# War 3.0: the Rapid Change of Warfare
# – Deepening Deterrence in the New (Space and Cyber) Domains –

March 2024

SPF 笹川平和財団
SASAKAWA PEACE FOUNDATION
Think, Do, and Innovate-Tank

Security Studies Program

# Table of Contents

# Introduction

The present report is the final report for the “Deterrence in the New Domains” project carried out in 2021–2022 by the Security Studies Program of the Sasakawa Peace Foundation.

In contemporary war, the importance of not only the three traditional domains of land, sea, and air, but also of such “new domains” as space and cyber domains is increasing. Reliance on these domains is growing when it comes to the exercise of military operations, and a loss of superiority in these new domains is coming to be seen as fatal. For that reason, the premise behind contemporary military operation is that they are to be implemented as a Multi-Domain Operation (MDO), which necessarily includes space and cyber domains. At the same time, the issue of how to achieve deterrence (or escalation control) in wars involving operations in new domains is also of growing interest.

Considering this, the Security Studies Program established a “Deterrence in the New Domains Study Group” composed of nine experts in deterrence and space/cyber domains. In the activities in the past two years, the Study Group has conducted various investigations related to “Deterrence in the New Domains.” The present report is one part of its findings.

Using the concept of “War 3.0,” in this report, we pursue the characteristics of war in the present age. In keeping with the growing importance of such new domains as space and cyber domains, we investigate how various issues surrounding deterrence may change. Specifically, through having played out a scenario game two times (please refer to the appendix at the end of the report), it has become clear that the impacts of the new domains are particularly notable at the gray zone stage just short of an armed attack. We emphasize that among this attention should be paid in particular to “the effects of new domains on law enforcement agencies that are at the center of dealing with a gray zone” and “the impact on escalation dynamics of new domains being added to the process of escalation from gray zone to armed conflict.”

In addition, the present report attempts an analysis of “Deterrence in the new domains” from diverse perspectives. The points under discussion are wide-ranging and include sorting out the concepts of deterrence and new domains, how to approach deterrence in the space domain, how to approach deterrence in the cyber domain, the issue of cyber operations by Japan and the U.S. in a Taiwan contingency, and the evolution of air and space power and deterrence.

There are many arguments that emphasize the importance of new domains in contemporary military operations, but one senses that there are not many in which directly take up the relationship between new domains and deterrence (or escalation control). For Japan standing on the frontlines of “competition among great powers” including Taiwan strait contingency, we would have no greater joy than if the present report could contribute greatly to the debate over “Deterrence in the new domains.”

Junichi FUKUDA<br>
Senior Research Fellow, Security Studies Program<br>
Sasakawa Peace Foundation

# Members of "Deterrence in the New Domains Study Group"

All **titles as of the time of writing** at the end of March 2023
(* indicates a writer of the present report)

| | |
|---|---|
| (Chair) | |
| Sugio Takahashi* | Head, Defense Policy Division, Policy Studies Department,<br>National Institute for Defense Studies, Ministry of Defense |
| (Members) | |
| Jun Osawa | Senior Research Fellow, Nakasone Peace Institute |
| Kimitoshi Sugiyama* | Colonel, Director of Air & Space Studies Institute,<br>The Center for Air and Space Power Strategic Studies, JASDF |
| Kazuo Tokito* | Defense Systems Division Advisor, Hitachi, Ltd.; and Maj Gen (Ret.), Former Deputy Commander of Northern Air Defense Command, JASDF |
| Hiroshi Nakatani* | Major, Research fellow of Air & Space Studies Institute,<br>The Center for Air and Space Power Strategic Studies, JASDF |
| Yasuhito Fukushima* | Senior Research Fellow, Global Security Division, Policy Studies Department,<br>National Institute for Defense Studies, Ministry of Defense |
| Satoru Mori* | Professor, Faculty of Law, Keio University |
| (Observer) | |
| Hiroyuki Akita | Commentator, Nihon Keizai Shimbun |
| (Member and Head of the Secretariat) | |
| Junichi Fukuda* | Senior Research Fellow, Security Studies Program,<br>Sasakawa Peace Foundation |

# Chapter Overview

## Chapter 1
## The Era of War 3.0: Changes of “Deterrence” due to New Domains? (Sugio Takahashi)

The patterns of war go through changes together with history. The premise behind the considerations of Carl von Clausewitz—the writer of *On War*—was that one could clearly separate out the people, the army and the government (“the trinitarian model of war”) (War 1.0). However, should this premise collapse, the character of war would also change.

Since the end of the Cold War, dealing with terrorist organizations has been regarded as a major issue, and cooperative responses to Islamic extremism have progressed. These can also be taken to be confrontations between state and non-state actors and are conflicts (War 2.0) of a schema that differs from that of the “trinitarian model of war.” However, beginning around 2010, conflicts among great powers intensified once again, and as in the case of the Russia–Ukraine war, have even reached the point of wars actually taking place in which a great power is involved.

How should we see this? In the present research project, we reached the conclusion that it was necessary to again come up with a new concept of war (War 3.0). There are two reasons for this. One, in light of advancing globalization, wars are being fought in dimensions other than that of military power, and two, the monopoly on military power held by states is collapsing. Thus, the present research project has as its theme the question of how various problems surrounding deterrence will change in keeping with the increase in the importance of the so-called “new domains” of space and cyber.

As premises for advancing our arguments, first with respect to the context of “what” is being deterred, the issue that must be considered in deterrence surrounding new domains is deterrence of threats from states fundamentally aroused by the revival of “competition among great powers.”

Next, today’s competition among great powers is not limited to a matter of it being sufficient to prepare only for full-scale wars between states as during the Cold War period. It is necessary to also prepare for attempts to change the status quo in forms that do not take the patterns of regular warfare, such as hybrid warfare and attempts to change the status quo in the gray zone. Since the ways in which the space and cyber domains are used in gray zone situations and hybrid warfare differ from those in large-scale conflicts, it will be necessary to take these patterns of conflict into consideration when constructing a concept of deterrence that includes new domains.

