese claim. In other words, we can reasonably assume that our legitimate views based on the good-faith interpretation of international law raised the reputation cost to China. This is a benefit of international law.¹⁴

A Chinese researcher, Zhang Junshe, expressed a view similar to that

of Ambassador Liu, writing, “It is ironic that the biggest rogue disregarding international law is pretending to be a flag-bearer in this term. Washington has a blemished record of contempt of the International Court of Justice (ICJ) and its decision in the 1986 Nicaragua vs. U.S. case. The ICJ ruled that the U.S. had violated international law by supporting rebels in Nicaragua and mining Nicaragua’s harbors. The U.S. refused to participate in the case and blocked the enforcement of the judgment by the United Nations Security Council. Despite the veneer of international law, the U.S. actually believes in nothing but ‘might makes right’. As a non-signatory of the UN Convention on the Law of the Sea (UNCLOS), the U.S. groundlessly demands that China comply with the Convention. Although vowing to protect freedom of navigation from China, the U.S. cannot find one example of China blocking international waterways in the South China Sea.”¹⁵ This opinion shows that the U.S. refusal to participate in the ICJ case in the mid-1980s now militates against the U.S.. It is considered another example of reputation cost raised by not abiding by the rules of international law.¹⁶ As the U.S. did show up before the ICJ in the preliminary defense phase, the U.S. attitude toward the ICJ in the Nicaragua vs. U.S. case should not be considered the same as China’s attitude toward the Permanent Court of Arbitration on the South China Sea dispute, but the U.S. has to be aware that its attitude toward the ICJ in the past makes the position of the U.S. and other like-minded countries on the 2016 Award of the Permanent Court of Arbitration less convincing.

The East China Sea Issue

The relationship between Japan and China is improving. Three meetings between Japan’s Prime Minister Shinzo Abe and China’s President Xi Jinping in 2018, including the first official visit of Japan’s Prime Minister to China in the past seven years, epitomize the shift of the bilateral relation to a course of mutual cooperation. It is often said that this improvement is due to the confrontation between China and the U.S., but as Japan and China are eternal neighbors, a stable relationship should be established, regardless of the state of U.S.-China relations.

The apparent rapprochement notwithstanding, no major security issues involving the two countries have been resolved yet. In the Japan-China prime ministers’ meeting on October 26, 2018 in Beijing, Prime Minister Abe conveyed Japan’s understanding of the East China Sea issue based on the recognition that there will be no genuine improvement in the Japan-China relationship without stability in the East China Sea. This view was confirmed by Prime Minister Abe and President Xi when they met on the margins of the G-20 Summit Meeting in Buenos Aires on November 30, 2018. Politically, it is good that on this basis Japan and China now agree on the importance of making concrete progress in the area

of maritime security. However, no substantial progress has been seen so far, as Chinese public vessels' operations in the vicinity of the Senkaku Islands indicate.

As of July 15, 2019, Chinese public vessels had entered the contiguous zone around the Senkaku Islands every day for 64 straight days from April 12 to June 14 and for 30 straight days from June 16 to July 15. More problematically, the frequency of Chinese public vessels' intrusion into the Japanese territorial waters around the Islands shows a certain pattern. The statistical data of the past three years shows that from November 2016 to July 2017 the frequency of intrusions was three per month (except February 2017 when it was two), that from August 2017 to August 2018 the number decreased to two (except October 2017 when it was only one), that from September to November 2018 the number was one, and that there was no intrusion in December 2018. However, there were three intrusions every month from January to April 2019, four intrusions in May, two in June, and two between July 1 and July 15.¹⁷ It is highly possible that the Chinese government has been trying to accumulate *faits accomplis* through these regular intrusions, while showing some willingness to improve the overall relationship.

The U.S. Government has made it clear that Article 5 of the Security Treaty covers the Senkaku Islands, as per the remarks of President Donald Trump and key figures of his administration.¹⁸ However, China's approach seems to be intended to achieve its territorial claim by circumventing the U.S. defense commitment.

Repeated intrusion of Chinese public vessels into Japanese waters surrounding the Senkaku Islands is not considered to be an exercise of the right of innocent passage. It is a violation of Japan's sovereignty, yet it fails to amount to an armed attack against Japan.

In this case, it is obvious that Japan cannot exercise the right of self-defense based on Article 51 of the UN Charter. Then, how about the right of self-defense in customary international law? According to the ICJ's decision of 1986 on the *Nicaragua v. United States* case, self-defense is only available against use of force that amounts to an armed attack under customary international law as well as under Article 51. A use of force of a lesser degree of gravity could justify proportionate counter-measures on the part of the victim state, according to the decision. It is clear in the decision that collective countermeasures cannot involve use of force, but the decision is not clear on whether the victim state itself can use force as individual proportionate counter-measures.¹⁹

The new NDPG states Japan's response to "gray zone" situations, as follows: "SDF will, in coordination with the police and other agencies, immediately take appropriate measures in response to actions that violate Japan's sovereignty including incursions into its territorial airspace and waters." This is just a general principle to guide the relevant organizations. As the essential role of the NDPG is to define the roles of Japan's military defense capability and to establish the goal of defense force development, one cannot

expect more specific guiding principles in the NDPG for operational cooperation and coordination of the relevant organizations.

Nonetheless, the awareness of the necessity and urgency to address maritime gray zone situations is increasing among policy experts in Japan.²⁰ In addition, American experts have begun to take up this issue as a matter of Japan-U.S. Alliance cooperation. According to the CSIS report “More Important than Ever,” one of the challenges the alliance faces is that “military competitors are narrowing the allies’ military edge. China, in particular, has engaged in rapid military modernization and embraced ‘gray zone’ operations, which have reduced the gap between it and the United States, forcing the alliance to reassess its ability to deter and defeat aggression.”²¹ Based on this recognition, the report makes a recommendation: “the allies should consider involving U.S. forces earlier in so-called ‘gray zone’ incidents, which include aggression that occurs below the level of major conflict. This step would make clear that any acts of aggression would trigger deeper alliance cooperation, regardless of whether they cross the threshold of an armed attack under Article V of the U.S.-Japan Security Treaty. Therefore, the allies should engage in more structured combined planning, pursuant to relevant legal restrictions.”²²

The alliance cooperation does not necessarily have to entail the use of force. There are many things that can be done collectively to address “gray zone” situations. Japan and the U.S. should work together more extensively to address these serious challenges, and communicate strategically with China in international legal terms. As the basis for this effort to counter China, Japan and the U.S. should exchange candid views on the concept of “proportionate counter-measures.” ■

Hideshi Tokuchi joined the Defense Agency (the predecessor of the Ministry of Defense) of Japan in 1979 as a civilian and served as the nation's first Vice-Minister of Defense for International Affairs from July 2014 to October 2015 after completing several senior assignments at the Ministry of Defense, including as Director-General of the Operations Bureau, of the Personnel and Education Bureau, of the Finance and Equipment Bureau, and of the Defense Policy Bureau.

During most of his service, Tokuchi focused on Japan-U.S. defense cooperation, security-related legislation, defense buildup programs, and operations of the Japanese Defense Forces. He participated in the review work of the "Guidelines for Japan-U.S. Defense Cooperation" twice (in 1997 and 2015), and in the establishment of the "National Defense Program Guidelines" twice (in 2004 and 2013), and also in security-related legislation, including Peace-Keeping Operations Law, a set of legislation to deal with contingency, Counter-Piracy Law, and most recently the new security legislation to put the new interpretation of the Japanese Constitution into practice.

Tokuchi is a visiting professor of the National Graduate Institute for Policy Studies (GRIPS) and of the National Defense Academy of Japan. He received his Bachelor of Laws degree from the University of Tokyo in 1979, and received a Master of Arts in Law and Diplomacy (M.A.L.D.) degree from the Fletcher School of Law and Diplomacy in 1986.

- 1 Daniel Bush, *Read James Mattis' Full Resignation Letter*, PBS News Hour (Dec. 28, 2018), <https://www.pbs.org/newshour/politics/read-james-mattis-full-resignation-letter> (citing Letter from James N. Mattis, U.S. Sec'y of Def., to Donald J. Trump, U.S. President (Dec. 20, 2018) (on file with author), available at <https://d3i6fh83elv35t.cloudfront.net/static/2018/12/mattis-letter2.pdf>).
- 2 President Trump said: "No, I'm not thinking about that at all. I'm just saying that it's an unfair agreement. And I've told him [Japan's Prime Minister Shinzo Abe] that for the last six months. I said, 'Look, if somebody attacks Japan, we go after them and we are in a battle — full force in effect.' We are locked in a battle and committed to fight for Japan. If somebody should attack the United States, they don't have to do that. That's unfair." Donald J. Trump, U.S. President, Remarks by President Trump in Press Conference in Osaka, Japan (June 29, 2019), available at <https://www.whitehouse.gov/briefings-statements/remarks-president-trump-press-conference-osaka-japan/>.
- 3 Masataka Kosaka, *Gendai no Kokusai Seiji* (現代の国際政治) [Contemporary International Politics] 215 (Kodansha 1989).
- 4 James Stavridis, *Sea Power: The History and Geopolitics of the World's Oceans* 2 (2017).
- 5 James Mayall, *World Politics: Progress and its Limits* 94 (2000).
- 6 E.H. Carr, *The Twenty Years' Crisis 1919-1939, An Introduction to the Study of International Relations* 97, 213 (2001).
- 7 *Id.* at 216.
- 8 *Id.* at 164.
- 9 Ryan Martinson, *China's Great Balancing Act Unfolds: Enforcing Maritime Rights vs. Stability*, Nat'l Interest (Sept. 11, 2015), <http://nationalinterest.org/feature/chinas-great-balancing-act-unfolds-enforcing-maritime-rights-13821>.
- 10 The South China Sea's Third Force: Understanding and Countering China's Maritime Militia: Testimony Before the Subcomm. on Sea Power & Projection Forces of the H. Armed Serv. Comm., 114th Cong. 4–5 (2016) (statement of Andrew S. Erickson, Professor of Strategy, Naval War College).
- 11 Liu Xiaoming, *China will not tolerate U.S. military muscle-flexing off our shores*, Guardian (June 27, 2018), <https://www.theguardian.com/commentisfree/2018/jun/27/china-not-tolerate-trump-military-muscle-south-china-sea#img-2>.
- 12 General Wei Fenghe, State Councilor & Minister of Nat'l Def. of China, Address at the 4th Plenary Session of the International Institute for Strategic Studies Shangri-La Dialogue (June 2, 2019), available at <https://www.iiss.org/-/media/files/shangri-la-dialogue/2019/speeches/plenary-4---general-wei-fenghe-minister-of-national-defence-china-transcript.ashx>.
- 13 James Kraska & Raul Pedrozo, *The Free Sea: The American Fight for Freedom of Navigation* 261 (2018).
- 14 Anzen Hoshō-gaku Nyūmon (安全保障学入門) [Introduction to Security Studies] 371–72 (Yasuhiro Takeda & Mataka Kamiya eds., Aki Shobo 5th ed. 2018); Yasuaki Onuma, *Kokusai-hō* (国際法) [International Law] 61–62 (Chikuma Shobo 2018).
- 15 Zhang Junshe, *South China Sea ruling: Views from China and the U.S. on the South China Sea ruling*, Strait Times (July 15, 2016), <https://www.straittimes.com/opinion/views-from-china-and-the-us>.

16 Introduction to Security Studies, *see supra* note 14, at 371–72.

17 “The numbers of Chinese government and other vessels that entered Japan’s contiguous zone or intruded into territorial sea surrounding the Senkaku Islands Kaijō Hoan-chō (海上保安庁) [Japan Coast Guard], <https://www.kaiho.mlit.go.jp/mission/senkaku/senkaku.html> (last visited March 11, 2020).

18 The Joint Statement of President Trump and Prime Minister Abe on February 10, 2017, states: “The two leaders affirmed that Article V of the U.S.-Japan Treaty of Mutual Cooperation and Security covers the Senkaku Islands. Shortly before the summit meeting, U.S. Defense Secretary Mattis had stated to Prime Minister Abe on February 3 in Tokyo that the Senkaku Islands are in the territories under the administration of Japan, and are within the scope that is covered by Article 5 of the Japan-U.S. Security Treaty.” See Press Release, Ministry of Foreign Affairs of Japan, Joint Statement (February 10, 2017), available at <https://www.mofa.go.jp/files/000227768.pdf>.

19 Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ¶¶ 211, 249 (June 27).

20 See the policy recommendations by several Japanese think tanks in 2018, particularly Nakasone Yasuhiro Peace Inst., Umi to Sora no Gurēzōn Jitai e no Taisho: Sono Mondai to Taisaku (海と空のグレーゾーン事態への対処 - その問題と対策 -) [Response to Maritime and Air Gray Zone Situations: Issues and Measures] (2018), available at http://www.iips.org/research/grayzone_teigen.pdf.

21 Richard L. Armitage & Joseph S. Nye, Ctr. for Strategic & Int’l Studies, More Important Than Ever: Renewing the U.S.-Japan Alliance for the 21st Century 2 (2018).

22 *Id.* at 8.



Julian G. Ku

Hofstra University

How the Law of Collective Self-Defense Undermines the Peace and Security of the Taiwan Strait

Introduction

There are few principles more central to the United Nations Charter than its prohibition on a state's use of military force against another state without authorization of the Security Council or without the justification of self-defense. The UN Charter's legal prohibition on the routine use of force has been lauded as a cornerstone of the post-World War II order.¹ Yet, as this essay will suggest, strict adherence to that principle in managing the complex relations between China and Taiwan will actually encourage the aggressive use of military force by China against Taiwan and discourage outside powers such as the United States from intervening to prevent such military actions.

The possibility of a Chinese invasion of Taiwan is quite real. In July 2019, China's Ministry of National Defense issued a national defense strategy paper reiterating that it was prepared to use military force to prevent Taiwan's secession from China.²

When China then followed up the paper's release with military naval exercises off the northeastern and southwestern coasts of the island, it reinforced the view that China remains prepared to use military force against Taiwan to prevent formal independence.²

While China has been clear and consistent in its willingness to use military force against Taiwan, the attitude of Taiwan's allies, especially the United States, has been less clear. The U.S. government has continued to sell arms to Taiwan to help it defend itself and has declared its opposition to coercive reunification of China and Taiwan. At the same time, the U.S. has studiously avoided recognizing Taiwan as an independent state and carefully sidestepped questions of whether it would use military force to support Taiwan in the event of a Chinese invasion. U.S. administrations also have never ruled out such a military intervention.³

Though U.S. analysts and observers have long debated whether the U.S. should use force to defend Taiwan in the event of a military invasion by China, few

of those analysts have considered the legality of such an action under international law.⁴ To be sure, international law may not be the most important factor shaping any decision by U.S. policymakers considering a military intervention over Taiwan. As some commentators have noted, the U.S. has been willing to use military force on numerous occasions when its legality was questionable.⁵ But the international lawfulness of such an act will, at the very least, shape the attitudes and actions of the United States and its allies.

Most scholars that have considered the international legality of defending Taiwan have focused on Taiwan's contested international legal status. As a state lacking recognition from most countries in the world, some scholars have argued that the Chinese government is correct to treat a China-Taiwan conflict as a domestic conflict where foreign military intervention would be an unlawful act of aggression.⁶ Because the statehood question seems paramount, scholars seeking to defend the legality of foreign military action on Taiwan's behalf have sought to bolster Taiwan's claim to international statehood.⁷

Because almost no states, including the United States and all of its military allies, recognize Taiwan as a nation-state, this road to international legality is likely a dead-end in the short term. Unless the U.S. abandons its long-standing approach to Taiwan, a U.S. military intervention into a Taiwan conflict is likely to rest on an "illegal but legitimate" justification such as that which supported U.S. strikes into Kosovo, Libya or Syria.⁸

But this very shaky international legal foundation is still insufficient if one considers the importance of U.S. military allies in the region. As the host of the largest U.S. naval base in the Western Pacific, Japan's role in any U.S. operation to defend Taiwan is likely to be significant. Because Japan's domestic legal limitations on its use of military force are well known, a dispute over the international legality of a U.S. intervention in Taiwan could undercut a U.S. military response. The credibility of a U.S. defense of Taiwan is seriously weakened if key allies like Japan cannot endorse the international legality of U.S. actions. Since neither Japan nor the U.S. recognize Taiwan's international legal status, both governments would have to overcome serious international legal obstacles in order to come to Taiwan's aid in an action by China.

In 2014, the Japanese Cabinet adopted a "reinterpretation" of the Japanese Constitution incorporating the concept of "collective self-defense" (CSD). While the meaning of CSD was a hotly debated issue within Japan, the broader international implications of applying CSD to U.S.-Japanese military cooperation has not received sufficient attention.⁹ Moreover, Japan's own concept of CSD under international law is neither static nor universally shared. The U.S. has long adhered to a broader conception of both individual and collective self-defense rights under international law.

This essay explores how the evolving concept of "collective self-defense"

affects the international legal basis for both U.S. and Japanese military intervention into a Taiwan-China conflict. It concludes that the U.S. and Japan adhere to different conceptions of individual and collective self-defense under international law. But Taiwan's closest ally, the United States, cannot muster an effective legal theory of either individual self-defense or CSD that would apply to Taiwan, even under the capacious version of those legal doctrines followed by the U.S. Meanwhile, Japan's narrow and extra-restrictive visions of individual self-defense and CSD also prohibits any theory of Japanese intervention into a Chinese-Taiwanese military conflict.

This legal vulnerability reveals a paradox: Taiwan has a strong legal incentive to formalize its independence from China in order to bolster its claim to the right to seek assistance from foreign states such as the U.S. and Japan. But while formalizing Taiwan's independence would bolster its legal right to seek support from outside powers, formalizing Taiwan's independence is also a likely *casus belli* triggering a Chinese invasion. In this way, the law of *jus ad bellum* is working to make an armed conflict more likely, rather than less.

In Part I of this short essay, I review the murky international legal status of Taiwan as a quasi-independent state unrecognized by most nations and international organizations. In Part II, I discuss the international law governing the use of force between states and its preservation of a right of both individual self-defense and collective self-defense. In Part III, I explain how the existing understandings of collective self-defense, especially in Japan, means that both the U.S. and Japan would likely have to decide whether to violate international law if they acted to use force to defend Taiwan from a Chinese military action.

Taiwan's Murky International Legal Status

The curious and contested international legal status of Taiwan has been the subject of numerous academic legal studies.¹⁰ Almost all of those studies have grappled with the difficulty of determining Taiwan's legal status given its complex and disputed history. Although the international legal debate is fascinating and important, it is the lack of consensus on Taiwan's international legal status that makes application of international laws on the use of military force so difficult and complicated.

Taiwan began its long official association with the mainland of China in the mid-seventeenth century when the remnants of the dying Ming Dynasty in China expelled Dutch colonialists during their retreat to Taiwan as a refuge from their Qing Dynasty enemies. This Ming Dynasty in exile, however, eventually itself succumbed to a Qing invasion and that ruling dynasty, which had assumed control

of the rest of what is today understood as China, extended its administrative control to Taiwan. The Qing government imposed taxes, regulated the activities of local pre-Chinese indigenous groups, and controlled immigration from the mainland. During the period of Qing governance, which lasted until 1895, there were frequent rebellions against the Qing administration and some historians argue that the Qing exercised very little actual control of the island for much of this period. Indeed, the Qing government did not designate Taiwan as an official province until 1887, and that same government was shortly thereafter forced to cede Taiwan to Japan after China's defeat in the 1895 Sino-Japanese War.¹¹

Japan occupied and administered Taiwan until 1945 when it relinquished all legal claims to sovereignty over Taiwan upon its surrender at the end of World War II. The Republic of China (ROC) government then in control of mainland China occupied and began exercising sovereignty over Taiwan. This exercise of sovereignty continued after the ROC moved its seat of government to Taiwan after its own defeat in the Chinese Civil War. It continues to exercise sovereignty over Taiwan today.

Some scholars have noted that the 1951 San Francisco Peace Treaty, which formally ended the U.S.-Japan conflict in WWII, did not specify that Taiwan was part of China. Instead, it merely confirmed that Japan renounced any and all claims to Taiwan. On the other hand, in that same treaty, Japan did recognize the independence of Korea, whereas it did not recognize Taiwan's independence.¹²

The U.S., which recognized the ROC government as the legitimate government of all of China until 1979, has maintained a studied ambiguity on the legal status of Taiwan. When the U.S. entered into a mutual defense treaty with the ROC, it agreed that the treaty could be triggered by an armed attack on the "territories" of the ROC. Moreover, for the purposes of the treaty, the ROC "territories" falling within the scope of the defense treaty were defined in Article VI as "Taiwan and the Pescadores." This strongly suggested that the U.S. government viewed Taiwan and the Pescadores (which Japan had renounced claims to in 1951) as part of the ROC and therefore part of China.¹³

But the U.S. took a more ambiguous stance when, establishing relations with the People's Republic of China (PRC) in 1979, the U.S. merely "acknowledge[d]" that Chinese people on both sides of the Taiwan Strait agree that Taiwan is part of China. It did not fully commit itself to recognizing Taiwan as part of China (although it has not opposed this concept either). Japan also adopted similarly ambiguous language about Taiwan when it re-established relations with China in 1973.¹⁴

In the 1979 Taiwan Relations Act, the U.S. committed itself to maintain relations with the "people of Taiwan."¹⁵ It also promised to oppose "coercive action" and promised to oppose any non-peaceful reunification of the two sides. But it did not in any way refer to Taiwan as a state. Moreover, in recent years, the U.S.

government has also repeatedly stated its opposition to a referendum on Taiwanese independence. While this does not mean the U.S. has recognized Taiwan is part of China, it strongly indicates the U.S. government is opposed to any declaration by the government in Taiwan that it is formally independent of China.¹⁶

Since 1971, when the ROC was ejected from the “China” seat in the United Nations, Taiwan has become increasingly isolated on the international stage. Following the 1971 UN ejection and the 1972 U.S.-PRC rapprochement, most countries recognized the PRC as the sole legitimate government of China and ended official diplomatic relations with the ROC. While some countries maintained their diplomatic relations, that number has shrunk year by year so that the ROC maintains official diplomatic relations today with only 15 states, most of them tiny in both land size and population.¹⁷

International Law and the Use of Force

It is thus fair to say that Taiwan is not a separate nation-state in the eyes of most states and international organizations in the world today. This non-state status calls into question Taiwan’s ability to invoke the rights and protections of states under the United Nations Charter. Most importantly, it calls into question whether the UN Charter’s prohibition of the use of military force against another state would apply if China invaded Taiwan.

THE LAW OF *JUS AD BELLUM*

Although philosophers and theologians long debated the morality of war, the regulation of a state’s use of military force under international law only began during the 20th Century. This effort culminated in the adoption of Article 2(4) of the United Nations Charter in 1945, which prohibits all member states from the “threat or use of force” against the “territorial integrity or political independence” of any other state.

Article 2(4) represents a clear legal prohibition on the “threat or use of force” but other sections of the Charter provide explicit exceptions. First, the Charter authorizes the Security Council to use force if it determines force is necessary to “maintain international peace and security.” Second, Article 51 makes clear that nothing in the Charter restricts the “inherent right of individual or collective self-defense if an armed attack occurs against a member of the United Nations.”

THE RIGHT OF SELF DEFENSE

Because formal UN Security Council authorizations for the use of force are rare, most states that have used force since the Charter’s adoption have sought

justification in a theory of self-defense. Because the Charter does not define self-defense and refers to an “inherent” right, the definition of the terms is not provided by the plain language of the Charter. This has led states, scholars, and international judicial bodies to offer various formulations to clarify its scope and meaning.

Individual Self Defense

The classic form of self-defense found in traditional pre-Charter customary international law concerned the right of an “individual” state to exercise self-defense. While all scholars agree that such an individual right exists, debates have arisen over when such a right might be invoked. In particular, debates have centered over what constitutes an “armed attack” that would trigger the right of self-defense. For instance, states and scholars have continued to debate whether and how a cyber-attack would fall within the meaning of an “armed attack” for purposes of Article 51. Debate has also flowed over the U.S.’s assertion of a legal right of self-defense to use force against terrorist groups not acting under the authority of a particular state. The United States has also sparked criticism and debate over its claim that its right to self-defense may also allow the preemptive use of force. In other words, the right of self-defense could be triggered even before an actual armed attack has occurred if that armed attack is imminent.

States and scholars considering these issues have generally fallen into the “restrictivist” and “extensivist” schools.¹⁸ Restrictivists generally interpret the right of self-defense narrowly and restrictively. Thus, those in the restrictivist school have generally criticized the invocation of self-defense against non-state actors, arguing that the right can only be invoked against armed attacks by states. They have also sharply criticized the U.S. version of the “preemptive self-defense” argument. In both of these situations, restrictivists claim that their narrower reading of the Charter’s right of self-defense comports with the Charter’s overall stated goal of ending the “scourge of war.”¹⁹ While there is some force to their arguments, the practice of states has not always conformed to the strict reading advocated by restrictivists. Still, it is fair to say that the restrictivist view has strong scholarly support and also receives at least rhetorical support from many states.

Collective Self-Defense

While the idea of an “individual” right of self-defense was not controversial at the framing of the Charter (even if its meaning has become contested in the decades since), the term “collective” self-defense seems to have more recent origins under international law. To be sure, states had long formed alliances of joint military cooperation and defense, but the term “collective” self-defense had not been widely in use until the middle of the twentieth century.²⁰

Scholars generally point to World War II era negotiations between the U.S. and the states of Central and South America to create joint defense arrangements as the immediate pre-cursor to the insertion of “collective self-defense” into the UN Charter.²¹ A month before delegates convened in San Francisco to discuss and draft the Charter, a group representing almost all states in the Western Hemisphere signed the “Act of Chapultepec” providing pledges to provide mutual support, including the use of force, to meet threats or acts of aggression against other Western Hemisphere countries. Importantly, the Act of Chapultepec declared that an armed attack on one member state would trigger the self-defense rights of other states. The initial declaration was codified into the 1948 formal Inter-American Treaty of Reciprocal Assistance, later known as the Rio Treaty.

Historians and scholars have also typically credited U.S. concern with maintaining the legality of arrangements like the Rio Treaty for the pressure exerted on the Charter’s drafters to include a specific insertion of the language exempting “collective” self-defense from the Charter’s prohibition on the use of force.²² The original concern related to legalizing regional arrangements like the pending Rio Treaty, but the Charter’s final version endorsed a broad collective self-defense right untethered to regional treaties or rights to regional self-defense. This broadened the collective self-defense right to any two states, whether or not they had a prior treaty for self-defense and whether or not they were nations concerned with regional security.²³

Thus, the only predicate for invoking the right of collective self-defense is the consent of the state that has sought assistance. Although some have argued that the assisting state must have some substantive interests affected by the attacking state’s actions, the majority view is that “[a]ny assisting state may act out of general interest in preserving international peace and security, and can do so without a formal treaty as long as the target state consents.”²⁴

The International Court of Justice explored the right of collective self-defense under international law in the well-known decision involving challenges to U.S. support for rebel groups in Nicaragua. The U.S. had argued its activities could be justified under the doctrine of collective self-defense since its actions were taken in order to support the self-defense rights of Nicaragua’s neighbor El Salvador.²⁵ The ICJ recognized that the right of collective self-defense did indeed exist prior to the Charter and it further held that these principles were embedded in customary international law.²⁶

The ICJ outlined its view as to the legal requirements for a state to invoke CSD. First, it held that the target state that is seeking assistance must be able to legitimately invoke its own right of individual self-defense in order to legalize the assisting state’s use of force. There seems little disagreement among states or scholars on this point, or on the ICJ finding that the rules of necessity and proportionality governing the use of force under customary international law also

govern the use of force when used in self-defense. Additionally, the Charter requires a state invoking the right of CSD or individual self-defense to make a report to the UN Security Council.

But not all of the ICJ's criteria for the invocation of CSD have been accepted uncritically.

For instance, the ICJ went so far as to require that the target state "will have declared itself to be the victim of an armed attack."²⁷ Other states, such as the United States, have accepted that the target state must have suffered an armed attack but have not accepted a "declaration" requirement. Indeed, the basis under customary law for the ICJ's declaration requirement is uncertain. Recent scholarship surveying traditional sources of customary law, including state practice, has found support for the idea that a target state must make a formal request for assistance, but no evidence of a declaration-of-armed-attack requirement.²⁸

This disagreement matters because the Nicaragua court relied heavily on the lack of a timely "armed attack" declaration by El Salvador, Honduras, or Costa Rica to conclude the U.S. had no right to exercise its own right of collective self-defense on those countries' behalf. Although the ICJ accepted for the record evidence showing Nicaragua had supplied arms to rebels in those countries, the fact that none of those countries had declared that those supplies constituted an "armed attack" weighed heavily in the ICJ's ultimate decision to find that no such armed attack triggering the right of self-defense had occurred.

Critics have also taken issue with the Nicaragua court's assessment that the supply of weapons by Nicaragua to rebel groups in neighboring countries did not reach the level of "gravity" necessary to satisfy the definition of armed attack in Article 51.²⁹ This "gravity" requirement, critics have argued, also has no clear or obvious basis either in customary law or in the drafting of the Charter's provisions on self-defense.³⁰

The U.S. refused to accept the jurisdiction of the ICJ in the Nicaragua case. It has never publicly accepted either the "declaration of an armed attack" or "gravity" requirements. But in other public statements, it does seem to accept that the CSD right can only be engaged with the consent of "a State that can legitimately invoke its own right of national self-defense."³¹ In the view of the U.S., however, no explicit request is required much less a declaration of armed attack. It is worth noting, however, that other states, including close allies such as Japan, seem to have embraced the Nicaragua opinion's definition of collective self-defense without the same reservations and limitations.

The U.S. also has shown signs that it may consider invoking the right of collective self-defense on behalf of armed groups that do not constitute states under the UN Charter. Although there has been no official U.S. government statement on this question, the U.S. seemed to endorse this possibility in its actions in Syria during its ongoing war against the non-state group ISIS. In justifying its attack

against ISIS entities in Syria, the U.S. suggested it was acting on behalf of its anti-ISIS allies in Syria that were also combatants in the Syrian civil war.³² There seems no textual or historical support for this legal argument, but it appears to have been invoked as a secondary argument in the U.S.-ISIS action, along with the U.S.'s own claim that it could invoke its individual right of self-defense against non-state groups like ISIS.

Conclusion

In sum, the right of CSD is well settled as part of customary international law recognized by Article 51 of the UN Charter. The conditions for its invocation, however, depend on the target state's own right of individual self-defense. The ICJ has endorsed further requirements for the exercise of CSD such as a formal declaration by a state suffering an armed attack and a formal request for assistance from a third state. Although there have been hints that the U.S. might seek to expand CSD to non-state actors, its official statements thus far have limited such CSD rights to the protection of other states, whether or not those states have made an explicit request for assistance or a formal declaration that they have suffered an armed attack.

Collective Self-Defense and Taiwan

TAIWAN'S CONTESTED RIGHT OF INHERENT SELF-DEFENSE

As discussed above, Taiwan's murky international legal status has denied it recognition as a state by most nations in the world as well as membership in the United Nations. As a non-state, non-member, Taiwan seems to lack the protection of Article 2(4) of the Charter. That provision prohibits the "threat or use of force against the territorial integrity or political independence of any *state*." In this view, a Chinese military action against Taiwan would simply not fall within the purview of Article 2(4). Moreover, Taiwan would also presumably lack the "inherent right of self-defense" because Article 51 seems only to apply when an "armed attack occurs against a Member of the United Nations." Taiwan has also repeatedly been denied the right to join the United Nations since it was ejected in 1971.

China also has invoked the customary international law right against interference in its domestic affairs to justify its freedom to handle Taiwan as it pleases. In China's view, this principle obligates other states to refrain from interfering to support a secessionist or independence movement in Taiwan.

In this way, China is able to muster a plausible international legal argument that any outside support for Taiwan's secession, especially military assistance, would violate international law. Taiwan's lack of statehood and membership in the

United Nations combined with the widely accepted principle of non-interference would call into serious question the legality of any U.S. military intervention in a Taiwan military crisis. As I have argued elsewhere, the U.S. has a difficult and potentially impossible legal problem to justify a military intervention in favor of Taiwan against China.³³ This does not mean the U.S. should not intervene to defend Taiwan, but it does mean the U.S. will have to address and face the substantial legal obstacles facing such an intervention.³⁴

CSD AND THE UNITED STATES

As noted earlier, the U.S. appears to have been instrumental in ensuring the concept of CSD was incorporated into the United Nations Charter. Since that time, the United States placed itself at the center of the most expansive set of CSD treaty obligations in the world. The U.S. has by treaty entered into CSD relationships with NATO, Australia, South Korea, the Philippines, Japan, Thailand, and most of the countries in South and Central America.³⁵ It has also invoked CSD in a variety of circumstances to justify its use of military force. Most famously, the U.S. argued that CSD for Honduras, Costa Rica and El Salvador legally justified its support for military activities against the government of Nicaragua during the 1980s.³⁶

The U.S. CSD treaty with Taiwan ended in 1979 when it terminated that treaty and established diplomatic relations with the People's Republic of China. But it continues to maintain CSD treaty obligations with two of Taiwan's closest geographic neighbors: Japan and the Philippines.

Under the U.S.-Philippines Mutual Defense Treaty,³⁷ the U.S. and the Philippines both have promised to treat an armed attack in the Pacific on either of its territories or either of its armed forces, public vessels or aircraft in the Pacific as "dangerous to its own peace and safety." Both have also pledged that in the event of an armed attack, the other country would act to "meet the common danger." In the past year, the U.S. has clarified that the scope of this defense guarantee extends to the Philippines' activities in the South China Sea. This clarification was sought by the Philippines due to the ongoing territorial disputes and tensions with China over the land features and maritime rights in that region.

The U.S.-Philippines Mutual Defense Treaty imposes reciprocal obligations. Thus, it is conceivable that the treaty's CSD obligations on the Philippines would be triggered by an attack on U.S. naval vessels or aircraft operating around Taiwan. As Taiwan and the waters around it would certainly constitute part of the "Pacific Area," a Chinese-U.S. conflict in those waters would in theory obligate the Philippines to provide support under its own CSD obligations to the U.S.³⁸

In addition to its conventional support for the principle of CSD through treaty obligations, the U.S. government has sometimes returned to its broader conception of CSD that it endorsed in the 1980s during its actions in Central

America. In 2014, the U.S., together with an international coalition, launched an attack on the self-declared Islamic State which had taken over large areas of Iraq and Syria. While Iraq had satisfied the traditional requirements of CSD by declaring itself under an armed attack and requesting international military assistance from the United States, Syria had not. Indeed, Syria's government pointedly refused to give permission for U.S. military action on its territory directed toward Islamic State forces. Nonetheless, the U.S. sent both air and ground forces into Syrian territory. It justified those actions both on a theory of "individual self-defense" against the Islamic State terrorist group but also on a theory of "collective self-defense" triggered by the threats the Islamic State posed to Iraq from its bases in Syrian territory.³⁹

This broader invocation of CSD recalls the U.S. claims in the Nicaragua case that it had a CSD right to engage in military actions in Nicaragua's territory due to the threat Nicaragua's government posed to El Salvador, Costa Rica and Honduras through Nicaragua's support of rebels in those latter three countries. Although ultimately rejected by the ICJ as discussed above, the U.S. has never accepted the ICJ's definition of CSD or the requirements it imposed on CSD in the Nicaragua decision. It is likely that the U.S. government continues to adhere to this more expansive conception of CSD today. In such circumstances, the U.S. might treat the existence of hostile or dangerous military forces in a neighboring territory as triggering its CSD rights to act against that force inside such territory. In Nicaragua, the U.S. argued it could use force in Nicaragua to protect El Salvador, Costa Rica and Honduras from covert military aid to rebels emanating from Nicaragua. In Syria, the U.S. suggested it could use military force to suppress or eliminate threats to Iraq's territory irrespective of the gravity of the threat against Iraq.

This expansive legal conception of CSD has not been officially endorsed by the U.S. government in an authoritative statement. It seems likely that this conception is not shared by other nations, and it seems to fly in the face of the ICJ's decision in Nicaragua. But the U.S. has not expressly disclaimed this broader conception of CSD and its actions in Syria tend to affirm it as well.

CSD AND JAPAN

CSD is also an important principle for Japan. Indeed, Japan also has committed itself to one robust mechanism of collective self-defense in the form of its security treaty with the United States.⁴⁰ Under that treaty, the United States has pledged to treat an armed attack in the territories "under the administration of Japan" as a danger to its own peace and security. In essence, the U.S. seems to have promised to provide Japan with assistance, including military assistance, in the case of an armed attack against Japan. Indeed, the U.S. pledge could be interpreted as broader than whatever Japan's right of self-defense encompasses under the UN Charter since the defense guarantee encompasses "territories under

the *administration* of Japan” even if Japan’s sovereignty over those territories is disputed. Some of those territories, especially the Senkaku Islands, are also claimed by China and Taiwan.

Moreover, unlike the U.S.-Philippines Mutual Defense Treaty, Japan does not have fully reciprocal obligations with the United States. The CSD obligation found in Article 5 of the Security Treaty is triggered only by an “armed attack on either Party on the territories under the administration of Japan.” Unlike the Philippines’ CSD obligation to all U.S. forces in the “Pacific Area,” Japan has no CSD obligation under the treaty if U.S. forces suffer an armed attack outside the “territories under the administration of Japan”.

This curious imbalance in CSD obligations is almost certainly a reflection of Japan’s domestic constitutional law constraints on the use of military force. After its defeat in World War II, Japan adopted a new constitution which contains, in Article 9, a renunciation of “war as a sovereign right” and “the threat or use of force to settle international disputes.”⁴¹ This provision has been interpreted by the Japanese government to limit Japan’s ability to use military force to the self-defense of its own territories and to prohibit Japan’s involvement in any type of military conflict outside of Japan’s territories.⁴² Japan thus has never sent military forces overseas to directly support U.S. military action other than rear-area assistance not involving the use of force (unlike other U.S. CSD treaty partners like Taiwan, Korea, Australia, and the Philippines). Not only does Japan lack any broad CSD obligation under its treaty with the U.S., but such actions have also been interpreted by scholars to violate Article 9 of the Japanese Constitution.⁴³

To be sure, Japan has interpreted Article 9’s renunciation of war to allow for what would be considered individual self-defense under international law. This justified Japan’s maintenance of robust “self-defense” forces in land, air and sea despite the constitutional prohibition on maintaining a military.⁴⁴ In 2014, the Japanese Cabinet adopted a controversial “interpretation” of Article 9 that allowed Japan’s military to invoke the international law right of CSD. Under this 2014 interpretation, Japan can use military force to support another country under armed attack consistent with Article 9 if three conditions are met:

- The attack on that country poses a clear danger to Japan’s survival or could fundamentally overturn Japanese citizens’ constitutional rights to life, liberty and the pursuit of happiness
- There is no other way of repelling the attack and protecting Japan and its citizens
- The use of force is limited to the minimum necessary⁴⁵

It should be noted that this interpretation limits Japan’s actions much more than the international law of CSD would require. Under international law, Japan could

use military force as long as another state suffered an armed attack of sufficient gravity and requested assistance. But Japan's Article 9 interpretation limits any Japanese use of force to situations where Japan's "survival" or the "constitutional rights" of its citizens are under "clear danger." It further requires a determination that using force is a last resort to protect Japan and its citizens.

Nonetheless, the 2014 interpretation does make clear that the right of CSD can be invoked consistent with Article 9, albeit in a much narrower form. Prior to 2014, it was not entirely clear CSD could be invoked at all by Japan to use force in a manner distinct from its own rights of individual self-defense. In other words, Article 9 had always been interpreted to allow Japanese forces to defend Japanese territories against armed attack.⁴⁶ The 2014 interpretation expands the right of Japanese forces to support foreign forces under armed attack if attack on those foreign forces posed severe threats to Japan's survival or its people's constitutional rights.

The 2014 interpretation was widely understood to be aimed at clarifying that Japan's military cooperation was not strictly limited to operations in the territory of Japan.⁴⁷ Japanese government guidance on the new interpretation suggests that Japan's forces could act in a "situation in which a clear danger of the occurrence of armed attack is imminent" or a "tense situation in which armed attack [on Japan] is anticipated."⁴⁸ If, for instance, an attack on U.S. forces outside of Japan's territories posed a clear danger to Japan's survival, Japan's military could take action to support those forces. An attack on U.S. naval forces operating in international waters near Japan might qualify for Japanese support if those forces were conducting actions necessary for the military defense of Japan. Even an attack on U.S. or South Korean forces in South Korea might qualify depending the scale of that attack and the nature of the threat that attack might pose to Japan. There is no clear geographic limitation on Japan's collective self-defense rights under this interpretation. For instance, a threat to Japanese oil supplies from the Persian Gulf could, in theory, trigger Japan's CSD rights under the 2014 interpretation.

SUMMARY

Although CSD is a principle well grounded in customary international law and the United Nations Charter, it plays a very different role for Taiwan, the U.S. and Japan. Taiwan, under any classical definition of CSD, cannot avail itself of its legal rights or protections since it is neither a widely recognized state nor a member of the United Nations. The U.S. is probably the world's most ardent and aggressive exponent of the CSD as a principle of international law. But the U.S. has seen its interpretation of CSD rejected by the ICJ and it has struggled to gain acceptance for its more expansive conception of this legal principle. Meanwhile, Japan not only adheres to the ICJ's more restrictive conception of CSD, but it has also bound itself under its domestic constitution to an even more restrictive definition of CSD than

what would be permitted under international law. As the next section will point out, the practical result of this analysis is that CSD only operates to inhibit military support for Taiwan against a very real and credible threat of aggressive Chinese military action.

CSD's Impact on an Armed Attack on Taiwan by the Chinese People's Liberation Army

While the People's Republic of China regime has achieved near universal diplomatic recognition as the sole legal government of China, key states such as the United States and Japan have maintained ambiguity about their views on China's claim that it has sovereignty over Taiwan. This contested legal status has also raised difficult questions about the international legality of any Chinese use of force to conquer Taiwan.

THE PROSPECT OF A MILITARY ATTACK BY CHINA AGAINST TAIWAN

The prospect of China's use of force has always lurked in the background of cross-strait relations. China has pointedly never renounced its right to "re-unify" China using all means, including military force. Indeed, it legalized this right in 2005 when its legislature enacted the Anti-Secession Law.⁴⁹ That law set forth China's overall policy of seeking peaceful reunification through negotiations and consultations. But it also stated in Article 8 that the government "shall employ non-peaceful means and other necessary measures to protect China's sovereignty and territorial integrity" should Taiwan's secession occur or other possibilities for peaceful reunification are exhausted. The refusal to take the use of force off the table was reiterated publicly as recently as January 2019 when China's leader Xi Jinping opened the New Year with a speech noting the importance of Taiwan and adding a clear warning.⁵⁰ After noting that Taiwan "must and will" be reunified with China, he added that "[w]e do not promise to renounce the use of force."⁵¹

The Chinese government has reinforced these threats by conducting military exercises in the seas near Taiwan as well as sending military jets to encircle the island's airspace. As the U.S. Defense Department has noted, China has maintained and improved its military capacity to use force to harm, invade, and occupy Taiwan.⁵² At the same time, Taiwan's military capabilities are not believed to have kept pace, thus shifting the military balance of power further toward China.

The scenarios for the use of force against Taiwan range from long-range missile attacks of the kind demonstrated during the 1996 Taiwan Strait crisis to a naval blockade to outright invasion and occupation. While military experts have debated whether and how Taiwan's military might resist such Chinese military actions, there are few military experts who think Taiwan would prevail in a long-

term military conflict with China without substantial military assistance from other nations. The United States, which had previously offered a defense guarantee for Taiwan prior to its 1979 decision to recognize the PRC, has continued to pledge support for Taiwan and to oppose a coercive reunification. But it no longer offers a formal legal pledge to come to Taiwan's defense if it suffers an armed attack, as it had done during the postwar period when the U.S. and Taiwan were parties to a mutual defense treaty. The outsized importance of the United States in any military conflict between China and Taiwan spotlights the importance of assessing the legal basis for such an intervention. The weak legality of such an outside intervention, for instance, could reduce the credibility of perceived U.S. support for Taiwan against China.

THE U.S., CSD, AND TAIWAN

As discussed earlier, the U.S. terminated its formal mutual defense treaty with Taiwan in 1979. It replaced this international law framework with a much more ambiguous set of commitments under domestic legislation called the Taiwan Relations Act. Under that 1979 law, the U.S. government has declared that it opposes any unification between China and Taiwan “by other than peaceful means.” It also commits the United States to provide Taiwan with “arms of a defensive character” while also maintaining the “capacity of the United States to resist any resort to force or other forms of coercion that would jeopardize the security, or the social or economic system, of the people on Taiwan.”

In some ways, the U.S. legal commitment to Taiwan is deeper than its standard CSD treaty commitments. In those treaties, the U.S. typically promises to act in response to an “armed attack.” But in the Taiwan Relations Act, the U.S. policy is to oppose all forms of coercion and to provide defensive arms. On the other hand, unlike in its CSD treaties, the Taiwan Relations Act does not commit the U.S. government to act beyond continuing to sell defensive weapons. In a situation where there is “any threat to the security or the social or economic system of the people on Taiwan,” the President is directed to inform Congress and the two branches will decide together the appropriate response.

This ambiguity as to the depth of U.S. commitment to the military support of Taiwan may also be affected by Taiwan's uncertain international legal status. Under U.S. government definitions of CSD, the right to act under international law pursuant to CSD is triggered by an armed attack on another *state*. The U.S. government does not currently recognize Taiwan as a state so it cannot invoke CSD in such a circumstance based merely upon an armed attack on Taiwan.

JAPAN, CSD, AND TAIWAN

As a fully-fledged member of the United Nations, Japan could invoke its individual right of self-defense. But could it claim that right arising out of a Chinese invasion of Taiwan? If it could legitimately do so, then the United States could invoke the

collective self-defense right to intervene in Taiwan on *Japan's* behalf.

It is clear that the text of Article 51 requires a member state to suffer an “armed attack” in order to invoke its right of self-defense. Yet it is less than clear that a state must suffer such an armed attack on its own territory in order to invoke its right of self-defense and its right to request assistance. In 2014, the Government of Iraq sought assistance from the United Nations and other countries to repel attacks by the Islamic State, a non-state actor operating on its own territory but also in Syria. Iraq specifically sought assistance for the United States to launch attacks on Islamic State groups operating inside of Syria.⁵³ This request for assistance by Iraq served as one of the legal bases for the United States to justify its actions in Syria on the basis of collective self-defense.

In the Iraq-Islamic State scenario, Iraq had suffered armed attacks inside its own territory. But it also claimed that the Islamic State's existence across the border in Syria also constituted a threat to Iraq. Japan could, in theory, claim an attack on Taiwan constitutes an armed attack on itself or would trigger its own rights of individual self-defense.

Although the main Japanese islands are nearly a thousand miles from Taiwan, Japan administers or has sovereignty over various island territories quite close to Taiwan's northern coasts. Indeed, Japan's westernmost inhabited island, Yonaguni Island, lies merely 67 miles from Taiwan's east coast. Not only does the U.S. maintain a robust CSD treaty relationship with Japan, but it also has two of its largest military facilities in the region located in Japan's Okinawa Island. U.S. bases on Okinawa are the geographically closest U.S. military facilities to Taiwan at barely 400 miles off Taiwan's eastern coast. Japan claims sovereignty over the Senkaku Islands, which China also claims and which are also within 100 miles of Taiwan.

A Chinese attack on Taiwan could arguably trigger Japan's individual self-defense rights in at least two ways. A Chinese occupation of Taiwan would place China astride one of the main air and sea routes for shipping between the Persian Gulf and Japan. Second, Japan's territorial sovereignty over islands close to Taiwan would be endangered by China's occupation of Taiwan. In particular, China's domination of Taiwan would place even more pressure on Japan's control of the disputed Senkaku Islands.

To make this argument work, the U.S. and Japan would have to seek acceptance for the very broad conception of CSD that the U.S. advanced in Iraq in 2014 and in Central America during the 1980s. This makes Japan and its response to a possible Chinese invasion of Taiwan a crucial factor in the outcome of any such conflict.

There is an obvious objection to this rather aggressive approach to CSD.

As discussed above, Japan's definition of individual and collective self-defense is narrower than what could be permitted under international law. Japan's definition of individual self-defense is traditionally limited to armed attacks on its

territory. Under the new interpretation of the Japanese Constitution, a Chinese attack on Taiwan would have to endanger Japan's survival or the constitutional rights of its people for Japan to allow a Japanese invocation of a right of collective self-defense. But since Japan, like the United States, limits the right of CSD to support other *states* suffering armed attacks, it would not be able to apply this principle toward non-state Taiwan.

Moreover, under the ICJ's definition of CSD, Japan would have to publicly declare itself under an armed attack and publicly request assistance from the United States. Japan, and not the United States, would hold the key to determining whether or not U.S. forces could invoke CSD for Japan and Taiwan. Thus, while the U.S. has at times endorsed an expansive notion of self-defense and CSD under international law, it is Japan's own views on these international law concepts that would govern. Unless Japan adopted a more expansive conception of the international law of self-defense to treat an assault on Taiwan as a threat to itself, and an expansive conception of CSD endorsed by the United States, it is unlikely that Japan could serve as a vehicle to legalize a U.S. military intervention on Taiwan's behalf.

Conclusion

The interpretation of the law of *jus ad bellum* remains hotly contested between states and commentators arguing for a "restrictivist" narrow approach and those that have endorsed a more "extensivist" conception. This divide exists both in the interpretation of individual and collective self-defense. Extensivists have argued for a broad right of individual right of self-defense that might include anticipatory self-defense against both states and non-state actors. Extensivists have also argued for a right of CSD upon an armed attack even if that attack does not have the gravity required by the ICJ in the Nicaragua case.

No country has been more extensivist in its approach to both individual self-defense and CSD than the United States. The U.S. has more CSD treaty obligations than any other single country in the world, and no country has invoked this principle to justify its use of military force more than the United States. It has most recently invoked this principle in the Middle East, at least in part, to justify its use of force in Syria.

Yet even the United States would be hard-pressed to legally justify an intervention to defend Taiwan against a Chinese military assault. Even the United States has clearly limited its understanding of its CSD rights to other *states*. Taiwan is not, in the view of the United States, a sovereign state. It would not, therefore, be entitled to invoke CSD on behalf of Taiwan.

On the flip side, no country is more firmly in the restrictivist camp than

Japan. Japan's domestic law definition of individual self-defense is arguably more restrictive than that permitted by international law. Japan has never endorsed the broad U.S. views of individual self-defense that would allow anticipatory action or self-defense against non-state actors. Japan has also endorsed a strict definition of CSD that would limit its rights beyond that imposed by even restrictivist interpretations of international law.

Japan's position in the restrictivist camp severely restricts the options that could legally justify a U.S. military defense of Taiwan. If Japan altered its approach to move closer to the extensivist views of the United States, it might offer a path to legalize a U.S. defense of Taiwan. But in its current legal worldview, Japan can neither provide a legal basis for U.S. intervention through its own international legal rights nor fully support a questionably lawful U.S. intervention.

There is a larger conclusion from this survey of CSD and the law of *jus ad bellum*. Taiwan's lack of international legal status as a state creates a real vulnerability. China feels unconstrained by this law because it does not consider Taiwan a state. The U.S. and Japan cannot invoke CSD to defend Taiwan because neither country considers Taiwan a state. While the law of *jus ad bellum* may operate to constrain the use of armed force by states, paradoxically, its limitations could actually encourage the use of force in the contested Taiwan Strait. Even more paradoxically, Taiwan's legal vulnerability as a non-state without any right to seek foreign assistance against a military invasion suggests Taiwan should declare formal independence. But formal independence is exactly one of the actions that would be most likely to trigger China's resort to military force.

The law of *jus ad bellum* is ultimately designed to deter the use of military force, including by preserving the right of nations to deter the use of force through collective self-defense arrangements. In the strange and unusual context of Taiwan's military confrontation with China, the law of *jus ad bellum* works against this overarching goal in surprising and potentially tragic ways. While international law does not necessarily control the decisions of policymakers, the Taiwan case study suggests that ignoring the international law of *jus ad bellum* is sometimes a better choice than adhering to it. ■

Julian G. Ku is the Maurice A. Deane Distinguished Professor of Constitutional Law and Senior Associate Dean for Academic Affairs at Hofstra University. He conducts academic research on a wide range of topics including U.S. foreign relations law, international dispute resolution, international criminal law, and China's relationship with international law. He has also been selected as the John DeWitt Gregory Research Scholar and as a Hofstra Law Research Fellow. He is a member of the American Law Institute. He is a graduate of Yale Law School and Yale College.

He is the co-author, with John Yoo, of *Taming Globalization: International Law, the U.S. Constitution, and the New World Order* (Oxford University Press 2012). He also has published more than 40 law review articles, book chapters, symposia contributions, and essays. He has given dozens of academic lectures and workshops at major universities and conferences in the United States, Europe and Asia. He is also a contributing editor to Lawfareblog.com and the co-founder of Opinio Juris.

- 1 See, e.g., Oona Hathaway & Scott Shapiro, *The Internationalists: How a Radical Plan to Outlaw War Remade the World* (2017).
- 2 Li Yan, *PLA conducts joint land assault exercises near Taiwan*, China News Serv. (Sept. 9, 2019), <http://www.ecns.cn/news/2019-09-09/detail-1fzntuwi2502283.shtml>.
- 3 Shirley A. Kan & Wayne M. Morrison, Cong. Research Serv., R41952, *U.S.-Taiwan Relationship: Overview of Policy Issues* (2014).
- 4 See, e.g., Ian Easton, *The Chinese Invasion Threat: Taiwan's Defense and American Strategy in Asia* (2017); Bill Gertz, *China's Secret Military Plan: Invade Taiwan by 2020*, Wash. Free Beacon (Oct. 3, 2017), <https://freebeacon.com/national-security/chinas-secret-military-plan-invade-taiwan-2020/>; Isaac Stone Fish, *Asia's Other Nightmare Scenario*, Slate (Oct. 4, 2017), <https://slate.com/news-and-politics/2017/10/what-would-a-chinese-invasion-of-taiwan-look-like.html>.
- 5 See, e.g., Oona Hathaway, *Turkey is violating international law. It took lessons from the U.S.*, Wash. Post (Oct. 22, 2019), <https://washingtonpost.com/outlook/2019/10/22/turkey-is-violating-international-law-it-took-lessons-us/>; Scott Horton, *Six Questions for Mary Ellen O'Connell on the Purpose of International Law*, Harper's Mag. (Dec. 6, 2008), <https://harpers.org/blog/2008/12/six-questions-for-mary-ellen-connell-on-the-power-of-international-law>.
- 6 See, e.g., Phil C.W. Chan, *The Legal Status of Taiwan and the Legality of the Use of Force in a Cross-Taiwan Strait Conflict*, 8 Chinese J. Int'l L. 455, 482–85 (2009).
- 7 Mikaela L. Ediger, *International Law and the Use of Force Against Contested States: The Case of Taiwan*, 93 N.Y.U. L. Rev. 1668, 1684–85 (2018); Anne Hsiu-An Hsiao, *Is China's Policy to Use Force Against Taiwan a Violation of the Principle of Non-Use of Force Under International Law?*, 32 New Eng. L. Rev. 715, 730–32 (1998).
- 8 Anthea Roberts, *Legality vs Legitimacy: Can Uses of Force be Illegal but Justified?*, in *Human Rights, Intervention, and the Use of Force* 179 (Philip Alston & Euan Macdonald eds., 2008).
- 9 See *Fundamental Concepts of National Defense*, Ministry of Def. of Japan, https://www.mod.go.jp/e/d_act/d_policy/dp01.html (last visited Nov. 29, 2019); see also Ian E. Rinehart, *Collective Self-Defense and U.S. Japan Security Cooperation* (E.-W. Ctr. Politics, Governance, & Sec. Series, Working Paper No. 24, 2013).
- 10 See, e.g., Lung-chu Chen, *The U.S.-Taiwan-China Relationship in International Law and Policy* (2016); Jianming Shen, *Sovereignty, Statehood, Self-Determination, and the Issue of Taiwan*, 15 AM. U. INT'L L. REV. 1101 (2000); Tzu-wen Lee, *The International Legal Status of the Republic of China on Taiwan*, 1 UCLA J. INT'L L. & FOREIGN AFF. 351, 353 (1996).
- 11 For a discussion of this history, see, e.g., Tzu-wen Lee, *The International Legal Status of the Republic of China on Taiwan*, 1 UCLA J. Int'l L. & Foreign Aff. 351, 353 (1996).
- 12 Lung-Chu Chen & W.M. Reisman, *Who Owns Taiwan: A Search for International Title*, 81 Yale L.J. 599, 616 (1972).
- 13 United States-Republic of China Mutual Defense Treaty, China [Taiwan]-U.S., Dec. 2, 1954, 6 U.S.T. 433, T.I.A.S. No. 3178.

- 14 See Joint Communiqué of the United States of America and the People's Republic of China, Feb. 27, 1972, in 66 Dep't St. Bull. 435, 437–38 (1972).
- 15 Taiwan Relations Act, Pub. L. No. 96-8, 93 Stat. 14 (1979) (codified at 22 U.S.C. §§ 3301-3316 (1982)).
- 16 Kan & Morrison, *supra* note 4.
- 17 Martina Hukel, *Taiwan's Allies Dropping Like Flies*, Geo. Security Stud. Rev. (Oct. 1, 2019), https://georgetownsecuritystudies-review.org/2019/10/01/taiwans-allies-dropping-like-flies/#_edn1.
- 18 Olivier Corten, *Use of Force in International Law*, Oxford Bibliographies (Oct. 27, 2016), <http://www.oxfordbibliographies.com/view/document/obo-9780199796953/obo-9780199796953-0005.xml#obo-9780199796953-0005-bib-Item-0001> (citing as examples of this extensivist approach Anthony Arend & Robert J. Beck, *International Law and the Use of Force* (1993); Thomas Franck, *Recourse to Force: State Action against Threats and Armed Attacks* (2002)).
- 19 See, e.g., Olivier Corten, *The Law against War* (2010); Christine Gray, *International Law and the Use of Force* (2008).
- 20 See George K. Walker, *Anticipatory Collective Self-Defense in the Charter Era: What the Treaties Have Said*, 31 Cornell Int'l L.J. 321, 324–25 (1998).
- 21 Stanimir A. Alexandrov, *Self-Defense Against the Use of Force in International Law* 101–02 (1996); D.W. Bowett, *Self-Defense in International Law* 187–93 (1958).
- 22 Bowett, *supra* note 22, at 187–93.
- 23 As one scholar notes, “[a]ny Member . . . is therefore authorized by the Charter to assist with its armed force an attacked State, whether or not there has been any previous arrangement to that effect.” Alexandrov, *supra* note 22, at 102.
- 24 *Id.*; see also J.G. Starke, *The ANZUS Treaty Alliance* 98–99 (1965) (discussing Security Treaty Between the United States, Australia, and New Zealand, Sept. 1, 1951, pmbl., 3 U.S.T. 3420, 3422, 131 U.N.T.S. 83, 84 [hereinafter ANZUS Pact]).
- 25 *Military and Paramilitary Activities in and Against Nicaragua* (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ¶ 126 (June 27) [hereinafter ICJ Opinion].
- 26 *Id.* ¶ 193.
- 27 *Id.* ¶ 195.
- 28 James A. Green, *The ‘additional’ criteria for collective self-defence: request but not declaration*, 4 J. Use Force & Int'l L. 4–13 (2017).
- 29 ICJ Opinion, *supra* note 26, ¶ 191.
- 30 See, e.g., Abhimanyu George Jain, *Rationalising International Law Rules on Self-Defence: The Pin-Prick Doctrine*, 14 Chi.-Kent J. Int'l & Comp. L. 23, 70 (2014); W. Michael Reisman, *Allocating Competences to Use Coercion in the Post-Cold War World: Practices, Conditions, and Prospects*, in *Law and Force in the New International Order* 26, 29 (Lori Fisler Damrosch & David Scheffer, eds., 1991).
- 31 Dep't of Def., *Law of War Manual* 49 (2016) (citing Bruno Simma, *The Charter of the United Nations: A Commentary* 675 (1994) (“Art. 51 of the Charter allows not only individual, but also collective self-defence. The latter is not, as the wording might suggest, restricted to a common, co-ordinated exercise of the right to individual self-defence by a number of states. . . . It is not required for the exercise of the right of collective self-defence that the state invoking the right be under an obligation resulting from a treaty of assistance. Rather, it is sufficient, but also necessary, that the support be given with the consent of the attacked state. But this consent does not, as the ICJ states for the right of self-defence under customary law, need to be declared in the form of an explicit ‘request’.”)).

- 32 Kinga Tibori-Szabó, *The Downing of the Syrian Fighter Jet and Collective Self-Defence*, *Opinio Juris* (June 23, 2017), <https://opiniojuris.org/2017/06/23/the-downing-of-the-syrian-fighter-jet-and-collective-self-defence/>.
- 33 Julian Ku, *Why Defending Taiwan is Illegal*, *Diplomat* (July 12, 2014), <https://thediplomat.com/2014/07/why-defending-taiwan-is-illegal/>.
- 34 Julian Ku, *International Law Is Taiwan's Enemy: Although protecting Taiwan is worthwhile, international law is not on Taipei's side*, *Diplomat* (July 16, 2014), <https://thediplomat.com/2014/07/international-law-is-taiwans-enemy/>.
- 35 See U.S. Collective Defense Arrangements, U.S. State Dep't, <https://2009-2017.state.gov/s/l/treaty/collectivedefense/index.htm> (last visited Nov. 30, 2019).
- 36 ICJ Opinion, *supra* note 26, ¶ 126 ("[T]he assertion that the United States, pursuant to the inherent right of individual and collective self-defence, and in accordance with the Inter-American Treaty of Reciprocal Assistance, has responded to requests from El Salvador, Honduras and Costa Rica, for assistance in their self-defence against aggression by Nicaragua.").
- 37 Mutual Defense Treaty Between the United States and the Republic of the Philippines, Phil.-U.S., Aug. 30, 1951, 3 U.S.T. 3947, T.I.A.S. No. 2529.
- 38 *Id.* art. V.
- 39 Permanent Rep. of the United States of America to the U.N., Letter dated Sept. 23, 2014 from the Permanent Representative of the United States of America to the United Nations addressed to the Secretary-General, U.N. Doc. S/2014/695 (Sept. 23, 2014) ("Accordingly, the United States has initiated necessary and proportionate military actions in Syria in order to eliminate the ongoing ISIL threat to Iraq . . .").
- 40 Security Treaty Between the United States and Japan, Japan-U.S., Sept. 8, 1951, 3 U.S.T. 3329.
- 41 Nihonkoku Kenpō [Kenpō] [Constitution], art. 9, para. 1 (Japan).
- 42 Theodore Mcnelly, *The Origins of Japan's Democratic Constitution* 134–35 (2000) (describing interpretation of Article 9 to allow for a "self-defense" force).
- 43 See Hajime Yamamoto, *Interpretation of the Pacifist Article of the Constitution by the Bureau of Cabinet Legislation: A New Source of Constitutional Law?*, 26 Wash. Int'l L.J. 99, 107 (2017).
- 44 See *id.* at 107–08.
- 45 See Government of Japan, Cabinet Decision on Development of Seamless Security Legislation to Ensure Japan's Survival and Protect its People (2014), available at https://www.cas.go.jp/jp/gaiyou/jimu/pdf/anpoho-sei_eng.pdf.
- 46 See, e.g., Masahiro Kurosaki, *The 'Bloody Nose' Strategy, Self-Defense and International Law: A View from Japan*, *Lawfare Blog* (Feb. 15, 2018), <https://www.lawfare-blog.com/bloody-nose-strategy-self-defense-and-international-law-view-japan>.
- 47 Masahiro Kurosaki, *Japan's Evolving Position on the Use of Force in Collective Self-Defense*, *Lawfare Blog* (Aug. 23, 2018), <https://www.lawfareblog.com/japans-evolving-position-use-force-collective-self-defense>.
- 48 *Id.*
- 49 Fan Fenlie Guojia Fa (反分裂国家法) [Anti-Secession Law] (promulgated by the Standing Comm. Nat'l People's Cong., Mar. 13, 2005, effective Mar. 13, 2005), art. 1 (China), available at http://en.people.cn/200503/14/eng20050314_176746.html

50 Xi Jinping says Taiwan 'must and will be' reunited with China, BBC (Jan. 2, 2019), <https://www.bbc.com/news/world-asia-china-46733174>.

51 Tim Hains, *Xi Jinping on Taiwan: "We Do Not Promise To Renounce The Use Of Force"*, RealClear Pol. (Jan. 2, 2019), https://www.realclearpolitics.com/video/2019/01/02/xi_jinping_on_taiwan_we_do_not_promise_to_renounce_the_use_of_force.html.

52 Military and Security Developments Involving the People's Republic of China 2019, 83 (May 2019) available at https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf

53 Letter dated 23 September 2014 from the Permanent Representative of the United States of America to the United Nations addressed to the Secretary-General, S/2014/695 (available at http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2014_695.pdf)



Hitoshi Nasu

Exeter University

Japan's Legal Readiness in the Event of Hostilities on the Korean Peninsula

Introduction

The use of military power is a controversial issue in Japan, primarily because of the “war renunciation clause” of the Japanese Constitution. Article 9 of the Constitution imposes restrictions on the extent to which the Japanese Self-Defense Forces (SDF) can operate overseas.¹ The issue of Japan’s use of armed force raised a public furor in 2015 when the new security bills were introduced as an attempt, ostensibly, to authorize the SDF to act in “collective” self-defense as a means to strengthen the U.S.-Japan alliance.² Despite the public outcry, the new security legislation was enacted on September 30, 2015 and came into force on March 29, 2016. The new legislation aimed to enable Japan to take a “seamless response” to any international security situation that might arise.³ In accordance with the “proactive contribution to peace” policy adopted by Prime Minister Shinzo Abe, the 2015 security legislation has achieved an overhaul of the Japanese security law regime that had, over time, developed as a patchwork of technical amendments and special legislation. Nevertheless, the security law of Japan still contains many legal gaps and uncertainties that prevent Japan from harnessing the full potential of the re-interpretation of Article 9 in the contemporary security environment.⁴

Since the entry into force of Japan’s new security legislation, tensions in Northeast Asia have significantly increased as the Democratic People’s Republic of Korea (North Korea) conducted aggressive missile and nuclear tests in 2017, while the U.S. President Donald Trump continued to post provocative messages alluding to the possibility of resorting to military action. Any eruption of hostilities on the Korean Peninsula—whether it be a small-scale “bloody nose” attack or full-blown warfare—will test Japan’s legal readiness under its overhauled security law regime, as well as its defense capabilities and the robustness of its emergency planning. This paper examines how the U.S.-Japan alliance operates within the legal framework for the use of force in terms of both international law and Japanese security law, in the event of an outbreak of hostilities on the Korean Peninsula.

After providing a brief review of the legal and political developments relevant to tensions on the Korean Peninsula, this paper outlines the legal framework for the use of force by the SDF. It then critically examines Japan's legal readiness to engage in combined security operations with U.S. forces, non-combatant evacuation operations, and maritime security operations in the event of hostilities on the Peninsula.

Legal and Political Developments relating to Security Tensions on the Korean Peninsula

Security tensions on the Korean Peninsula have primarily evolved around two inter-related military concerns: (i) the development of North Korea's nuclear weapons; and (ii) North Korea's ballistic missile capabilities. North Korea's nuclear weapons program has been an international concern since the country's announcement of its withdrawal from the Treaty on the Non-Proliferation of Nuclear Weapons in 1993.⁵ Given the potential of ballistic missile systems to deliver nuclear, chemical or biological payloads,⁶ the level of global concern has increased considerably since July 2006 when North Korea began engaging in multiple ballistic missile launches.

Condemning the nuclear test conducted on October 9, 2006 as "a clear threat to international peace and security", the UN Security Council demanded that North Korea suspend and abandon all activities related to its ballistic missile program and all nuclear weapons programs in a complete, verifiable and irreversible manner,⁷ imposing sanctions in relation to specific items.⁸ On June 12, 2009, the Security Council adopted Resolution 1874 calling upon all states to inspect vessels on the high seas, with the consent of the flag state, in the event that vessels are suspected of violating the obligations imposed under the sanctions regime.⁹ A series of UN Security Council Resolutions and Presidential Statements have subsequently been issued each time North Korea conducted a nuclear test or a ballistic missile launch, reaffirming the obligations imposed upon North Korea in the previous resolutions and occasionally reinforcing the sanctions regime that has been built against it.¹⁰

The cause of tensions on the Korean Peninsula is not limited to armament issues alone. The hostile relationship between North Korea, the Republic of Korea (South Korea) and Japan continues to pose a threat to the region. On May 27, 2009, North Korea announced that it would no longer be bound by the 1953 Armistice Agreement that ended the Korean War. Even though the announcement was not considered sufficient to give rise to a resumption of an armed conflict,¹¹ it heralded a period of renewed hostilities. North Korea allegedly launched an

attack on March 26, 2010 which led to the sinking of the South Korean Navy vessel *Cheonan* with the tragic loss of 46 lives.¹² In November 2010, the island of Yeonpyeong near the disputed maritime border was bombarded, leaving two civilians and two soldiers dead. In August 2015, South Korea accused North Korea of planting land mines that injured two South Korean soldiers, which triggered an exchange of artillery fire in the demilitarized zone.

In addition, the humanitarian crisis facing North Korea has been a growing concern, with chronic malnutrition and systematic, widespread and grave violations of human rights drawing the attention of the international community.¹³ The crisis presents a precarious situation for the People's Republic of China (PRC), because of the possible mass influx of refugees across the border into the PRC in the event of hostilities on the Korean Peninsula. For Japan, the repatriation of Japanese nationals abducted by North Korea remains an important political consideration.

Tensions escalated rapidly in 2017 when North Korea was reported to have been edging close to acquiring the capability to launch a nuclear attack against the U.S. and President Trump threatened to unleash “fire and fury” against North Korea. The crisis was defused when North Korea made a historic commitment in 2018 to work towards complete denuclearization of the Korean Peninsula.¹⁴ However, the situation remains precarious due to the sluggish and difficult process of political negotiations, with the persistent risk that a breakdown in negotiations could potentially lead to military confrontation.

The Legal Framework for the Use of Force by the Self-Defense Forces

The operation of the SDF is subject to constraints under international law as well as Japanese domestic law, in particular under Article 9 of the Japanese Constitution. The use of force or threat of force is prohibited under international law,¹⁵ which is reflected in Article 9(1) of the Constitution. There are two exceptions to this principle under international law: (i) the authorization of the use of force by the United Nations; and (ii) the exercise of the inherent right of individual or collective self-defense.

While the Japanese Constitution does not explicitly recognize these exceptions, the “war-renunciation” clause must be interpreted in light of the applicable rules of international law, including the 1960 Treaty of Mutual Cooperation and Security between Japan and the United States,¹⁶ as prescribed under Article 98(2) of the Constitution.¹⁷ This means that notwithstanding the constitutional commitment not to maintain land, sea, and air forces, or other war potential under Article 9(2) of the Constitution, the clause must be read to allow

the SDF to engage in the use of force under United Nations authorization or in the exercise of the inherent right of individual or collective self-defense, so long as such force is limited to the minimum extent necessary to implement the UN mandate or to repel armed attacks. In other words, Article 9 of the Constitution does not entirely deprive Japan of justifications for the use of force available under international law, but rather limits the way in which, and the extent to which, the nation may engage in the use of force.

Under Japanese domestic law, the legislative bases for resorting to the use of armed force are restricted due to Article 9 of the Constitution. The primary legislative basis for resorting to the use of armed force is codified in Article 76 of the Law concerning the Self-Defense Forces (SDF Law),¹⁸ which authorizes the prime minister to direct deployment of SDF units in the event of an armed attack against Japan (i.e., an exercise of national defense power). Amendments introduced by the 2015 security legislation have expanded the scope of Japan's national defense power in cases where an armed attack occurs against a country that has a close relationship with Japan and, as a result, threatens Japan's survival and poses a clear danger that fundamentally undermines the lives and freedoms of its nationals and their right to pursue happiness (i.e., when there is an existential threat to Japan).¹⁹

In exercising the national defense power, the prime minister may authorize the SDF to use armed force to the extent necessary to defend the nation in accordance with Article 88 of the SDF Law.²⁰ The Defense Against an Armed Attack Law establishes procedural requirements that must be met in order for the prime minister to exercise this national defense power.²¹

The official Japanese government position that has traditionally been adopted is that an overseas deployment of SDF units for the purposes of the use of force in a foreign territory, its territorial sea or the airspace above it, is prohibited under the Constitution.²² This is because such action generally goes beyond the minimum level of force necessary for self-defense.²³ Prime Minister Abe reaffirmed this official position at the Budget Committee of the House of Counsellors on August 24, 2015, stating that the SDF's participation in combat operations in a foreign territory would amount to an overseas deployment prohibited under the Constitution.²⁴ This excludes the SDF's participation in the theater of combat in and around the Korean Peninsula in the exercise of the right of self-defense when hostilities have erupted.

This does not mean, however, that Japan is constitutionally prohibited from defending or assisting U.S. forces in the exercise of the right of collective self-defense. Upon the adoption of the U.S.-Japan Security Treaty in 1960 the official position of the Japanese government was essentially that Japan had the right of collective self-defense, but its exercise involving the use of force to defend other countries on foreign soil would exceed the minimum level of force necessary for self-defense.²⁵ In other words, Article 9 of the Constitution does not necessarily

prohibit Japan from exercising the right of self-defense as the legal basis for justifying SDF action in and around Japan to defend the U.S. and its interests when an armed attack occurs against the latter. The minimum level of force required for self-defense is not a static concept, but evolves over time as the geopolitical climate and technological capabilities change. In situations where the defense system of two nations is integrated to the extent that the survival of either nation is interdependent on the other's defense capabilities, it naturally follows that the line between individual and collective self-defense becomes blurred. Thus, the 2015 security legislation aimed to clarify that the SDF is not precluded from engaging in the use of force to defend and assist U.S. forces, including on the high seas—which are outside the jurisdiction of any foreign state.

Also, in cases where UN Command is engaged with a resumption of hostilities on the Korean Peninsula,²⁶ the Constitutional restriction does not prevent Japan from authorizing the deployment of the SDF. Japan indeed enacted special legislation to provide support activities in the Indian Ocean for military operations in Afghanistan and to engage in humanitarian and reconstruction support activities in Iraq.²⁷

Prior to making such a decision, however, questions might arise as to whether the U.S. assets in Japan can be deployed without prior consultation with Japan under the terms of the U.S.-Japan Security Treaty.²⁸ Notwithstanding Japan's official position ostensibly to the contrary, there is sufficient evidence to suggest that the U.S. does not believe prior consultation is required for the use of its military facilities and equipment in Japan, in the event of hostilities on the Korean Peninsula.²⁹ In any event, neither party to a bilateral treaty can be bound by any particular interpretation unless the other party is fully aware of such an interpretation and has accepted it as the shared understanding of the relevant treaty term.³⁰

In addition, the SDF is authorized under the SDF Law to use “weapons” in limited circumstances. This authorization for the use of “weapons” does not constitute a “use of force” as an exercise of national defense power as far as Japanese domestic law is concerned, even though it might constitute a “use of force” that requires legal justification under international law. For example, the use of weapons is authorized when it is necessary to:

- destroy ballistic missiles directed at Japan;³¹
- protect Japanese nationals and other designated foreign nationals in a foreign country;³²
- protect individuals under the SDF's control during a transport operation;³³
- protect SDF's defense assets;³⁴ and
- protect the defense assets of U.S. forces or other countries that contribute to the defense of Japan³⁵

In these situations, the legitimate use of weapons is permitted only to the

extent reasonable under the attendant circumstances and must not cause death or injury unless it can be justified as self-defense or necessity under Articles 36 and 37 of the Criminal Code of Japan.³⁶ Amendments introduced by the 2015 security legislation have expanded the scope within which the SDF personnel are authorized to use weapons. They are now allowed to protect not only themselves but also other individuals under their control or in the same compound, when engaging in support activities under grave circumstances affecting Japan's peace and security (e.g., when Japan might be subject to an armed attack if the situation were left unattended, but the SDF may operate only outside combat zones).³⁷

The decision as to which of these legislative bases might actually be used in the event of hostilities on the Korean Peninsula ultimately depends on the Japanese government's assessment of the attendant circumstances and various political considerations. This political decision will inform the SDF of the relevant legal framework for action. However, as will be explained below, each of these legislative bases is tightly regulated due to the constitutional limitation on the use of force and the controversies related thereto.