Furthermore, the strategic context is also important. Strategy is a combination of “ends,” “ways,” and “means.” “Ways” and “means” are significant in composing the roadmap for achieving the "ends." Namely, so long as a strategic purpose exists in the physical space (e.g., Taiwan or Ukraine for China or Russia), the elements of space and the cyber are not themselves "ends" but rather the "ways" and "means" for achieving that "ends." In that sense, at the center of "power" in the new domains are its effect of multiplying physical capabilities like land, sea, and air power, and its effect of reducing the effectiveness of the other party's physical capabilities.

Also, a distinctive characteristic of the new domains in the military field is that attacks not accompanied by physical destruction are possible. This might have great significance particularly with respect to gray zones. One issue is the effects of new domains on law enforcement agencies that are at the center of dealing with a gray zone. For example, if China has engaged in large-scale GPS jamming in the vicinity of the Senkaku Islands, it would become difficult for the Japan Coast Guard patrol boats on watch to respond appropriately to the actions of the opposite parties. Furthermore, if through their jamming of communication satellites and ground facilities they can cut communications with central authorities, the Chinese side naturally will have an advantage.

The second issue is how the dynamics of escalation change when new domains are added in, when projecting the process of escalation from gray zone to armed conflict. On this point, the following hypotheses can be made. First, in terms of nonphysical uses in a gray zone, it is very likely that escalation will occur. However, even in new domains, it will be necessary to be prepared for even greater risks even for the party disrupting the status quo when a physical attack is carried out. Furthermore, if malware is used, the possibilities are great that its existence will be exposed and it will be eliminated. For that reason, one expects that the malware devised will be of a form that can be put into motion at a time when it will produce its maximum effect, and that it will be done when taking decisive action in existing domains.

Accordingly, escalation toward physical uses will be very likely done in concert with escalation in existing domains to maximize its impact. Once one party has decided on escalation from gray zone to conflict, one imagines that escalation including the new domains would rapidly occur.

## Chapter 2
## Sorting Out Concepts in Deterrence and New Domains (Junichi Fukuda)

To investigate "deterrence in the new domains," this chapter intends to sort out concepts with respects to "deterrence" and "new domains."

First, there are multiple definitions for deterrence. For example, "deterrence is simply the persuasion of one's opponent that the costs and/or risks of a given course of action he might take outweigh its benefits." When it comes to what elements are fundamentally important, one can bring up such things as rationality of the opponent, deterrent that provides capabilities sufficient for achieving deterrence, signaling or communicating a message to the other party, credibility of such signaling, and so forth. Furthermore, there are also distinctions in deterrence:

narrow deterrence and broad deterrence, central deterrence and extended deterrence, deterrence by denial and deterrence by punishment, and general deterrence and immediate deterrence.

There are five elements that make deterrence difficult. First, there is the opposite party not being rational. Next, there is the possibility that, while the opposite parties might be rational beings, one might misread the fact that the premises behind their determinations of costs and risks might differ owing to differences in strategic culture and the like. Third, it is possible that one might wind up relying on the mistaken premise that is the "unified Rational Actor model of state" hypothesis. Fourth, there is the possibility that credible signaling may become difficult owing to uncertainties in international relations and states having incentives to misrepresent their own preferences. Finally, there is the possibility that the emergence of new technologies and the involvement of non-state actors will complicate the deterrence situation.

Escalation as a concept closely related to deterrence has been defined as "an increase in the intensity or scope of conflict that crosses threshold(s) considered significant by one or more of the participants." Escalation control is an extension of deterrence, but the aim is not simply to alleviate escalation. There are also cases in which deliberate escalation is sought that calls for an escalation dominance. There are three types of escalation: vertical, horizontal, and compound, and that which stacks the vertical thresholds particularly is the escalation ladder. The question of how to apply this concept of an escalation ladder to the strategic environment of today has been an issue, but the diversification of operational domains in recent years has been the greatest challenge to this concept.

Furthermore, when it comes to concepts that are closely related to but separate from deterrence, one can offer compellence, defense, the status quo, dissuasion, strategic stability, the stability-instability paradox, re-assurance, and arms control, confidence building, and the formation of codes of conduct.

With regard to deterrence in new domains, firstly while there are multiple definitions of domains, most military organizations around the world tend to regard the three domains of land, sea, and air as existing or traditional domains. They tend to treat the "space" and "cyber" (and "electromagnetic") domains as new ones that now become of vital importance for winning advantage in military operations. However, the concept of new domains always leaves room for expansion. For example, the notion of a "cognitive" domain that overlaps with but is not limited to the cyber domain has also been accepted.

There is distinction in deterrence in the new domains between "intra-domain" deterrence and "cross-domain" deterrence. The former is a matter involved with how to deter attacks within the domain in question, while the latter is a matter involved with how to achieve deterrence in a manner that cross with other domains. The former may be effective, for example, in working to improve resilience within the domain and in the planning of deterrence by denial or defense initiatives, but above all at the strategic level, it is no exaggeration to say that all kinds of deterrence should be seen as cross-domain deterrence.

When it comes to the characteristics of the new domains, the space and cyber domains have the following points in common. First, achieving situational awareness is difficult. Second, defense is also difficult. Third, the threshold for attack is low. Fourth, there are multiple kinds of actors. Fifth, codes of conduct are lacking. Due to these conditions, the new domains are prone to offense dominance over defense, and likely to cause deterrence failures.