Legal Challenges in the Event of Hostilities on the Korean Peninsula

COMBINED SECURITY OPERATIONS

It is generally understood among security experts that key to the maintenance and enhancement of the U.S.-Japan alliance is Japan's legal readiness to effectively use the technological capabilities it has in a combined security operation to track missiles launched by North Korea.³⁸ Under the 2015 security legislation, there are three different legislative bases for the protection of U.S. forces by the SDF:

1. the protection of U.S. defense assets, with the limited use of weapons to the extent reasonable under the attendant circumstances;³⁹
2. the protection of individuals within the SDF's control during support activities under grave circumstances affecting Japan's peace and security (e.g., when Japan might be subject to an armed attack if the situation were left unattended, but the SDF may operate only outside combat zones);⁴⁰ and
3. the authorization of the use of force in situations where an armed attack occurs against a country that is in a close relationship with Japan and, as a result, threatens Japan's survival and poses a clear danger that fundamentally undermines the lives and freedoms of its nationals, and their right to pursue happiness (i.e., when there is an existential threat to Japan).⁴¹

The first two legislative bases allow SDF personnel to use weapons to a limited

extent within the law enforcement paradigm. This means that weapons can only be used to the extent reasonable to execute their mission (e.g., the protection of U.S. defense assets), and such use of weapons must not result in injury or death unless it is justifiable as self-defense or necessity under Articles 36 and 37 of the Japanese Criminal Code.⁴² On the other hand, the third legislative basis triggers the SDF's action in situations of national self-defense, with authority to use armed force to the extent necessary to repel armed attacks.

The first possible scenario where Japan might participate in a combined security operation with the U.S., in the event of hostilities on the Korean Peninsula, is when Japan recognizes itself as being subject to an armed attack or, in accordance with the new security legislation, when facing an existential threat resulting from an armed attack against the U.S.. Indeed, Prime Minister Abe observed during the 2015 Diet debate that the new security legislation would extend to the protection of U.S. Navy vessels from a missile attack launched by North Korea when those vessels form an integral part of Japan's missile defense system.⁴³ This statement indicates political readiness to invoke the national defense power under Article 76 of the SDF Law when hostilities on the Korean Peninsula threaten Japan's missile defense system and U.S. defense assets that form an integral part thereof. The decision might cause domestic controversy as to whether the missile attack amounts to an armed attack directed against Japan or whether the launch poses an existential threat to Japan, but in such a scenario, it can legitimately be justified as an exercise of the right of national self-defense under Article 51 of the UN Charter.

The alternative scenario could arise if Japan authorizes the SDF, in accordance with the Law Concerning Grave Circumstances, to undertake support activities for armed forces of other countries that are contributing to Japan's peace and security or to international peace and security. Operating within the law enforcement paradigm, the SDF's actions must comply with stringent regulations governing the use of weapons and are prohibited in areas where combat activities are taking place.⁴⁴ Nevertheless, during the Diet debate in August 2015, then Defense Minister Nakatani indicated that the SDF could defend a U.S. Navy vessel engaged in a combined security operation from an incoming missile attack by using a defensive missile under the new legislation concerning grave circumstances affecting Japan's peace and security.⁴⁵

Under international law, however, such action clearly constitutes a use of force that requires justification based on the right of self-defense or UN authorization. It is widely accepted that force may be used in law enforcement provided that such force is unavoidable, reasonable and necessary for the purpose of effecting the objects of law enforcement such as boarding, searching, seizing and bringing into port a suspected vessel.⁴⁶ Defending a foreign warship goes beyond the strict limitation imposed upon the use of force in maritime law enforcement

under international law and can only be justified as an exercise of the right of collective self-defense or as an action under UN authorization.

An attempt to justify the SDF's actions to defend U.S. Navy vessels based on the Law Concerning Grave Circumstances thus creates a legal paradox—it is a law enforcement action under Japanese domestic law, but the same conduct constitutes a use of force under international law that requires justification as an exercise of the right of collective self-defense. Even though the public debate concerning the 2015 security legislation focused on the constitutionality of the right of collective self-defense, the actual scope of the use of force newly authorized is so narrowly confined that it does not support a clear case of collective self-defense.

NON-COMBATANT EVACUATION OPERATIONS (NEO)

Prior to and in the event of hostilities on the Korean Peninsula, Japan and the U.S., among many other countries, will be involved in rescue and evacuation operations for the relocation to a place of safety of designated non-combatants, namely their own nationals and other designated foreign nationals residing in South Korea. Although each state is responsible for the development and execution of its own national evacuation plan, multiple states are likely to coordinate their rescue efforts according to their own legal framework and operational capabilities. Coordination with other states will help optimize limited assets available for the evacuation of foreign nationals. However, the requirement of consent as the legal basis for the SDF's deployment within South Korean territory would necessarily constrain the SDF's ability to facilitate and carry out rescue and evacuation operations. Japan's legal position is that rescue and evacuation operations must be conducted with the consent of South Korean authorities or, alternatively, under UN authorization.⁴⁷ In other words, the SDF's overseas rescue missions are strictly prohibited without consent of the host state or UN authorization. Also, its ability to use weapons necessary to perform rescue and evacuation operations is restricted to areas where no combat is taking place.⁴⁸ The United States, on the other hand, merely requires that "the NEO planners are aware of sovereignty of other foreign nations and the constraints and restraints on violating the sovereignty".⁴⁹ Under international law, the legality of the use of force by a state to protect its own nationals in a foreign state without consent of the latter is far from established, due to inconsistent and equivocal state practice.⁵⁰

The use of force necessary to protect Japanese and foreign nationals from attacks or the effects of attacks is one of the critical areas in which the SDF's ability to facilitate rescue and evacuation operations will be restricted unless South Korean authorities are prepared to provide an express consent thereto. This is a particularly acute area of concern for political reasons (e.g., the territorial dispute over Dokdo/Takeshima, among others), as well as historical reasons (e.g., Japan's occupation of the Korean Peninsula and forced labour during World War II). Due

to these concerns, South Korea would likely be reluctant to allow the SDF to engage in any military operation on its soil.

During a rescue and evacuation operation, any engagement between the SDF and members of North Korean forces, militia or voluntary corps, or anyone acting under the direction and control of the North Korean regime, would constitute hostilities in an international armed conflict. In such a situation, the SDF would be required to comply with the full range of rules under international humanitarian law, including the law of targeting, and would not be able to circumvent its obligations by asking other states to intervene. It follows that the SDF are under the obligation to verify legitimate military targets, to exercise all feasible precautions to minimize collateral damage, and to refrain from or stop executing an attack if it is reasonably expected to cause excessive collateral damage relative to the concrete and direct military advantage anticipated.⁵¹ Furthermore, Japan will be required to respect and ensure respect for international humanitarian law,⁵² arguably with the positive obligation to take action when the SDF have the capabilities and opportunities to prevent or stop war crimes being committed.⁵³ As such, the SDF cannot disregard relevant rules of international law applicable to an international armed conflict, even if they participate in rescue and evacuation operations with the consent of South Korean authorities. These rules apply in parallel to Japanese domestic law regulating the conduct of the SDF and within the parameters of the consent provided by South Korean authorities. These legal complexities, as well as associated legal risks, must be carefully assessed before the deployment of the SDF to complex operational environments that are expected to develop during rescue and evacuation operations.

MARITIME SECURITY OPERATIONS

The maritime domain is likely to be another major theater in which the SDF must operate. In the event of hostilities, civilians and defectors are likely to flee hostilities in large numbers by seeking refuge through maritime routes or by crossing the border into the PRC. Among those fleeing could be North Korean operatives on a covert mission to sabotage search and rescue operations at sea or infiltrate South Korean or Japanese territories. Depending on how the PRC and Russia engage with such hostilities, their navy vessels could be present in the vicinity of the maritime routes used by asylum seekers. These factors complicate the maritime conditions under which SDF vessels might be required to operate in facilitating the evacuation of Japanese and foreign nationals or their protection from hostilities.

First, the SDF could face a situation where the obligation to assist people in distress arises under the law of the sea or international human rights law. Japan has ratified the 1982 UN Convention on the Law of the Sea and the 1974 International Convention for the Safety of Life at Sea, which requires the master of a ship to render assistance to persons in distress.⁵⁴ Japan is also a party to the International

Covenant on Civil and Political Rights, which arguably imposes on it positive obligations to protect the right to life at sea within its jurisdiction.⁵⁵ Depending on how wide the scope of jurisdiction is interpreted for the purposes of applying the Covenant, the SDF may be required to protect the human rights of any individuals with whom it comes into contact at sea, for example, those on board any ships which SDF personnel visit and search to verify their nationality.⁵⁶ These obligations include non-refoulement when there are substantial grounds to believe that the relevant individuals would face a real risk of being persecuted or subject to torture and cruel, inhuman or degrading treatment upon return.

Second, further complication might arise when hostile actors, with the intent to engage in subversive activities and disrupt evacuation operations, disguise themselves as asylum seekers or civilians on merchant vessels. SDF vessels may be authorized to inspect foreign-flagged ships, with the consent of the flag state, when the situation is recognized as constituting grave circumstances affecting Japan.⁵⁷ Alternatively, the SDF may be authorized to use armed force in the exercise of national defense power under Articles 76 and 88 of the SDF Law in response to an armed attack directed against Japan or its close ally. Yet, the application of national defense power to maritime security operations in such a scenario depends upon whether subversive activities form part of the larger context of the armed attack to which the SDF are responding. Likewise, the applicability of international humanitarian law in such a scenario also depends on whether the subversive activities form part of the larger context of hostilities. When their identity or link to the larger context of hostilities is unclear, the SDF would face a legal “grey zone” due to uncertainty as to which body of international law applies to the use of force (including weapons) and to the treatment of hostile actors who are captured.⁵⁸

Third, Article 9 of the Constitution restricts the ways in which the SDF may engage in hostilities in the maritime context. The explicit denial of the right of belligerency in the second paragraph of the war-renunciation clause imposes not only stricter requirements on the justification for the use of force (under *jus ad bellum*) but also precludes Japan from engaging in certain types of belligerent acts that are traditionally permitted for the navy (under *jus in bello*). Therefore, without prejudice to any UN-authorized maritime enforcement operations, there are constitutional limitations on the extent to which the SDF may participate in naval operations such as naval blockade, interdiction of neutral ships, seizure of enemy ships, or employing naval mines in foreign territorial waters.⁵⁹

Conclusion

In the event of hostilities on the Korean Peninsula, there will be many scenarios where Japan is required to consider use of force options—such as defending U.S. navy vessels engaged in combined security operations, protecting Japanese and foreign nationals during rescue and evacuation operations, and engaging in various maritime security operations—either by stretching the meaning of an existential threat or by an expansive reading of the permitted use of weapons during support activities within the law enforcement paradigm. The benefit of such an attempt to stretch the legislative grounds for justifying specific use of physical force must be weighed against its political, diplomatic, constitutional and operational ramifications. As examined above, the constraints of the legislative framework limit Japan's legal options to justify the use of force in prosecuting various missions in the event of hostilities on the Korean Peninsula.

Even though the 2015 security legislation aimed to enable Japan to adopt a “seamless response” to contemporary security threats, it did not go far enough to address the inherent gap in Japan's security law regime so as to allow the SDF to employ armed force as necessary in a variety of settings. This problem is not unique to SDF's operations in and around the Korean Peninsula, but applies equally to hostilities in Taiwan and other parts of Asia. For the U.S.-Japan alliance to remain as the anchor of regional security in the Asia-Pacific, the U.S. and Japanese defense agencies will have to work together to develop a mutual understanding of legally defensible options for each country in a wide range of operational scenarios that are expected to arise in the event of hostilities in the region. ■

Hitoshi Nasu joined the Exeter Law School in January 2018. Prior to his current appointment, he taught at Australian National University, where he was Co-Director of the Centre for Military and Security Law and the Australian Network for Japanese Law. Currently, he is also an adjunct senior fellow of S. Rajaratnam School of International Studies at Nanyang Technological University in Singapore and managing co-director of the Woomera Manual Project on the International Law of Military Space Operations.

He publishes widely in the field of public international law, especially international security law and the law of armed conflict. His expertise extends to a wide range of international security law issues, such as collective security, peacekeeping, the protection of civilians in armed conflict, the responsibility to protect, maritime security, cyber security, human security, national security and the protection of state secrets, regional security, disaster relief and management, security institutions and international rule of law, and new technologies and the law of armed conflict, with over 70 scholarly publications.

- 1 Article 9 of the Constitution reads: "(1) Aspiring sincerely to an international peace based on justice and order, the Japanese people forever renounce war as a sovereign right of the nation and the threat or use of force as means of settling international disputes. (2) In order to accomplish the aim of the preceding paragraph, land, sea, and air forces, as well as other war potential, will never be maintained. The right of belligerency of the state will not be recognized." Constitution of Japan, art. 9.
- 2 Cabinet Bill No. 72 of the 189th Diet (Japan); Cabinet Bill No. 73 of the 189th Diet (Japan).
- 3 Law No. 76 of 2015 (Japan); Law No. 77 of 2015 (Japan).
- 4 For the author's analysis of the 2015 security legislation, see Hitoshi Nasu, *Japan's 2015 Security Legislation: Challenges to its Implementation under International Law*, 92 Int'l L. Stud. 249 (2016).
- 5 Treaty on the Non-Proliferation of Nuclear Weapons, July 1, 1968, 729 U.N.T.S. 161. See also Int'l Atomic Energy Agency [IAEA], *Report of the Implementation of the Agreement between the Agency and the Democratic People's Republic of Korea for the Application of Safeguards in connection with the Treaty on the Non-Proliferation of Nuclear Weapons*, IAEA Doc. Gov/2636 (Feb. 25, 1993).
- 6 S.C. Res. 1695, pmb. ¶ 4 (July 15, 2006).
- 7 S.C. Res. 1718, ¶¶ 5–7 (Oct. 14, 2006).
- 8 *Id.*, ¶ 8.
- 9 S.C. Res. 1874, ¶¶ 11–13 (June 12, 2009).
- 10 See, e.g., S.C. Res. 2397 (Dec. 22, 2017); S.C. Res. 2375 (Sep. 11, 2017); S.C. Res. 2371 (Aug. 5, 2017); S.C. Res. 2321 (Nov. 30, 2016); S.C. Res. 2270 (Mar. 2, 2016); S.C. Res. 2094 (Mar. 7, 2013); S.C. Res. 2087 (Jan. 22, 2013); Statement by the President of the Security Council, U.N. Doc. S/PRST/2012/13 (Apr. 16, 2012).
- 11 For commentaries, see Dapo Akande, *The Korean War Has Resumed!! (Or So We Are Told)*, EJIL: Talk! (July 22, 2009), <http://www.ejiltalk.org/the-korean-war-has-resumed-or-so-we-are-told/>; Seunghyung Sally Nam, *Has North Korea Terminated the Korean Armistice Agreement?*, EJIL: Talk! (July 24, 2009), <http://www.ejiltalk.org/has-north-korea-terminated-the-korean-armistice-agreement/>.
- 12 See Statement by the President of the Security Council, U.N. Doc. S/PRST/2010/13 (July 9, 2010).
- 13 See U.N. Human Rights Council, *Report of the Commission of Inquiry on Human Rights in the Democratic People's Republic of Korea*, UN Doc. A/HRC/25/63 (Feb. 7, 2014).
- 14 The White House, Joint Statement of President Donald J Trump of the United States of America and Chairman Kim Jong Un of the Democratic People's Republic of Korea at the Singapore Summit ¶ 3 (2018), <https://www.whitehouse.gov/briefings-statements/joint-statement-president-donald-j-trump-united-states-america-chairman-kim-jong-un-democratic-peoples-republic-korea-singapore-summit/>; Repub. of Kor. Ministry of Foreign Affairs, Panmunjom Declaration for Peace, Prosperity and Unification of the Korean Peninsula (2018), <http://www.mofa.go.kr/viewer/skin/doc.html?fn=2018091804122336&rs=/viewer/result/20191>.
- 15 U.N. Charter art. 2(4). Its status as customary international law has been confirmed by the International Court of Justice in *Military and Paramilitary Activities in and Against Nicaragua (Nicar. v U.S.)*, Merits, 1986 I.C.J. Rep. 14, ¶¶ 99–101, 188–90 (June 27).
- 16 Treaty of Mutual Cooperation and Security Between the United States of America and Japan, Japan-U.S., Jan. 19, 1960, 11 U.S.T. 1632, T.I.A.S. No. 4509.
- 17 Article 98(2) of the Constitution reads: "The treaties concluded by Japan and established laws of nations shall be faithfully observed." Constitution of Japan, art. 98(2).

This by no means suggests any normative hierarchy between international law and Japanese domestic law, but simply provides a constitutional basis for the interpretative principle. See Hitoshi Nasu, *Article 9 of the Japanese Constitution: Revisited in the Light of International Law*, 19 J. Japanese L. 50 (2004).

18 Law No. 165 of 1954 (Japan) [hereinafter SDF Law].

19 Law No. 76 of 2015, *supra* note 3, arts. 1, 5.

20 The use of armed force must comply with the relevant rules and customs of international law and must not exceed what is considered reasonable under the attendant circumstances. SDF Law, *supra* note 18, art. 88(2).

21 Law No. 79 of 2003 (Japan).

22 Resolution against Overseas Deployment of the Self-Defence Forces, adopted at the House of Councillors, 19th Diet Sess. (1954).

23 See Takeshi Nakano (仲野武志), *Buryoku Kōshi Buki Shiyō no Hōteki Kisei (II) (武力行使・武器使用の法的規制 (二))* [The Legal Regulation of the Use of Force/ Use of Weapons (II)], 93(10) *Jichi Kenkyū (自治研究)* [Autonomy Stud.] 49, 56–57 (2017).

24 Remarks before the Budget Committee of the House of Counsellors, 189th Diet Sess. Official Record of Proceedings, No. 20, at 12 (Aug. 24, 2015).

25 See, e.g., Prime Minister Nobusuke Kishi, Remarks before the Special Committee of the House of Representatives on the Japan-U.S. Security Treaty and Other Matters, 34th Diet Sess. Official Record of Proceedings, No. 21, at 27, 31, 33–34, (Apr. 20, 1960); Remarks before the Budget Committee of the House of Councillors, 34th Diet Sess. Official Record of Proceedings, No. 23, at 24, 27 (Mar. 31, 1960); Masami Takatsuji, Dir. of Cabinet Legislative Bureau, Remarks before the Budget Committee of the House of Councillors, 61st Diet Sess. Official Record

of Proceedings, No. 5, at 12 (Mar. 5, 1969). The official position has since then been simplified with reference to the exercise of the right of collective self-defense more generally, but without clarifying whether the exercise of the right envisaged is limited to overseas deployment or more broadly includes assistance in and around Japan. See, e.g., Prime Minister Zenko Suzuki, Response to House Member Seiichi Inaba (May 29, 1981). See also Takahiro Suzuki (鈴木尊紘), Kenpō dai 9-jō to Shūdantekijieiken (憲法第9条と集団的自衛権) [Article 9 of the Constitution and the Right of Collective Self-Defence], 11 Reference 2, 37–40 (2011); Kiyoshi Sakaguchi (坂口規純), Shūdantekijieiken ni Kansuru Seifu Kaishaku no Keisei to Tenkai (I) (集団的自衛権に関する政府解釈の形成と展開 (上)) [The Formation and Development of Government Interpretation Regarding the Right of Self-Defence (I)], 1330 *Gaikou Jihou (外交時報)* [Dipl. Rev.] 70, 79–84 (1996).

26 The U.N. Command in Korea has continued to operate since its establishment under S.C. Res. 84, ¶ 3 (July 7, 1950) to preserve the 1953 Armistice Agreement and to maintain control of U.N. Forces. Sixteen nations that contributed troops pledged that they should be “united and prompted to resist” if there was a renewal of the armed attack: Joint Policy Declaration Concerning the Korean Armistice, July 27, 1953, 4 U.S.T. 230, T.I.A.S. No. 2781.

27 Law No. 113 of 2001 (Japan) (expired in 2007 after extended three times); Law No. 137 of 2003 (Japan) (expired in 2009 after extended once).

28 Prior consultation is required for any military use of facilities and areas in Japan for the purpose of contributing to the security of Japan and the maintenance of international peace and security in the Far East, except when the U.S. takes action in self-defence under Article V of the U.S.-Japan Security Treaty. See *Exchange of Notes Regarding the Implementation of Article VI of Treaty of Mutual Cooperation and Security between Japan and the United States of America*, 42 Dep’t St. Bull. 198 (1960) (in which both

parties shared understanding that “[m]ajor changes in the deployment into Japan of United States armed forces, major changes in their equipment, and the use of facilities and areas in Japan as bases for military combat operations to be undertaken from Japan *other than those conducted under Article V of the said Treaty*, shall be the subjects of prior consultation with the Government of Japan”) (emphasis added).

29 For details, see Kazuya Sakamoto (坂元一哉), *Nichibeidōmei no Kizuna* (日米同盟の絆) [The Bonds of the Japan-U.S. Alliance] 257–66 (2000).

30 See *Kasikili/Sedudu Island* (Bots. v. Namib.), Judgment, 1999 I.C.J. Rep. 1045, ¶ 74 (Dec. 13); *Dispute between Argentina and Chile concerning the Beagle Channel*, 21 R.I.A.A. 53, ¶ 169 (Perm. Ct. Arb. 1977).

31 SDF Law, *supra* note 18, arts. 82.3, 93.3.

32 *Id.* arts. 84.3, 94.5.

33 *Id.* arts. 84.4, 94.6.

34 *Id.* art. 95.

35 *Id.* art. 95.2 (as amended by Law No. 76 of 2015).

36 Law No. 45 of 1907 (Japan).

37 Law Concerning Measures to Ensure Peace and Security of Japan in Situations that Constitutes Grave Circumstances Affecting Japan, Law No. 60 of 1999, as amended by Law No. 76 of 2015 (Japan) [hereinafter Law Concerning Grave Circumstances], arts. 1, 2(3), 11; SDF Law, *supra* note 18, arts. 84.5, 94.7.

38 Report of the Advisory Panel on the Reconstruction of the Legal Basis for Security 7 (2008), <http://www.kantei.go.jp/jp/singi/anzenhosyou/houkokusho.pdf>.

39 SDF Law, *supra* note 18, art. 95.2.

40 Law Concerning Grave Circumstances, *supra* note 37, arts. 1, 2(3), 11; SDF Law, *supra* note 18, arts. 84.5, 94.7.

41 SDF Law, *supra* note 18, arts. 76, 88.

42 Law No. 45 of 1907 (Japan).

43 Remarks before the Budget Committee of the House of Counsellors, *supra* note 24, at 12.

44 Law Concerning Grave Circumstances, *supra* note 37, art. 2(3).

45 Remarks before the Special Committee of the House of Councillors on the Bills for Peace and Security of Japan and the International Community, 189th Diet Sess. Official Record of Proceedings, No. 11, at 5 (Aug. 21, 2015).

46 *Dispute Concerning Delimitation of the Maritime Boundary between Guyana and Suriname* (Guy. v. Sur.), Award, 30 R.I.A.A. 1, ¶ 445 (Perm. Ct. Arb. 2007); *M/V Saiga* (No. 2) (St. Vincent and the Grenadines v. Guinea), Judgment of July 1, 1999, 3 ITLOS Rep. 10, ¶ 155; *Fisheries Jurisdiction* (Spain v. Can.), Judgment, 1998 I.C.J. Rep. 432, ¶ 84 (Dec. 4); S.S. “I’m Alone” (Can. v. U.S.), Final Award, 3 R.I.A.A. 1609, 1617 (Perm. Ct. Arb. 1935). See also Agreement for the Implementation of the Provisions of the United Nations Convention on the Law of the Sea of 10 December 1982 Relating to the Conservation and Management of Straddling Fish Stocks and Highly Migratory Fish Stocks art. 22(1)(f), Dec. 4, 1995, 2167 U.N.T.S. 3.

47 SDF Law, *supra* note 18, art. 84.3(2).

48 *Id.* art. 84.3(1).

49 U.S. Joint Chiefs of Staff, Joint Publication 3-68 on Noncombatant Evacuation Operations, Appendix B Legal Considerations ¶ f(2) (2015).

50 See, e.g., Tom RuyRuys, ‘Armed Attack’ and Article 51 of the UN Charter: Evolutions in Customary Law and Practice 213–43 (2011).

51 Note that the SDF would also be subject to South Korean jurisdiction unless Japan has concluded a status of force agreement with South Korea with a view to enabling the SDF to operate without facing criminal liability for their actions during rescue and evacuation operations.

52 Common Article 1 to the Convention for The Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31; Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85; Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135; Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, 1125 U.N.T.S. 3. For the customary international law status, see Jean-Marie Henckaerts & Louise Doswald-Beck, Customary International Humanitarian Law r. 139 (2005), as updated by the International Committee of the Red Cross (ICRC) at <https://ihl-databases.icrc.org/customary-ihl/eng/docs/home>.

53 Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field ¶¶ 169–72 (Knut Dörmann, Liesbeth Lijnzaad, Marco Sassòli & Philip Spoerri eds., 2016).

54 United Nations Convention on the Law of the Sea art. 98(1), Dec. 10, 1982, 1833 U.N.T.S. 397 [hereinafter LOSC]; International Convention for the Safety of Life at Sea ch. V, Regulation 10(a), Nov. 1, 1974, 1184 U.N.T.S. 278.

55 International Covenant on Civil and Political Rights arts. 2, 6, Dec. 16, 1966, 999 U.N.T.S. 171.

56 LOSC, *supra* note 54, art. 110. Cf. Medvedyev and Others v. France, App. No. 3394/03, Eur. Ct. H.R. ¶ 67 (2010) (determining that the non-flagged vessel *Winner* and its crew were within the jurisdiction of France for having exercised, *de facto*, full and exclusive control over them).

57 Law Concerning the Implementation of Ship Inspection Activities in Situations that Constitute Grave Circumstances Affecting Japan, Law No. 45 of 2000 (Japan), arts. 2, 6 (amended by Law No. 76 of 2015).

58 For the author's analysis of the challenges posed to the implementation of international humanitarian law by hybrid warfare employed in the maritime context, see Hitoshi Nasu, *Challenges of Hybrid Warfare to the Implementation of International Humanitarian Law in the Asia-Pacific*, in Asia-Pacific Perspectives on International Humanitarian Law 220 (Suzannah Linton, Tim McCormack & Sandesh Sivakumaran eds., 2019).

59 See, e.g., Masasuke Ohmori, First Dir. of Cabinet Legislative Bureau, Remarks before the Special Security Committee, 120th Diet Sess. Official Record of Proceedings, No. 5, at 26 (Mar. 13, 1991).



Michael J. Adams

Commander (ret.),
U.S. Navy

Reconsidering International Law and Cyberspace Operations Through the Lens of the U.S.- Japan Alliance

Introduction

The U.S.-Japan Alliance, rooted in the 1952 Security Treaty Between the United States and Japan and reinforced by amendment through the 1960 Treaty of Mutual Cooperation and Security, is built upon presumptions of clarity in international law. Implicitly these foundations embrace Westphalian concepts of sovereignty, jurisdiction, and geography and presuppose that clear lines exist between peace and war. More directly, the treaties accept that the use of force and armed attack, as reflected in the United Nations Charter and international law, are prohibited, widely understood, and applicable to the types of security concerns most relevant to the U.S.-Japan Alliance.

However, it is not at all clear that these assumptions are valid in cyberspace or that Japan's developing security ambitions will allow the government to remain tethered to the physical territories of Japan or legal archetypes bound by geography. Japan is actively exploring its future role in the global commons.¹

This move may be driven by the realities of the increasingly globalized security environment and political necessity as regional threats are manifesting at sea, in space, and in cyberspace.² Yet whatever the cause, the Japanese government seems to be weighing whether cyberspace presents conditions that deviate from the order envisioned in the Charter, Alliance treaties, and Japan's Constitution. There appears to be real interest in assessing whether international law may provide room to maneuver towards a more "proactive" cyber security posture and, if so, whether Japan's domestic laws might permit such an approach.

While embracing the applicability of international law to cyberspace operations,³ the U.S. government has determined that a great deal of freedom exists in the domain—particularly when acting on the international plane in individual or collective self-defense. After spending years building infrastructure and cyber operations teams,⁴ military commanders have now been granted broader authorities at lower levels to conduct cyber operations.⁵ What precisely this means

in practice is hard to determine outside of highly classified environments. Still, a clear shift in the United States' approach to cyber operations has occurred, and that shift is organized to a great degree towards more persistent operations and defensive activities.⁶

Japan has embarked on a broader transformation of its historically inward-looking, peace-seeking security posture. For nearly a decade, the Japanese government has been working to enhance coordination and optimize efficiencies within the nation's national security architecture, and much attention has been given to Japan's role in cyberspace. However, the lack of consensus about how international law applies in the cyber context has left the Japanese government questioning how to best adapt to cyber threats while still comporting with Japan's international and domestic legal obligations.

This essay explores contemporary understandings of international law and cyberspace operations through the lens of the U.S.-Japan Alliance. Part I presents cyber operations as an instrument of national power and highlights the “defend forward” posture of the U.S. government as well as the Japanese government's move to a more proactive role in cyberspace. Part II outlines the international legal framework applicable to cyber operations and gaps therein and presents contested subjects such as sovereignty and notice of countermeasures. Part III describes at a high-level how the United States and Japan might partner in defensive cyber scenarios. It explores the possibility that malicious cyber operations not rising to the level of use of force directed against the United States and Japan may present more frequent, and perhaps more substantial, occasions for U.S.-Japan Alliance forces to conduct “self-help and mutual aid.”⁷

DEFENDING FORWARD AND PROACTIVE SECURITY

“Globally, the scope and pace of malicious cyber activity continues to rise. The United States’ growing dependence on the cyberspace domain for nearly every essential civilian and military function makes this an urgent and unacceptable risk to the nation.”

—U.S. DEPARTMENT OF DEFENSE CYBER STRATEGY (2018)⁸

“In the international community, there is a broadening and diversifying array of security challenges that cannot be dealt with by a single country alone.”

—DEFENSE OF JAPAN WHITE 2019⁹

It is not difficult to identify the gravity of threats faced by the U.S.-Japan Alliance in the cyber domain. China, North Korea, and Russia have been repeatedly identified as malicious actors in cyberspace that exist in geographic proximity to Japan and to U.S and Japanese forces operating in the region.¹⁰ Their presence in the cyber domain is even closer at hand, with evidence that they and those working

on their behalf have already established placement and access in commercial and governmental systems and networks and are the most active among U.S.-Japan Alliance cyber adversaries.¹¹

Much has been made of Russia's cyber operations directed at the 2016 U.S. presidential election and of Russia's continuing misinformation campaigns. The production and rapid dissemination of false or misleading facts and narratives is certainly an issue worthy of attention, particularly when such occurrences negatively impact national security, economies, or political independence.¹² Yet constant changes in the cyber domain require routine reassessment of the realities of the realm. Threat assessments and descriptive devices—whether addressing technologies, activities by states and non-state actors, or the legal and policy regimes at play—have exceedingly limited shelf lives.

The United States is particularly concerned about cyber threats from China, Russia, North Korea, and Iran.¹³ This threat landscape may be due in no small part to the propensity of states to deliberately operate in the “grey zone”¹⁴ and employ “hybrid warfare” tactics.¹⁵ The Defense Department asserts that states are “deterred from engaging the United States and [its] allies in an armed conflict” and, instead, “are using cyberspace operations to steal [its] technology, disrupt [its] government and commerce, challenge [its] democratic processes, and threaten [its] critical infrastructure.”¹⁶ The targets of these threats are spread across public and private institutions.¹⁷

What may be most concerning about the operational environment is not the actors themselves as this cast has changed little in recent years, but the cumulative effects of their persistent cyber campaigns and the increasing technological proficiency, reach, and impact of states, non-state actors, and those who would act on their behalf.¹⁸ Impacts from attacks against critical infrastructure remain of utmost concern.¹⁹ These challenges are exacerbated by methods of obfuscation and deliberate efforts to limit the ability of states to act decisively in their defense. Timely attribution has long been a challenge in cyberspace, notwithstanding recent advancements in technology and attribution methods,²⁰ as states continue to leverage technical and legal ambiguity to avoid accountability.²¹

Japan shares many of these concerns and faces unique cyber challenges of its own.²² Japan has faced tens of billions of cyber attacks in a single year.²³ China, North Korea, and Russia are the Japanese government's leading concerns.²⁴ Yet “Japan's [cyber defenses] remain underdeveloped compared to the country's great reliance on information and communications technology.”²⁵ Cyber attacks in 2011 and 2015 were especially impactful—both to their targets and politically in Japan²⁶—leading the “reluctant cyberpower” to spend much of the past decade adjusting its approach to cyberspace.²⁷

The Japanese government has made clear that cybersecurity is central to its national security—implementing a series of legislative, strategic, and structural

changes focused on defense of the cyber domain²⁸ and embarking on an active campaign of cyber diplomacy.²⁹ Public-private partnerships are strengthening, and Prime Minister Abe's push for "Proactive Contribution to Peace" is manifesting in work underway to enhance the U.S.-Japan Alliance in cyberspace.³⁰

As the U.S. and Japanese governments implement their respective cyber initiatives, the 2015 Guidelines for U.S.-Japan Defense Cooperation (the "Guidelines") have focused military planners on specific national security goals. The Guidelines explain:

The United States Armed Forces and the Self-Defense Forces will:

- maintain a posture to monitor their respective networks and systems;
- share expertise and conduct educational exchanges in cybersecurity;
- ensure resiliency of their respective networks and systems to achieve mission assurance;
- contribute to whole-of-government efforts to improve cybersecurity; and
- conduct bilateral exercises to ensure effective cooperation for cybersecurity in all situations from peacetime to contingencies.³¹

Furthermore, the Guidelines describe in general terms plans for responding to "cyber incidents against Japan" and "serious cyber incidents that affect the security of Japan":

In the event of cyber incidents against Japan, including those against critical infrastructure and services utilized by the United States Armed Forces in Japan and the Self-Defense Forces, Japan will have primary responsibility to respond, and based on close bilateral coordination, the United States will provide appropriate support to Japan. The two governments also will share relevant information expeditiously and appropriately. In the event of serious cyber incidents that affect the security of Japan, including those that take place when Japan is under an armed attack, the two governments will consult closely and take appropriate cooperative actions to respond.³²

Note, however, that by their terms these response plans, which were built in the framework of a greater post-World War II defense strategy, would be entirely reactive.

But the U.S.-Japan Alliance is adjusting. As the U.S. and Japanese governments continue to discuss threats, capabilities, legal interpretations, and opportunities to partner in the future, there are additional measures being undertaken. For example, in 2018 U.S. Cyber Command reset its strategic concept, moving from "cyber response" to "cyber persistence"³³ and cyber forces began "defending forward."³⁴ In Japan, the government is working to "secure Japan's

resilience against cyberattacks and increase Japan's ability to defend the state (defense capabilities), deter cyberattacks (deterrence capabilities), and be aware of the situation in cyberspace (situational awareness capabilities)."³⁵ Furthermore, in 2019 U.S. and Japanese officials moved to deepen the Alliance in cyberspace and other cross-domain operations—a commitment recognizing that much could be done in the grey zone, that the U.S.-Japan Security Treaty does not prohibit cooperative activities in the absence of armed attack, and that it is not in the interests of the U.S.-Japan Alliance to wait for harmful cyber incidents to occur.³⁶

General Paul M. Nakasone summarized the need for change: “Our naval forces do not defend by staying in port, and our airpower does not remain at airfields. They patrol the seas and skies to ensure they are positioned to defend our country before our borders are crossed. The same logic applies in cyberspace.”³⁷

The United States

In 2018, the United States updated its National Cyber Strategy³⁸ and Department of Defense Cyber Strategy³⁹, which collectively set forth new ambitions and approaches for the U.S. government in cyberspace. The policy documents addressed the importance of cyber strength and resiliency for the United States, its allies, and partners. They were shaped by realities of the “day-to-day competition” in the cyber domain, of constant contact initiated by adversaries seeking to access, disable, or otherwise malign U.S. systems and networks.⁴⁰ They also outlined important measures being undertaken to ensure “a prosperous cyber future.”⁴¹

Significantly, the Department of Defense Cyber Strategy committed to preparing for “crisis or conflict” and “defending forward.”⁴² It envisions sustained operations across cyberspace, primarily outside of armed conflict and below the use of force.⁴³ As General Nakasone would later explain, this new approach was required because “the locus of struggle in the revived great-power competition has shifted toward cyberspace and ... decisive action can occur below the level of armed conflict.”⁴⁴ Thus, as a practical matter, the Department of Defense Cyber Strategy expresses the urgency for more robust, persistent cyber intelligence and defense operations.

This shift in approaches was possible because the Defense Department had spent years building U.S. military cyber architecture and forces. Because substantially more military cyber forces were in place than in years prior and because cyber forces were better organized, trained, and equipped, the Defense Department was able to adjust its mission to “move beyond the blue”⁴⁵ and start “imposing costs” on cyber adversaries.⁴⁶ The Department of Defense Cyber Strategy set forth the following areas of focus:

- conduct cyberspace operations to collect intelligence and prepare military cyber capabilities;

- defend forward to halt or disrupt malicious cyber activity at its source, including activity that falls below the level of armed conflict;
- strengthen the security and resilience of networks and systems;
- collaborate with interagency, industry, and international partners; and employ offensive cyber capabilities.⁴⁷

Further to the goals of moving more swiftly and effectively in cyberspace, in 2018 the Trump Administration issued National Security Presidential Memorandum-13, “United States Cyber Operations Policy” (NSPM-13).⁴⁸ NSPM-13 “allows for the delegation of well-defined authorities to the Secretary of Defense to conduct time-sensitive military operations in cyberspace.”⁴⁹ The primary effect of NSPM-13 was to replace prior administrations’ more deliberate, interagency review of cyber proposals at the highest levels of government—particularly outside of armed conflicts—with a broader delegation of authorities to the Defense Department. This design attempted to combat better the depth, breadth, and speed of actors in cyberspace.

The shift was not driven exclusively by the Executive Branch. U.S. federal law has also embraced the “need for speed”⁵⁰ and a more robust Defense Department cyber posture. Existing law that permitted defensive cyber operations⁵¹ was augmented by clear Congressional policy statements and requirements pertaining to cyberspace, cybersecurity, cyber warfare, and cyber deterrence.⁵² The principal message from Congress was that “the United States should employ all instruments of national power, including the use of offensive cyber capabilities, to deter if possible, and respond to when necessary, all cyber attacks or other malicious cyber activities of foreign powers that target United States interests.”⁵³

Japan

Although Japan is taking a more deliberate and seemingly less aggressive approach to defending cyberspace than the United States, nevertheless, there has been a significant move by the Japanese government in recent years to implement a more “proactive” and less isolated cybersecurity posture. The rationale behind the Abe administration’s approach is explained in the 2013 National Security Strategy:

The key of national security is to create a stable and predictable international environment, and prevent the emergence of threats. It is thus necessary for Japan to realize an international order and security environment that are desirable for Japan, by playing an even more proactive role in achieving peace, stability and prosperity of the international community as a “Proactive Contributor to Peace” based on the principle of international cooperation.