In new domains that have these characteristics, there are four countermeasures that one might anticipate in a deterrence context. The first is improvements in situational awareness capabilities. The second is improvements in resilience (as means of deterrence by denial). The third is possessing attack (or counterattack) capabilities (as forms of deterrence by denial or punishment). Fourth, while it is not deterrence, there is the promotion of initiatives such as arms control, confidence building, and the formation of codes of conduct.

Deterrence is something that frequently fails, and achieving deterrence in new domains is increasingly difficult. However, we, who are directly confronted with the era of War 3.0, are living in a time in which one must face up to these difficulties.

## Chapter 3
## The Pursuit of Deterrence in Space and the Importance of Resilience and Protection (Yasuhito Fukushima)

Space deterrence has two aspects: “space in deterrence” and “deterrence in space.” The former refers to the role played by space systems and offensive counterspace capabilities when deterring attacks on one’s own country and so forth, while the latter means deterring attacks on space systems. This paper examines the relationship between space and deterrence, focusing on “deterrence in space.”

Looking back on the relationship between space and deterrence during the Cold War, space systems were an indispensable component of the nuclear deterrent while their contribution to conventional deterrence was limited. For that reason, deterrence of attacks on space systems was basically one part of nuclear deterrence.

However, in the 2010s a major change began to take place. The role of space systems in conventional deterrence expanded globally, and not only the U.S. but also France, Russia, China, and others pursued such initiatives. Under these circumstances, the necessity has grown to deter attacks on space systems  as research, development, testing, deployment, and use of offensive counterspace capabilities became noticeable.

If we look at space deterrence in the Russia–Ukraine war as a specific example, firstly in the context of “space in deterrence,” space systems contribute to nuclear deterrence in that they offer functions related to nuclear command, control, and communications of the U.S. and others. It also contributes to deterrence against Russia by making it possible to operate conventional armed forces of NATO countries, etc., more effectively.

In the context of “deterrence in space,” it was unable to deter Russian cyber and electronic attacks against space systems used by Ukraine. Electronic attacks on downlink signals and cyber attacks on user terminals have relatively localized effects, so it would be difficult to say that the attack threshold is high.

Meanwhile, no attacks on the space segment have been confirmed. For one thing, deterrence by punishment may have been effective, and Russia hesitates to attack satellites. The second possibility is that deterrence by denial is functioning. However, it could be that rather than deterrent against Russia having effect, Russia may simply have no plans to attack satellites or that attacks against satellites have taken place, but they have not been made public. It also would be no surprise in the future if Russia destroyed the commercial satellites of other countries that are being used for Ukrainian operations.

How should one pursue “deterrence in space”? One approach is to possess and demonstrate capabilities. Possessing capabilities related to the resilience and protection of space systems and demonstrating externally that those capabilities are possessed contributes to deterrence by denial. Also, in pursuing deterrence by punishment, the determination to use retaliatory capabilities has to be communicated to the adversary in advance. A third one is to pursue cross-domain deterrence. For example, in the case of deterrence by punishment, it is possible that not only showing its intention to retaliate against an attack on a satellite with a satellite attack but also demonstrating the determination to retaliate in the land, sea, air, and cyberspace could help to improve deterrent.

However, one should note that there are limits to deterrence. Working to improve the resilience and protection of space systems so the use of space can continue even after deterrence fails is also significant. According to the U.S. Space Force, there are measures for securing the resilience of space systems like disaggregation, distribution, diversification, proliferation, and deception, as well as protective measures such as electromagnetic spectrum operations, movements and maneuvers, hardening, and cyber security.

The role that space systems play in Japan’s defense has been increasing, and pursing deterrence of attacks on space systems is becoming a crucial issue for the country. At the same time, Japan also has to work on the resilience and protection of space systems in case of deterrence failure.

## Chapter 4
## Approaches to and Issues in Deterrence in Cyberspace（Kazuo Tokito）

This chapter considers cyberspace and deterrence and discusses the approaches and issues to deterrence based on the characteristics and case studies. First, as a distinguishing feature of cyberspace, one can point out that various cyber attacks regularly take place because the distinction between private and military actors is muddled owing to the anonymity and lack of centralized control. Also, conditions now are such that, thanks to technological developments, one cannot completely protect against attacks out of the previously held conception that closed systems are safe.

Cyber attacks come in many varieties, and they are constantly evolving. Attempts to capture each stage of an attack in the kill chain such as reconnaissance, intrusion, malware injection, and the removal of traces, have also appeared, and they can be used effectively as countermeasures.

If we look at a comparison of offense and defense in cyber space, first of all when it comes to the comparative advantages held by the parties (such as China and Russia) working to change the status quo, they include "few legal and moral restrictions based on democratic control," "there are advantages from information manipulation," and "the distinctive characteristics of a cyber attack are easily used." On the other hand, when it comes to the comparative advantages of the parties preserving the status quo (such as Japan, the U.S., and Europe), they include "disclosing the truth," "the development of traceback technology," and a "monopoly over crucial internet functions." Furthermore, we might also bring up "the uses of artificial intelligence (AI) technology" and "rebuilding the supply chain" as factors highly uncertain of which parties may gain comparative advantage.

If we think about cyber warfare in the invasion of Ukraine, cyber warfare represents an asymmetrical approach. Russia conducted cyber attacks against Ukraine from the perspective of such asymmetrical superiority, but it was difficult to say that it maximized the asymmetrical impact of cyber warfare because Ukraine worked out suitable countermeasures. Russia has also used cyber attacks as a means of hybrid warfare and information warfare. From this perspective, cyber warfare becomes a tool for skillfully contriving a strategic and operational environment just short of armed aggression and manipulating a conflict threshold. However, one can also point out that in times of conflict it can be changed into a tool that adds to military capabilities.