... Japan must have the power to take the lead in setting the international agenda and to proactively advance its national interests, without being confined to a reactionary position to events and incidents after they have already occurred.⁵⁴

The new tone and focus of the 2013 National Security Strategy were followed by substantial transformation efforts across Japanese national security policies, programs, and law.⁵⁵ Japan's National Security Council was established and charged with streamlining and unifying efforts across the government.⁵⁶ The Diet enacted legislation and interpretations that would permit the Self-Defense Force to expand its role in peacekeeping operations, asset protection, and logistics support, and potentially exercise a broader form of collective self-defense.⁵⁷ National Defense Program Guidelines were updated to expand defense roles and partnerships, as well as the domains in which Japanese forces will operate.⁵⁸

These advancements set the stage for progressive cyber moves as well. The government recognized cyberspace as a "frontier for creating infinite value" and committed to "us[ing] all means under its disposal to undertake cybersecurity initiatives in order to ensure that cyberspace remains ['free, fair and secure']."⁵⁹ Japanese cyber forces have been growing in size and responsibilities.⁶⁰ The Ministry of Defense and Self-Defense Force have been preparing a cross-domain architecture to address cyber operations as part of a new, streamlined joint operations system.⁶¹ A new "Multi-Domain Defense Force" is tasked with integrating cyber capabilities into operations across all domains.⁶² National Defense Program Guidelines now directly link national defense objectives to "deep[er] ... operational cooperation and policy coordination with the United States" in cyberspace.⁶³ Preparation for the 2020 Olympics has fast-tracked even more cybersecurity initiatives that have been developing under the Abe administration. Over time the aggregate impact of these measures should include improving national resilience, enhancing deterrence, and strengthening cyber situational awareness.⁶⁴

Might this proactive security approach grow into a Japanese version of defending forward? The Japanese government's renewed attention to action⁶⁵ echoes messages of its United States ally.⁶⁶ Still it seems unlikely that Japan's role in cyberspace will fundamentally transform the nation's restrained approach to national security. It may be true that "national security reforms under Abe, in the aggregate, constitute a significant and historic shift for Japan,"⁶⁷ but many observers believe that the government's "proactive security" posture still only extends so far as Japan is directly impacted or, at the most, to operations through which there is little chance of drawing Japan into armed conflict or requiring Japanese troops to use force.⁶⁸ Even the ground-breaking 2014 Diet reinterpretation permitting collective self-defense under the Japanese Constitution

is qualified by three substantial domestic legal conditions, including the existence of an existential threat.⁶⁹ Efforts to maintain Japan's peace and security may become less inward-looking and reactionary, but substantial historical, cultural, and legal barriers prevent Japan from changing into something other than the pacifist state that the Japanese Constitution envisioned.⁷⁰

Ultimately, the more interesting questions may be how far Japan is willing to extend into or “beyond the blue” of the cyber domain, how quickly it can bring tools and talent to bear in cyber operations, and what Japan's role will be in relation to other states that Japan may partner with in cyberspace operations. The Abe administration has promoted Japan's image as a “commons' guardian” and “effective ally and partner to the U.S. and other democracies.”⁷¹ But will the guardian's roles⁷² be limited to diplomacy, information sharing, capacity building, supply chain security, and other measures that might be accomplished without deliberately—and directly—confronting the “great-power competition” in cyberspace?⁷³ Or will increasing cyber situational awareness, deepened partnerships, the push for proactive security contributions, and constant contact with adversaries in and through cyberspace result in Japanese cyber forces bearing more profound responsibilities for the U.S.-Japan Alliance?

The Japanese government does not hide the fact that it must turn to broader cooperative security arrangements to preserve its security interests, and that foremost among such protections is the U.S.-Japan Alliance. The reality that, in cyberspace, “it is not possible for Japan to secure its peace and stability only by itself” underscores the importance of the U.S.-Japan Alliance.⁷⁴ Yet questions remain about how far the Japanese government will allow its forces to venture into the cyber domain over time.

In theory, Japan's interest in proactive security and the United States' defend forward posture could converge under the Treaty of Mutual Cooperation and Security (the “U.S.-Japan Security Treaty”). Those provisions of the U.S.-Japan Security Treaty that do the work—primarily Articles III, IV, V, and VI—acknowledge the importance of individual and collective preparatory measures to “resist armed attack,” agree to collective self-defense in the event of armed attack, and allow for staging U.S. forces in Japan for such purposes.⁷⁵ The Articles are concise instruments of constraint, collaboration, and accountability. Yet because the U.S.-Japan Security Treaty is largely a bare bones document—reflecting Articles 2(4) and 51 of the United Nations Charter and providing mechanisms for coming to the defense of the other party but deferring most other matters to implementing arrangements and the inter-workings of the governments—the most relevant security provisions are significant in the event of armed attack but matter little when facing conduct that does not rise to the level of using force.⁷⁶

Consequently, Japan's Constitution, implementing security legislation, other cyber-related laws, and Cabinet interpretations are particularly important. While

the United States maintains one of the most expansive state views of self-defense, Japan sits close to the other end of the spectrum. Government interpretations of the Japanese Constitution's war-renouncing clause, found in Article 9, generally prevent the use of force except when defending Japanese nationals' "right to life, liberty, and the pursuit of happiness" and even then only through the use of minimum force necessary.⁷⁷

This is a restrictive approach—understandable in light of Japan's "exclusively national defense-oriented policy"⁷⁸ but certainly more constraining than what international law permits under individual or collective self-defense doctrine.⁷⁹ Still these constraints may not matter much in cyberspace as a matter of law.

II. International Law and Cyberspace

"International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful [information and communications technologies] environment."

—UN GGE 2015 REPORT⁸⁰

It is not a question of "if" but "how."

International law applies to states' actions in and through cyberspace—the United States, Japan, the United Kingdom, France, China, Russia, Brazil, Egypt, Estonia, the Netherlands and numerous (but not all) other states have said so.⁸¹ Yet even those states agreeing that international law applies in cyberspace⁸² readily acknowledge that there is great uncertainty about how international legal norms, rules, and principles apply in the cyber domain.⁸³

Today there is no comprehensive treaty addressing international law in cyberspace. Customary international law for cyberspace is still developing. General principles of law are contested vigorously—including within the U.S. government. And most states—even those actively engaged in discussions about international law and cyberspace—have not articulated governmental positions with much specificity or consequence.⁸⁴

Some scholars speak with great clarity and optimism about the application of international law to cyberspace.⁸⁵ Certainly strong interest exists within the international community in building consensus on substantive legal issues. Cyber diplomacy has been shaping states' understanding of critical topics and unsettled areas while promoting responsible behavior.⁸⁶ Noteworthy contributions have been made in the field. States are making progress on "norms of behavior of responsible states" in cyberspace.⁸⁷ The Budapest Cybercrime Convention⁸⁸ and the European General Data Protection Regulation⁸⁹ are major international agreements addressing subjects of relevance to security issues in cyberspace. The Tallinn Manual and Tallinn 2.0 are thoughtful, detailed works that provide a great deal

of insight about international law but, read carefully, underscore the uncertainty prevalent in the area.⁹⁰

Discussions among the aforementioned groups are unlikely to bring near-term clarity on matters that have long been debated among international lawyers, such as sovereignty, non-intervention, and coercion. These vigorously debated issues seem even more complex than ever in cyberspace, with states offering seemingly irreconcilable views.⁹¹ It has also been emphasized that “[i]nitiatives by non-governmental groups like those that led to the Tallinn Manual can be useful to consider, but they do not create new international law, which only states can make.”⁹² Ultimately, with limited, macro-level exceptions, states have yet to agree to how international law applies to cyberspace and *opinio juris* remains a work in progress.

This leaves the U.S.-Japan Alliance in an apparently awkward position where the certainty envisioned in the UN Charter and the U.S.-Japan Security Treaty is inconsistent with the scarcity of consensus among states as to how international law applies in the cyber context.

Yet viewed through the light of international law as it exists today, for better or worse, the Alliance actually shares great freedom in cyberspace.⁹³ Ultimately much of what the U.S. and Japanese governments must decide with regard to their cyber operations will be governed more by domestic considerations and “policy prudence” than by international legal prohibition.⁹⁴

The State’s Right

“How do we apply old laws of war to new cyber-circumstances, staying faithful to enduring principles, while accounting for changing times and technologies?”

—HAROLD HONGJU KOH

LEGAL ADVISER, U.S. DEPARTMENT OF STATE (2012)⁹⁵

When the U.S. State Department Legal Adviser posed the question above at U.S. Cyber Command in 2012, he offered a very important, thoughtful, and problematic question. Koh’s interrogative was important because it framed a broader conversation in which the U.S. government clearly laid out its position on ten important—and specific—cyber law questions.⁹⁶ It was thoughtful because it reflected a commitment to values imbued in law and commitments of the U.S. government, while looking prospectively at emerging technologies and the conflicts that would grow across cyberspace over time. The question was problematic because it slid into the trap that has ensnared countless persons working in national security—by its terms, the question cast cyberspace as a domain necessarily governed by the “laws of war.”

Very few cyber activities could reasonably be considered to have risen to the level of armed attack. Even those that have approached the use of force threshold

would be hard to label as violating Article 2(4)⁹⁷ or implicating Article 51⁹⁸ of the United Nations Charter without significant disagreement among the international community. In reality, cyber operations most frequently occur outside of armed conflict and are rarely of a character as to create a close call about whether they implicate use of force or armed attack provisions of the UN Charter or, by extension, the U.S.-Japan Security Treaty.

Consequently, *jus ad bellum* may be appropriate to analyze as a preliminary matter—under the UN Charter, against the U.S.-Japan Security Treaty, in relation to domestic law and implementing arrangements—and *jus in bello* may guide the conduct of hostilities of armed conflict—even in cyberspace—but *jus ad bellum* and *jus in bello* are rarely of much legal significance for cyber operations.

Why would states “apply old laws of war to new cyber-circumstances” outside of armed conflict and when the use of force is not at issue?⁹⁹ Perhaps such efforts would be made in an attempt at analysis by analogy or as a limiting policy choice,¹⁰⁰ but such methods are of little utility in preparing authoritative opinions on the legality of cyber operations.¹⁰¹ Unfortunately, in their conversations many states and scholars continue to default to suggesting the law of war be applied to cyber operations irrespective of whether armed conflict or force are involved.¹⁰²

Uncertainty about what legal obligations may exist in cyberspace, and the relative ease of applying well-established law of war rules and principles, are resulting in a blurring of the lines between what is legally required and that which is prudent policy. Consequently, some states that focus on ensuring the rule of law extends to cyberspace and that the domain is not a “law-free zone”¹⁰³ seem to have reverted to select application of the laws of war for the time being. This has produced great confusion about which international law regimes apply, and when and how they apply.

Meanwhile, “sub-use-of-force” cyber activities have propagated, and international law has done little to reign in such conduct.¹⁰⁴ States and non-state actors have taken advantage of legal ambiguity and ineffective (or non-existent) accountability mechanisms while many states have been reluctant to defend forward or impose costs due to the absence of clear agreement on how to apply legal regimes to cyberspace.¹⁰⁵

However, all is not lost. Cyber operations have not fractured the entire international legal order nor have they made the UN Charter and the U.S.-Japan Security Treaty irrelevant. Prohibitions against the threat or use of force and armed attack remain enduring safeguards against state aggression. Cyber norms are shaping states’ understanding of their existing and potential future legal obligations, such that *opinio juris* may follow over time.¹⁰⁶

In the interim, malicious “sub-use-of-force” cyber operations directed against the United States and Japan may present more frequent and perhaps more substantial occasions for Alliance forces to leverage their respective capabilities

unilaterally or combine efforts as they conduct “self-help and mutual aid.”¹⁰⁷ Legal considerations normally applicable to defending against the use of force or armed attack may have significantly less influence over “sub-use-of-force” cyber operations.¹⁰⁸

Despite much uncertainty, what is clear is that defaulting to decision-making bound by the laws of war and standards repeated in agreements but not applicable to facts-at-hand could be unnecessary and self-defeating.¹⁰⁹ The gray zone will likely continue to be an arena in which proactive security measures face few directly applicable international legal prohibitions, and where the U.S.-Japan Alliance may enjoy states’ rights that support their cyber strategies. The risk of inaction deriving from legal uncertainty in cyberspace is very real. It is a problem that the U.S. and Japanese governments know well and that the allies are working to overcome.

Rules and Principles of International Law

Much of the uncertainty about applying international law to cyberspace reflects the scarcity of constraints directly applicable to the domain. States consider certain areas to be largely settled—among them, that the UN Charter’s protections generally apply and that state responsibility attaches to state cyber activities. There are also specific subjects governed by international agreements that regulate cyber conduct by states parties. Examples include the Constitution and Convention of the ITU, the Budapest Convention, and the European Union’s General Data Protection Regulation.

Still “states may face a general international legal prohibition on the initiation of armed conflict, subject to certain exceptions, but they do *not* face a similar general international legal prohibition against all uses of state or military power.”¹¹⁰ “Sub-use-of-force” cyber operations employed defensively are generally permissible under international law, so long as they do not violate specific international legal prohibitions such as prohibitions on the use of force or unlawful coercion.¹¹¹

Generally, rules and principles of international law in cyberspace can be divided into two categories: (a) those aspects of international law for which general consensus exists among states as to their applicability in cyberspace, including limitations against state action; and (b) unresolved international legal questions bearing on cyber operations. The sections that follow are framed by remarks recently made by U.S. Department of Defense General Counsel, Paul C. Ney, Jr. and relevant “rules” drawn from Tallinn 2.0.

The author follows Ney’s choice of topics because of the subject matter’s relevancy to this paper, because his remarks present existing U.S. Defense Department views that will shape U.S.-Japan Alliance planning and (at least) U.S. cyber operations and because these remarks present more specific application of

key international legal principles to cyberspace than any public positions presented by the Government of Japan to date. Additionally, prominent speeches by senior U.S. government attorneys in recent years have often been utilized to make clear or reinforce U.S. positions while hinting at other issues that may be contentious or unsettled but are important matters on which the government is working.

Tallinn 2.0 “Rules” are then quoted and discussed to highlight analysis already performed by experts in the field. Although the author has found some of the experts’ work to mischaracterize *lex ferenda* as *lex lata*, Tallinn 2.0 provides ample quality analysis and context, captures many disagreements among the volume’s collaborators, and shines light on some of the more significant points of contention. Thus, it is a useful instrument through which to examine settled and unsettled issues of law in this area.

GENERALLY SETTLED

“It continues to be the view of the United States that existing international law applies to State conduct in cyberspace. Particularly relevant for military operations are the Charter of the United Nations, the law of State responsibility, and the law of war.”

—HONORABLE PAUL C. NEY, JR.

GENERAL COUNSEL, U.S. DEPARTMENT OF DEFENSE (2020)¹¹²

The UN Charter’s applicability to cyberspace is widely accepted within the international community. “States’ adherence to international law, *in particular their UN Charter obligations*, is an essential framework.”¹¹³ The U.S. and Japanese governments are leading contributors to this viewpoint.¹¹⁴ Of particular importance is the consensus opinion of states that Article 2(4)’s general obligation to “refrain ... 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” applies in the cyber domain.¹¹⁵

Strong evidence indicates that states generally agree that state responsibility attaches to state conduct undertaken in or through cyberspace. Rule 14 of Tallinn 2.0 speaks to the law of state responsibility under the label “internationally wrongful acts” and explains, “A State bears international responsibility for a cyber-related act that is attributable to the State and that constitutes a breach of an international legal obligation.”¹¹⁶ Although states have debated whether draft articles of state responsibility should guide state conduct or be transformed into a more permanent convention, the broader assessment that the laws of state responsibility apply in cyberspace is widely accepted.¹¹⁷ In fact, the 11 “voluntary, non-binding norms of responsible State behaviour” recommended in the 2015 UN GGE report are expressions of support for applying state responsibility to cyberspace. Recent remarks by representatives of the governments of the United

States and Japan offer strong evidence of the allies' commitment as well.¹¹⁸

The third generally settled area—the laws of war—is a bit more complicated. Following the deliberate, progressive developments under the UN GGE process, including publication of the group's fourth report in 2015, a fifth UN GGE was commissioned. Its conclusions were expected to promote further the rule of law and emerging norms in cyberspace.¹¹⁹ Instead, among other difficulties, the “UN GGE did not reach a consensus on whether or not international humanitarian law applies to cyber operations, thereby shaking one of the very cornerstones of the whole discourse of cyber law, something that has been affirmed by the [International Court of Justice (ICJ)] and was thought to be beyond challenge.”¹²⁰ Observers considered this a shocking result with one scholar noting that the “issues that ... divided the GGE were objectively legal soft-balls.”¹²¹

Two of the topics contributing to disagreement among states should not have been all that surprising: the right to respond to internationally wrongful acts and the right to self-defense.¹²² These matters have long been contentious among states—and not just in cyberspace. The complexities of cyberspace and concerns about state responses made it even less likely that a consensus understanding would be reported by the UN GGE in 2017.

But the third issue—the applicability of *jus in bello* to cyberspace—was viewed by some as settled law about which the group would provide a clear consensus statement at least for those operations conducted as part of an armed conflict. Notwithstanding, Cuba, Russia, and China were among the states that would not commit to applying *jus in bello* to cyberspace.¹²³ While Russia and China were conspicuously quiet at the time, Cuba argued that “the supposed applicability in the context of [information and communications technologies] of the principles of International Humanitarian Law ... would legitimize a scenario of war and military actions in the context of ICT.”¹²⁴

Professor Michael Schmitt, Director of the Tallinn 2.0 Project, expressed his dismay:

This assertion runs counter to the long-standing acceptance of [International Humanitarian Law (IHL's)] application to new means and methods of warfare. Indeed, China, Russia and Cuba are Party to Additional Protocol I, Article 36 of which obliges them to review new weapons and methods of warfare for compliance with IHL. It is unclear how this obligation would not attach to cyber operations during an armed conflict that could, for instance, injure or kill individuals.

States cannot simply wish away their legal obligations under IHL treaty and customary international law. The Cuban contention that the mere applicability of IHL “legitimizes” war confuses the *jus in bello* with the *jus ad bellum*. The former,

which encompasses IHL, governs how armed conflict is to be conducted. It applies irrespective of whether a party to the conflict has violated the prohibition on the use of force in Article 2(4) of the UN Charter and customary law. Applying IHL to cyber operations during an armed conflict has nothing to do with the legality or legitimacy of a conflict.¹²⁵

Despite Cuba's assertions and the lack of a consensus UN GGE opinion about *jus in bello* resulting from the fifth session, Schmitt is entirely correct on these points. At least in the context of armed conflict,¹²⁶ *jus in bello* applies to cyber operations—especially when considering those cyber operations that would create effects comparable to effects that other means and methods of warfare would produce. Schmitt also properly frames the distinction between *jus ad bellum* and *jus in bello* and how they should be considered in relation to cyber operations.¹²⁷ These are well established matters in international law.¹²⁸

There may be validity in raising concerns over the potential for further blurring of the lines around when and how *jus in bello* applies during competition between states in cyberspace. However, that does not alter the easy conclusions that *jus in bello* applies to at least some forms of state conduct in cyberspace and that *jus ad bellum* remains a binding body of international law against which state cyber conduct can be measured.

UNRESOLVED QUESTIONS

"We recognize that State practice in cyberspace is evolving. As lawyers operating in this area, we pay close attention to States' explanations of their own practice, how they are applying treaty rules and customary international law to State activities in cyberspace, and how States address matters where the law is unsettled."

—HONORABLE PAUL C. NEY, JR.

GENERAL COUNSEL, U.S. DEPARTMENT OF DEFENSE (2020)¹²⁹

The number of unresolved questions that might arise when applying international law to cyberspace is limited only by one's imagination and ability to predict future developments in technology and global security. In the interest of cabining the paper to particularly important and challenging issues, this paper addresses four important but unsettled topic areas: (i) sovereignty, (ii) use of force and armed attack, (iii) non-intervention and coercion, and (iv) countermeasures.

Sovereignty

"The principle of State sovereignty applies in cyberspace."

—TALLINN 2.0 – RULE 1: SOVEREIGNTY (GENERAL PRINCIPLE)¹³⁰

At least four noteworthy and competing views of sovereignty in cyberspace have been embraced by states featuring prominently in the domain and the international dialogue. The United States, British, Chinese, and Dutch views present a range

of widely divergent positions shaped by competing conceptions of sovereignty in cyberspace.¹³¹ The United States Department of Defense asserts sovereignty as a guiding principle.¹³² Britain takes a similar position, opining that sovereignty is not a rule itself in cyberspace but is given life in the context of the non-intervention principle.¹³³ China regards sovereignty as an instrument of the state.¹³⁴ The Netherlands applies sovereignty as a primary rule.¹³⁵ Furthermore, the Japanese government seems inclined to work towards a view of sovereignty that best balances the competing interests of free expression and innovation against the need for cybersecurity.¹³⁶

Whatever commonality exists among state positions on sovereignty appears to reside in sovereignty's internal characteristics. The general principle expressed about internal sovereignty in Tallinn 2.0 reads, "[a] State enjoys sovereign authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations."¹³⁷ This comports with the public U.S. position and seems to align with the views of the Japanese government and most states on record.¹³⁸ It also may be why the UN GGE was able to agree to a voluntary, non-binding norm designed to protect critical infrastructure in 2015. Again, there is little reason to believe that new international agreements or consensus *opinio juris* will emerge on cyber sovereignty in the near future.

But the lack of clarity about sovereignty's overall standing under international law, including how it applies externally, presents an interesting point of inflection for states and international lawyers. As presented by Rules 3 and 4 of Tallinn 2.0: a state is "free to conduct cyber activities in its international relations, subject to any contrary rule of international law binding on it" but also "must not conduct cyber operations that violate the sovereignty of another State."¹³⁹ If the Tallinn Manual's framing of Rules 3 and 4 is correct,¹⁴⁰ what then if sovereignty in cyberspace is unsettled as a matter of international law?¹⁴¹

An obvious area of consideration is intelligence collection or espionage. As U.S. and Japanese forces work to enhance their situational awareness across cyberspace, Alliance forces would benefit from early detection and identification of malicious cyber activities. It might also be advantageous to know where prospective cyber targets are as well as what their access routes and vulnerabilities might be in the event that defensive measures are required. These seem like necessary measures in a world of advanced, persistent cyber threats.

Therefore, to the extent that cyber forces could reach across the cyber domain to identify threats or perhaps establish placement and access to facilitate future responsive measures,¹⁴² it could be important to understand whether sovereignty operates as a legal prohibition to cyber intelligence collection. Here the U.S. Department of Defense's perspective on sovereignty as a guiding international law principle pertains.¹⁴³ "[I]t does not appear that there exists a rule

that all infringements on sovereignty in cyberspace necessarily involve violations of international law.” Like their British colleagues, the American viewpoint accepts that there is “no *per se* international legal prohibition” on intelligence or counterintelligence activity.¹⁴⁴

So far it is unclear what position Japan will take on the sovereignty question. To date, Japanese government officials have been supportive of state responsibility and due diligence obligations during UN GGE sessions, but no publicly available remarks provide an official, detailed position on the cyber sovereignty question. Japan shows no inclination of supporting China’s state-centric sovereignty stance. Meanwhile, the differences between the United States and British “sovereignty as a guiding principle” and the Dutch “sovereignty as a primary rule” positions may seem subtle, but they are strategically and tactically significant. Both positions accept that certain cyber operations could violate sovereignty, but much more room exists to maneuver “proactively” under the U.S. model.¹⁴⁵ Moreover, in the absence of consensus among states, the U.S. position seems to be the most likely to guide activities within the framework of the U.S.-Japan Alliance.

Japan’s plans to increase cyber situational awareness and information sharing would benefit from the Japanese government adopting the “sovereignty as a guiding principle” position. This viewpoint would still require considering sovereignty when conducting cyber operations, and it could help to preserve Japan’s standing as a promoter of, and adherent to, the rule of law. Yet treating sovereignty as a guiding principle in the cyber context would also provide Japan with considerable freedom to decide when and how to conduct cyber operations.

USE OF FORCE AND ARMED ATTACK

“A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force.”

—TALLINN 2.0 – RULE 69: DEFINITION OF USE OF FORCE¹⁴⁶

As with sovereignty, states take differing views on what constitutes a use of force or armed attack in cyberspace. Yet the general consensus does seem to center on the proposition that “Whether a cyber operation constitutes an armed attack depends on its scale and effects.”¹⁴⁷ This issue is of particular interest to the U.S.-Japan Alliance since the U.S.-Japan Security Treaty focuses so heavily on armed attack as the standard triggering much of the cooperative arrangement.¹⁴⁸ Understandings articulated by the United States, the United Kingdom, the Netherlands, and the French Ministère des Armées¹⁴⁹ are illustrative of states’ diverging viewpoints.

Then State Department Legal Adviser Harold Koh first firmly established the U.S. government’s position in 2012, explaining that “[c]yber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force.”¹⁵⁰ Koh cited as examples: “(1) operations that trigger a nuclear

plant meltdown; (2) operations that open a dam above a populated area causing destruction; or (3) operations that disable air traffic control resulting in airplane crashes.”¹⁵¹ At a high level, this U.S. position is largely unchanged.¹⁵² However, the Department of Defense more recently has expressed the standard without presenting such extreme examples. Recently U.S. Department of Defense General Counsel, Paul Ney, Jr., announced, “DoD lawyers consider whether the operation causes physical injury or damage that would be considered a use of force if caused solely by traditional means like a missile or a mine.”¹⁵³

The United Kingdom, the Netherlands, and France have presented opinions that have some common foundations but also offer important distinctions. The United Kingdom’s position has been presented in language that reflects the UN Charter closely, speaking to the prohibition on the threat or use of force and describing armed attack via cyber operations as those that “result in, or present an imminent threat of, death and destruction on an equivalent scale to an armed attack.”¹⁵⁴ The Netherlands makes case-by-case determinations based on “how serious and far-reaching the cyber operation’s consequences are, whether it is military in nature, and whether it is carried out by a state” with, again, primary focus on “when the effects of the operation are comparable to those of a conventional act of violence covered by the prohibition.”¹⁵⁵

France takes an effects-based test like the others, but it does not require *physical* effects to find a use of force—turning instead to a non-exhaustive list of criteria to be considered, including: “the overall circumstances surrounding the operation, the origin of the operation and the nature of the attacker (i.e., the military character of the operation), the degree of intrusion, the effects intended or achieved by the operation and the nature of the target.”¹⁵⁶ Additionally, France distinguishes between uses of force and armed attack. “Only those operations which are comparable to an armed attack by conventional means would fall under Art. 51 UN Charter. This, in turn, depends on the gravity of the effects caused by the cyber operation, their reach and reversibility.”¹⁵⁷ There are criteria to be considered for armed attack, as well.¹⁵⁸ Finally, France argues that an “accumulation of events” is also a basis for concluding that an armed attack has occurred, meaning that the cumulative effects of events that would not otherwise themselves constitute armed attack could nevertheless cross the threshold collectively.¹⁵⁹

The distinction that France draws between the use of force and armed attack is an understanding under international law espoused by many states (not just in cyberspace, but generally). Japan agrees that international law draws a distinction between lesser forms of the use of force and armed attack¹⁶⁰ as reflected in the International Court of Justice’s *Nicaragua*¹⁶¹ decision.

Furthermore, for Japan armed attack means the “organized and premeditated use of force against Japan.”¹⁶² The Japanese government has also commented that a “cyberattack carried out as part of an armed attack” and a

“cyber-only attack” could both themselves rise to the level of armed attack, but it has not expounded on this view publicly or offered public comment on applying effects-based tests in the cyber context. Presumably, Japan would continue to focus on organization and premeditation as leading elements of the state’s analysis.¹⁶³ To the extent that collective self-defense might be implicated, there would also be reason to analyze the Cabinet’s relatively recent move to reinterpret Article 9 and the potential for that reinterpretation to allow Japan to “use force in response to infringements of Japanese sovereignty that do not amount to an armed attack.”¹⁶⁴

The U.S.-Japan Alliance Security Consultative Committee’s Joint Statement in April 2019 indicated that the procedures utilized by the U.S.-Japan Alliance to review such matters remain largely unchanged. “The Ministers also affirmed that a decision as to when a cyber attack would constitute an armed attack under Article V would be made on a case-by-case basis, and through close consultations between Japan and the United States, as would be the case for any other threat.”¹⁶⁵ This suggests that the United States and Japan, in the context of the Alliance, like other states will consider such circumstances as they arise and that they should have an opportunity to share perspectives and potentially make joint declarations about adversaries’ cyber operations. It also presents an opportunity for Japan to disagree with U.S. viewpoints—possibly characterizing incidents as more or less severe or differing on the propriety of response options.¹⁶⁶

It may be most advantageous for the Japanese government to withhold presenting a detailed position on what, precisely, constitutes armed attack or use of force in the cyber context until such circumstances arise. Acknowledging that cyber operations can manifest as armed attack or use of force has been helpful in advancing international law and establishing expectations for state conduct. However, the self-interests of the United States and Japan weigh in favor of maintaining flexibility in future legal policy decisions—of waiting to assess the gravity of cyber incidents, the circumstances prevailing at some future time, and how such choices will impact interests of the U.S.-Japan Alliance. This approach should also permit the allies, in the interim, to move forward with proactive security measures in and through cyberspace and to consider carefully how best to stay below the use of force threshold while protecting “beyond the blue” and across the gray zone.

Non-intervention

“A State may not intervene, including by cyber means, in the internal or external affairs of another State.”

—TALLINN 2.0 – RULE 66: INTERVENTION BY STATES¹⁶⁷

Although the principle of non-intervention is widely recognized under

international law,¹⁶⁸ its application is very much contested. The lines between sovereignty and non-intervention are often blurred.¹⁶⁹ The parameters of unlawful coercion, an element of the principle, are unsettled even outside of cyberspace,¹⁷⁰ thereby making it exceedingly difficult for states to agree—internally or externally—on how the principle might apply to cyberspace.¹⁷¹ Furthermore, among other factors, the geopolitical implications of Russian misinformation campaigns, Chinese hacking and broader information warfare, and the United States’ generally active role on a number of fronts in cyberspace have turned discussion about non-intervention into more of a political arena than a true consensus building initiative or legal discourse.

Arguably, coercion is the most important element of unlawful intervention.¹⁷² International law does not define coercion and its application to matters of national security has long been debated. Still, coercion is generally understood as involving an element of compulsion (i.e., compelling a state to take a certain action or act in a certain way, or to refrain from taking action in a particular context).¹⁷³ Furthermore, “the coercion must take place in relation to ‘matters of an inherently sovereign nature’, i.e. those over which the state has exclusive authority, including a state’s political, economic, social and cultural systems.”¹⁷⁴

Tallinn 2.0 demonstrates difficulties in building consensus around the element of coercion within the broader non-intervention principle—even among scholars. While recognizing that “[c]oercion sufficient to support a finding of unlawful intervention may take either a direct or indirect form,” the group of experts could not agree on a number of points regarding unlawful coercion as an element of intervention.¹⁷⁵ Issues that were debated but ultimately not resolved involved causality, knowledge of the operation creating the effects, protection of nationals abroad, and humanitarian intervention.¹⁷⁶

Additionally, coercion, in and of itself, is insufficient to find unlawful intervention. Unlawful intervention is generally understood to require both coercion and interference into another state’s *domaine réservé*. Thus, a second element of intervention is whether the cyber operations interfered with “matters in which each State is permitted, by the principle of State sovereignty, to decide freely.”¹⁷⁷

Despite the absence of international consensus on a number of details, the Netherlands provides a useful summary of the non-intervention principle and its importance in cyberspace:

The development of advanced digital technologies has given states more opportunities to exert influence outside their own borders and to interfere in the affairs of other states. Attempts to influence election outcomes via social media are an example of this phenomenon. International law sets boundaries on this kind of activity by means of the non-intervention

principle, which is derived from the principle of sovereignty.

...Intervention is defined as interference in the internal or external affairs of another state with a view to employing coercion against that state. Such affairs concern matters over which, in accordance with the principle of sovereignty, states themselves have exclusive authority. National elections are an example of internal affairs.

...The precise definition of coercion, and thus of unauthorised intervention, has not yet fully crystallised in international law. In essence it means compelling a state to take a course of action (whether an act or an omission) that it would not otherwise voluntarily pursue. The goal of the intervention must be to effect change in the behaviour of the target state.¹⁷⁸

France's position goes a bit further, explaining that a cyber operation "interfering in its internal or external affairs constitutes prohibited intervention if it is likely to affect the French political, economic or social system." This statement generally aligns with the concept of France's military and economy falling within the state's *domaine réservé* as a matter of international law.¹⁷⁹

In summary, discussions about non-intervention are colored by states' concerns about the perceptions of allies and partners, as well as the potential for adversaries' reciprocal conduct.¹⁸⁰ Most public remarks by states fail to offer much clarity on non-intervention beyond vague attestations to the principle's importance and political statements about issues like election interference. Nevertheless, this is clearly a topic of great importance.

It is a subject that will likely lend itself to contesting the United States' defend forward posture, and perhaps Japan's more proactive approach, depending on how such policies manifest themselves. Japanese government officials interested in ensuring that Self-Defense Force cyber units have sufficiently forward-looking authority to protect Japan's political, economic, social and cultural systems might consider bolstering National Defense Program Guidelines and Guidelines of U.S.-Japan Defense Cooperation with legislation that focuses more directly on sub-use of force activities threatening Japan's *domaine réservé*. Additionally, the rule of non-intervention should be expected to continue to provide the allies with a basis to decry as illegal such coercive cyber activities that intervene in the *domaine réservé* of the United States and Japan.

COUNTERMEASURES: COLLECTIVE RESPONSES AND NOTICE

“A state may be entitled to take countermeasures, whether cyber in nature or not, in response to a breach of an international legal obligation that it is owed by another State.”

—TALLINN 2.0 – RULE 20: COUNTERMEASURES (GENERAL PRINCIPLE)¹⁸¹

In May of 2019, the President of the Republic of Estonia offered a low-key but potentially significant announcement before the international community. Speaking at the opening of CyCon 2019, President Kersti Kaljulaid declared:

Estonia is furthering the position that states which are not directly injured may apply countermeasures to support the state directly affected by the malicious cyber operation. ... International security and the rules-based international order have long benefitted from collective efforts to stop the violations. ... The threats to the security of states increasingly involve unlawful cyber operations. It is therefore important that states may respond collectively to unlawful cyber operations where diplomatic action is insufficient, but no lawful recourse to use of force exists. Allies matter also in cyberspace.¹⁸²

Estonia’s on-record support for the proposition that states could conduct countermeasures in response to acts affecting other states flew in the face of established views of international law on countermeasures.

Countermeasures, of course, are “actions or omissions by an injured State directed against a responsible State that would violate an obligation owed by the former to the latter but for qualification as a countermeasure.”¹⁸³ Furthermore, it has been understood that countermeasures must follow very specific criteria.¹⁸⁴ Among those requirements, “[o]nly an injured State may engage in countermeasures, whether cyber in nature or not.”¹⁸⁵ Admittedly, rumblings have existed for years about whether there might be ways around this limitation.¹⁸⁶

But Kaljulaid chose instead to tackle the topic head on. She couched Estonia’s position in terms that were pragmatic, embracing mutual defense precedent and reflecting the interconnected nature of the contemporary world. Although it is too soon to know whether other states might embrace (or reject) this position, a movement to overcome the classic understanding that countermeasures are limited to the injured state could be useful for the U.S.-Japan Alliance’s plans for increased and enhanced cooperation in cyberspace.

Another aspect of countermeasures worth monitoring is the issue of notification. In his March 2020 remarks at U.S. Cyber Command, the Department of Defense General Counsel commented:

In the traditional view, the use of countermeasures must be preceded by notice to the offending State, though we note that there are varying State views on whether notice would be necessary in all cases in the cyber context because of secrecy or urgency. In a particular case it may be unclear whether a particular malicious cyber activity violates international law. And, in other circumstances, it may not be apparent that the act is internationally wrongful and attributable to a State within the timeframe in which the DOD must respond to mitigate the threat. In these circumstances, which we believe are common, countermeasures would not be available.¹⁸⁷

The United Kingdom Attorney General offered a similar perspective in 2018:

The one area where the UK departs from the excellent work of the International Law Commission on this issue is where the UK is responding to covert cyber intrusion with countermeasures. In such circumstances, we would not agree that we are always legally obliged to give prior notification to the hostile state before taking countermeasures against it. The covertness and secrecy of the countermeasures must of course be considered necessary and proportionate to the original illegality, but we say it could not be right for international law to require a countermeasure to expose highly sensitive capabilities in defending the country in the cyber arena, as in any other arena.¹⁸⁸

To emphasize the point, notice of countermeasures in cyberspace is a contentious issue. The large majority of states and scholars would likely consider the requirements of countermeasures to be well-settled law outside of the cyber domain. Yet many would still deem the countermeasures requirements to apply in cyberspace as well.

Nevertheless, there are certainly aspects of cyberspace that are fundamentally different than other domains, and due consideration should be given to the uniqueness of the environment as it pertains to the applicability of international law. If Japan wishes to engage in necessary, temporary responsive measures sufficient to subdue cyber threats (or to ask for assistance from others on its behalf, whether under the Estonian collective countermeasures position or other legal justifications), speed and discretion will be key to successful cyber defenses.

As General Nakasone explained, ultimately, “in cyberspace it’s the *use* of cyber capabilities that is strategically consequential. The *threat* of using something in cyberspace is not as powerful as *actually* using it because that’s what our adversaries are doing to us. They are actively in our network communications, attempting to steal data and impact our weapons systems. So advantage is gained by those who maintain a continual state of action.”¹⁸⁹

On this issue Japan would clearly benefit from supporting Estonia's view that collective countermeasures can be necessary and lawful in the cyber context. Japan might also want to endorse the U.S. and U.K. government views that notice of countermeasures is not feasible or legally required in certain circumstances. Both of these positions could be of great importance to mutual defense within the U.S.-Japan Alliance.

Scenarios

Part III of this paper considers the foregoing principles in the context of three scenarios involving hypothetical, adversarial action in and through cyberspace. It addresses each by considering how international law might shape the use of cyber capabilities by the United States and Japan as well as broader actions that the U.S.-Japan Alliance could take in response.

The scenarios presented herein are: (1) an armed attack conducted through cyberspace and causing significant physical injury and damage; (2) cyber operations resulting in minimal physical injury or damage but that might still be considered a use of force; and (3) persistent, malicious cyber operations below the use of force threshold. These fact patterns are analyzed through the lens, mechanisms, and objectives of the U.S.-Japan Alliance.

This section embraces a generalized notion of the United States' defend forward posture and an emerging vision of Japanese proactive cyber defenses, allowing for the possibility of combined operations and perhaps a mutually reliant defensive cyber architecture to be developed over time.¹⁹⁰ Furthermore, it assumes an operational environment in general terms as described throughout this paper. U.S. and Japanese cyber forces will be dealing with sophisticated, persistent cyber threats across all three scenarios irrespective of whether so stated within individual fact patterns.

As a preliminary matter, it should also be noted that the author's commentary assumes that some amount of U.S. and/or Japanese government cyber intelligence collection will occur throughout the scenarios and that establishing placement and access in foreign systems and networks prior to the incidents described in the scenarios may be necessary to facilitate cyber intelligence collection and defensive measures.¹⁹¹ This framing relies to an extent on the U.S. and U.K. governments' position that international law does not specifically prohibit intelligence collection and that espionage is left to states to criminalize.¹⁹² It also reflects Japan's 2019 National Defense Program Guidelines for the Self-Defense Force to "conduct on a steady-state basis persistent monitoring as well as collection and analysis of relevant information."¹⁹³ However, this section does acknowledge, where appropriate, states' competing conceptions of cyber sovereignty and the non-

intervention principle as well as how those views bear on the facts presented.

The author also takes into account the U.S.-Japan Alliance's concept of operations for cross-domain operations¹⁹⁴ and its stated goals for cooperation in cyberspace.¹⁹⁵ This section attempts to give credence to the Defense Cooperation Guidelines' focus on "flexible, timely, and effective bilateral coordination tailored to each situation."¹⁹⁶ Of greatest significance, the scenarios that follow accept the U.S. and Japanese governments' basic plan for responding to "cyber incidents against Japan" and "serious cyber incidents that affect the security of Japan."¹⁹⁷

Ultimately this section focuses on the ability of U.S. and Japanese cyber forces to conduct defensive measures consistent with international law¹⁹⁸ and treaty obligations, their respective domestic legal regimes, and implementing arrangements for the U.S.-Japan Alliance. In particular, the scenarios should test the extent to which Japan and the United States might more effectively defend their computer systems and networks unilaterally or bilaterally and how the aforementioned settled and unsettled areas of international law weigh on legal policy choices that will be made during the implementation of the defend forward and proactive defense strategies.

Scenario 1

Japan suffers large-scale cyber operations against its commercial and governmental infrastructure, relying on placement and access established in cyberspace over the preceding years. These cyber operations cause a meltdown in a Japanese nuclear plant. The meltdown causes substantial loss of life, physical damage, and economic harm. To cause a meltdown appears to have been the intent of the perpetrators of the operations. These events occur following a period of high tensions with State A, which is unhappy with Japan's persistent public opposition to its ballistic missile program.

Scenario 1 will likely be considered an armed attack conducted through cyberspace. The Japanese government has stated that "cyberattack carried out as part of an armed attack" and "cyber-only attack" could both themselves rise to the level of armed attack; however, Japan has otherwise not specified its views on what constitutes armed attack in or through cyberspace. Nevertheless, the facts presented in Scenario 1 suggest significant organization and premeditation¹⁹⁹ and align directly with examples provided by the U.S.²⁰⁰ and U.K. governments.²⁰¹ Furthermore, the same conclusion would almost certainly be drawn under the factors embraced by the Dutch and French and outlined in Tallinn 2.0. The deliberate initiation of a nuclear meltdown in one state by another, whatever the means, would be a grave use of force. The Japanese government would have to take an extremely conservative position to conclude that these cyber operations do not rise to the level of armed attack.²⁰²

Any response would need to consider the issue of attribution.²⁰³ With what

degree of confidence and how quickly could the cyber operations be attributed to State A? Would State A acknowledge that it conducted the cyber operations? If State A disavowed its role in the operations, could the denial be challenged publicly and by convincing means? Two prevailing views exist on what is required for attribution prior to taking action against an offending state. One view holds that attribution requires certainty; the other takes the position that attribution must be reasonable and based on facts available at the time of response.²⁰⁴ The United States takes the latter position:

“[A] State acts as its own judge of the facts and may make a unilateral determination with respect to attribution of a cyber operation to another State. Absolute certainty is not—and cannot be—required. Instead, international law generally requires that States act reasonably under the circumstances when they gather information and draw conclusions based on that information.”²⁰⁵

The relevance of this position to the U.S.-Japan Alliance should not be underestimated. Attribution of cyber operations can be a complex and uncertain endeavor. Yet it is also necessary and often times quite feasible. Speed of attribution can be a challenge—particularly when working to combat ongoing activities and develop response options and legal justifications—but it, too, can be achieved in many instances. If the Japanese government was to instead turn to a more onerous standard of certainty in attribution, it seems likely that responding in self-defense in a timely manner, if ever, could prove challenging.²⁰⁶

Assuming that the operations are attributable to State A, State A's cyber operations would violate Article 2(4) of the UN Charter and implicate Article 51 of UN Charter and Article V of the U.S.-Japan Security Treaty. The Japanese government would be expected to notify the UN Security Council of the armed attack, seek assistance, and consult with the U.S. government.²⁰⁷ Consultation with the U.S. government would be consistent with the Guidelines for U.S.-Japan Cooperation based upon “serious cyber incidents that affect the security of Japan.”²⁰⁸

It is unclear whether the Japanese government would wait for UN Security Council action or, instead, respond immediately and perhaps in partnership with the United States in light of the gravity of the attack and presumably the necessity of taking immediate action in self-defense.²⁰⁹ Self-defense under international law would permit the use of necessary and proportional force, including lethal force, in response.²¹⁰ International law would not require a response to be conducted in or through cyberspace.

Other questions that might be raised—perhaps further into the future—include how State A was able to conduct this attack and whether its cyber

placement and access in the years leading up to the attack constituted violations of sovereignty or the prohibition against unlawful intervention. Here competing international law perspectives of states might inform the review. It might be difficult for British or U.S. officials to conclude that the placement and access, in and of itself, constituted violations of international law since both states view intelligence collection and some degree of nonconsensual entry as historic state practice not prohibited by international law. Perhaps identification of some coercive activities might give rise to unlawful intervention even under these views. On the other hand, certain other states might suggest that both sovereignty and the non-intervention principle were violated.²¹¹

However, as a practical matter, questions about sovereignty and non-intervention might be of little consequence in this scenario relative to the conclusion that the cyber operations constitute armed attack. The armed attack determination would provide legal justification for the most significant potential response that Japan might make, whether individually or in partnership under the U.S.-Japan Alliance.²¹²

The consequences of Scenario 1 weigh in favor of robust and proactive cybersecurity measures that do not wait for armed attack to manifest in or through cyberspace. Not every cyber operation can be prevented, and it is unclear whether the U.S.-Japan Alliance could have prevented or detected the placement and access gained by State A even had the Alliance been defending forward in an aggressive, collaborative, and cost-imposing posture. Yet certainly some degree of risk can be mitigated through the more proactive approaches the allies are instituting. Taking positions that would view sovereignty as an international law principle in the cyber context and that would permit collective countermeasures, even without giving notice to the offending state in certain circumstances, could lead to significant improvements in cyber situational awareness and information sharing, enhanced cyber deterrence, and necessary responsive actions, thereby mitigating the risk of Scenario 1 unfolding.

Scenario 2

State B, seeking to refine its tactics and measure effects in advance of the next phase of its cyber campaign targeting U.S. elections, initiates cyber operations targeting Japanese media platforms and public transportation.²¹³ Servers are taken offline, Tokyo trains stop running, and emergency communications networks in three Japanese cities are temporarily degraded or disabled. It is unclear whether any physical injury or damage resulted directly from the cyber operations, but preliminary reports suggest that any physical injury or damage was “minimal.” Meanwhile, false information about Japanese government officials, which has been filling social media for weeks, has begun to appear in the form of scrolling banners at the bottom of television stations that appear to be real news updates presented by the

television stations. However, State B makes a major error in its tradecraft and these activities are quickly attributable (i.e., while State B's cyber operations continue). Prominent Japanese government officials are questioning whether State B's actions constitute armed attack and whether there may be implications under the U.S.-Japan Security Treaty.

Scenario 2 is not likely to be considered armed attack. Nevertheless, it is possible that the Japanese government would determine that State B's cyber operations violate the use of force prohibition under Article 2(4) of the UN Charter. The Japanese government also would have a reasonable basis to conclude that these activities constitute an unlawful intervention in Japan's sovereign affairs, thereby providing legal justification to resort to countermeasures if necessary. Japan could respond in or through cyberspace, by other means not involving cyber operations, or through some combination of the two.

When analyzing whether the facts presented constitute armed attack through cyberspace, other states' views are informative in the absence of a more detailed public statement of the Japanese government position.²¹⁴ Scenario 2 does not reach the baselines for armed attack (or use of force) that the U.S. State and Defense Departments have explained publicly and that were reviewed under Scenario 1.²¹⁵ The cyber operations did not “proximately result in death, injury, or significant destruction” or cause “physical injury or damage that would be considered a use of force if caused solely by traditional means like a missile or a mine.”²¹⁶

The Japanese government also could look to other views on armed attack in cyberspace. The Dutch position is particularly interesting under Scenario 2 because it asserts that if “a cyber-attack ... prevents the government from carrying out essential tasks such as policing or taxation ... it would qualify as an armed attack.”²¹⁷ This may be the most expansive state view on cyber armed attack, presenting a lens through which the Japanese government might consider effects on the Japanese government itself—which might be significant because emergency communications networks, servers, and railways were interrupted.

Embracing this approach could have profound implications for the U.S.-Japan Alliance. Most directly, while a conclusion that an armed attack has occurred does not *require* injured states to respond with force, such a determination would trigger Article V of the U.S. Japan Security Treaty, lead to the initiation of consultations between the allies, and create a justification for response.²¹⁸ This would give Japan greater freedom to respond to State B's cyber operations, but it might also serve as precedent for other states that might want to characterize future cyber operations as armed attack. For example, might North Korea argue that operations targeting its ballistic missile program “prevent the government from carrying out essential tasks”? Could China take a similar position over

cyber operations that interfere with the state's internal control over information content?²¹⁹

There may be a better legal policy choice to be made—and a stronger case under international law—that State B's cyber operations violate Article 2(4) of the UN Charter. Japan is one of the many states that recognize a substantive difference between armed attack under Article 51 and use of force under Article 2(4). Such views tend to rely on the *Nicaragua* judgment—reserving the concept of armed attack to only the “most grave” uses of force and accepting that certain “scale and effects” of operations can, in the aggregate, still rise to the level of violating Article 2(4).²²⁰ In cyberspace, this proffered distinction between armed attack and use of force is not insignificant.

Tallinn 2.0 attempts to apply this reasoning to cyberspace, suggesting “[a] cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force.”²²¹ Furthermore, this general approach is not merely a concept embraced by a group of experts. The Netherlands and France are among the states that would apply their own factors to use of force analysis.²²² They would look at what is being done, by whom, and how and consider the totality of effects on the state—without necessarily requiring any physical injury or damage.

In this scenario, the Japanese government might look towards these other (non-U.S. government) perspectives as persuasive arguments for why the use of force question should be answered without a strict requirement for physical injury or damage.²²³ Japan might then reasonably conclude that State B's cyber operations violated Article 2(4).

The consequences of finding a violation of Article 2(4) could be significant. The Japanese government would almost certainly notify the UN Security Council of these events and seek assistance while also consulting with its American allies.²²⁴ The U.S.-Japan Alliance would likely consider in this context the U.S. positions that “the inherent right of self-defense potentially applies against any illegal use of force” and that “any cyber operation that constitutes an illegal use of force against a State potentially gives rise to a right to take necessary and proportionate action in self-defense.”²²⁵ Concluding that Article 2(4) was violated could provide legal justification for a wide range of responses, including self-defense and operations conducted in or through cyberspace, outside of cyberspace, or some combination of the two.²²⁶

Even if the cyber operations were not deemed to constitute armed attack or use of force, they might still be viewed as violations of the international law prohibition on coercive intervention in foreign sovereign affairs.²²⁷ Under the law of state responsibility²²⁸, the non-intervention principle would be examined for breach by State B.²²⁹ The non-intervention rule “prohibits coercive intervention, including by cyber means, by one State into the internal or external affairs of another.”²³⁰ On

their face, the facts—cyber operations impacting public transportation, emergency communications, and media platforms—might sound like obvious examples of interference in the internal dealings of another state. But the element of coercion is a required—and elusive—element necessary for finding unlawful intervention.

Had these operations been designed to impact *Japanese* elections instead of to refine tactics and measure effects in preparation for future operations against *U.S.* elections, there may have been a clearer case of coercion. Instead, Scenario 2 leads to an unsettled area of international law. Some debate exists about whether coercion requires attempting to influence outcomes or conduct in the targeted state or whether in cyberspace merely taking control out of the hands of the state or its citizens can be coercion.²³¹ Under the former majority position, it would be difficult to find coercion in Scenario 2 (i.e., What would State B be seeking to compel the Japanese government or its citizens to do or not do?). Under the latter minority view, the revocation of control over transportation, emergency communications, and media from the state and its citizenry to State B might allow for a finding of coercion and unlawful intervention.

The U.S. Department of Defense has asserted that “a cyber operation by a State that interferes with another country’s ability to hold an election or that tampers with ‘another country’s election results would be a *clear violation* of the rule of non-intervention.”²³² That position, while not defined in great detail in public, likely focuses on political choice as a matter fundamental to states and not open to external coercion.²³³ It also echoes the 1970 Friendly Relations Declaration:

No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of another State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are in violation of international law.²³⁴

And if election interference constitutes a *clear violation*, then the Japanese government might have a reasonable case to make that the invasive activities directed into Japan could also be unlawful intervention.

Based on a conclusion of unlawful intervention, the Japanese government (or perhaps the U.S.-Japan Alliance) might resort to countermeasures.²³⁵ “The customary international law doctrine of countermeasures permits a State that is the victim of an internationally wrongful act of another State to take otherwise unlawful measures against the responsible State in order to cause that State to comply with its international obligations, for example, the obligation to cease its internationally wrongful act.”²³⁶ Here countermeasures would need to target State B,²³⁷ be necessary and proportional, be designed to compel State B to meet its obligations under international law, and stop when State B complies. The

traditional view of countermeasures doctrine has limited their use such that only the affected state (here, Japan²³⁸) can engage in countermeasures.

However, Estonia's argument as to why international law should be understood to allow collective countermeasures in the interconnected and increasingly interdependent cyber domain warrants attention. "Allies matter also in cyberspace."²³⁹ This position aligns well with Article IV of the Guidelines for U.S.-Japan Defense Cooperation and recent statements by the U.S. and Japanese governments about their intentions to collaborate in cyberspace.²⁴⁰ There might be countermeasures opportunities that could only be accomplished through the more robust cyber architecture, more substantial cyber forces, or perhaps unique placement and access that the U.S. government would have. If cyber countermeasures were determined by the allies to be the most legally appropriate and effective response to Scenario 2, it would be difficult to envision the U.S. and Japanese governments refraining from conducting some form of combined or U.S. cyber operations as countermeasures solely out of deference to the historic view that countermeasures could only be undertaken by the affected state.²⁴¹

Japan might also be required as a matter of international law to give State B notice prior to initiating countermeasures. Although "there are varying State views on whether notice would be necessary in all cases in the cyber context because of secrecy or urgency,"²⁴² the U.S. government is among those states that believe that notice of countermeasures may not always be required in cyberspace. The United States takes the position that notice of countermeasures "should be evaluated on a case-by-case basis in light of the particular circumstances of the situation at hand and the purpose of the requirement."²⁴³ The United Kingdom agrees and has explained, "The covertness and secrecy of the countermeasures must of course be considered necessary and proportionate to the original illegality, but we say it could not be right for international law to require a countermeasure to expose highly sensitive capabilities in defending the country in the cyber arena, as in any other arena."²⁴⁴

This, too, is an important position that Japan could consider—ideally, well in advance of circumstances like those described in Scenario 2. The Japanese government might view notice as an opportunity to de-escalate while informing State B that the cyber operations have been attributed to them and to warn of consequences should the violation persist. On the other hand, the Japanese government might determine that notice could foreclose opportunity to take more decisive action against State B's cyber capabilities through means and methods that might be rendered ineffective, or that might be inappropriately disclosed if advance notice was provided. Whichever option the Japanese Government might want to choose under Scenario 2, clearly the most advantageous legal policy position to take regarding notice is one that accepts the relatively unique circumstances of cyberspace as a basis for rejecting the traditional view that notice

of countermeasures is always required.

Scenario 3

State C has long-standing maritime and territorial disputes with Japan. State C also does not appreciate the U.S.-Japan Alliance and regularly objects to American military presence in the region. State C is known to have been probing Japanese and U.S. command and control systems for years, looking for vulnerabilities to exploit. As U.S. and Japanese ships are conducting close quarters naval and air exercises in and above international waters in the region, State C, relying on previously unknown vulnerabilities in Alliance networks, launches a cyber attack that deliberately disrupts command and control of the two nations' ships and aircraft. This disruption creates a significant risk of damaging or deadly collision, but thanks to the skill of the relevant crews no injuries or damage occur.

Although Scenario 3 likely does not rise to the level of armed attack, it skirts the edges of use of force and unlawful intervention. Most likely, the facts presented herein would be viewed as another example of persistent, malicious state cyber activity for which arguments could be made that international law was violated but that the U.S.-Japan Alliance might instead address through the defend forward and proactive security strategies.²⁴⁵

The absence of any physical injury or damage makes it unlikely that Scenario 3 would be viewed as armed attack.²⁴⁶ The limited duration and effects also make it doubtful, although not impossible, that the cyber operations would constitute use of force. The cyber operations likely involved substantial organization and premeditation. However, the “scale and effects” of the cyber operations were limited and ultimately inconsequential, which weighs against concluding that this was a use of force under *Nicaragua*.²⁴⁷ Likewise, factors used by the U.S., Dutch, and French governments to consider cyber use of force questions, as well as those promoted in Tallinn 2.0, suggest that this incident does not rise to the level of use of force.²⁴⁸ For example, the operations were not particularly severe or far-reaching. They appear to have disrupted command and control systems temporarily and without further incident and are not known to have interfered with anything other than the targeted ships and aircraft. Their impact may have been seen as dramatic at the time of occurrence, and the safety of the ships and aircraft and their crew is certainly highly significant; however, it would be difficult to point to consequences of any real gravity that might approach the use of force.²⁴⁹ To the extent that the United States or Japan were to conclude though that the disruption was intended to produce or would have a reasonably foreseeable effect of damage to equipment or injury or death of the crews, they might conclude that it was indeed an armed attack, albeit an ineffectual armed attack.

Whether the disruption constitutes a prohibited coercive intervention

in U.S. or Japanese sovereign prerogatives is a closer call.²⁵⁰ As a preliminary matter, command of military forces is a core sovereign prerogative of states. Even while beyond the respective territorial seas, warships and military aircraft enjoy sovereign immune status, although with somewhat narrower protections against interference than international law provides for the geographic territory of states.²⁵¹ Thus, deliberate disruption of command and control of those units raises generally the issues of a prohibited coercive intervention discussed previously in this paper. In essence, it matters little that these exercises were being conducted at sea and in the air beyond the territorial seas of any coastal state. In fact, operations targeting military assets conducting close quarters exercises, and the inherent danger of such conduct, might cause heightened interest in more aggressive, cost-producing cyber operations targeting State C.

Additionally, a strong basis does appear to exist to conclude that the cyber attack involved coercion—perhaps that State C was seeking to compel the allies to stop the combined exercise and/or reduce the United States’ role in the region.²⁵² And State C did disrupt military command and control systems, thereby implicating the minority, control theory of coercion discussed under Scenario 2. Moreover, in *Nicaragua*, the International Court of Justice placed particular emphasis on military acts and implications in analyzing unlawful intervention.

But coercion, in and of itself, is insufficient to find unlawful intervention. Unlawful intervention is generally understood to require both coercion and interference into another state’s *domaine réservé*. Thus, a second element of intervention is whether the cyber operations interfered with “matters in which each State is permitted, by the principle of State sovereignty, to decide freely.”²⁵³

The general inviolability of state sovereign vessels and aircraft and the core nature of the sovereign interest in command and control of state military forces might suggest that these operations crossed a line into the *domaine réservé* of the United States and Japan. However, the contours of *domaine réservé* under international law are vague and not well-developed—especially in cyberspace. There may be, for example, distinctions between intrusion into military systems for intelligence collection, non-intrusive disruption of military systems on the high sea, and intrusion to usurp command of the victim’s forces. Historically, states have accessed other nations’ military systems for a variety of purposes, including intelligence collection and placement and access in advance of potential future operations. The absence of *opinio juris* in this area of customary international law, combined with state practice, casts doubt that the mere disruption of military command and control systems is *per se* an intervention within states’ *domaine réservé*.

It is certainly possible that the U.S. and Japanese governments might jointly conclude, even in secret, that the rule of non-intervention was violated and that response via countermeasures would be legally justified. Such a conclusion could

feed into the U.S.-Japan Defense Cooperation process, with the incident likely to be viewed from the Japanese perspective as a “cyber incident against Japan” for which “Japan will have primary responsibility to respond, and ... the United States will provide appropriate support to Japan.”²⁵⁴ The U.S. government would be expected to draw its own legal conclusions—informed by, but independent of, what might be discussed with Japanese officials—and to be prepared to exercise its rights in response to Scenario 3.²⁵⁵

Ultimately, while it may be unclear where the U.S.-Japan Alliance would come down on the issue of unlawful intervention under Scenario 3, the question may be of little practical consequence. Unless the violation continues (i.e., State C continues to disrupt or resumes disrupting Alliance command and control systems), the violation appears to have ended. Countermeasures would normally not be permitted as a response to conduct that has terminated.

Rather Scenario 3 might be an example of the types of circumstances against which Japan and the United States would look to more effectively defend their networks, unilaterally or bilaterally, in the future without needing to conclude that armed attack, use of force, or unlawful intervention had occurred, was occurring, or was imminent²⁵⁶ and without necessarily seeking broader international support or UN Security Council sanctions.²⁵⁷ Instead of waiting for similar operations to cause actual harm in the future, the U.S.-Japan Alliance might find even greater merit in the states’ strategies to defend forward and conduct proactive defense.

This raises the plea of necessity as a final legal justification for action.²⁵⁸ In the future, the U.S.-Japan Alliance may very well find sufficient room to maneuver without resorting to necessity. Some combination of diplomacy, retorsion²⁵⁹, self-defense, countermeasures, and the general freedom to operate under *jus extra bellum* may prove adequate for defending forward and proactive security. If not—and if there is no other way to “safeguard an essential interest against a grave and imminent peril”²⁶⁰—then necessity is another option. While some view reliance on the plea of necessity with skepticism, nevertheless necessity is a well-established legal justification in international law.

The plea of necessity, which applies equally inside and outside of cyberspace,²⁶¹ does present a high bar. “Acting on the basis of necessity is only permissible when a State’s essential interests are gravely threatened.”²⁶² Yet it would seem that any of the three scenarios discussed might involve essential interests of the targeted states (e.g., a nuclear plant, public transportation, emergency communications, media, and military ships and aircraft).

Moreover, necessity may be invoked as legal justification without attribution of unlawful conduct to a state (e.g., no requirement to demonstrate that State C used force or engaged in an unlawful intervention).²⁶³ This could present much greater freedom in cyberspace if the United States and/or Japan lawfully invoke the plea. Furthermore, necessity seems a rather significant foundation atop which some

substantial amount of the U.S.-Japan Alliance's future cyber operations might rest.

Necessity might support precisely what would be required going forward from Scenario 3 and, more broadly, for the future of the U.S.-Japan Alliance: more proactive defenses that impose costs; defending forward in the proactive pursuit of peace; and collective self-defense, countermeasures, and other means and methods of combatting advance persistent threats.

Conclusion

As the United States moves ahead with clear authority to defend forward and directly address the most pressing threats the nation faces across cyberspace, the Japanese government is also well-positioned to assume the more substantial and impactful cyber role it seeks. The complexity, severity, and pervasiveness of cyber threats to the U.S.-Japan Alliance will continue to grow for the foreseeable future. Although cyber armed attack and use of force remain significant concerns, they likely will rarely manifest into concrete events. Instead, malicious “sub-use of force” cyber operations may present more frequent and perhaps more substantial occasions for Alliance forces to conduct self-help and mutual aid. The gray zone will likely continue to be an arena in which proactive security measures face few directly applicable international legal constraints and where the United States and Japan will retain states’ rights that support their cyber strategies. It is in this space where the United States and Japan can most effectively defend their computer systems and networks instead of waiting for adversaries to cause harm.

Japan might view the generally permissive international legal environment surrounding “sub-use of force” operations as an opportunity to further advance its ambitions as a guardian and trusted ally in cyberspace. The principles of sovereignty and non-intervention should be given due regard, as should other aspects of international law applicable to cyber operations. But the U.S.-Japan Alliance should not feel unnecessarily constrained by international legal considerations when they are not applicable to facts at-hand. Rather the U.S. and Japanese governments might embrace the general applicability of international law to states’ actions in and through cyberspace while carefully considering the legal policy choices they will make in unsettled areas of international law.

There is room to maneuver, and U.S. and Japanese cyber forces will undoubtedly want the ability to move with speed and agility. To do so, both U.S. and Japanese domestic law and policy will need to continue to adjust to meet challenges presented by new threats and technologies. Just as U.S. cyber forces will need to maintain operational authority to meet cyber adversaries “beyond the blue” in “sub-use of force” situations, Japanese cyber forces could benefit from clear, forward-looking domestic laws that permit engagement in persistent

cyber activities tailored to address advanced persistent threats without necessarily requiring further Cabinet decisions and Diet approval to act when time and circumstances do not allow.

Both nations appear to recognize a model of cyber collaboration. The model requires something more than diplomacy, information sharing, and capacity building. As the Japanese government has explained, a profound need exists for both states to “*take actual action*.”²⁶⁴ The international legal framework can support the allies engaging in mutual defense in and through cyberspace. The necessary domestic legal and policy architectures will likely always be under construction to some degree, but the foundations have been laid for more proactive and effective mutual defense. ■

Michael J. Adams, Commander (ret.) USN, served as Special Advisor to the Judge Advocate General for International and Operational Law and as Deputy Counsel to the Chairman of the Joint Chiefs of Staff, where he advised Chairmen Dempsey and Dunford and the Joint Staff on matters of international and national security law affecting military operations, including emerging technologies, the law of armed conflict, and cyberspace, intelligence, special operations, maritime, and other U.S. government activities. He is a graduate of Harvard Law School (LL.M), Georgetown University Law Center (J.D.), and the United States Naval Academy (B.S.).

1 See generally Gov't of Japan, National Security Strategy (2013).

2 Gov't of Japan, Cybersecurity Strategy 37 (2018) ("It is the mission of governmental bodies to protect and support people's lives and socio-economic activities. Any failure in playing their role is a significant concern for national security.").

3 See Harold Hongju Koh, Legal Advisor, Dep't of State, Prepared Remarks at USCYBERCOM Inter-Agency Legal Conference: International Law in Cyberspace (Sept. 18, 2012); Brian J. Egan, Legal Advisor, Dep't of State, Remarks on International Law and Stability in Cyberspace at University of California, Berkeley School of Law (Nov. 10, 2016); Paul C. Ney, Jr., Gen. Counsel, Dep't of Def., Remarks at U.S. Cyber Command Legal Conference (Mar. 2, 2020).

4 *Cyber Mission Force achieves Full Operational Capability*, U.S. Cyber Command Pub. Aff. (May 17, 2018), <http://www.cybercom.mil/Media/News/News-Display/Article/1524492/cyber-mission-force-achieves-full-operational-capability/>.

5 Mark Pomerleau, *New authorities mean lots of new missions at Cyber Command*, Fifth Domain (May 8, 2019), <https://www.fifthdomain.com/dod/cybercom/2019/05/08/new-authorities-mean-lots-of-new-missions-at-cyber-command/>.

6 Paul M. Nakasone, *A Cyber Force for Persistent Operations*, 92 Joint Force Q. 10, 12 (2019); C. Todd Lopez, *DOD More Assertive, Proactive in Cyber Domain*, U.S. Cyber Command Pub. Aff. (June 28, 2019), <https://www.defense.gov/Explore/News/Article/Article/1891495/dod-more-assertive-proactive-in-cyber-domain/>. General Nakasone serves as Commander of the U.S. Cyber Command, Director of the National Security Agency, and Chief of the Central Security Service. For the purposes of this paper, the term "defensive" is not limited to internal network cybersecurity operations. Rather, the term "defensive" connotes a broad range of activities that respond to cyber threats, even where the responsive action extends outside of the

defender's computer systems and networks. The author's working definition is akin to the definition of "defensive cyberspace operations" in Joint Chiefs of Staff, Joint Publication 3-12: Cyberspace Operations, at GL-4 (2018) ("[Defensive cyberspace operations are] . . . [m]issions to preserve the ability to utilize blue cyberspace capabilities and protect data, networks, cyberspace-enabled devices, and other designated systems by defeating on-going or imminent malicious cyberspace activity.").

7 Treaty of Mutual Cooperation and Security, Japan-U.S., art. III, Jan. 19, 1960, 11 U.S.T. 1632 [hereinafter U.S.-Japan Security Treaty].

8 Dep't of Def., Summary: Department of Defense Cyber Strategy 1 (2018).

9 Ministry of Def., Defense of Japan 2019, at 391 (2019).

10 See *id.* at 167. Note that geographic proximity does not matter much in cyberspace—Iran, ISIS, and others present threats as well—but regional disagreements often fuel activities in cyberspace.

11 Interview, *An Interview with Paul M. Nakasone*, 92 Joint Force Q. 4 (2019) [hereinafter Nakasone Interview] ("They are actively in our network communications, attempting to steal data and impact our weapons systems.").

12 See Nat'l Intelligence Council, Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent U.S. Elections (2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf.

13 "Our adversaries and strategic competitors will increasingly use cyber capabilities—including cyber espionage, attack, and influence—to seek political, economic, and military advantage over the United States and its allies and partners. China, Russia, Iran, and North Korea increasingly use cyber operations to threaten both minds and machines in an expanding number of ways—to steal information, to influence our citizens, or to disrupt critical infrastructure." *Worldwide Threat Assessment of the U.S. Intelligence Community: Statement for the Record Before the S. Select Comm. on Intelligence*, 116th Cong.

5 (2019) (statement of Daniel R. Coats, Dir. of Nat'l Intelligence).

14 See generally Joseph L. Votel, Charles T. Cleveland, Charles T. Connett & Will Irwin, *Unconventional Warfare in the Gray Zone*, 80 Joint Force Q. 101, 102 (2016); Rosa Brooks, *Rule of Law in the Gray Zone*, Modern War Inst. (July 2, 2018), <https://www.mwi.usma.edu/rule-law-gray-zone/>. Japan's Ministry of Defense describes "gray-zone situations" as "neither purely peacetime nor contingency situations." Ministry of Def., Defense of Japan 2019, *supra* note 9, at 41.

15 See Joint Chiefs of Staff, *The National Military Strategy of the United States of America* 2015, at 4 (2015); Aurel Sari, *Legal Aspects of Hybrid Warfare*, Lawfare (Oct. 2, 2015), <https://www.lawfareblog.com/legal-aspects-hybrid-warfare>. Japan's Ministry of Defense explains that "hybrid warfare" is a "method of altering the status quo that intentionally blurs the boundaries between the military and non-military realms." Ministry of Def., Defense of Japan 2019, *supra* note 9, at 17.

16 Certainly, these are not new concerns at the macro-level (e.g., theft of defense technology has been a problem throughout history). Yet, the persistency, scale, and potential impact of these activities have surged in such a way that, arguably, there is even less incentive for states to challenge the United States and its allies in armed conflict. Dep't of Def., Summary: Department of Defense Cyber Strategy, *supra* note 8, at 1. The Department focuses particularly on China and Russia, explaining that their "campaigns in and through cyberspace . . . pose long-term strategic risk to the [United States] as well as to [its] allies and partners." *Id.*

17 See U.S. Cyberspace Solarium Comm'n, *Cyberspace Solarium Commission Final Report* 8 (2020). The Commission reports that major U.S. public-sector cyber threats include: (1) "[a]ttacks on election processes and other democratic institutions designed to damage American legitimacy and weaken the nation", (2) "[e]spionage efforts intended

to undermine both U.S. military capability and the Defense Industrial Base", (3) "[t]argeting of civilian agencies for intelligence collection and to obtain other advantages over the United States", and (4) "[l]oss of leadership in research and development of key technologies." *Id.*

18 Ney, *supra* note 3 ("[B]ecause cyberspace is a relatively cheap form of gaining real power, especially for impoverished adversaries like North Korea: a cyber operation can require nothing more than a reasonably skilled operator, a computer, a network connection, and persistence."); U.N. Secretary-General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, ¶ 7, U.N. Doc. A/70/174 (July 22, 2015) [hereinafter UN GGE Report] ("The diversity of malicious non-state actors (including criminal groups and terrorists), their differing motives, the speed at which malicious ICT actions can occur, and the difficulty of attributing the source of an ICT incident, all increase risk."); see also Gabriella Blum, *Technology & the Future of Violence*, Defining Ideas: Hoover Inst. J. (Aug. 17, 2012), <https://www.hoover.org/research/technology-future-violence>.

19 UN GGE Report, *supra* note 18, ¶ 5 ("The most harmful attacks using [Information and Communications Technology] include those targeted against a State's critical infrastructure and associated systems. The risk of harmful ICT attacks against critical infrastructure is both real and serious.").

20 See Office of Dir. of Nat'l Intelligence, *A Guide to Cyber Attribution* (2018), available at https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf.

21 See generally Joint Chiefs of Staff, *National Military Strategy*, *supra* note 15.

22 Ministry of Def., Defense of Japan 2019, *supra* note 9, at 167 ("Types of cyber attacks include functional disruption, data falsification and data theft caused by unauthorized access to information and communications networks or through the transmission of viruses via e-mail, functional impairment of the networks

through simultaneous transmission of large quantities of data, and attacks intended to shut down or take over a system belonging to critical infrastructure, such as power systems. Also, Internet-related technologies are constantly evolving, with cyber attacks becoming more and more advanced and sophisticated by the day.”).

23 Franz-Stefan Gady, *Japan Hit by Cyberattacks at an Unprecedented Level*, *Diplomat* (Feb. 20, 2015), <https://www.thediplomat.com/2015/02/japan-hit-by-cyberattacks-at-an-unprecedented-level/>; see also Paul Kallender & Christopher W. Hughes, *Japan's Emerging Trajectory as a Cyber Power: From Securitization to Militarization of Cyberspace*, 40 *J. Strategic Stud.* 118, 124 (2017). Kallender and Hughes do not define “cyber attack” in this article. Instead, they provide wide-ranging examples of malicious actions conducted in and through cyberspace and directed against financial institutions, media, government, and various other entities. The U.S. military defines “cyberspace attack” as “[a]ctions taken in cyberspace that create noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial that appears in a physical domain, and is considered a form of fires.” Joint Chiefs of Staff, *Cyberspace Operations*, *supra* note 6, at GL-4.

24 Ministry of Def., *Defense of Japan* 2019, *supra* note 9, at 168–69.

25 Franz-Stefan Gady, *Japan: The Reluctant Cyberpower*, 91 *Notes de l'Ifr* *Asie Visions*, at abstract (2017).

26 See generally Kallender & Hughes, *supra* note 23.

27 Gady, *supra* note 25. Note the recent attention given to protecting information in the Basic Act on the Advancement of Public and Private Sector Data Utilization and the Amended Act on the Protection of Personal Information. Note also the Legislation for Peace and Security, which is not focused on cyber operations but is important legislation that provides Japan Self-Defense Forces with broader mission authorities and generally

allows for combined operations with non-Japanese forces. Gov't of Japan, *Japan's Legislation for Peace and Security* (2016), <https://www.mofa.go.jp/files/000143304.pdf>

28 A non-exhaustive list of significant developments includes:

- Establishment of the “Act on Protection of Specially Designated Secrets” (2013) and the “Basic Act on Cybersecurity” (2014);
- Updates to the “First National Strategy on Information Security” (2006) and “Second National Strategy on Information Security” (2009) through the Information Security Policy Council's (ISPC) “Information Security 2012” and “Cybersecurity Strategy” (2013) and Cabinet-approved updates to the Strategy in 2015 and again in 2018;
- Establishment of the Japanese National Security Council in 2013, splitting responsibilities held by ISPC between the Cyber Security Strategy Headquarters and National Center for Incident Readiness and Strategy for Cybersecurity; and
- Creation of the Japanese Self-Defense Forces Cyber Defense Unit.

29 Gov't of Japan, *Cybersecurity Strategy*, *supra* note 2, at 35–36 (“In order to realize a free, fair, and secure cyberspace at the global level, Japan will communicate its idea in the international fora and take an active role in promoting the rule of law in cyberspace.”).

30 Gady, *Japan Hit by Cyberattacks at an Unprecedented Level*, *supra* note 23; see also Gov't of Japan, *National Security Strategy*, *supra* note 1, at 13–20 (explaining that Japan's “strategic approaches” involve “strengthening and expanding Japan's capabilities and roles” and include “strengthening cyber security, international counterterrorism, intelligence capabilities . . . and technological capabilities”).

31 Dep't of Def., *Guidelines for U.S.-Japan Defense Cooperation* 23 (2015), available at https://archive.defense.gov/pubs/20150427_-_GUIDELINES_FOR_US-JAPAN_DEFENSE_COOPERATION.pdf.

32 *Id.*

33 Nakasone, *supra* note 6, at 12. General Nakasone emphasized that “[p]ersistence should not be mistaken for engagement for engagement’s sake; instead, it is an approach that empowers U.S. cyber forces to achieve more decisive results in pursuit of objectives set by national leaders.” *Id.* at 11.

34 To “defend forward” in cyberspace is to “maneuver seamlessly across the interconnected battlespace, globally, as close as possible to adversaries and their operations, and continuously shape the battlespace to create operational advantage for us while denying the same to our adversaries.” *Id.* at 13.

35 Gov’t of Japan, Cybersecurity Strategy, *supra* note 2, at 37. Another component of both nations’ efforts is capacity building. As the 2015 UN GGE Report explains, “States bear primary responsibility for national security and the safety of their citizens, including in the ICT environment, but some States may lack sufficient capacity to protect their ICT networks. A lack of capacity can make a State’s citizens and critical infrastructure vulnerable, or make a State an unwitting haven for malicious actors. International cooperation and assistance can play an essential role in enabling States to secure ICTs and ensure their peaceful use.” UN GGE Report, *supra* note 18, ¶ 19.