To date, Japan has mainly been implementing protection against cyber attacks, but the need is growing now for active defense. The three strategic documents from the end of 2022 hammered out a course of action for strengthening cyber warfare capabilities in cross-domain operations. Specifically, the emphasis was on encouraging information sharing, active cyber defense, strengthening capabilities in cyberspace, securing the capability to obstruct the use of cyberspace, promoting legislative preparations in cyberspace, and cultivating human resources.

As courses of action for demonstrating a deterrent in cyberspace, these entail advance detection of cyber attacks and preventing them through countermeasures; and discovering cyber attacks at an early stage, taking countermeasures, and obtaining the resilience that leads to deterrence by denial such that systems continue to function even when an intrusion has occurred. Regarding counterattacks, it is effective to impose costs on the opposite party by working not just in cyberspace but in close concert with other domains including the kinetic, or with various domains such as the diplomatic and the economic. This leads to deterrence by punishment. The means of delivering such capabilities to the opposite party is also important.

One should also take note that cyberspace is effecting dramatic changes that are visible to the eye. It is necessary to pay attention to the development of cloud computing, diverse network environment, practical application of quantum technology, connections with the cognitive domain, and practical application of AI technology.

This chapter holds up the following five points as issues for deterrence in cyberspace. (1) Secure the functions that are a system's purpose and strengthen its power to execute them by strengthening deterrence by denial and maintaining resilience. (2) With respect to deterrence by punishment, from the perspective of active cyber defenses, build up offensive capabilities and prepare their legal basis, and guarantee effective capabilities with good governance. (3) With respect to developing the systems for strengthening cyberspace capabilities including training personnel, it is necessary to conceptualize and disseminate the strengthening of cyber warfare capabilities. (4) Guaranteeing superiority in cyberspace including public-private partnerships is crucial. (5) In regards to cyber attacks, building an integrated response system that includes diplomatic inquiries, sanctions, and litigation is necessary.

## Chapter 5
## Issues for Japan and U.S. Cyber Operations in a Taiwan Contingency (Satoru Mori)

This chapter investigates what roles Japan and the U.S. would play and whatever mission they must carry out in terms of cyber operations in the event a Taiwan contingency occurs; and also what capabilities Japan needs in regard to the missions it should bear in the cyber domain and what the issues are from a development perspective. Based on the premises that China has as its strategic objective changing the status quo by having control over Taiwan or ascendancy over the Senkaku Islands, and that Japan and the U.S. have as their objective denying a change in the status quo through armed force, if deterrence should break down, a joint operation between Japan and the U.S. will be necessary. This operation would have a double-sided nature: it will be offensive operations to diminish the capabilities and will that China needs for its "Theory of Victory" (TOV), and defensive operations to protect the capabilities and will that the U.S. and Japan need for TOV in order to accomplish their strategic objectives (the denial of China's strategic objectives). Based on that premise, we will investigate what roles and capabilities Japan and the U.S. have in terms of cyber operations, and what the development issues are with respect to those capabilities.

First, in the context of offensive operations that diminish the capabilities and will that China needs for its TOV, one can conceive of a counterforce cyber attack mission targeting each functional phase of the Observe-Orient-Decide-Act (OODA) loop of the People's Liberation Army (PLA). At the same time, it is also possible that in those phases where the target of an attack is forced to escalate from counterforce to countervalue, countervalue cyber attack missions will play a major role operationally. When it comes to cyber operations that diminish the will, the strategic objective would be to persuade China's supreme decision-makers to abandon changing the status quo through armed force or at least get them to halt (postpone) it, but the question is which indicators China's decision-makers will focus on to decide their response. General forecasts are probably impossible, but depending on the situation one imagines that countervalue cyber attack missions whose goal is to influence and divide public opinion will be of great significance.

Next, in the context of defensive operations that protect the capabilities and will that Japan and the U.S. need to achieve the denial of China's strategic objectives, as defense against attacks from China against Japanese and U.S. capabilities, counterforce cyber attack missions will be needed that target the PLA that will come to hinder the anti-ship attack capabilities of the U.S. military and the SDF. At the same time, efforts will also be necessary to defend against Chinese cyber attacks on private networks. In addition, as a defense against attacks by China aimed at diminishing the will of Japan and the U.S., it is possible that through information operation China will work to mold public opinion in both Japan and the U.S. against intervention in a Taiwan contingency. The issue is how to deal with information operations in the so-called cognitive domain.

Based on the above, we sort out the various types of operational missions and issues for Japan and the U.S. as follows. In view of the capabilities that Japan and the U.S. currently have, it would likely be reasonable for the roles to basically be divided, with the U.S. military in charge of offensive operations in cyberspace and the SDF in charge of defensive operations.

First, in terms of missions in offensive operations by the U.S., one can bring up counterforce cyber attack missions against the PLA's OODA loop, countervalue cyber attack missions against China's private and social infrastructure, and cyber attack missions on the cognitive domain that would include information operations targeting the PRC citizens. Next, in terms of Japan's missions and capabilities in defensive operations, one can offer the mission to defend national defense network/government ministry and law enforcement agency network/private network, and the defense mission in the cognitive domain to prevent information operations carried out by China that target the cognitive domain of the general publics of the U.S. and Japan.

The capabilities that Japan will need to acquire with regard to the former are those cyber situational awareness and cyber resilience, and in the future precision cyber counterattack capabilities. With regard to the latter, the government will always have to make efforts to win the trust of the people, and a platform will be necessary for analyzing comprehensive and automated data forensics analysis as a means for countering disinformation.

## Chapter 6
## The Evolution of Air and Space Power and Deterrence
## (Kimitoshi Sugiyama and Hiroshi Nakatani)

This chapter takes up the example of air and space power. Based on their characteristics and evolution, it discusses how dominance in new domains contributes to aerial warfare and deterrence.