36 The U.S.-Japan Security Consultative Committee “decided that cooperation in cross-domain operations, enhancing the Alliance’s capabilities, and increasing operational readiness and cooperation should be core objectives to advance [the] defense relationship . . . [and] committed to enhance cooperation on cyber issues, including deterrence and response capabilities.” Joint Statement, U.S.-Japan Sec. Consultative Comm. (Apr. 19, 2019). They also explained that “each nation is responsible for developing the relevant capabilities to protect their national networks and critical infrastructure.” *Id.* Media outlets quickly reported that the United States was now committed “to defend Japan from cyber-attack.” See, e.g., *U.S. to defend Japan from*

cyberattack under security pact, Japan Times (Apr. 20, 2019), <https://www.japantimes.co.jp/news/2019/04/20/national/politics-diplomacy/first-japan-u-s-say-security-treaty-cover-cyber-attacks/#.XoqG5C85Tyg>.

37 Nakasone, *supra* note 6, at 12.

38 The 2018 National Cyber Strategy of the United States committed to “protecting networks, systems, functions, and data”; “nurturing a secure, thriving digital economy and fostering strong domestic innovation”; “strengthening the ability of the United States – in concert with allies and partners – to deter and, if necessary, punish those who use cyber tools for malicious purposes”; and “[expanding] American influence abroad to extend the key tenets of an open, interoperable, reliable, and secure internet.” White House, National Cyber Strategy of the United States of America, at I (2018). The specified objective under “Preserve Peace Through Strength,” the third of four pillars in the National Strategy, is to “[i]dentify, counter, disrupt, degrade, and deter behavior in cyberspace that is destabilizing and contrary to national interests, while preserving United States overmatch in and through cyberspace.” *Id.* at 20.

39 The 2018 Department of Defense Cyber Strategy “represents the Department’s vision for addressing [the cyber] threat and implementing the priorities of the National Security Strategy and National Defense Strategy for cyberspace. It supersedes the 2015 DoD Cyber Strategy.” Dep’t of Def., Summary: Department of Defense Cyber Strategy, *supra* note 8, at 2.

40 “Competitors deterred from engaging the United States and our allies in an armed conflict are using cyberspace operations to steal our technology, disrupt our government and commerce, challenge our democratic process, and threaten our critical infrastructure.” *Id.* at 1.

41 White House, National Cyber Strategy, *supra* note 38, at II. One might reasonably expect, based on public reporting, that below these policy documents sit certain orders and rules of engagement that prescribe in more

detail the left and right limits of U.S. military cyber operations.

42 Defending forward involves “continuously engaging and contesting adversaries and causing them uncertainty wherever they maneuver,” also known as persistent engagement. Ney, *supra* note 3. U.S. Cyber Command provides an illustrative example. Based on the author’s personal notes from participating in unclassified events, the Command’s public statements (and presumably its internal deliberations and military planning) have evolved from, roughly, “we are in constant contact from cyberattacks by our adversaries” in 2017 to “we have the need for speed . . . especially in gray space” in 2018 to “we are conducting effective cyber operations as we defend forward” in 2019.

43 The Department of Defense Cyber Strategy states that the “Department must take action in cyberspace during day-to-day competition to preserve U.S. military advantages and to defend U.S. interests. Our focus will be on the States that can pose strategic threats to U.S. prosperity and security, particularly China and Russia. We will conduct cyberspace operations to collect intelligence and prepare military cyber capabilities to be used in the event of crisis or conflict. We will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict.” Dep’t of Def., Summary: Department of Defense Cyber Strategy, *supra* note 8, at 1.

44 Nakasone, *supra* note 6, at 12.

45 “The term ‘blue cyberspace’ denotes areas in cyberspace protected by the U.S., its mission partners, and other areas DOD may be ordered to protect. Although DOD has standing orders to protect only the Department of Defense information network (DODIN), cyberspace forces prepare on order, and when requested by other authorities, to defend or secure other United States Government (USG) or other cyberspace, as well as cyberspace related to critical infrastructure and key resources (CI/KR) of the U.S. and PN[s] [partner nations].” Max Smeets, *Cyber*

Command’s Strategy Risks Friction With Allies, Lawfare (May 28, 2019), <https://www.lawfare-blog.com/cyber-commands-strategy-risks-friction-allies>.

46 *Id.* The Department of Defense Cyber Strategy emphasized that it would “take action in cyberspace during day-to-day competition to preserve U.S. military advantages and to defend U.S. interests.” Dep’t of Def., Summary: Department of Defense Cyber Strategy, *supra* note 8, at 1.

47 *Id.*

48 Dwight Weingarten, *Congress Receives Long-Awaited Memorandum From White House on Cyber Policy*, MeriTalk (Mar. 17, 2020), <https://www.meritalk.com/articles/congress-receives-long-awaited-memorandum-from-white-house-on-cyber-policy/>.

49 Ney, *supra* note 3.

50 See Sydney J. Freedberg, Jr., ‘Desperate Need for Speed’ As Army Takes on Chinese, Russian, ISIS Info Ops, *Breaking Def.* (Aug. 21, 2019), <https://breakingdefense.com/2019/08/desperate-need-for-speed-as-army-takes-on-chinese-russians-isis-trolls/>.

51 See 10 U.S.C. § 130(g).

52 See National Defense Authorization Act of 2019, Pub. L. 115-232, § 1636.

53 *Id.* Section 1636 further states:

(a) In General—It shall be the policy of the United States, with respect to matters pertaining to cyberspace, cybersecurity, and cyber warfare, that the United States should employ all instruments of national power, including the use of offensive cyber capabilities, to deter if possible, and respond to when necessary, all cyber attacks or other malicious cyber activities of foreign powers that target United States interests with the intent to—

(1) cause casualties among United States persons or person of United States allies;

(2) significantly disrupt the normal functioning of United States democratic society or government (including attacks against critical infrastructure that could damage systems

used to provide key services to the public or government);

(3) threaten the command and control of the Armed Forces, the freedom of maneuver of the Armed Forces, or the industrial base or other infrastructure on which the United States Armed Forces rely to defend United States interests and commitments; or

(4) achieve an effect, whether individually or in aggregate, comparable to an armed attack or imperil a vital interest of the United States.

54 Gov't of Japan, National Security Strategy, *supra* note 1, at 14.

55 See generally Adam P. Liff, *Japan's Security Policy in the 'Abe Era': Radical Transformation or Evolutionary Shift?*, 1 Tex. Nat'l Security Rev. 9 (2018); Jeffrey W. Hornung, *Gauging Japan's 'Proactive Contributions to Peace'*, Diplomat (Oct. 27, 2015), <https://thediplomat.com/2015/10/gauging-japans-proactive-contributions-to-peace/>.

56 See Adam P. Liff, *Japan's National Security Council at Five*, Brookings (Dec. 4, 2018), <https://www.brookings.edu/blog/order-from-chaos/2018/12/04/japans-national-security-council-at-five/>.

57 See Michael Bosack, *Japan's Security Legislation Turns Two*, Tokyo Rev. (Sept. 29, 2017), <https://www.tokyoreview.net/2017/09/japan-peace-security-legislation/>; Masahiro Kurosaki, *Japan's Evolving Position on the Use of Force in Collective Self-Defense*, Lawfare (Aug. 23, 2018), <https://www.lawfareblog.com/japans-evolving-position-use-force-collective-self-defense>.

58 See Gov't of Japan, National Defense Program Guidelines for FY 2019 and Beyond (2018).

59 The 2018 Cybersecurity Strategy explained that "[a] free, fair, and secure cyberspace contributes to the peace and stability of the international community and to Japan's national security." Gov't of Japan, Cybersecurity Strategy, *supra* note 2, at 35.

60 Defense of Japan 2019 reported that "(1) organizations related to cybersecurity

that are spread over multiple departments and agencies are being integrated, and their operational units are being centralized; (2) policy and research units are being enhanced by establishing specialized posts, creating new research divisions and enhancing such functions; (3) the roles of intelligence agencies in responding to cyber attacks are being expanded; and (4) more emphasis is being given to international cooperation. At the level of the defense ministry, various measures have been taken, such as establishing a new agency to supervise cyberspace military operations and positioning the effort to deal with cyber attacks as an important strategic objective." Ministry of Def., Defense of Japan 2019, *supra* note 10, at 169. The Ministry of Defense "plans to use 25.6 billion yen for beefing up defense capabilities in the cyber domain. . . . This year, the MOD will increase the number of staff in the Cyber Defense Group from 220 to 290, and establish a Cyber Protection Unit (tentative name) inside the Ground Self-Defense Force (GSDF). The Japanese Defense Ministry will utilize cutting-edge technology in the field of cybersecurity by procuring a Cyber Information Gathering System with 3.4 billion yen, designing an 'AI-enabled system to respond against cyberattack' with 30 million yen, and researching the security of network devices in the so-called 5G era with 20 million yen. The MOD will attempt to secure and develop a cyber workforce by dispatching SDF personnel to U.S. Cyber Commander Education Courses (a budgeted cost of 40 million yen), developing a posture of internal knowledge and skills on cyber, hosting a cyber completion tentatively named MOD-CTF (4 million yen), improving the Defense Information Infrastructure (7.6 billion yen), and enhancing Controllability and Situation Awareness of System Network (1.2 billion yen)." Daisuke Akimoto, *Japan's Emerging 'Multi-Domain Defense Force'*, Diplomat (Mar. 18, 2018), <https://thediplomat.com/2020/03/japans-emerging-multi-domain-defense-force/> (internal quotation marks omitted).

61 Ministry of Def., Defense of Japan 2019, *supra* note 9, at 204.

- 62** Gov't of Japan, National Defense Program Guidelines, *supra* note 58, at 11.
- 63** *Id.* at 8, 14.
- 64** Gov't of Japan, Cybersecurity Strategy, *supra* note 2, at 37.
- 65** "[T]he government will proactively contribute to various international discussions and work for the sharing of information and development of common understanding regarding cyber related issues. The government will also share expertise with foreign countries, promote specific cooperation and collaboration, and take actual action." *Id.* at 41 (emphasis added).
- 66** "[I]n cyberspace it's the use of cyber capabilities that is strategically consequential. The threat of using something in cyberspace is not as powerful as actually using it." Nakasone Interview, *supra* note 11, at 12.
- 67** Liff, *Japan's Security Policy*, *supra* note 55.
- 68** See Hornung, *supra* note 55; Emma Hutchinson & Adam May, *Is the Cruz Report the end of peacekeeping for Japan?*, Japan Times (June 12, 2018), <https://www.japan-times.co.jp/opinion/2018/06/12/commentary/japan-commentary/cruz-report-end-peace-keeping-japan/#.Xqg8pC85TxU>.
- 69** Kurosaki, *supra* note 57.
- 70** See generally Emma Chanlett-Avery et al., Cong. Research Serv., RL33740, *The U.S.-Japan Alliance* (2019).
- 71** Shinzo Abe, Prime Minister of Japan, Remarks at Ctr. for Strategic & Int'l Studies: Japan is Back (Feb. 22, 2013).
- 72** The particular capabilities for defense, deterrence, and situational awareness that the Japanese government is addressing are outlined in Gov't of Japan, Cybersecurity Strategy, *supra* note 2, at 37–41.
- 73** See Terri Moon Conk, *DOD's Cyber Strategy of Past Year Outlined Before Congress*, DOD News (Mar. 6, 2020), <https://www.defense.gov/Explore/News/Article/Article/2103843/dods-cyber-strategy-of-past-year-outlined-before-congress/>.
- 74** Gov't of Japan, Cybersecurity Strategy, *supra* note 2, at 41. The message that Japan seems most acutely attuned to is the warning that "if we find ourselves defending inside our own networks, we have lost the initiative and the advantage." Nakasone, *supra* note 6, at 10.
- 75** U.S.-Japan Security Treaty, *supra* note 7, art. VII.
- 76** The U.S.-Japan Security Treaty articles are obvious reflections of U.N. Charter arts. 2(4), 51. Also, the Japanese Diet's 2014 reinterpretation of the war-renouncing clause of Article 9 of the Japanese Constitution is unlikely to have much effect in the cyber context, where the vast majority of malicious cyber activities do not amount to use of force and do not implicate self-defense under international law. This means that Japan's new collective self-defense rules, while important to the U.S.-Japan Alliance generally, may matter less in cyberspace.
- 77** Nihonkoku Kenpō [Kenpō] [Constitution], arts. 9, 13 (Japan).
- 78** Dep't of Def., Guidelines for U.S.-Japan Defense Cooperation, *supra* note 31, art. II.C.
- 79** The door opened a bit in 2014 when the Japanese Cabinet expanded its position on self-defense, allowing collective self-defense of other states subject to three conditions. However, government positions are still being developed and it is too soon to say that Japan will fundamentally alter its long-standing approaches.
- 80** UN GGE Report, *supra* note 18 ¶ 24 (adopting and restating the experts' prior position that international law applies to information and communications technologies).
- 81** See *id.*; see also Gary Corn, *Punching on the Edges of the Grey Zone: Iranian Cyber Threats and State Cyber Responses*, Just Security (Feb. 11, 2020), <https://www.justsecurity.org/68622/punching-on-the-edges-of-the-grey-zone-iranian-cyber-threats-and-state-cyber-responses/>.

82 The 2015 UN GGE Report recorded consensus among 20 states featuring prominently in cyberspace. It indicates that the UN GGE, in furtherance of its mandate to determine how international law applies in cyberspace, was able to agree on six principles of international law: state sovereignty, sovereign equality, the settlement of disputes by peaceful means, refraining from the threat or use of force in international relations, non-intervention in the internal affairs of other states, and respect for human rights and fundamental freedoms. The 20 states composing the 2015 UN GGE were: Belarus, Brazil, China, Colombia, Egypt, Estonia, France, Germany, Ghana, Israel, Japan, Kenya, Malaysia, Mexico, Pakistan, the Russian Federation, Spain, the United Kingdom, and the United States. They were selected based on “equitable geographic distribution” and involving “cyber powers.” The consensus achieved in 2015 may represent some degree of success for the UN GGE, but these were mostly very broad principles, many of which seemed obvious before the UN GGE. UN GGE discussions continue and these efforts are not insignificant.

83 Michael Schmitt, *Norm-Skepticism in Cyberspace? Counter-factual and Counterproductive*, Just Security (Feb. 28, 2020), <https://www.justsecurity.org/68892/norm-skepticism-in-cyberspace-counter-factual-and-counterproductive/>.

84 Efforts such as the Tallinn Manual and Tallinn 2.0 should not be mistaken for *lex lata*; by and large, they are *lex ferenda* projects. Emerging state positions are discussed later in this section.

85 See Schmitt, *supra* note 84.

86 Arguably, Japan’s cyber diplomacy has been the leading edge of the Japanese government’s cyber strategies. Meanwhile, various state officials and scholars have endeavored to provide greater clarity for states. See, e.g., UN GGE Report, *supra* note 18; G20, *G20 Leaders’ Communiqué Antalya Summit* (Nov. 16, 2015), <https://www.consilium.europa.eu/media/23729/g20-antalya-leaders-summit-communicue.pdf>; G7,

Declaration on Responsible States Behavior in Cyberspace (Apr. 11, 2017), <https://mofa.go.jp/files/000246367.pdf>; Tallinn Manual on the International Law Applicable to Cyber Warfare (Michael N. Schmitt ed., 2013); Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Michael N. Schmitt ed., 2d ed. 2017).

87 The fourth session of the UN GGE recorded 11 recommendations for norms and principles that were ultimately approved. See G7, *supra* note 86.

88 The Convention on Cybercrime of the Council of Europe (CETS No. 185) is also known as the Budapest Convention. “It serves as a guideline for any country developing comprehensive national legislation against Cybercrime and as a framework for international cooperation between State Parties to [the] treaty.” There are more than 50 state parties, most of which are Western states. See *Budapest Convention and related standards*, Council of Eur., <https://www.coe.int/en/web/cybercrime/the-budapest-convention> (last visited Apr. 12, 2020).

89 The General Data Protection Regulation is the European Union’s extraterritorial privacy regime that impacts the treatment of data and privacy across borders around the world. It has a significant national security carve-out, and so far, seems to have little impact in the national security context. See *Complete guide to GDPR compliance*, GDPR, <https://gdpr.eu> (last visited Apr. 12, 2020).

90 But see Michael J. Adams, *A Warning About Tallinn 2.0 ... Whatever It Says*, Lawfare (Jan. 4, 2017), <https://www.lawfareblog.com/warning-about-tallinn-20-...-whatever-it-says>.

91 For example, see positions of the United Kingdom, Jeremy Wright, Att’y Gen., Speech on Cyber and International Law in the 21st Century (May 23, 2018), and China, Niels Nagelhus Schia & Lars Gjesvik, Nor. Inst. Int’l Aff., *China’s Cyber Sovereignty* (2017), https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/NUPI-Policy_Brief_2_17_Schia_Gjesvik.pdf, on sovereignty.

92 Ney, *supra* note 3.

93 *Id.* ("For cyber operations that would not constitute a prohibited intervention or use-of-force, the Department [of Defense] believes there is not sufficiently widespread and consistent state practice resulting from a sense of legal obligation to conclude that customary international law generally prohibits such non-consensual cyber operations in another state's territory. This proposition is recognized in the Department's adoption of the 'defend forward' strategy. . . . The Department's commitment to defend forward including to counter foreign cyber activity targeting the United States—comports with our obligations under international law and our commitment to the rules-based international order.").

94 See *id.* ("To determine whether a rule of customary international law has emerged with respect to certain State activities in cyberspace, we look for sufficient State practice over time, coupled with *opinio juris*—evidence or indications that the practice was undertaken out of a sense that it was legally compelled, not out of a sense of policy prudence or moral obligation.").

95 Koh, *supra* note 3.

96 Koh further outlined the U.S. government's stance on several key issues, including:

- "Cyberspace is not a 'law-free' zone where anyone can conduct hostile activities without rules or restraint."
- "Cyber activities may in certain circumstances constitute uses of force within the meaning of Article 2(4) of the UN Charter and customary international law."
- "A State's national right of self-defense, recognized in Article 51 of the UN Charter, may be triggered by computer network activities that amount to an armed attack or imminent threat thereof."
- "In the context of an armed conflict, the law of armed conflict applies to regulate the use of cyber tools in hostilities, just as it does other tools. The principles of necessity and proportionality limit uses of force in

self-defense and would regulate what may constitute a lawful response under the circumstances."

- "States conducting activities in cyberspace must take into account the sovereignty of other States, including outside the context of armed conflict."
- "States are legally responsible for activities undertaken through 'proxy actors,' who act on the State's instructions or under its direction or control."

Id. These positions remain largely unchanged, although they have been updated in international forums and in remarks by key figures such as State Department Legal Adviser Brian Egan and, most recently, Department of Defense General Counsel Paul Ney, Jr.

97 U.N. Charter art. 2(4) ("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.").

98 U.N. Charter art. 51 ("Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.").

99 Tallinn Manual 2.0, *supra* note 86, at 375 ("A condition precedent to the application of the law of armed conflict is the existence of an armed conflict."). For an example on Estonia, see *id.* at 376 ("[T]arget of persistent cyber operations."). See also *id.* ("However, the law of armed conflict did not apply to those cyber operations because the situation did not rise to the level of an armed conflict."). But

see *id.* for examples on Georgia-Russia and Ukraine-Russia.

100 For the U.S. Department of Defense, “[i]t is also longstanding DoD policy that U.S. forces will comply with the law of war ‘during all armed conflicts however such conflicts are characterized and in all other military operations.’ Even if the law of war does not technically apply because the proposed military cyber operation would not take place in the context of armed conflict, DoD nonetheless applies law-of-war principles.” Ney, *supra* note 4; see also Dep’t of Def., 2311.01E, DoD Law of War Program ¶ 4.1 (2011) available at <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/231101e.pdf>.

101 The authors of the Tallinn Manual confronted this dilemma. Their original work may have had reason to be applied within the context of armed conflict, but there continue to be serious concerns about applying the Manual to sub-use of force activities occurring outside of armed conflict. See Adams, *supra* note 90.

102 Interestingly, at least in part due to the Russian Federation’s objections, the 2015 UN GGE was unable to develop the degree of consensus that some may have hoped for on applying *jus in bello* to cyberspace. The Russian Presidential Special Envoy for International Cooperation in Information Security, Andrei Krutskikh, stated, “[W]e and a number of other countries were against singling out the Article 51. . . . The report reflects the position of Russia and its partners in the [Shanghai Cooperation Organization] and BRICS, that the main goal is not to legalize and not to regulate conflicts in the information space, but to prevent using [information and communication technologies] in the political and military purposes.” Henry Röigas & Tomáš Minárik, 2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law, NATO Cooperative Cyber Def. Ctr. Excellence, <https://ccdcoe.org/incyber-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law/> (last visited May 8,

2020). For competing approaches offered at the United Nations by Russia and the United States for regulating cyberspace, see also Alex Grigsby, *Unpacking the Competing Russian and U.S. Cyberspace Resolutions at the United Nations*, Council Foreign Rel. (Oct. 29, 2018), <https://www.cfr.org/blog/unpacking-competing-russian-and-us-cyberspace-resolutions-united-nations>.

103 Koh, *supra* note 3.

104 It is not clear that states necessarily constrain their cyber activities out of sense of legal obligation, even when applying rules or principles taken from the laws of war. Motives for activities not pursued can be difficult to ascertain, particularly when opportunities may never be known or discussed in public.

105 UN GGE Report, *supra* note 18, ¶ 10 (“Voluntary, non-binding norms of responsible State behaviour can reduce risks to international peace, security and stability. As such, norms do not seek to limit or prohibit action that is otherwise consistent with international law.”) (emphasis added). There is also the practical issue, of course, that few states have the capabilities to defend forward or impose costs in cyberspace due to limited technological resources and skills.

106 For the full list of the 11 “voluntary, non-binding norms of responsible State behaviour” recommended by the 2015 UN GGE, see *id.* ¶ 13.

107 U.S.-Japan Security Treaty, *supra* note 7, art. III.

108 Similarly, Japan’s constitutional and legislative constraints on individual and collective self-defense may prove largely irrelevant in the context of “sub-use-of-force” cyber defenses. This topic is discussed in Parts II and III of this paper.

109 For example, because the Japanese Constitution and the U.S.-Japan Security Treaty are oriented heavily towards preventing the use of force against allies, much of the legal discourse about U.S.-Japan collective self-defense following the 2014 Cabinet reinterpretation has naturally focused on the limits of U.S.-Japan

cooperation in the event of an armed attack (e.g., the geographic boundaries for mutual defense). But what of incidents not rising to the level of armed attack? And what of the reality that cyber operations do not normally involve the use of force or produce effects equivalent to those historically associated with force? Should the U.S. and Japanese governments refuse to defend through cyberspace because certain experts have asserted that altering code could violate international law?

110 Michael J. Adams, *Jus Extra Bellum: Reconstructing the Ordinary, Realistic Conditions of Peace*, 5 Harv. Nat'l Sec. J. 377, 402 (2014) (emphasis added).

111 "[S]tates conduct most national security activities as a matter of sovereign right. Below the threshold of armed conflict, states gather intelligence, conduct activities to improve partner nation security capacity, create cyberspace effects, influence foreign populations, and even detain suspected terrorists abroad without necessarily violating international law. These actions, which can occur outside of the responsible state's borders and may produce effects across boundaries, rarely trigger *jus ad bellum* or *jus in bello* analysis when conducted away from hot battlefields. International humanitarian law is simply not applicable to a wide range of transnational security activities, including military activities." *Id.* at 405. Although not yet widely recognized as a category of legal archetype, *jus extra bellum* presents the appropriate descriptive framework for considering cyber operations conducted outside of armed conflict and below the use of force. Labeled broadly as "the state's right outside of war," *jus extra bellum* was designed to close the enormous gap in international and national security-focused legal architectures, which tend to steer too frequently towards *jus ad bellum* or *jus in bello*, or get stuck in limited categories such as international criminal or human rights law. Instead, *jus extra bellum* helps to frame facts very much at hand in cyberspace, where competition among states is rampant and states resort to cyber operations to protect their national and collective interests.

112 Ney, *supra* note 3. The U.N. Charter and the law of state responsibility are discussed under the ensuing Part II(B)(1) titled "Generally Settled." Application of the laws of war to cyberspace is reviewed under the Part II(B)(2) "Unresolved Questions" because of lingering questions about what constitutes the use of force and armed attack and recent objections raised by a small number of states—some of which are very prominent players in cyberspace—to how *jus in bello* might be applied in the cyber domain.

113 UN GGE Report, *supra* note 18, ¶ 25.

114 Gov't of Japan, Cybersecurity Strategy, *supra* note 2, at 39 ("Existing international law, including the Charter of the United Nations, applies to cyberspace.").

115 U.N. Charter art. 2(4); see also UN GGE Report, *supra* note 18. The U.S. government and other states have noted that "there are exceptions to this rule," including "in the cyber context just as in any other context." Ney, *supra* note 4. Use of force and armed attack are also addressed in Part II(B)(2), as the general obligation of Article 2(4) has been accepted, but states have not agreed to a common understanding of what constitutes "use of force" in cyberspace, or "armed attack" under Article 51.

116 Tallinn Manual 2.0, *supra* note 86, at 84 (stating further that "States bear 'responsibility' for their internationally wrongful acts pursuant to the law of State responsibility") (citing Int'l Law Comm'n [ILC], *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, art. 1, U.N. Doc. A/56/10 (Oct. 24, 2001), and referencing U.N. Secretary-General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, ¶ 23, U.N. Doc. A/68/98 (June 24, 2013); UN GGE Report, *supra* note 19, ¶ 28(f)).

117 See Julian Simcock, Deputy Legal Adviser, U.S. Mission to the U.N., Remarks at a U.N. General Assembly Meeting of the Sixth Committee on Agenda Item 75: Responsibility of States for Internationally Wrongful Acts

(Oct. 14, 2019), available at <https://usun.ushra.gov/remarks-at-a-un-general-assembly-meeting-of-the-sixth-committee-on-agenda-item-75-responsibility-of-states-for-internationally-wrongful-acts/>.

118 Ney, *supra* note 3 (“Particularly relevant for military operations [is] . . . the law of State responsibility.”); Takeshi Akahori, Ambassador in Charge of Cyber Pol’y, Deputy Assistant Minister, Foreign Pol’y Bureau, Ministry of Foreign Aff. Japan, Statement at the Open Ended Working Group on Information and Communications (Sept. 9, 2019) (“Who could object that internationally wrongful acts by States are governed by international law on State responsibility?”).

119 See Ann Väljataga, *Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly*, NATO Cooperative Cyber Def. Ctr. Excellence, <https://ccdcoe.org/incyber-articles/back-to-square-one-the-fifth-un-gge-fails-to-submit-a-conclusive-report-at-the-un-general-assembly/> (last visited Apr. 13, 2020).

120 *Id.*

121 Michael Schmitt & Liis Vihul, *International Cyber Law Politicized: The UN GGE’s Failure to Advance Cyber Norms*, Just Security (June 30, 2017), <https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/>.

122 See *id.*

123 See Väljataga, *supra* note 119.

124 Miguel Rodríguez, Rep. of Cuba, Declaration at the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (June 23, 2017), available at <https://www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf>.

125 Schmitt & Vihul, *supra* note 121.

126 Tallinn Manual 2.0, *supra* note 86, at 375 (“A condition precedent to the application of the law of armed conflict is the existence of an armed conflict.”).

127 He thereby implicitly notes that each of the two bodies of law has application in at least some cyber contexts. “The law of war has been categorized into *jus ad bellum* (law concerning the resort to force) and *jus in bello* (law concerning conduct during war).” Dep’t of Def., Law of War Manual 39 (2015), available at <https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190>.

128 Tallinn Manual 2.0, *supra* note 86, at 375 (“As with other operations, the law of armed conflict applies to cyber operations undertaken in the context of an armed conflict. Despite the novelty of cyber operations and the absence of specific rules within the law of armed conflict explicitly dealing with them, the International Group of Experts was unanimous in finding that the law of armed conflict applies to such activities during both international and non-international armed conflicts.”).

129 Ney, *supra* note 3.

130 Tallinn Manual 2.0, *supra* note 86, at 11.

131 The Dutch view is similar in substance to conclusions presented in Tallinn 2.0. See *id.* at 3–11.

132 There are three components to the broader U.S. government view of sovereignty. First, the U.S. government takes the position that “[a]ctivities in cyberspace must take into account the sovereignty of other States, including outside the context of armed conflict.” Koh, *supra* note 4. Second, the Department of Defense has offered that sovereignty is a guiding principle. Ney, *supra* note 4 (“As a threshold matter, in analyzing proposed cyber operations, DoD lawyers take into account the principle of State sovereignty.”). It is not clear whether this position is limited currently to the Defense Department or whether the Executive branch may have embraced this stance as its uniform view. See also Egan, *supra* note 4 (referring to the “principle of State sovereignty”). Third, there are aspects of how sovereignty is to be applied in the cyber context that are unresolved. Ney, *supra* note 4

("States have sovereignty over the information and communications technology infrastructure within their territory. The implications of sovereignty for cyberspace are complex, and we continue to study this issue and how State practice evolves in this area."); see also Gary P. Corn & Robert Taylor, *Sovereignty in the Age of Cyber*, 111 Am. J. Int'l L. Unbound 207, 208–11 (2017).

133 Wright, *supra* note 91 ("Some have sought to argue for the existence of a cyber specific rule of a 'violation of territorial sovereignty' in relation to interference in the computer networks of another state without its consent. Sovereignty is of course fundamental to the international rules-based system. But I am not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention. The UK Government's position is therefore that there is no such rule as a matter of current international law.").

134 See Major Michael Kolton, *Interpreting China's Pursuit of Cyber Sovereignty and its Views on Cyber Deterrence*, 2 Cyber Def. Rev. 119, 120 (2017) (concluding that China's version of sovereignty involves a unification of Chinese cyber activities, a "new international code of conduct for cyberspace . . . in which the principle of sovereignty enshrined in the UN Charter extends to cyberspace," and avoiding the internet's "latent power to destabilize social and political order").

135 See Letter from the Minister of Foreign Aff. to the President of the H.R. on the International Legal Order in Cyberspace, at app. (July 5, 2019), available at <https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace>. The French Ministère des Armées also takes the position that sovereignty is a rule of international law applicable to cyberspace. See Ministère des Armées, République Française [Ministry of Armed Forces, France], *Droit International Appliqué aux Opérations dans le Cyberspace* [International

Law Applicable to Operations in Cyber-space] 6–7 (2019), available at <https://www.justsecurity.org/wp-content/uploads/2019/09/droit-internat-applique-aux-operacions-cyberspace-france.pdf>.

136 See Akahori, *supra* note 118. To date, the Japanese government's statements and strategy documents that touch on sovereignty seem designed to underscore the critical importance of protecting Japanese interests related to cyberspace and impacted by operations, while also making clear that Japan does not support more authoritarian, content-controlling approaches taken by China, Russia, and certain other governments.

137 Tallinn Manual 2.0, *supra* note 86, at 13.

138 Ney, *supra* note 4 ("States have sovereignty over the information and communications technology infrastructure within their territory.").

139 Tallinn Manual 2.0, *supra* note 86, at 16–17.

140 It may be the case that Rule 4 is actually more restrictive than what international law permits.

141 But see Corn, *supra* note 81 (explaining that a Chatham House report "adopts the same flawed syllogism used in the Tallinn Manual 2.0 that rests on the erroneous premise that international law contains a blanket trespass rule against states sending their agents into the territory of another state without consent" and emphasizing "[o]verwhelming state practice, most notably in the context of espionage, says otherwise; a point that neither the report nor the Tallinn Manual 2.0 account for adequately"). Another scholar has offered that Japan does not face the same collective self-defense restrictions that it normally would in areas with no sovereignty. "The primary operating domains of Japan's collective self-defense of the United States could thus be at the high seas, and depending on future circumstances, in cyberspace and in outer space." Masahiro Kurosaki, *Legal Frameworks on Japan's Self-Defense with the United States*, in *Strengthening the U.S.-Ja-*

pan Alliance: Pathways for Bridging Law and Policy 36 (Nobuhisa Ishizuka, Masahiro Kurosaki & Matthew Waxman eds., 2020).

142 Intelligence collection and establishing placement and access to facilitate future operations are distinct concepts. However, for the purposes of this paper, the author accepts that preparatory measures that would be conducted through cyberspace for each, in most instances, would be unlikely to cause more than *de minimis* effects. This topic could be explored in more detail and that basic understanding might be contested, but research is beyond the scope of this paper.

143 As would be the United Kingdom's view, where the real question would be one of intervention and coercion—two conditions that would not normally apply to cyber intelligence collection. The French position might even be more challenging for intelligence collection than Tallinn 2.0's positions on sovereignty. "France goes even further than the proponents of the sovereignty-as-a-rule-approach. The Tallinn Manual 2.0, for instance, argues that a violation of State sovereignty occurs when remote cyber operations manifest themselves on a State's territory either through physical damage, loss of functionality (but only in some cases) or the interference with or usurpation of inherently governmental functions. The Manual's experts could not agree on whether a cyber operation which affects only data, but does not lead to physical effects or loss of functionality, also violates the target State's sovereignty. However, this appears to be exactly the position France takes." Przemysław Roguski, *France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I*, Just Security (Sept. 24, 2019), <http://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peace-time-cyber-operations-part-i/>.

144 Ney, *supra* note 3 ("[M]ost countries, including the United States, have domestic laws against espionage, but international law, in our view, does not prohibit espionage *per se* even when it involves some degree of physical or virtual intrusion into foreign

territory.").

145 The author has not been able to identify any other domestic Japanese law bearing directly on these issues. Outside of Article 9's war-renouncing clause and the constitutional considerations already discussed, the closest apparent constitutional limitation, which would not seem to apply to cyber threats emanating from outside of Japan, would be the domestic prohibition against violating the secrecy of communications. See Nihonkoku Kenpō [Kenpō] [Constitution], art. 21, ¶ 2 (Japan) ("[N]or shall the secrecy of any means of communication be violated."). The Act on Prohibition of Unauthorized Computer Access is intended to "prevent computer-related crimes committed via telecommunications links and maintain telecommunications-related order as means of access control features by prohibiting acts of unauthorized computer access." Fusei akusesu kōi no kinshi-tō ni kansuru hōritsu [Act on Prohibition of Unauthorized Computer Access], Law No. 128 of 1999, art. 1 (Japan). However, this too seems generally inapplicable to the matters under consideration, as does the Basic Act on Cybersecurity, Law No. 104 of 2014 (providing a broad cybersecurity framework for Japan but not bearing on the sovereignty question).

146 Tallinn Manual 2.0, *supra* note 86, at 330.

147 *Id.* at 339.

148 As discussed, there is strong consensus that the U.N. Charter, and particularly arts. 2(4) and 51, applies to cyber operations. But exactly how it does so is unsettled. What is clear is that the United States and Japan are obligated "individually and in cooperation with each other, by means of continuous and effective self-help and mutual aid [to] maintain and develop, subject to their constitutional provisions, their capacities to resist armed attack." U.S.-Japan Security Treaty, *supra* note 7, art. III.

149 See Ministère des Armées, *supra* note 135. It is unclear whether the French Ministère des Armées view represents the official position of the French Government or whether this stance has only been endorsed by the Ministry of Defense. See Corn, *supra* note 81 (“[D]espite numerous assertions to the contrary, the French document does not claim to be the official position of the French government.”); see also Michael Schmitt, *France’s Major Statement on International Law and Cyber: An Assessment*, Just Security (Sept. 16, 2019), <https://www.justsecurity.org/66194/frances-major-statement-on-international-law-and-cyber-an-assessment/>. Throughout this paper, the author refers to the positions articulated by France, referring in each instance to those viewpoints offered by the French Ministère des Armées.

150 Koh, *supra* note 3.

151 *Id.*; but see Michael J. Adams & Megan Reiss, *How Should International Law Treat Cyberattacks like WannaCry?*, Lawfare (Dec. 22, 2017), <https://www.lawfareblog.com/how-should-international-law-treat-cyber-attacks-wannacry> (“We have repeatedly witnessed confusion among American politicians and policymakers regarding what legal thresholds are applicable to cyberattacks, confusion that does not exist when discussing the average kinetic attack. . . . [O]ur leading concern is that U.S. elected officials and their appointees sometimes appear ill-informed about, or unencumbered by, the use of force and armed attack thresholds established in Articles 2(4) and 51 of the U.N. Charter, respectively. There is such dissatisfaction with international law in this area—its constraints and uncertainty being foremost among the complaints—that leading political authorities tend to discount the utility of international law in favor of political discourse centered on even looser concepts.”).

152 Ney, *supra* note 3.

153 *Id.*

154 Wright, *supra* note 91. The UK Attorney General also provided examples of cyber armed attack as “interfer[ence] with the

operation of one of our nuclear reactors, resulting in widespread loss of life” and “us[ing] a hostile cyber operation to disable air traffic control systems which results in . . . lethal effects.” *Id.* The 2018 United Kingdom speech outlining this standard offers a similar approach and examples as to what Koh offered for the United States in 2012.

155 Letter from the Minister of Foreign Aff., *supra* note 136, app. An example presented of a possible (“cannot be ruled out”) use of force presented by the Netherlands that might not qualify as a use of force if using the U.S. approach is a “cyber operation with a very serious financial or economic impact.”

156 Przemyslaw Roguski, *France’s Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part II*, Just Security (Sept. 24, 2019), <http://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyber-operations-part-ii/>. Examples given include “penetrating military systems in order to attack French defensive capabilities or financing and even training individuals to carry out cyberattacks against France.”

157 *Id.*

158 They include “substantial loss of life, considerable physical or economic damage, significant impact on critical infrastructure, in particular when resulting in paralysis of large parts of the country’s activities, technological or ecological catastroph[es] or a significant amount of victims.” *Id.*

159 *Id.*

160 See Craig Martin, *Japan’s Definition of Armed Attack and “Bloody Nose” Strikes Against North Korea*, Just Security (Feb. 1, 2018), <https://www.justsecurity.org/51678/japans-definition-armed-attack-bloody-nose-strikes-north-korea/>. However, the U.S. government holds a different understanding of international law in this area.