The characteristics of air power offered include responsiveness and mobility, superb ISR (intelligence, surveillance, reconnaissance) capabilities, and long-range strike abilities. On the other hand, air power as represented by fighter aircrafts and the like also has weaknesses. They are vulnerable on land, their activities are easily restricted by climate conditions, and the demonstration of their military capabilities can be dramatically deteriorated by the loss of some of its functions.

Backgrounded by these characteristics, today the concept of air superiority is going through fluctuations. Air superiority means that our air power is superior, and that the situation is such that we can execute various operations without serious interference from our enemies. However, promoting the use of the space, cyber, and electromagnetic domains is having a major impact on the entire process known as the so-called kill chain, or F2T2EA. In other words, while the space, cyber, and electromagnetic domains are closely connected to the battles in the existing domains, and play a role as devices for greatly increasing military capabilities (force multiplier), they can also vastly diminish the opposite party's demonstration of their military capabilities by interfering with those capabilities. Accordingly, superiority in the space and cyber domains will have a major impact on the battle in the air over superiority in existing domains. As a result, a reassessment would seem to be necessary such as how to turn the conventional concept of "gaining air superiority" into one that also includes superiority in the new domains.

What sorts of contributions can Japan's own air and space power make to deterrence? Focusing on air and space power, the first is the importance of surveillance of the airspace surrounding Japan. Second is implementing an air defense operation when there is situational escalation. Third is neutralizing missiles flying to Japan with missile defense capabilities (active defenses). Fourth is to harden and improve survivability of SDF bases. Fifth are measures to improve the possibility of air power on the ground surviving through reciprocal use of Japanese and U.S. bases. Furthermore, the capability to deny an opposite party from crossing the sea is also crucial. From a deterrence perspective it is important that through such efforts Japan and the U.S. demonstrate a persistent posture dedicated to defense, and make attackers realized that achieving their objectives quickly will be rejected.

Also, the distinctive feature of air and space power that they provide "eyes" from a high place cannot be ignored. Air and space are the strategic high ground of the contemporary era from which one can view the entire tactical situation. Partnering with regional countries, sharing and combining the latest local information that each has and creating a Common Operational Picture (COP) for the Indo-Pacific are necessary. Through this, an opposite party can be made to feel insecure and suspicious by making them aware that their own unlawful acts and military actions are constantly being watched by someone, and depending on the situation the actions of the opposite party may be checked by jointly revealing their actions and wrongdoings to the international community. This leads to deterrence. Of course, given that the eyes of surveillance by themselves are not enough, action will also be needed to punish unlawful acts after early discovery and detection of abnormalities.

Multilateral cooperation, exercises and training are also crucial. There are analyses that say, historically, exercises that have had the goal of improving joint operational capabilities not only demonstrate the closeness of participating countries, but also have deterrence effect based on their potential to offset the advantages in capabilities of the other. Japan traditionally has emphasized joint exercises with its ally the U.S., but also with other countries and Australia in particular. Furthermore, as part of multilateral cooperation with the QUAD and AUKUS countries, if fuel and munitions could be made mutually interchangeable, this would also lead to improvements in the ability to sustain a war. With regard to the space domain, if hosted payload collaborations can be expanded beyond Japan and the U.S. to further regional countries, it could improve the deterrent. The important thing is that working together with allies and if possible like-minded countries from the strategy conceptualization stage would also serve as pragmatic deterrence partnership against an opposite party.

It is true that deterrence wielding only air and space power alone plays an indirect role rather than a direct one and is nothing more than one element of deterrence. However, for Japan making full use of air and space power and check countries that threaten regional stability not only with Japan's own powers but also together with allies and like-minded countries is growing in importance with each passing day. Fulfilling that obligation will likely indirectly lead to regional stability.

# Chapter 1

# The Era of War 3.0: Changes of "Deterrence" due to New Domains?

**Sugio Takahashi**

## 1. The Advent of the Era of War 3.0

The Patterns of war go through changes together with history. Written in the 19th century by Prussian general Carl von Clausewitz, *On War*[1] set a baseline for subsequent contemplations about war. It considered the phenomenon of war against the backdrop of an age when—owing to the emergence of "national armies" that originated with the French Revolution—wars that until then had been waged between dynasties were turning into wars waged between nations' peoples. War is the act of states using armed force to contest one another. However, the phenomenon of war also changes as the relationship between society and the state and place of a state within the international system changes with the times. In the contemporary context, an important section of Clausewitz's considerations is that war is regarded as an extension of politics—in short, that military power is used as a tool of state policy. As Martin van Creveld points out, the premise behind this section is that the people, the army, and the government can be clearly distinguished. Creveld has labeled this "the trinitarian model of war[2]," but if this premise breaks down, then the nature of war will also change.

Such debate was stirred up by the end of the Cold War. The Cold War period was in which the two superpowers of the U.S. and the Soviet Union confronted one another with enormous nuclear capabilities, and had to live with the threat of human extinction caused by nuclear war. At its root was an ideological clash among states in which the people, the army and the government were clearly distinguished, well-suited for literal form of a trinitarian model of war. At the time, economic interdependence advanced among the Western countries themselves, but economic interdependence between East and West developed very little. With the end of the Cold War, "globalization" developed in a way that came to include the former East into the interdependence of the West. Furthermore, there was a time when it came to be thought that, given the Cold War's end was brought about by the collapse of the Eastern bloc, cooperation between the great powers would progress. For example, debates such as those over "cooperative security[3]" emerged aimed at great powers cooperating in dealing with issues of

[1] Carl von Clausewitz, *On War*, trans. Shimizu Takichi, Chūō Kōron Shinsha, 2001.

[2] Martin van Creveld, *The Transformation of War*, New York: The Free Press, 1991, pp. 35–42.

[3] Ashton B. Carter, William J. Perry, and John D. Steinbruner, *A New Concept of Cooperative Security*, Washington D.C.: Brookings Institution Press, 1992.

global security.