161 See *Military and Paramilitary Activities in and Against Nicaragua* (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ¶¶ 195, 199

(June 27). First, there must be a request for assistance because customary international law does not permit, according to the Court, the exercise of collective self-defense “in the absence of a request by the State which regards itself as the victim of an armed attack.” *Id.* ¶ 199. Second, the State for whose benefit the right of collective self-defense is exercised must declare itself to be the victim of an armed attack, as “there is no rule in customary international law permitting another State to exercise the right of collective self-defense on the basis of its own assessment of the situation.” *Id.* ¶ 195. See also Aurel Sari & Hitoshi Nasu, *Collective Self-Defense and the “Bloody Nose Strategy”: Does it Take Two to Tango?*, Just Security (Jan. 26, 2018), <https://www.justsecurity.org/51435/collective-self-defense-bloody-nose-strategy-tango/>.

162 Junichiro Koizumi, Prime Minister of Japan, Reply to the Questions Concerning an Armed Attack Submitted by Seiichi Kaneda (May 24, 2003). Japanese domestic law provides the government with bases to respond with force to three categories of incidents: armed attack, anticipated armed attack, and threats to Japan’s survival. See Gov’t of Japan, Japan’s Legislation for Peace and Security, *supra* note 27.

163 Premeditation analysis might involve the foreseeability of the consequences of cyber operations. “Of course, foreseeability is a notoriously malleable and indeterminate legal requirement, since it is extremely difficult to specify in advance exactly how long a causal chain must stretch before it is no longer appropriate to find liability—particularly in the area of cyber-attacks.” Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue & Julia Spiegel, *The Law of Cyber-Attack*, 100 Calif. L. Rev. 817, 848 (2012).

164 Martin, *supra* note 160.

165 Joint Statement, U.S.-Japan Sec. Consultative Comm., *supra* note 36.

166 While most other states believe that a “State can use force in self-defense only in response to an ‘armed attack,’ which is importantly defined as the gravest forms of force in scale and effects,” the United States holds to the position that a “State can use force in self-defense in response to any amount of force by another State.” Ryan Goodman, *Cyber Operations and the U.S. Definition of “Armed Attack”*, Just Security (Mar. 8, 2018), <https://www.justsecurity.org/53495/cyber-operations-u-s-definition-armed-attack/>. This is especially important in the context of defending forward against a malicious cyber activity that might arguably be viewed as a use of force but which falls short of any reasonable interpretation of armed attack.

167 Tallinn Manual 2.0, *supra* note 86, at 312 (“This Rule prohibits coercive intervention, including by cyber means, by one State into the internal or external affairs of another. It is based on the international law principle of sovereignty, specifically that aspect of the principle that provides for the sovereign equality of States.”).

168 “Expressions of *opinion juris* regarding the existence of the principle of non-intervention in customary international law are numerous and not difficult to find.” *Nicaragua*, *supra* note 161, ¶ 202. For a list of “non-exhaustive views on how international law applies to the use of ICTs by States”, see UN GGE Report, *supra* note 18 (“In their use of ICTs, States must observe, among other principles of international law, State sovereignty, sovereign equality, the settlement of disputes by peaceful means and *non-intervention in the internal affairs of other States*.”) (emphasis added).

169 Harriet Moynihan, Chatham House, *The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention 2* (2019), available at <https://www.chathamhouse.org/publication/application-in-international-law-state-cyberattacks-sovereignty-and-non-intervention> (“In practice, activities that contravene the non-intervention principle and activities that violate sovereignty will often overlap.”).

170 See Comment, *The Use of Nonviolent Coercion: A Study in Legality under Article 2(4) of the Charter of the United Nations*, 122 U. Pa. L. Rev. 983, 987–88 (1974).

171 Ney, *supra* note 3 (“[T]he international law prohibition on coercively intervening in the core functions of another State (such as the choice of political, economic, or cultural system) applies to State conduct in cyberspace. . . . There is no international consensus among States on the precise scope or reach of the non-intervention principle, even outside the context of cyber operations.”).

172 *Nicaragua*, *supra* note 161, ¶ 205 (“Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones . . . the element of coercion . . . defines, and indeed forms the very essence of, prohibited intervention.”).

173 Tallinn Manual 2.0, *supra* note 86, at 318.

174 Moynihan, *supra* note 169, at 27.

175 Tallinn Manual 2.0, *supra* note 86, at 319 (citing Declaration on Friendly Relations, Principle 3, and Declaration on the Inadmissibility of Intervention and Interference, Preamble).

176 *Id.* at 320–24.

177 *Nicaragua*, *supra* note 161, ¶ 205.

178 Letter from the Minister of Foreign Aff., *supra* note 135, app.; see generally Moynihan, *supra* note 169.

179 Schmitt, *France’s Major Statement on International Law and Cyber: An Assessment*, *supra* note 150; Ney, *supra* note 3 (“For example, ‘a cyber operation by a State that interferes with another country’s ability to hold an election’ or that tampers with ‘another country’s election results would be a clear violation of the rule of non-intervention.’ . . . Other States have indicated that they would view operations that disrupt the fundamental operation of a legislative body or that would destabilize their financial system as prohibited interventions.”).

180 Ney, *supra* note 3 (“Because States take different views on this question, DoD lawyers examining any proposed cyber operations must tread carefully, even if only a few States have taken the position publicly that the proposed activities would amount to a prohibited intervention.”). This is also an area of law in which Japan may be interested in developments under NATO and how states’ differing views shape collective security measures. NATO continues to put significant resources towards studying Russia’s misinformation campaigns and implications for the organization’s security obligations, particularly in the cyber context. Japan’s participation in NATO’s Cooperative Cyber Defense Centre of Excellence should provide important insights about partnering in cyber operations, states’ perspectives on the non-intervention principle, and other important issues in international law. See *Japan Joins NATO’s Cooperative Cyber Defense Centre of Excellence*, CISOMAG (Dec. 4, 2019), <https://www.cisomag.com/japan-joins-natos-cooperative-cyber-defense-centre-of-excellence/>.

181 Tallinn Manual 2.0, *supra* note 86, at 111.

182 Kersti Kaljulaid, President, Republic of Est., Remarks by President of the Republic at the opening of CyCon 2019 (May 5, 2019), available at <https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html> [hereinafter Kaljulaid Remarks].

183 Tallinn Manual 2.0, *supra* note 86, at 111; Wright, *supra* note 92 (“Put simply, if a hostile state breaches international law as a result of its coercive actions against the target state’s sovereign freedoms, then the victim state can take action to compel that hostile state to stop.”).

184 Tallinn Manual 2.0, *supra* note 86, at 111–34.

185 *Id.* at 130.

186 See Sari & Nasu, *supra* note 161.

187 Ney, *supra* note 3.

188 Wright, *supra* note 91.

189 Nakasone, *supra* note 6, at 4.

190 Although not providing much in the way of publicly released details, the Guidelines for U.S.-Japan Defense Cooperation make clear that the allies will partner even in the absence of armed attack. Dep't of Def., Guidelines for U.S.-Japan Defense Cooperation, *supra* note 32, art. IV ("In this increasingly complex security environment, the two governments will take measures to ensure Japan's peace and security in all phases, seamlessly, from peacetime to contingencies, including situations when an armed attack against Japan is not involved."). It would be expected that defensive measures are designed to be necessary and proportional to the threats encountered, whether defending forward or responding to cyber operations that amount to armed attack.

191 This is in furtherance of the United States' defend forward strategic concepts and Japan's stated goals to "defend the state (defense capabilities), deter cyberattacks (deterrence capabilities), and be aware of the situation in cyberspace (situational awareness capabilities)." Gov't of Japan, Cybersecurity Strategy, *supra* note 2, at 37.

192 The United States' view on the absence of a *per se* international law prohibition against intelligence collection is not universally accepted by states. But recall that *jus extra bellum*—the rights of states outside of armed conflict—recognizes that "national security activities outside of armed conflict . . . occur within a generally permissive international legal regime and are shaped by domestic legal authorities and obligations." Adams, *Jus Extra Bellum*, *supra* note 110, at 382. This framing offers as permissible examples "intelligence sharing and collection; influence operations that do not intrude on sovereignty, territory, or political independence as a matter of law, but inform and shape the perspectives of foreign populations; cyber defense and other cyber activities not rising to the level of a use of force . . . [and] other national security actions undertaken pursuant to a UN Security Council

resolution or other international authorization." *Id.*; see also Act for the Establishment of the Ministry of Defense, Law No. 164 of 1954, art. 4(18) (Japan) (providing broad authority for the Japanese Self-Defense Forces to conduct survey and research).

193 Gov't of Japan, National Defense Program Guidelines, *supra* note 58, at 12 ("In space, cyber and electromagnetic domains, to prevent any actions that impede its activities, SDF will conduct on a steady-state basis persistent monitoring as well as collection and analysis of relevant information. In case of such event, SDF will promptly identify incidents and take such measures as damage limitation and recovery."). The security tenet reflected in Japan's approach mirrors the American warning that "if we find ourselves defending inside our own networks, we have lost the initiative and the advantage." Nakasone, *supra* note 6, at 10.

194 Dep't of Def., Guidelines for U.S.-Japan Defense Cooperation, *supra* note 31, art. IV.C.2.b.v ("The United States Armed Forces and the Self-Defense Forces will conduct bilateral operations across domains to repel an armed attack against Japan and to deter further attacks. These operations will be designed to achieve effects across multiple domains simultaneously.").

195 *Id.*, art. VI.B ("To help ensure the safe and stable use of cyberspace, the two governments will share information on threats and vulnerabilities in cyberspace in a timely and routine manner, as appropriate.").

196 *Id.*, art. IV ("Therefore, the two governments will utilize the whole-of-government Alliance Coordination Mechanism, as appropriate, to: assess the situation; share information; and develop ways to implement the appropriate Alliance response, including flexible deterrent options, as well as actions aimed at de-escalation.").

197 "In the event of cyber incidents against Japan, including those against critical infrastructure and services utilized by the United States Armed Forces in Japan and the Self-Defense Forces, Japan will have primary

responsibility to respond, and based on close bilateral coordination, the United States will provide appropriate support to Japan. The two governments also will share relevant information expeditiously and appropriately. In the event of serious cyber incidents that affect the security of Japan, including those that take place when Japan is under an armed attack, the two governments will consult closely and take appropriate cooperative actions to respond." *Id.*, art. VI.B.

198 Both states have committed to complying with international law, as well as their respective domestic legal frameworks. "All actions and activities undertaken by the United States and Japan under the Guidelines will be consistent with international law, including the Charter of the United Nations and its provisions regarding the peaceful settlement of disputes and sovereign equality of states." *Id.*, art. II.B.

199 Traditional considerations for Japan when analyzing armed attack.

200 Koh, *supra* note 3 ("Cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force. In assessing whether an event constituted a use of force in or through cyberspace, we must evaluate factors: including the context of the event, the actor perpetrating the action (recognizing challenging issues of attribution in cyberspace), the target and location, effects and intent, among other possible issues. Commonly cited examples of cyber activity that would constitute a use of force include, for example: (1) operations that trigger a nuclear plant meltdown; (2) operations that open a dam above a populated area causing destruction; or (3) operations that disable air traffic control resulting in airplane crashes.").

201 See Wright, *supra* note 91.

202 This would seem to be an unlikely outcome in the face of the impact that would be felt in Japan.

203 For the purposes of this scenario, the author focuses on attribution of the cyber operations to State A as a precondition for the defensive actions of the Japanese government. Of course, attribution can support many forms of response (e.g., diplomatic or law enforcement) and each action can have its own threshold for attribution (e.g., no formal standard for *démarche*, or criminal standard for indictment). But since this scenario is focused on armed attack, the author focuses here on attribution in that context for the purpose of exercising self-defense.

204 See Tallinn Manual 2.0, *supra* note 86, at 115–16. State responsibility is another issue that could be examined further if the facts were presented differently such that State B was acting through a non-government proxy. See Egan, *supra* note 4 ("[C]yber operations conducted by non-State actors are attributable to a State under the law of state responsibility when such actors engage in operations pursuant to the State's instructions or under the State's direction or control, or when the State later acknowledges and adopts the operations as its own. Thus, as a legal matter, States cannot escape responsibility for internationally wrongful cyber acts by perpetrating them through proxies. When there is information—whether obtained through technical means or all-source intelligence—that permits a cyber act engaged in by a non-State actor to be attributed legally to a State under one of the standards set forth in the law of state responsibility, the victim State has all of the rights and remedies against the responsible State allowed under international law.").

205 Egan, *supra* note 3 (addressing the law of state responsibility but speaking more generally about attribution in cyberspace, noting also that "despite the suggestion by some States to the contrary, there is no international legal obligation to reveal evidence on which attribution is based prior to taking appropriate action. There may, of course, be political pressure to do so, and States may choose to reveal such evidence to convince other States to join them in condemnation, for example. But that is a policy choice—it is not compelled

by international law”).

206 But see the discussion of the plea of necessity under Scenario 3 and the absence of a requirement to attribute unlawful conduct to a state when relying on necessity as legal justification.

207 See Kurosaki, *Japan’s Evolving Position*, *supra* note 57.

208 Dep’t of Def., Guidelines for U.S.-Japan Defense Cooperation, *supra* note 31, art. VI.B.

209 For discussion of self-defense considerations specific to the Japanese government and the U.S.-Japan Alliance, see generally Kurosaki, *supra* note 141; Julian Ku, *How the Law of Collective Self-Defense Undermines the Peace and Security of the Taiwan Strait*, in Strengthening the U.S.-Japan Alliance, *supra* note 141.

210 Egan, *supra* note 3 (“In certain circumstances, a State may take action that would otherwise violate international law in response to malicious cyber activity. One example is the use of force in self-defense in response to an actual or imminent armed attack.”).

211 See discussion in Section II.B.2.a. and II.B.2.c.

212 If armed conflict ensued, *jus in bello* would apply to operations conducted both in and out of cyberspace.

213 Note that these operations do not target Japanese elections. State B targets Japanese infrastructure and media in preparation for follow-on operations directed against U.S. elections, selecting these particular Japanese targets as representative of those that might be attacked via cyber means at a later date in the United States.

214 Recall that the Japanese government takes the position that “cyberattack carried out as part of an armed attack” and “cyber-only attack” could both themselves rise to the level of armed attack.

215 Egan, *supra* note 3 (“Not all cyber operations, however, rise to the level of an ‘attack’ as a legal matter under the law of armed conflict. When determining whether a cyber

activity constitutes an “attack” for purposes of the law of armed conflict, States should consider, among other things, whether a cyber activity results in kinetic or non-kinetic effects, and the nature and scope of those effects, as well as the nature of the connection, if any, between the cyber activity and the particular armed conflict in question.”). Note also that the U.S. government does not draw a meaningful distinction between armed attack under Article 51 and use of force under Article 2(4); therefore, U.S. government officials’ remarks about cyber operations have referred to the standards for armed attack and use of force in a largely interchangeable manner. Dep’t of Def., Law of War Manual, *supra* note 127, at 1017 (“The United States has long taken the position that the inherent right of self-defense potentially applies against any illegal use of force. Thus, any cyber operation that constitutes an illegal use of force against a State potentially gives rise to a right to take necessary and proportionate action in self-defense.”).

216 Koh, *supra* note 3 (“Cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force. In assessing whether an event constituted a use of force in or through cyberspace, we must evaluate factors: including the context of the event, the actor perpetrating the action (recognizing challenging issues of attribution in cyberspace), the target and location, effects and intent, among other possible issues. . . . Only a moment’s reflection makes you realize that this is common sense: if the physical consequences of a cyber attack work the kind of physical damage that dropping a bomb or firing a missile would, that cyber attack should equally be considered a use of force.”); Ney, *supra* note 4 (“In assessing whether a particular cyber operation—conducted by or against the United States—constitutes a use of force, DoD lawyers consider whether the operation causes physical injury or damage that would be considered a use of force if caused solely by traditional means like a missile or a mine.”).

217 Ank Bijleveld, Minister of Def., Neth., Keynote address marking the first anniversary of the Tallinn Manual 2.0 (June 21, 2018), available at <https://english.defensie.nl/downloads/speeches/2018/06/21/keynote-address-by-the-minister-of-defence-ms.-ank-bijleveld-marking-the-first-anniversary-of-the-tallinn-manual-2.0-on-the-20th-of-june-2018> [hereinafter Bijleveld Keynote].

218 Response options could include a wide range of cyber and non-cyber measures, up to and including necessary and proportional use of force.

219 See David E. Sanger, *U.S. Decides to Retaliate Against China's Hacking*, N.Y. Times (July 31, 2015), https://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html?_r=0.

220 See generally *Nicaragua*, *supra* note 161. Meanwhile, “the Japanese government has consistently defined an ‘armed attack’ [under Article 51] as meaning ‘an organized, planned use of force against a state.’ As the term ‘planned’ suggests, the Japanese government views hostile intent of an opponent as the most crucial element in determining the occurrence of an armed attack, not the criteria of scale and effects applied by the International Court of Justice in its *Nicaragua* decision (though scale and effects may serve as evidence of intent as was implied by its 2003 *Oil Platform* decision—‘specific intention of harming’ for the grave form of the use of force).” Kurosaki, *supra* note 141, at 31.

221 See Tallinn Manual 2.0, *supra* note 86, at 330–36 (embracing the “scale and effects” test of the *Nicaragua* judgment, arguing that “scale and effects is a shorthand term that captures the quantitative and qualitative factors to be analyzed in determining whether a cyber operation amounts to a use of force,” and proposing the following factors “that States are likely to consider and place great weight on . . . when deciding whether to characterize any operation, including a cyber operation, as a use of force”: severity, immediacy, directness, invasiveness, measurability of effects, military character, state involve-

ment, and presumptive legality). While the Manual argues that “non-destructive cyber psychological operations intended solely to undermine confidence in a government” would not “qualify as uses of force,” Scenario 2 presents scale and effects—and, among Tallinn 2.0 factors, at least severity, immediacy, directness, invasiveness, and state involvement—that may weigh in favor of finding that Article 2(4) was violated. Tallinn Manual 2.0, *supra* note 86, at 331.

222 See Bijleveld Keynote, *supra* note 218; Ministère des Armées, *supra* note 136; see also Koh, *supra* note 4 (“In assessing whether an event constituted a use of force in or through cyberspace, we must evaluate factors: including the context of the event, the actor perpetrating the action (recognizing challenging issues of attribution in cyberspace), the target and location, effects and intent, among other possible issues.”). The factors that Tallinn 2.0 proposes for states to consider in assessing cyber operations under U.N. Charter Article 2(4) could also lead to the conclusion that Scenario 2 rises to the level of a use of force.

223 Japan also could explain that causing even “minimal” physical injury or damage might arguably be viewed as use of force, but the additional, significant effects caused by the cyber operations present an even stronger case that this is a violation of Article 2(4).

224 As with Scenario 1, these actions would comport with the Japanese government’s understanding of its obligations under the U.N. Charter as well as bilateral commitments under the U.S.-Japan Security Treaty. Consultation with the U.S. government would be consistent with the Guidelines for U.S.-Japan Cooperation based upon “serious cyber incidents that affect the security of Japan.” Dep’t of Def., Guidelines for U.S.-Japan Defense Cooperation, *supra* note 32, art. VI.B. The U.S. government would also likely make its own determination as to whether Article 2(4) was violated.

225 Dep’t of Def., Law of War Manual, *supra* note 127, at 1017 (“The United States has

long taken the position that the inherent right of self-defense potentially applies against any illegal use of force. Thus, any cyber operation that constitutes an illegal use of force against a State potentially gives rise to a right to take necessary and proportionate action in self-defense.”).

226 Other options for responses include “lesser means” such as retorsion or diplomacy.

227 Ney, *supra* note 3 (“[T]he international law prohibition on coercively intervening in the core functions of another State (such as the choice of political, economic, or cultural system) applies to State conduct in cyberspace.”); Tallinn Manual 2.0, *supra* note 86, at 84 (“A State bears international responsibility for a cyber-related act that is attributable to the State and that constitutes a breach of an international legal obligation.”); *id.* at 80 (“The International Group of Experts agreed that the customary international law of State responsibility undeniably extends to cyber activities.”); see also *id.* at 157 (“An international organisation bears international legal responsibility for a cyber operation that breaches an international legal obligation and is attributable to the organization.”); Wright, *supra* note 91 (“The international law rules on the attribution of conduct to a state are clear, set out in the International Law Commissions Articles on State Responsibility, and require a state to bear responsibility in international law for its internationally wrongful acts, and also for the acts of individuals acting under its instruction, direction or control. These principles must be adapted and applied to a densely technical world of electronic signatures, hard to trace networks and the dark web. They must be applied to situations in which the actions of states are masked, often deliberately, by the involvement of non-state actors. And international law is clear - states cannot escape accountability under the law simply by the involvement of such proxy actors acting under their direction and control.”).

228 Egan, *supra* note 3 (“From a legal perspective, the customary international law of state responsibility supplies the standards for attributing acts, including cyber acts, to States. For example, cyber operations conducted by organs of a State or by persons or entities empowered by domestic law to exercise governmental authority are attributable to that State, if such organs, persons, or entities are acting in that capacity. Additionally, cyber operations conducted by non-State actors are attributable to a State under the law of state responsibility when such actors engage in operations pursuant to the State’s instructions or under the State’s direction or control, or when the State later acknowledges and adopts the operations as its own.”).

229 Tallinn Manual 2.0, *supra* note 86, at 312 (“A State may not intervene, including by cyber means, in the internal or external affairs of another State.”).

230 *Id.*

231 See Tallinn Manual 2.0, *supra* note 86, at 318.

232 Ney, *supra* note 3 (emphasis added).

233 See also *Nicaragua*, *supra* note 161, ¶ 205 (“A prohibited intervention must . . . be one bearing on matters in which each State is permitted, by the principle of sovereignty, to decide freely [such as] choice of a political, economic, social, and cultural system, and the formulation of public policy.”). The U.S. position may also be influenced significantly by geopolitics in light of Russia’s interference in the 2016 U.S. elections and reports of continued efforts by Russia and other states to engage in similar future activities by cyber means.

234 G.A. Res. 2625, Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States (Oct. 24, 1970).

235 Discussion of collective countermeasures follows later in this section.

236 Egan, *supra* note 3 (“[C]ountermeasures taken in response to internationally wrongful cyber activities attributable to a State generally may take the form of cyber-based countermeasures or non-cyber-based countermeasures. That is a decision typically within the discretion of the responding State and will depend on the circumstances.”). It should be emphasized that countermeasures involve the victim state engaging in “otherwise unlawful measures.” *Id.* (emphasis added). Depending on where the Japanese government stands on the sovereignty question, not all counter-cyber operations require justification as a countermeasure. To the extent an action is not prohibited (e.g., a retorsion), there is nothing that prevents taking it in a collective construct.

237 The issue of attribution would, of course, need to be addressed as well. The attribution analysis tracks largely the analysis presented under Scenario 1. As explained by the U.S. government, “[t]he law of state responsibility does not set forth explicit burdens or standards of proof for making a determination about legal attribution.” *Id.*

238 Absent facts that State B’s cyber operations are also impacting the United States (e.g., U.S. forces stationed in Japan).

239 “Among other options for collective response, Estonia is furthering the position that states which are not directly injured may apply countermeasures to support the state directly affected by the malicious cyber operation. The countermeasures applied should follow the principle of proportionality and other principles established within the international customary law. International security and the rules-based international order have long benefitted from collective efforts to stop the violations. We have seen this practice in the form of collective self-defense against armed attacks. For malicious cyber operations, we are starting to see this in collective diplomatic measures I mentioned before. The threats to the security of states increasingly involve unlawful cyber operations. It is therefore important that states may respond collectively to unlawful cyber operations where diplomatic action is insufficient, but no lawful recourse to

use of force exists. Allies matter also in cyberspace.” Kaljulaid Remarks, *supra* note 182.

240 “The United States Armed Forces and the Self-Defense Forces will conduct bilateral operations across domains to repel an armed attack against Japan and to deter further attacks. These operations will be designed to achieve effects across multiple domains simultaneously.” Dep’t of Def., Guidelines for U.S.-Japan Defense Cooperation, *supra* note 31, art. IV.C.2.b.v.

241 “Japan’s collective self-defense is tailored and limited to the defense of the United States, Japan’s only ally. Nevertheless, this would not include a request to assist in anticipatory self-defense against an imminent threat of armed attack. . . . Japan has rejected that doctrine as a matter of international law.” Kurosaki, *supra* note 141, at 11.

242 Ney, *supra* note 3.

243 Egan, *supra* note 3.

244 Wright, *supra* note 91 (“The one area where the UK departs from the excellent work of the International Law Commission on this issue is where the UK is responding to covert cyber intrusion with countermeasures. In such circumstances, we would not agree that we are always legally obliged to give prior notification to the hostile state before taking countermeasures against it. The covertness and secrecy of the countermeasures must of course be considered necessary and proportionate to the original illegality, but we say it could not be right for international law to require a countermeasure to expose highly sensitive capabilities in defending the country in the cyber arena, as in any other arena.”).

245 Ney, *supra* note 3 (“We will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict.”); Dep’t of Def. Cyber Strategy, *supra* note 8, at 1. Scenario 3 would also implicate Section IV.A.4 of Dep’t of Def., Guidelines for U.S.-Japan Defense Cooperation, *supra* note 31 (“The United States Armed Forces and the Self-Defense Forces will provide mutual protection of each other’s

assets, as appropriate, if engaged in activities that contribute to the defense of Japan in a cooperative manner, including during training and exercises.”).

246 Scenario 3 would not implicate the armed attack provisions of the U.S.-Japan Security Treaty. See also CDR Peter Pascucci, *Distinction and Proportionality in Cyber War: Virtual Problems with a Real Solution*, 26 Minn. J. Int’l L. 419, 443 (2017) (“[T]he focus of the definition of a cyber attack, for the purposes of IHL [International Humanitarian Law] and this Article, is whether the effect can reasonably be expected to cause more than de minimis damage to or destruction of objects. Because determination of whether an action constitutes a cyber ‘attack’ is an effects-based determination, an operation targeting data that ‘results in the . . . damage or destruction of physical objects . . . qualifies as an attack.’ However, targeting that results in de minimis damage or no loss of functionality is not an attack and, therefore, all the protections afforded civilian objects subject to an attack by the principles of distinction and proportionality do not apply.”).

247 See generally *Nicaragua*, *supra* note 161, ¶ 103–04.

248 See also the use of force discussion in Part III, Scenario 2.

249 Had the cyber operations proximately caused physical injury, death or severe, invasive, or far-reaching effects, this analysis would not be the same.

250 One might consider a number of international law rules that may have been violated (e.g., the prohibition against harmful interference under the International Telecommunication Union Constitution), thereby implicating the law of state responsibility. For brevity and analytical focus, the author limits his remarks about state responsibility to the application of the principle of non-intervention, consistent with the approach taken under Scenario 2.

251 See *International Status and Navigation of Warships and Military Aircraft*, in 73 Annotated Supplement to the Commander’s Handbook on the Law of Naval Operations 109–10 (A.R. Thomas & James C. Duncan eds., 1997).

252 Sean Watts, *Cyber War: Law and Ethics for Virtual Conflicts*, in *Low-Intensity Cyber Operations and the Principle of Non-Intervention* 256 (Jens David Ohlin et al. eds., 2015) (“Actions merely restricting a state’s choice with respect to a course of action or compelling a course of action may be sufficient to amount to violations of the principle of non-intervention.”).

253 *Nicaragua*, *supra* note 161, ¶ 205.

254 Dep’t of Def., *Guidelines for U.S.-Japan Defense Cooperation*, *supra* note 31, art. VI.B.

255 For example, if the Japanese government did not conclude that State C violated the non-intervention principle but the U.S. government disagreed, the United States might still conduct countermeasures, whether via cyber or other means based on the U.S. government’s own legal conclusion. Egan, *supra* note 4 (“[A] State acts as its own judge of the facts and may make a unilateral determination with respect to attribution of a cyber operation to another State.”).

256 “In Japan’s view, actual harm is not necessary for armed attack to occur as it includes its initiation phase. Take, for example, the time when a ballistic missile directed at Japan is being fueled. There is no need to wait until the attack hits the target.” Kurosaki, *supra* note 141, at 32.

257 The U.S.-Japan Security Consultative Committee prioritized such actions, including allied cooperation in cyberspace, in 2019. See Joint Statement, U.S.-Japan Sec. Consultative Comm., *supra* note 36.

258 Egan, *supra* note 3 (“[I]n exceptional circumstances, a State may be able to avail itself of the plea of necessity, which, subject to certain conditions, might preclude the wrongfulness of an act if the act is the only way for the State to safeguard an essential interest against a grave and imminent peril.”).

259 *Id.* (“As an initial matter, a State can always undertake unfriendly acts that are not inconsistent with any of its international obligations in order to influence the behavior of other States. Such acts—which are known as acts of retorsion—may include, for example, the imposition of sanctions or the declaration that a diplomat is *persona non grata*.”).

260 ILC, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, *supra* note 116, art. 25. According to Article 25:

1. Necessity may not be invoked by a State as a ground for precluding the wrongfulness of an act not in conformity with an international obligation of that State unless the act:

(a) is the only way for the State to safeguard an essential interest against a grave and imminent peril; and

(b) does not seriously impair an essential interest of the State or States towards which the obligation exists, or of the international community as a whole.

2. In any case, necessity may not be invoked by a State as a ground for precluding wrongfulness if:

(a) the international obligation in question excludes the possibility of invoking necessity; or

(b) the State has contributed to the situation of necessity.

261 See Tallinn Manual 2.0, *supra* note 86, at 135.

262 *Id.* Furthermore, “[t]he mere fact that a cyber operation targets an essential interest is insufficient to invoke the plea of necessity. In addition, the potential harm posed to that interest must be ‘graver.’” *Id.* at 136.

263 “This is of exceptional importance in the cyber context because the plea of necessity will lie when individuals or non-State groups such as companies, activist groups, or terrorists, conduct cyber operations that satisfy the standard set forth in this Rule. There is no need to attribute the underlying act to a State. Therefore, in cases where a non-State actor has launched an operation that falls below the armed attack threshold, the plea of necessity may present the sole option for a response that would otherwise be unlawful.” Tallinn Manual 2.0, *supra* note 86, at 137–38.

264 Gov’t of Japan, Cybersecurity Strategy, *supra* note 2, at 41 (emphasis added).



Kazuto Suzuki

Hokkaido University

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

Introduction

Space systems are inseparable from today's socio-economic activities and security. No planes can take off or land without Global Positioning System (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. Disaster response will be much more difficult if we don't have satellite images, and so on. Space systems are vital to human society and the security of mankind.

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 are the eyes, ears and nerve system of today's warfare¹.

As a consequence, if one can degrade or destroy the space capabilities of an enemy, it can potentially cripple the adversary's 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, can be a prime target.

Having established the importance of space-based systems to both modern life and modern combat operations, how can we defend the security of such space systems? Traditionally, military strategists have sought to prevent attacks on vulnerable systems through deterrence, or a mix of hardening and resiliency to convince the adversary their actions will fail to achieve the desired effect at an acceptable cost, plus threats of punishment designed to convince 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. However, such traditional

notions of deterrence do not work well in outer space due to the different physical characteristics of the space environment. Also, it would be difficult to assume that tit-for-tat space deterrence may work because of the asymmetric use of space. In cases where some states depend heavily on space infrastructure but others do not, degrading space capability would have less impact on the latter, so that the latter states may not fear retaliation to their space assets. For example, North Korea may kill U.S. satellites by exploding nuclear devices in outer space, but retaliation by the U.S. against North Korean space assets may have very limited impact since North Korea does not depend on space infrastructure.

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 warfighting, we need to develop a strategy for cross-domain deterrence situated within the context of the U.S.-Japan alliance.² 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, it is the central argument 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.

Vulnerabilities to Unintentional Incidents in Space

Space assets are vulnerable. They are designed to be light in order to reduce 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 travelling very fast (approximately 28,000km per hour), any collision can produce devastating effects. These are delicate machines carrying large numbers of electronic parts which are exposed to radiation, solar flares and electromagnetic pulses. Although they are not stationary, their orbits can be easily detected and predicted, and can therefore be targeted without much difficulty. Because of the physics of the space environment, space-based assets are extremely vulnerable and there are very few ways to improve their resilience other than duplication or reconstruction (both of which are extremely costly and/or time-consuming and neither of which does anything to make the targeted platform any more difficult to attack or capable of surviving an adversary's assault).

Further complicating matters, space assets are vulnerable to unintentional 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 10cm in diameter in orbit (about 3,000 of these were created by a Chinese anti-satellite (ASAT) weapon test in 2007 and approximately 40 by an Indian ASAT test in 2019), and estimated several millions of debris items smaller than 10cm diameter.³ The Combined Space Operations Center (CSpOC) 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 Space Situational Awareness (SSA) mission is an important contribution that the U.S.-Japan alliance can make for not only Japan and the U.S. but for 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 occurring during solar flares can impact the electronic systems onboard satellites; they can also impact 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, the bigger threat to space-based assets comes from intentional, hostile activities directed towards space assets.

Anti-Satellite (ASAT) Attack

Because space assets are highly vulnerable and at the same time 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 U.S. and any allies who may be supporting it, such as Japan. Attacks on space assets can be more appealing to adversaries since these are not as easily visible to terrestrially-based observers as, for example, aerial bombardment or missile attacks on ground targets. In addition, any casualties caused would largely be indirect as a result of systems knocked off-line 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 will be difficult to identify who carried out the attack and how it was executed because it is almost impossible to monitor space assets continuously due to the nature

of the monitoring systems. Satellites travel around the globe in 90 minutes, and 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 U.S. or Japan noticing⁴. While there are mathematical ways to analyze the trajectory of space objects so as to deduce the most likely perpetrators of any given attack, it is nonetheless 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 tests conducted by China in 2007 and by India in 2019 were a good example of countries 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 or India. The 2007 ASAT test was a wake-up call for all spacefaring nations that space assets are vulnerable and can be easy targets if a conflict takes place. India was the one which strongly reacted to this call and demonstrated that it can also destroy Chinese satellites if China attempted to disable Indian satellites. Thus, the 2019 Indian ASAT test was clearly a message to China to deter its activities. These tests also reminded observers that space is a vital domain for national security and that attacks aimed at degrading national space capabilities would significantly erode warfighting 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. As of March 2019 the number of operational Chinese satellites, including both civilian and military satellites, totals just 299 whereas the United States operates more than 900 satellites of all types⁵. So the likelihood of hitting U.S. satellites is higher than Chinese satellites, but the number of satellites that China owns and operates are increasing. India, on the other hand, has tried to minimize creation of debris when it conducted an ASAT test to its own satellite at lower orbit, in order to avoid increasing the risk of space debris to its own satellites, but there are a substantial number of debris remaining in orbit as of today.⁶

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 (UNCOPUOS) adopted "Debris Mitigation Guidelines"⁷ 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"⁸ 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. 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” (PPWT)⁹ as an alternative to the “International Code of Conduct”, China has at a minimum had to deal with international criticism towards its kinetic ASAT test. The lack of internationally agreed rules and norms facilitated India’s launch of its ASAT test in 2019.

India, unlike the case of China’s ASAT, was not heavily criticized by the international community. On the one hand, it was because the United States and many other spacefaring countries believed the Indian ASAT capability might deter Chinese counterspace activities. Although the Indian ASAT test created debris, it was not as serious as the Chinese one in 2007. The international community may have deemed it an acceptable risk, and decided to remain calm. On the other hand, China and Russia have promoted the right of ground-to-space ASAT in order to give them freedom to shoot down satellites, so they cannot blame India for exercising similar legal rights. Whether the Indian ASAT test will change the positions and strategic thinking of China and Russia is unknown, but they certainly have been aware of the risk that other countries might take down their satellites.

Non-kinetic ASAT: Cyber Attack on Space Systems

While the Chinese ASAT test 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 don’t subsequently distinguish between the space assets of the victim or the attacker in later years. Thus, non-kinetic methods are now seen by many observers as likely to be more attractive methods for taking out opponents’ 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 conducted both on satellites (i.e., by taking over control of the satellite), and through satellites (i.e., by taking over the communication network and hacking the satellite network). A number of studies have been conducted to improve cyber defenses and protect networks. However, the number of studies on how to defend against a cyber-attack on a satellite is much smaller.¹⁰ For military and civilian operators, the network is much more valuable than the satellite itself, so it is understandable that attention is paid to cyber-attacks 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 or Earth observation data, 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 electrical grid—also relies on the use of commercial and civilian 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. If ground stations are located in other countries (e.g., the Chinese ground station in Argentina), it would raise some suspicions of hosting countries when military personnel were located to secure protection of those ground stations.¹¹ Satellite communications involve lots of confidential transmissions including military communications, and depend on the security of ground stations of these satellites in other sovereign states (command and control of satellites as well as uplink and downlink of data requires ground stations all over the world).

It is well known that the radio frequency for satellite communications is limited. Traditionally, the radio frequency bands were distributed through the International Telecommunications Union (ITU), but the increase in the number of commercial and private satellites put huge pressure on the distribution of this scarce resource.¹² Some operators, particularly small satellite operators, are now using less secure frequencies, sometimes including ham radio frequency. This frequency is open to anyone, and therefore, it is easy to detect and hack if malign actors want to take over those satellites. Furthermore, the cost for upgrading security against cyber-attacks would discourage small satellite operators from taking appropriate measures to harden themselves against this threat. The cost of encrypting command and telemetry data and the cost of securing ground stations would put additional financial pressure on commercial ventures. Currently there is no regulatory mechanism to force these types of operators to improve their security against cyber-attacks.

Many satellites have a life expectation of 10-15 years. Satellites are, as discussed above, chunks of electronic hardware. Once a satellite is launched, it would be hard to fix or replace because of the cost of getting access to the machines in orbit. Therefore, the hardware on the satellite can be 10-15 years old. This would mean that the satellites are not fit for modern, up-to-date cyber security. Of course, software can be upgraded but given the speed of the evolution of computing hardware, new software may not be fit for the 10-15-year-old hardware in orbit (imagine that you are working on a 15-year-old computer at your workplace). Such

limitations on hardware replacement would also increase vulnerability to cyber-attacks in space.

Another aspect of cyber-attacks on satellite systems is the spoofing of telemetry data. Spoofing is a technique to provide false information about a satellite's location, its position and its 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 someone with malign 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 shows extreme abnormality from the original data.

Other ASATs

Apart from cyber-attacks on satellites, there are other methods for attacking adversaries' satellite capabilities without using kinetic forces. Jamming radio waves from satellites is one way to interfere with satellite communications. In 2013, for example, North Korea directed a very strong radio frequency signal towards South Korea so as to disrupt GPS signals. This mass-scale jamming caused huge confusion in air traffic and other vital socio-economic infrastructure. This incident took place using only local terrestrial means so the effect was geographically quite limited, but if it had been done using assets in orbit, the effect might have been more widespread 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 powerful devices, they can cause much wider area effects.