During this period, dealing with terrorist organizations was seen as an important issue. Cooperative responses to address Islamic extremism made progress, occasioned in particular by the 9/11 terrorist attacks in 2001. This can also be seen as a confrontation between state and non-state actors. Accordingly, it was also a conflict whose form differed from that of the trinitarian model of war. It is during this period that debates over war changing arose. For example, a concept called "fourth-generation warfare[4]" was presented at the time. This was based on the thinking that a new pattern of war was emerging because the premise of the trinitarian model of war, in which the state has a monopoly on military power, does not apply to non-state actors since the distinction between combatants and noncombatants is ambiguous and so is the distinction between peacetime and contingency.

However, beginning around 2010, antagonisms between great powers intensified once again. China repeatedly engaged in unilateral and aggressive actions in the South China Sea and East China Sea, worsening relations with neighboring countries and the U.S. In 2014, Russia unilaterally annexed the Crimean Peninsula, and naturally this worsened relations with the U.S. and Europe. In this way, as the view spread that the competition among great powers was revived, a military contingency in the Taiwan Straits came to be a concern in Asia, while in Europe the Russia–Ukraine war began in February 2022[5].

In this way, now not only has competition among great powers revived, but it has reached the point where wars that involve great powers are actually taking place. Should we really see this as a simple revival of wars based on a Clausewitzian trinitarian model of war? In this research project, we reached the conclusion that this is not a simple revival of that model of war, and that it was necessary to again come up with a new concept of war.

There are two main reasons for this. First, the Russia–Ukraine war is also being waged in dimensions other that of military power. In strategic theory, there is a term called "DIME," a word that stresses the importance of means other than military power. "D" stands for "diplomacy," "I" stands for "intelligence," "M" stands for "military," and "E" stands for "economy." In the Russia–Ukraine war, even after the outbreak of hostilities, DIME in its entirety has played a major role. First, there is diplomacy. For some time after the war's outbreak through early April 2022, ceasefire talks of course were held between Russia and Ukraine. However, not only did that take place, but Ukraine engaged in diplomacy to win the support of the U.S. and the European countries to put pressure on Russia. Russia likewise engaged in diplomacy to win China's support and strengthen its influence over former Soviet-bloc countries, as well as diplomacy meant to manage relations with the countries such as India that are referred to as the Global South. In the information arena, in the same way both sides

[4] Thomas X. Hammes, *The Sling and the Stone: On War in the 21st Century*, Voyageur Press, 2004.

[5] For an analysis of this war, please see Sugio Takahashi, ed. *Ukuraina sensō wa naze owaranai no ka: Dejitaru jidai no sōryokusen*, Bungeishunjuu, 2023.

are waging information campaigns to win the understanding of the international community, and Ukraine is conducting its operations based on intelligence on Russian intelligence gained from the U.S. and Europe. Military is obvious in this case. Regarding the economy, economic power naturally is also being used as a strategic means in such forms as economic sanctions against Russia and in the bargaining over energy supplies from Russia.

A war in which DIME in its entirety is involved this way has not really been seen in many post-Cold War conflicts. For the Western strategic community in particular, the interest has been biased toward military intervention in conflict areas by the "U.S. forces which possess an overwhelming military power." When it comes to the non-military aspects of a conflict, they meant the post-conflict recovery of those areas and stabilization operations toward that end. Also, Clausewitz argued that war is an extension of politics. This has been understood as expressing the view that, when a war begins military power in a sense becomes the principal tool, but that does not mean that destruction becomes its own goal but rather that they must be used in accordance with political goals.

However, what has been shown once again with the Russia–Ukraine war is that even after war has broken out, the three elements of DIME aside from the M have by no means lost their roles. Their roles have not even gone so far as to decline. These means have had the same importance as military power for achieving war goals. The progress of globalization is an important background element here. In a sense, this war can also be said to be the first war between great powers in the age in which globalization has advanced (Russia is a great power, of course, but Ukraine can also be said to be one in the sense that it has the second largest military force in the former Soviet Union). The web of economic interdependence includes countries at war with one another. The influence of the countries known as the Global South is also due to the economic growth that comes with the advances of globalization. Also, the impact of the Russia–Ukraine war that countries are feeling due to problems with grain and energy supplies are results of globalization.

Furthermore, the monopoly of states on military power is also breaking down. As analyzed in this research project, in the new domains states can no longer wield their military power without the cooperation of the private sector. In this view, we are no longer in a situation where the Clausewitzian model of war applies as is. This, too, is also one of the consequences of globalization.

In these ways, the Russia–Ukraine war demonstrates that war is changing greatly. In this research project, we investigated the relationship between new domains and deterrence. It is based on a critical awareness that a new concept of war was needed, in light of our thinking that the era from the time of Clausewitz's considerations through the Cold War was "War 1.0" and the era centered on "the war on terror" was "War 2.0." Then, backgrounded by globalization, we thought that war was changing qualitatively into something new, and we thought up the concept of "War 3.0" to give us a clue.

The change in war that the Russia–Ukraine war shows—in view of it being backgrounded by globalization—is likely a structural one and should be thought of as an important trend today. If so, a Taiwan Straits contingency or Korean Peninsula contingency will likely have similar characteristics. If it comes to that, Japan, too, will have to understand and digest this new concept of war. In this chapter, we will first sort out in a general way the distinctive features possessed by the new domains known as space and cyber.

## 2. The Staregic Premises Regarding New Domains

### (1) Strategic Environment

Here, we would first like to set out three presumptions along which we will advance our discussion. The first relates to the strategic environment. To engage in a discussion about deterrence is to think about "what" is being deterred and "by what." The present research project has as its theme the question of how various problems regarding deterrence will change in keeping with the increase in the importance of the so-called "new domains" of space and cyber, or how they will not change. Put another way, we can say that we will think about how "what" is being deterred (= goal) and "by what" it is being deterred (= means) are changing due to these new domains. Since the new domains are new technologies, it also means in a sense that we will also be thinking about how the phase of the problems that envelop deterrence will change due to the changes from technological trends actualized in the form of these new domains.

However, deterrence is a concept that supports the strategies of a state, while technology is nothing more than a means for the state's strategies. As the strategic environment itself changes, the nature of a threat changes. In short, the question "what" is being deterred changes. This change is one that occurs at an even more fundamental level than that of technological trends. This is clear if one simply reviews contemporary history. During the Cold War era, the "what" targeted for deterrence was nuclear war between the U.S. and the Soviet Union. That is to say, a full-scale war between states. However, from the 1990s to the start of the 21st century, when the Cold War ended and relations between great powers stabilized, particularly in Europe and the U.S. the object of deterrence was no longer seen as wars between states. Impacted by the terrorist attacks that took place in the U.S. on September 11, 2001, the question of how to deter terrorism due to Islamic extremism and so forth came to be thought of as the crucial problem.

The measures that need to be taken to deter a full-scale war between great powers accompanied by the use of nuclear weapons are considerably different from those to deter terrorism by a non-state actor. In that sense, what one must think about first when thinking about the nature of deterrence is "what" must be deterred as a strategic premise. Key to this point is that "competition among great powers" has revived in recent years due to such factors as the rise of China and Russia's resurgence, the worsening of U.S. relations with both those countries, and the strengthening of Sino–Russian relations. This became even more clear due to development in international politics surrounding Russia's invasion of Ukraine. With the revival of competition among great powers, deterring threats from states rather than non-state actors like terrorist organizations has once again become important. From this, we can say that the issue we should be thinking about with regard to deterrence in new domains as well fundamentally is deterrence of threats that originate from states.

### (2) The Patterns of Conflict

The second premise concerns the patterns of conflict. To speak of "competition among great powers" seems like something akin to the strategic environment of the Cold War period. However, today it is not enough to prepare only for full-scale wars between states as during the Cold War period. Even if antagonisms between states are the root cause, in reality there is a range in the actual patterns of conflict. For example, there were many debates in the U.S. during the 1990s around "information RMA," which forecast that military affairs would undergo revolutionary change due to the information revolution. The conflicts hypothesized at the time were large-scale Gulf War-type regular warfare. However, the conflicts that the U.S. actually had to deal with from the 2000s into the 2010s were the irregular warfare in Afghanistan and Iraq. One reason why the U.S. was forced to engage in bitterly fought struggles in Afghanistan and Iraq was because in this way its forecast about the pattern of conflicts it would have to deal with in the future was mistaken.

On this point, at the present stage it would be difficult to make forecasts of a narrowed-down sort. At present, there is the possibility of ongoing attempts being made that do not take on the forms of regular warfare, such as the attempts to change the status quo in the gray zone in the South China Sea and the East China Sea, and the hybrid warfare by Russia in which they attempted in former Soviet territories and succeeded the annexation of Crimea.

However, we cannot definitely state that future conflicts will be gray zone situations or hybrid warfare. Needless to say, the Russia–Ukraine war currently being fought is full-scale regular warfare. Should a Taiwan contingency or Korean Peninsula contingency by some chance occur, they would probably take on the form of large-scale regular warfare. Viewed this way, while we can forecast as a trend on a strategic level the continuation of competition among great powers, there is considerable uncertainty when it comes to the actual patterns of conflict. Since the ways in which the space and cyber domains are used in gray zone situations and hybrid warfare naturally differ from the ways they are used in large-scale conflicts, it will be necessary to take these two forms of conflict into consideration when constructing a concept of deterrence that includes new domains.

### (3) New Domains and Strategy

The third premise is "where" the goals for the state to implement security strategies are. In previous discussions around deterrence in new domains, a tendency has been observed to focus on the tactical situation and ignore questions such as "what are the political goals" and "what are the strategic premises" that are fundamental to strategic theory. For example, there is discourse that says "deterring attacks in space is difficult" and "deterring cyber attacks is difficult." The difficult-to-deter attacks spoken of here often refer to non-physical attacks such as the jamming targeting artificial satellites or low-intensity cyber attacks. However, deterrence against non-physical acts is difficult not only in the new domains but also in the existing physical domains as we know that even in the vicinity of Japan the Maritime SDF was targeted by fire control radars of China and South Korea in 2016 and 2018 respectively. Also, China and Russia's sporadic violations of air space are infringements of Japanese sovereignty, but they are difficult to deter. Similarly, the ongoing intrusions of Chinese government ships in territorial waters and contiguous zones around the Senkaku Islands are also difficult to deter.

Thus, deterrence against provocative behaviors in gray zones is difficult to begin with. This difficulty is not due to the characteristics of a domain—that is to say, on whether it is a new domain or an existing physical domain. Rather, we should think of it as the principles that have existed to date—deterring a low intensity challenge, a gray zone, is difficult—apply to the new domains as well.

The term "strategic context" is used here. Strategy is a concept that is widely used in international politics, but in reality defining it specifically is difficult. If one were to offer a definition in a form that could be broadly agreed on, it would be, "Strategy signifies a combination of "ends," "ways, and "means[6]." "Ends" refers to the state of affairs that one seeks to ultimately realize. "Means" refers to the specific actions themselves for accomplishing the ends and the tools necessary for those actions, while "ways" refers to how those specific actions and tools are combined and put to use. The "ends," "ways," and "means" are combined by the strategy. It logically and systemically lays what you want to achieve and how you will achieve it.

Regardless of whether a document in which it is stipulated has been settled upon or not, whatever the state it has a strategy that serves as the background to its security policy. Further, the "ends," "ways," and "means" are linked like a chain, and a strategy is formed in multilayered fashion. While lower-level strategies are the "means" for upper-level strategies, they have their own "ends," "ways," and "means."