Another method of non-kinetic attack on satellites is dazzling. Dazzling is 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 already have 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.

One final 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. 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 Space Situational Awareness (SSA), which detects any satellite or debris approaching existing space assets. With a more complete picture of the space domain, it becomes more difficult for an attacking nation to avoid attribution when using these methods to perpetrate an attack.

Deterrence in Space?

In order to prevent kinetic, cyber-based, and other attacks on space assets, nations need to develop a space deterrence strategy. However, as discussed above, deterrence in space is quite different from other conventional or nuclear deterrence strategies.

First of all, it is impossible to develop a space deterrence strategy based on concepts of territorial control. Space objects in orbit are very high-speed, high-velocity objects that are moving in a vacuum of space across foreign territories on the ground. 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, Republic of Congo, Democratic Republic of Congo, Indonesia, Kenya and Uganda)—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 have the actual 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 analogous to a vessel operating on the high seas. Even in the case of high seas, there is a concept of A2/AD (Anti-Access and Area Denial) based on certain geographical control by excluding foreign vessels from the geographical area. Thus, any deterrence strategy in space is different from traditional ones and has to be based on concepts of non-territorial control.

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 more space-dependent

country 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 (such as is largely the case with North Korea today), it would be ineffective to retaliate against that nation's space assets because either they do not exist or they hold very little value to the country in question. Even though China is increasingly dependent on space assets for its military operation, the degree of dependence on space is less significant than that of the United States and its allies. If the United States launches a tit-for-tat retaliation, it may not be proportional to the damage incurred. Since countries hold substantially differing attachment to and dependency on space-based assets, deterrence in space cannot simply rely on "in-kind" responses the way 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 be able to exercise denial against attacks on space assets. Since there are many ways to attack space assets, 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, to pursue deterrence by denial a state would need to defend its satellites against jamming, which requires protecting a satellite's ability to receive and deliver its signals through the use of frequency hopping and encryption. This is possible too, but it would increase the cost of building and operating satellites. To defend against the threat of dazzling, one has to improve the protection of sensors, but at present this is not technically feasible. The adversaries may use co-orbital satellites which operate in proximity to critical space assets and interfere with electronic communications or use robot arms to manipulate those assets. It is possible to evade such attacks by co-orbital satellites but evasion requires constant monitoring of the movement of all satellites, which would require large scale investment in ground-based monitoring systems with international partners. Overall, the cost of attacking a satellite is extremely low whereas the cost of denying an attack is very high. Thus, the strategy of deterrence by denial may be applicable in theory but practically very fragile and costly. It may reduce

incentives for adversaries to take certain actions, but attacking satellites is much easier and cheaper than defending them. In other words, attacks on satellites are effective cost-imposing strategies for adversaries.

Fourth, like the case of cyber security, there is an attribution problem. 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 CSpOC, so if a collision in space occurs, ownership of the assets involved in the collision can be identified. 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 only detect space debris bigger than the size of a softball, there is always a possibility that a malfunction occurred due to collision with space debris smaller than 10cm in diameter. Even if the collision took place between active satellites, one cannot be sure whether the collision occurred due to 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 countries like Russia and China, the recognition and identification of hostile action may be even more difficult since a given adversary may choose to employ such a strategy to exploit the gray area nature of outer space.¹³

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 cyber security where actions can be taken without kinetic force, with difficulties of attribution, territorial control and effective retaliation. In fact, both cyber and space security issues were discussed at the United Nations by the Groups of Governmental Experts (GGE) in a similar timeframe (early 2010's).

One achievement that grew out of the international discussions on how to establish norms governing cyber security was the *Tallinn Manual on the International Law Applicable to Cyber Warfare*, which was published in 2013.¹⁴ 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 non-conventional 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-attacks, which can be regarded as “armed attacks” during periods of armed conflict, and reaffirms that inherent rights of self-defense can be applied to these attacks. It defines the means and methods of warfare in retaliation to cyber-attacks with principles of necessity and proportionality. The *Tallinn Manual* is a collection of existing international law on armed conflict applied to the cyber domain, but cyber-attacks 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 2017.¹⁵

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 is not legitimate unless authorized by the United Nations Security Council. If a cyber-attack is conducted by a non-state actor, countermeasures can only be taken 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 non-state actors.

In case of space, there is no equivalent to the *Tallinn Manual*, but there is a project launched in 2016 by McGill University and the University of Adelaide to develop a Manual on International Law Applicable to Military Uses of Outer Space (MILAMOS).¹⁶ Some participants of MILAMOS have left the project and established another group to discuss the Woomera Manual on the International Law of Military Space Operations.¹⁷ Both are pursuing the same objectives but approaching the issue from different angles.

Such manuals for the military use of space would certainly contribute to the transparency and predictability of state actions. Although not legally binding documents, they would give some clarity as to what can be expected if a state or non-state actor tries to attack the space assets of another state. However, it is almost certain that existing international law is far from sufficient to define this 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 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 achieve deterrence to prevent adversaries from undertaking hostile actions against the two countries' space assets.

First, both 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 prefecture in order to enable it to detect space objects less than 1m in diameter (the exact capabilities of the system Japan is preparing to deploy have not been publicly disclosed). However, these facilities are owned and operated by a civilian space agency, JAXA (Japan Aerospace Exploration Agency). Because of the military nature of SSA data collected by the U.S. Air Force, the U.S. government demanded the Japanese Ministry of Defense to get involved to enhance the security of information exchange. Thus, Japan has decided to construct a new SSA facility in Yamaguchi prefecture, which will be operated by the Self-Defense Force (SDF). Japanese participation in the SSA network is extremely important because the current SSA network does not cover the western Pacific and Asian regions. Japanese SSA installations will help cover blind spots, including the space 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 anti-satellite 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 (IGS), and also 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 non-kinetic activities. Thus, the U.S.-Japan alliance also has to work together to improve detection of cyber and non-cyber 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 together to improve the resilience of space systems. Resilience (or mission assurance) is necessary because space assets are both vulnerable as well as crucial for socio-economic 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 can be small satellites that can be launched rapidly, but 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. In this context, the Space Security Working Group of the National Space Policy Committee of Japan has issued a policy paper on the “Basic Framework for Improving Mission Assurance of Space Systems” in 2018.¹⁸ In this document, Japan recognized its role in the alliance of providing mission assurance for the alliance as well as coordinating with allies in case of loss of Japanese satellite capabilities.

Last but not least, the U.S.-Japan alliance implies a ‘deterrence through punishment’ approach by planning possible military actions in 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 Defense Guidelines issued in 2015 to prepare for the worst-case scenario and demonstrate its determination to employ appropriate means to retaliate in case of intentional attacks on allied space assets. Furthermore, the 2018 National Defense Strategy of the United States has identified space as a warfighting domain, and its 2018 Nuclear Posture Review suggested that the United States may use nuclear forces as the ultimate form of retaliation for non-nuclear attacks, including attacks on space systems. In response to these U.S. actions, Japan has decided that “[t]o ensure superiority in use of space at all stages from peacetime to armed contingencies, SDF will also work to strengthen capabilities including mission assurance capability and capability to disrupt opponent’s command, control, communications and information” in its National Defense Program Guidelines in December 2018.¹⁹

Deterrence, by definition, is an intersubjective concept. The main purpose of deterrence is to convince adversaries not to take any action to harm the allies’ space assets in the first place. As discussed above, deterrence by denial and deterrence of attacks on space assets through retaliation in space does not seem persuasive because of physical and technical difficulties. Therefore, threats of punishment by means other than those in space should be used to convince the adversary to abjure such attacks. In other words, the alliance should prepare and plan for cross-domain deterrence in order to dissuade its enemies from striking at its space assets. Of course, Japan has constraints on its ability to take aggressive actions towards 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 deterrence posture toward potential adversaries.

Conclusion

There is no doubt that space systems are vital for our daily lives and security. But the security of space systems fall 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 been on the need to defend against direct ascent kinetic attacks such as the Chinese ASAT test in 2007 and the Indian ASAT in 2019, 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 U.S. and Japan but even those of Russia or China, because 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-attacks is an urgent priority for achieving a secure and sustainable use of space.

Once a satellite collision creates space debris, it will not only increase the risks to other satellites, but also create a situation which is 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 as to be fundamentally unsafe for human use²⁰. In such a situation, it would be impossible to use space for the benefit of mankind and our socio-economic welfare, not to mention our security.

In order to prevent such a catastrophic outcome, the U.S.-Japan alliance should prepare for all 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 global coverage of their SSA capabilities in order to make sure 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 their space systems to make sure that ASAT attacks do not achieve their objectives. And finally, the alliance should develop a plan to respond to any intentional attacks so that adversaries can understand that the cost of an attack on 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, and therefore, it should play a key role in developing a joint, cross-domain allied space deterrence strategy. ■

Kazuto Suzuki is Vice Dean and 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 Ph.D. from Sussex European Institute, University of Sussex, England. He has worked in the Fondation pour la Recherche Strategique in Paris, France as assistant researcher and as the Associate Professor at the University of Tsukuba from 2000 to 2008, before moving to Hokkaido University. He also spent one year at Woodrow Wilson School of Public and International Affairs at Princeton University from 2012 to 2013 as a visiting researcher. He served as an expert on the Panel of Experts for Iranian Sanction Committee under the United Nations Security Council from 2013 to 2015. He has contributed to the drafting of the Basic Space Law of Japan, and serves as a member of sub-committees of industrial policy and space security policy of the National Space Policy Commission. His recent work includes *Space and International Politics* (2011, in Japanese, awarded the Suntory Prize for Social Sciences and Humanities), *Policy Logics and Institutions of European Space Collaboration* (2003) and many other publications.

- 1 Def. Intelligence Agency, Challenges to Security in Space (2019), available at https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf.
- 2 Eric Gartzke & Jon R. Lindsay, Cross-Domain Deterrence: Strategy in an Era of Complexity (2019).
- 3 The European Space Agency provides statistical numbers of space debris and updates said data regularly. See *Space debris by the numbers*, Eur. Space Agency, https://www.esa.int/Safety_Security/Space_Debris/Space_debris_by_the_numbers (last visited Nov. 30, 2019).
- 4 Brian Weeden, Secure World Found., Going Blind: Why America Is on the Verge of Losing Its Situational Awareness in Space and What Can Be Done about It (2012), available at http://swfound.org/media/90775/going_blind_final.pdf.
- 5 UCS Satellite Database, Union of Concerned Scientists (Mar. 31, 2019), <https://www.ucsusa.org/nuclear-weapons/space-weapons/satellite-database>.
- 6 Loren Grush, *More than 50 pieces of debris remain in space after India destroyed its own satellite in March 14*, Verge (Aug. 8, 2019), <https://www.theverge.com/2019/8/8/20754816/india-asat-test-mission-shakti-space-debris-tracking-air-force>.
- 7 U.N. Office for Outer Space Affairs, Space Debris Mitigation Guidelines of the Committee on the Peaceful Uses of Outer Space, U.N. Doc. ST/SPACE/49 (2010).
- 8 Eur. External Action Serv., DRAFT International Code of Conduct for Outer Space Activities (2014), available at https://eeas.europa.eu/sites/eeas/files/space_code_conduct_draft_vers_31-march-2014_en.pdf.
- 9 Ministry of Foreign Affairs of the People's Rep. of China, Treaty on the Prevention of the Placement of Weapons in Outer Space, the Threat or Use of Force against Outer Space Objects (Draft) (2014), available at https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjfywj_665252/t1165762.shtml.
- 10 Rajeswari Pillai Rajagopalan, U.N. Inst. Disarmament Research, Electronic and Cyber Warfare in Outer Space, Space Dossier 3 (2019), available at <https://www.unidir.org/files/publications/pdfs/electronic-and-cyber-warfare-in-outer-space-en-784.pdf>.
- 11 Cassandra Garrison, *China's military-run space station in Argentina is a 'black box'*, Reuters (Jan. 31, 2019), <https://www.reuters.com/article/us-space-argentina-china-insight/chinas-military-run-space-station-in-argentina-is-a-black-box-idUSKCN1PP0I2>.
- 12 Adrian Copiz, *Scarcity in Space: The International Regulation of Satellites*, 10 CommLaw Conspectus: J. Comm. L. & Tech. Pol'y 207 (2002).
- 13 Jana Robinson, *Deterring Chinese and Russian space hybrid warfare by economic and financial means*, Space Rev. (Sept. 18, 2017), <http://www.thespacereview.com/article/3331/1>.
- 14 Tallinn Manual on the International Law Applicable to Cyber Warfare (Michael N. Schmitt ed., 2013).
- 15 Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Michael N. Schmitt ed., 2d ed. 2017).
- 16 See *Manual on International Law Applicable to Military Uses of Outer Space (MILAMOS)*, Inst. Air & Space L., McGill U., <https://www.mcgill.ca/iasl/milamos> (last visited Nov. 30, 2019).
- 17 See *The Woomera Manual on the International Law of Military Space Operations*, U. Adelaide, <https://law.adelaide.edu.au/woomera/> (last visited Nov. 30, 2019).

18 Cabinet Office, Uchū shisutemu zentai no kinō hoshō (Mission Assurance) no kyōka ni kansuru kihon-teki kangaekata (宇宙システム全体の機能保証(Mission Assurance)の強化に関する基本的考え方) [Basic Framework for Improving Mission Assurance of Space Systems] (2017), available at <https://www8.cao.go.jp/space/committee/dai57/siryō1-1.pdf>.

19 Ministry of Def., NATIONAL DEFENSE PROGRAM GUIDELINES for FY 2019 and beyond 20 (2018), available at https://www.mod.go.jp/j/approach/agenda/guideline/2019/pdf/20181218_e.pdf.

20 Donald J. Kessler, Nicholas L. Johnson, J.-C. Liou & Mark Matney, *The Kessler Syndrome: Implications to Future Space Operations*, (Am. Astronautical Soc’y, Preprint Paper AAS No. 10-016, 2010), <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.394.6767&rep=rep1&type=pdf>.



Ryan M. Scoville

Marquette University
Law School

Toward Meta-Knowledge of Foreign Relations Law in U.S.-Japan Relations

Introduction

It is well known that U.S. and Japanese positions on international law pertaining to the use of force do not always align. Japan reportedly holds the view that one state can engage in the collective self-defense of another only if the other has explicitly requested assistance, but the United States has at times suggested that an implied request is sufficient.¹ Japan “has repeatedly rejected the notion that the right to self-defense applies against imminent threats,”² but the United States supports this notion.³ And while the United States has endorsed the so-called “unwilling or unable” test for the use of force against non-state actors, Japan does not appear to take a position.⁴ These differences may generate conflicting views regarding the types of action that each state can undertake in furtherance of the alliance.

In contrast, this paper focuses on the role of foreign relations law in the U.S.-Japan alliance. As the municipal law that “governs how [a] nation interacts with the rest of the world,”⁵ foreign relations law implicates a wide variety of topics. In the United States, it encompasses everything from the War Powers Resolution to the Alien Tort Statute, the Treaty Clause of the Constitution, and federal common law on foreign official immunity, among other matters. Japanese academia has not traditionally conceived of foreign relations law as a distinct field of legal knowledge, but from an American perspective, Japanese foreign relations law includes Article 9 of Japan’s Constitution,⁶ the 2015 legislation that expanded the authority of Japanese self-defense forces to participate in foreign conflicts,⁷ and decisions from Japanese courts on the relationship between international and national law.⁸

My contention is that deficiencies in knowledge of *foreign* foreign-relations law can arise and are consequential but are also poorly understood in fact. Thus, to strengthen their alliance, the United States and Japan should develop bilateral meta-knowledge of their foreign relations laws and then strive to address any epistemic gaps through enhanced programs to educate relevant actors and foster and preserve institutional memory.

The Significance of Foreign Knowledge

The successful maintenance of U.S.-Japan relations is likely to depend not only on matters of international law, but also on whether and how each side understands the other's foreign relations law. As an illustration, consider Article V of the U.S.-Japan Security Treaty, which states that in the event of an armed attack against either party in Japanese-administered territory each "would act to meet the common danger in accordance with its constitutional provisions and processes."⁹ From the perspective of Japan, this provision is likely to be unclear and even misleading absent knowledge about the separation of war powers under the U.S. Constitution. At one extreme, if Japanese officials mistakenly perceive the Constitution as allocating to the president exclusive authority over the decision to use force, they might disregard the preferences of Congress in attempting to anticipate the likelihood and nature of an American response to an attack on Japanese territory. At the other extreme, if these officials mistakenly perceive the Constitution as allocating exclusive authority to Congress, they might disregard the president. In between, Japanese officials are likely to pay attention to both the president and Congress if they perceive the use of force as a domain of shared authority. Depending on the political alignments and policy preferences of the president and congressional majorities at any given point in time, these scenarios could yield materially different Japanese expectations regarding the willingness of the United States to use force under Article V.

Third-party dynamics are also possible. Imagine, for example, that China is contemplating an invasion of Taiwan and seeks to anticipate the responses of the United States and Japan. It is conceivable that China would view the foreign relations laws of these states as purely epiphenomenal and thus attempt to predict reactions exclusively by reference to other factors, such as state interests and the regional balance of power. But if China views American and Japanese laws as imposing even moderately effective restraints on each state's use of force, it seems likely that China would account for those laws in its models. In this latter scenario, China would prepare for an invasion at least in part by studying U.S. and Japanese law pertaining to the use of force, Japanese understandings of U.S. law, and American understandings of Japanese law. In turn, if there is Chinese law on the use of force and it is effective, Washington and Tokyo would do well to study not only that law, but also Chinese understandings of American and Japanese understandings of Chinese law.

Some legal scholars in the United States have acknowledged these dynamics. Jide Nzelibe and John Yoo have argued that the constitutionality of a unilateral use of force by the president should depend in part on the sophistication of the adversary: congressional authorization should be required when the adversary is likely to perceive it correctly as a signal of the seriousness of an American

commitment to use force, but not otherwise.¹⁰ One of the stated implications of this position is that congressional authorization should be unnecessary for military operations against terrorist organizations, which Nzelibe and Yoo presume to lack understanding of the “institutional context in which the President and Congress interact on war powers issues.”¹¹ More recently, Matthew Waxman has examined how legislative checks on executive war-making might shape the efficacy of threats to use force.¹² In his view, “the ultimate effects of any legal reform on war and peace will depend not just on the internal effects on U.S. government decision-making but the external perceptions of actors regarding U.S. signals.”¹³

But the issue also extends beyond the domain of military conflict. For example, the Agreement Regarding the Status of United States Armed Forces in Japan provides that U.S. military authorities shall have the right to exercise within Japan “all criminal and disciplinary jurisdiction conferred on them by the law of the United States over all persons subject to the military law of the United States.”¹⁴ In light of this provision, Japan cannot hope to understand U.S. assertions of jurisdiction over American forces in Japanese territory without knowledge of U.S. rules governing the extraterritoriality of U.S. law. Likewise, members of Congress frequently confer with Japanese officials in Tokyo and in doing so make representations that are at times contrary to the policy of the executive branch.¹⁵ This practice risks substantial confusion about the nature of U.S. policy unless Japanese interlocutors understand that the U.S. Constitution denies Congress authority to communicate and transact with foreign governments on behalf of the United States. And in the wake of the Trump Administration’s decision to withdraw from the Paris Agreement, American states and localities have pursued various arrangements with Japanese and other foreign partners to combat climate change.¹⁶ Those partners could misapprehend the nature and scope of the arrangements unless they are familiar with the Compact Clause, which prohibits U.S. states from entering into “any Agreement or Compact . . . with a foreign Power” absent approval from Congress.¹⁷

We know, moreover, that the risk of misunderstanding is not purely theoretical. Indeed, misperceptions of law have occurred on a number of occasions in the past. To name just one example, in the early 1970s Japanese officials acquiesced to an import-control plan that Japanese industry leaders had negotiated with a member of Congress on the assumption that the congressman spoke for President Nixon, only to later find that Nixon opposed the deal.¹⁸ In this case, Japan erred by instinctively projecting the institutional dynamics of its own parliamentary system, in which coordination between the prime minister and a legislator is not uncommon, onto the United States, where the separation of powers limits inter-branch cooperation, allocates power over diplomatic negotiations to the president rather than Congress, and thus diminishes the prospects for presidential approval of a congressionally negotiated agreement.¹⁹

Of course, knowledge gaps are just as plausible and problematic in reverse: Lack of U.S. knowledge of Japanese foreign relations law risks confusion about which Japanese institutions hold power to decide matters of foreign policy, the standards that govern their decision-making, and the nature of the policy itself. If, for example, relevant actors in the United States mistakenly perceive Article 98 of the Japanese Constitution as establishing that all treaties are self-executing,²⁰ those actors would likely misapprehend the available modes of domestic enforcement and perhaps the extent of compliance. Comparable risks are possible with respect to Article 9, among other laws.²¹

The Mystery of Foreign Knowledge

Although external knowledge of foreign relations law is an issue of significance to the U.S.-Japan alliance, we know very little about the epistemic conditions that prevail on each side. We can make certain reasonable assumptions: Presumably, Japanese officials understand U.S. law to the extent necessary to carry out their duties. Presumably, the average Japanese citizen knows less than the average government official. Presumably, Japanese knowledge is much more pervasive today than it was at the arrival of Commodore Matthew Perry in 1853.²² And presumably, relevant U.S. officials are aware of the famous Article 9, particularly given America's role in its drafting.²³

But conditions are otherwise far from obvious. On the one hand, foreign sophistication is entirely plausible. Although U.S. media coverage of Japan is comparatively limited, Japanese news media have historically covered developments in the United States rather extensively.²⁴ The United States and Japan are both wealthy countries that possess the financial resources necessary to develop expertise in foreign law. Both states respect the rule of law and exhibit high levels of education among their respective national publics. The global diffusion of governmental structures may help to ensure a basic familiarity with concepts such as the separation of powers, judicial review, and executive primacy in the conduct of diplomacy.²⁵ And the tempo and volume of security and economic contacts between the United States and Japan seem likely to generate considerable functional need in each state for knowledge of the other side's foreign relations law. For instance, when negotiating a trade agreement with the United States, Japanese officials may need to understand Trade Promotion Authority under U.S. law in order to assess their leverage in negotiations and ascertain the likelihood of U.S. ratification of any resulting text.

On the other hand, foreign naiveté also seems plausible. The United States and Japan have different legal traditions. There are considerable language barriers. The alliance is vital to both sides, but neither seems to have an incentive to study

the other's foreign relations law beyond what is strictly necessary. Differences between the governmental systems and foreign relations laws of the two countries create ample opportunities for misunderstanding. And domestic law is often abstruse even to native lawyers.

Moreover, important questions remain even if we assume that there are pockets of Japanese knowledge on discrete topics in U.S. foreign relations law: Who holds that knowledge? Are the ministries of Defense (MOD); Economy, Trade and Industry (METI); and Foreign Affairs (MOFA) equally well-informed? How pervasive is pertinent knowledge within academia, industry, and other sectors? Where knowledge exists, how accurate and up-to-date is it? How is it acquired and what motivates its acquisition? Are there programs to incorporate knowledge into the institutional memory of Japanese government ministries, or are relevant areas of U.S. law re-learned from scratch with each personnel rotation? Has the degree of Japanese sophistication evolved in recent decades? And how much weight do those on the Japanese side accord to U.S. foreign relations law in attempting to explain and predict the actions of the U.S. government? The simple answer is that American scholars do not know.²⁶ And with the possible exception of Article 9 of the Japanese Constitution, the same is probably true in reverse.

In certain ways, this all seems unsurprising. Those who conduct foreign relations have no incentive or even freedom to reveal the extent of their naiveté or sophistication. Most academic work on U.S. foreign relations law ignores the significance of foreign legal knowledge. And as a matter of legal doctrine, each state's interpretation and application of its own foreign relations law generally does not require knowledge of foreign understandings. In this context, there is little need for domestic practitioners to ascertain foreign knowledge.

Yet uncertainty about foreign knowledge of U.S. law seems consequential, not least because it can generate varying assumptions among U.S. officials. Sometimes the assumption has been one of foreign naiveté. For example, in *Zivotofsky v. Kerry*, the Supreme Court held that while Section 214 of the Foreign Relations Authorization Act of 2003 did not change U.S. policy on the status of Jerusalem, the statute nevertheless infringed the president's exclusive power to recognize foreign borders by requiring him to issue statements that contradict the policy in official passports.²⁷ In justifying this decision, the Court seemed to take for granted that important foreign audiences would incorrectly interpret the statements as evidence of a change in policy.²⁸ On other occasions, however, the assumption has been one of foreign sophistication. For instance, when President Nixon vetoed the War Powers Resolution in 1973, he did so partly on the view that the law would undermine deterrence by signaling that, absent congressional support, domestic authority to use military force expires after sixty to ninety days.²⁹ This position assumed that foreign governments would read the War Powers Resolution, understand it, and consider it in predicting the actions of the U.S.

government. Varying assumptions of naiveté and sophistication are also plausible in U.S.-Japan relations.

In this context, it is harder to ascertain whether foreign relations laws serve national interests. If foreign audiences are well informed, then the law is likely to succeed not only at allocating power internally, but also at facilitating cooperation and limiting miscalculation. But if foreign audiences are poorly informed, then the law might generate misunderstanding and even conflict on a wide range of issues. To name just one conceivable illustration, if China interprets the separation of war powers in the United States as preserving U.S. discretion with respect to the implementation of the Japan-U.S. Security Treaty, while Japan understands the treaty as obliging U.S. military assistance in the event of an attack notwithstanding the separation of powers, then the parties might draw different conclusions about the likelihood and nature of a U.S. military response to Chinese seizure of Japanese-administered territories. Unless China and Japan perceive U.S. law as purely epiphenomenal in this area, their disparate views could increase the risk of hostilities.

Toward Meta-Knowledge and Mutual Understanding

Current conditions thus suggest the need for meta-knowledge of foreign relations law in the U.S.-Japan alliance. How might we develop this knowledge? As I see it, the inquiry will be primarily sociological, focusing on the pathways of knowledge diffusion and maintenance. The knowledge of government officials will certainly be material, but the knowledge of actors in civil society (academics, business leaders, think tanks, law firms, etc.) may also carry significance, given that the United States and Japan are both relatively democratic states whose foreign policies appear to be subject to certain degrees of public influence.

With respect to government officials, the options for evidence-collection are probably limited to interviews with the officials themselves and private actors from whom the officials might acquire information. These interviews should seek to glean insights on professional backgrounds, including not just formal training but also interviewee encounters with officials from the other side of the alliance, exposure to legal resources and popular media from the other side, and perceptions of the pervasiveness and quality of official knowledge within the government. The interviews should also seek to glean information on the institutional location of relevant knowledge, any official modes of acquisition, the existence of any programs to train government officials or otherwise develop and protect institutional knowledge, any topics of frequent confusion, and views about the barriers to greater understanding.

With respect to civil society, the options for evidence-collection are more numerous. In addition to interviews, relevant academic literatures are likely to serve as sources of insight. We might draw inferences about the state of U.S. sophistication on Japanese law pertaining to national defense, for example, by reviewing U.S. publications for articles on that topic. We might also examine popular media coverage; if major news outlets such as the *Asahi Shimbun* and the *New York Times* contain varying degrees of coverage on the foreign policies and foreign relations laws of the foreign partner, we might infer differences in the sophistication of the American and Japanese publics. We might also ascertain public knowledge with tools such as Google Surveys.

I have used a number of these strategies over the past several months as part of an initial effort to evaluate conditions in Japan. I met with and interviewed numerous academics and officials from MOD, METI, and MOFA. I searched Japanese newspaper archives for pertinent coverage. I distributed surveys and collected a significant volume of legal academic literature from the National Diet Library. The process of organizing and writing about the resulting evidence is ongoing, but I would like to offer a few quick impressions from the work that I have completed so far.

First, formal education on U.S. foreign relations law is essentially non-existent in Japan. No law school offers a course on the topic. Survey courses on “Anglo-American law” do not touch upon it, other than through general and fairly superficial discussions about the separation of powers and federalism. Nor do government agencies formally train officials on U.S. foreign relations law. This is true, moreover, even when officials are on assignment to units such as MOFA’s First North America Division and the Americas Division of METI’s Trade Policy Bureau, and even though formal training occurs on other topics. Japan’s Foreign Service Training Institute, for example, educates trainees on contemporary political issues in U.S.-Japan relations, but does not cover the laws that govern the U.S. side of the relationship. As a result, the acquisition of legal knowledge tends to be highly informal.

There are a few potential explanations for this condition. One is that relevant actors in Japan generally view training as unnecessary. Another is that these actors view the training as helpful but operate under resource constraints that require them to prioritize training on topics that are more pressing. Still another possibility is a shortage of expert instructors: While a significant number of legal academics conduct research on U.S. law, most focus on topics other than foreign relations law, such as the rights provisions of the Constitution, which tend to be seen as more interesting and innovative than the structural provisions in light of recent case law on matters such as gay marriage. In fact, at present, there are only a few academics in Japan who publish with any degree of regularity on U.S. foreign relations law. Moreover, many of those who have written sporadically have

been international law scholars, rather than specialists in U.S. law. In contrast, the number of political scientists who study U.S.-Japan relations is significant—perhaps as many as one hundred, by one estimate. These conditions raise the possibility that Japan tends to view U.S. conduct vis-à-vis Japan through the lens of politics rather than law.

Second, notwithstanding the absence of formal training, there is a significant Japanese-language literature on U.S. foreign relations law. This literature extends back to well before World War II and includes major works on war powers and the relationship between domestic and international law in the United States, in addition to a significant number of articles on topics ranging from the Alien Tort Statute to Trade Promotion Authority and rules about the extraterritoriality of federal statutes. *Amerika Hou*—the leading publication on American law—regularly summarizes U.S. Supreme Court decisions and reviews U.S. law review articles, including a number that have addressed aspects of U.S. foreign relations law. This is an unacknowledged, shadow literature with which American scholars simply do not engage. By evaluating its timing, rigor, and topical tendencies, we might obtain fresh insights into Japan's concerns, interests, and potential misunderstandings.

Third, to the extent that questions about U.S. foreign relations law arise in Japan, Japanese government officials often seek answers in an ad hoc fashion. Sometimes officials at MOFA, for example, instruct embassy personnel in Washington to consult with think tanks and law firms. Less frequently, they consult with Japanese or American academics. Sometimes they acquire information directly from U.S. officials. And sometimes they seek out answers on their own, using common online search tools. As far as I can tell, there are no formal procedures that help officials choose among these options.

Although I have not examined American knowledge of Japanese foreign relations law, I suspect that many of the same limitations manifest in the United States to an equal or even greater degree. My sense is that, in comparison to Japan, American legal education and scholarship are generally quite parochial. Few law schools in the United States offer courses in Japanese law. Comparative research does not seem to be particularly popular. Even within American scholarship on Japanese law, Japanese foreign relations law seems to garner close to zero attention aside from Article 9. Moreover, knowledge of the English language is much more pervasive among Japanese officials and scholars than knowledge of the Japanese language among their American counterparts, and the Japanese government is generally less transparent than the U.S. government. These conditions likely inhibit the diffusion of knowledge and suggest a risk of law-based misunderstanding in the alliance.

Current conditions also raise questions about how to improve. What can each side do to build greater foreign sophistication with respect to its domestic law

of foreign relations, and greater domestic sophistication with respect to foreign law on foreign relations? There are a number of conceivable options, but most will require a significant commitment of resources. Given the financial conditions under which many American and Japanese law schools currently operate, I would be surprised if any schools outside of the upper ranks have capacity to add faculty or courses on *foreign* foreign-relations law. Indeed, most law schools in the United States and Japan do not even offer a course on their own domestic law of foreign relations. But top universities could conceivably play an important role. Columbia University, to name one example, could help to diffuse knowledge of Japanese foreign relations law by collaborating with Japanese experts in this area, just as the University of Tokyo could help to diffuse knowledge of U.S. foreign relations law in Japan by collaborating with American experts. The same might be said of prominent think tanks on both sides. Meanwhile, Japanese scholars might profitably study American knowledge of Japanese law with the support of Fulbright and other programs, and both governments might consider ways to improve institutional knowledge, including through database development and training programs for relevant officials. Together these efforts could help to reduce the risk of misunderstanding and miscalculation on both sides of the Pacific. ■

Ryan Scoville teaches and writes on U.S. foreign relations law and international law. He is a Fulbright grant recipient, a periodic contributor at Lawfare, and an associate managing editor for AJIL Unbound. Before entering academia, he worked as a litigation associate in the Denver and Tokyo offices of the law firm of Morrison & Foerster, and served as a law clerk for Judge Milan D. Smith, Jr. of the U.S. Court of Appeals for the Ninth Circuit and Judge Neil V. Wake of the U.S. District Court for the District of Arizona.

Professor Scoville holds a J.D. from Stanford Law School, where he was an executive editor of the Stanford Law Review, and a B.A. in International Studies from Brigham Young University.

- 1 See, e.g., Masahiro Kurosaki, *Japan's Evolving Position on the Use of Force in Collective Self-Defense*, Lawfare (Aug. 23, 2018), <https://www.lawfareblog.com/japans-evolving-position-use-force-collective-self-defense>.
- 2 Masahiro Kurosaki, *The Bloody Nose Strategy, Self-Defense and International Law: A View from Japan*, Lawfare (Feb. 15, 2018), <https://www.lawfareblog.com/bloody-nose-strategy-self-defense-and-international-law-view-japan>.
- 3 See, e.g., Brian Egan, *International Law, Legal Diplomacy, and the Counter-ISIL Campaign*, Annual Meeting of the American Society of International Law, Apr. 1, 2016.
- 4 See Elena Chachko & Ashley Deeks, *Who is on Board with "Unwilling or Unable"?*, Lawfare (Oct. 10, 2016), <https://www.lawfareblog.com/which-states-support-unwilling-and-unable-test>.
- 5 Curtis A. Bradley, *What is Foreign Relations Law?*, in *The Oxford Handbook of Comparative Foreign Relations Law* 3 (Curtis A. Bradley ed., 2019).
- 6 Nihonkoku Kenpō [Kenpō] [Constitution], May 3, 1947, art. 9 (Japan).
- 7 Cabinet Bill No. 72, 189th Diet Session (May 15, 2015); Cabinet Bill No. 73, 189th Diet Session (May 15, 2015).
- 8 See Yuji Iwasawa, *The Relationship Between International Law and National Law: Japanese Experiences*, 63 Brit. Y.B. Int'l L. 333 (1993).
- 9 Treaty of Mutual Cooperation and Security Between Japan and the United States of America art. V, Jan. 19, 1960, 11 U.S.T. 1633.
- 10 See Jide Nzelibe & John Yoo, *Rational War and Constitutional Design*, 115 Yale L.J. 2512 (2006).
- 11 *Id.* at 2534.
- 12 See Matthew C. Waxman, *The Power to Threaten War*, 123 Yale L.J. 1626 (2014).
- 13 *Id.* at 1680; see also W. Michael Reisman, *War Powers: The Operational Code of Competence*, 83 Am. J. Int'l L. 777, 784 (1989) ("Lack of clarity in the allocation of competence and the uncertain congressional role will sow uncertainty among those who depend on U.S. effectiveness for security and the maintenance of world order.").
- 14 Agreement Regarding the Status of United States Armed Forces in Japan art. XVII(1)(a), Jan. 19, 1960, 11 U.S.T. 1652.
- 15 See generally Ryan M. Scoville, *Legislative Diplomacy*, 112 Mich. L. Rev. 331 (2013).
- 16 See *U.S. and Japanese City, State and Business Networks Partner to Strengthen Global Climate Action, America's Pledge*, Am. Pledge (Sept. 13, 2018), <https://www.americaspledgeonclimate.com/news/u-s-japanese-city-state-business-networks-partner-strengthen-global-climate-action/>.
- 17 U.S. Const., art. I, § 10, cl. 1. *But see* Duncan B. Hollis, *Unpacking the Compact Clause*, 88 Tex. L. Rev. 741, 759 (2010) ("The states have simply not submitted the vast majority of their [agreements] to Congress or the Executive.").
- 18 I.M. Destler et al., *Managing an Alliance: The Politics of U.S.-Japanese Relations* 95 (1976).
- 19 *Id.* at 95–96.
- 20 Compare Kenpō, *supra* note 6, art. 98 ("The treaties concluded by Japan and established laws of nations shall be faithfully observed.") with Yuji Iwasawa, *International Law in the Japanese Legal Order: Recent Developments*, 91 Proc. Ann. Mtg. Am. Soc'y Int'l L. 301, 303–06 (1997) (explaining that some treaties are non-self-executing under Japanese law).
- 21 See, e.g., Destler et al., *supra* note 18, at 95 ("Perhaps the most prominent postwar misperception of this type has been Americans' overestimation of the Japanese premier's power.").

22 Given the national policy of seclusion that prevailed in Japan from the 1630s to Commodore Perry's arrival, we can imagine some of the earliest conversations that might have occurred. Perry: "I have in my possession an official letter from President Millard Fillmore." Japanese official: "What is a 'president'?" Etc.

23 See John W. Dower, *Embracing Defeat* 346–73 (1999) (explaining the U.S. government's role).

24 Laurie A. Freeman, *Media, in U.S.-Japan Relations in a Changing World* 125 (Steven Vogel ed., 2004).

25 See David S. Law & Mila Versteeg, *The Declining Influence of the United States Constitution*, 87 N.Y.U. L. Rev. 762, 785–96 (2012) (reporting that twelve percent of countries have a federal system while roughly forty percent have a presidential system and slightly less than half use an American form of judicial review); see also Martha Finnemore, *International Organizations as Teachers of Norms: The United Nations Educational, Scientific, and Cultural Organization and Science Policy*, 47 Int'l Org. 565 (1993) (arguing that international organizations such as UNESCO help to account for extensive structural isomorphism across national governments).

26 Cf., e.g., Waxman, *supra* note 12, at 1674 ("At this point there remains a dearth of good historical evidence as to how foreign leaders interpret political maneuvers within Congress regarding threatened force.").

27 *Zivotofsky v. Kerry*, 135 S. Ct. 2076 (2015).

28 *Id.* at 2082; see also Ryan Scoville, *The Role of Foreign Perceptions in Zivotofsky*, Lawfare (June 12, 2015), <https://www.lawfare-blog.com/role-foreign-perceptions-zivotofsky> (discussing this issue).

29 See 119 Cong. Rec. 34,990 (1973); see also Waxman, *supra* note 12, at 1676–77 (discussing this episode).

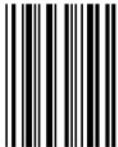
 **Columbia Law School**



ISBN 978-0-578-71877-4



90000>



9 780578 718774