What's important here is that it is necessary to distinguish between "ends," "ways," and "means" when thinking about strategy, and the "ways" and "means" form the roadmap for achieving the "ends." This is a basic but an important point when thinking about deterrence in new domains. The reason is because the ends for upper-level strategies in particular do not exist in outer space and cyberspace.

Humans still do not reside in outer space, nor do they exist in cyberspace. For that reason, acquiring specific coordinates in outer space or a specific territory in cyberspace (if the concept of territory in cyberspace existed) is never set as a strategic objective. If we consider

[6] For further details regarding the nature of strategy as a combination of "ends," "ways," and "means," please see Sugio Takahashi, *Gendai senryakuron: Taikokukankyōsō jidai no anzen hoshō*, Namiki shobō, 2022, pp. 18–24.

that China's highest priority strategic objective is Chinese unification, its strategic ends are an island called Taiwan that exists in physical space. Russia's present strategic ends in its invasion of Ukraine are Ukraine which also exists in physical space. In upper-level strategies at least, given that the strategic ends exist in physical space, the elements of space and cyber are not themselves "ends" ; rather, they are "ways" and "means" (strategic ends may be set in cyberspace in a lower-level strategy such as a cyber defense strategy).

If that is the case, whether space or cyber it will be combined with "power" that has effects in other traditional physical domains and used for achieving strategic "ends." In that sense, at the center of "power" in the new domains are its effect of amplifying physical capabilities like those of land, sea, and air power, and its effect of reducing the effectiveness of an opponent's physical capabilities. In that sense, it is precisely positioned as a force multiplier.

## 3. The Difficulties with responses in the Gray Zones that New Domains Produce

### (1) Issues for Law Enforcement Agencies

A distinctive characteristic of the new domains in the military field is that attacks not accompanied by physical destruction are possible. This may be a crucial point in particular to gray zones. The reason is because in a gray zone, the side challenging the status quo aims to change that status quo without wielding clear physical force. In that sense, new domains that are not accompanied by physical destruction can serve as extremely effective means.

In this respect, two important issues can be pointed out. One derives from the fact that at the center of responses in the gray zones are not military organizations but rather law enforcement agencies such as coast guard services (the Japan Coast Guard in Japan's case) and the police. Military organizations have long been aware that strengthening their capabilities in new domains like space and cyberspace is an important issue, and they maintain a critical awareness as they make a certain degree of progress in strengthening their capabilities. Law enforcement agencies, on the other hand, are not carrying out initiatives, at least not on the same level as military organizations. One of the roles of police is to deal with cyber crime. However, this is something they do to prevent crime in society. It is not an initiative that is being pursued based on a critical awareness that the police are continuing to operate in the gray zone.

This point is also the difficulty that derives from law enforcement agencies being called on to play a different role than their normal one in the gray zone. The role of law enforcement agencies basically is enforcing the law in order to maintain order at home. Crackdowns on various crimes take place in order to achieve this. However, in gray zones, the mission of law enforcement agencies is not to maintain domestic order, but rather to maintain their own country's sovereignty in conflicts with other countries over sovereignty. This was a role until now was thought of as one that military organizations would play.

However, it is difficult to exercise the right of self-defense and order in a military organization to protect sovereignty at any stage before a military organization on the challenging side has been ordered in—at a stage, for example, when disguised fishermen invade territorial waters or make an initial landing. At that stage, a law enforcement agency would deal with these disguised fishermen solely from the standpoint of enforcing Japanese law. However, if it's a case where those disguised fishermen are not engaged in simple illegal acts but rather are operating in Japanese territory with the intention of infringing on Japanese sovereignty with the clear political intentions of some country, then the actions that the law enforcement agencies shall take would have implications that they are done to protect Japan's sovereignty, rather than simply enforcing the law. This is exactly the role that the Japan Coast Guard are playing in the vicinity of the Senkaku Islands.

In this way, law enforcement agencies will be required to act in a gray zone in a fashion different from what was originally assumed. This fact complicates the problem of new domains in gray zones. This is because in the case of criminals at home that are the subjects that law enforcement agencies were originally intended to deal with, they cannot have capabilities of a sort that would significantly interfere with the use of outer space or cyberspace by national institutions such as law enforcement agencies. However, in a gray zone, because the opponent may be a state, there is the possibility that they can carry out large-scale interference in the new domains that would be inconceivable for an ordinary criminal.

For example, if China has engaged in large-scale GPS jamming in the vicinity of the Senkaku Islands, it becomes difficult for the Japan Coast Guard patrol boats on watch to determine their own positions. When that happens, precisely identifying territorial sea boundaries or the boundaries of the EEZ becomes difficult, and so does responding appropriately with respect to the actions of an opposite side.

### (2) Escalation that Includes New Domains

Furthermore, in gray zones, it is believed that micromanagement from the center will at times be necessary, owing to the need to delicately engage in escalation control. However, if it is able to carry out uplink jamming aimed at communications satellites and jamming directed at ground facilities and thus cut communications with the center, the Chinese side will naturally be able to achieve the advantage.

As noted earlier, generally speaking the abilities of law enforcement agencies to withstand jamming are weaker than military organizations. For that reason, there is the possibility that a non-physical attack in new domains in a gray zone launched against law enforcement agencies could have extremely significant effects. As will be discussed later, when a scenario game was played out over “the East China Sea gray zone” for the present research project, attacks against law enforcement agencies that used the new domains had an extremely large impact. Conversely, this also means that efforts to improve the resiliency of law enforcement agencies that use new domains must be pursued in a way that is on a different dimension from the past.

The second issue is, when projecting the process where there is escalation from a gray zone to armed conflict, how do the dynamics of escalation change or not change owing to the new domains being added in. This is a problem over the relationship between escalation in existing domains from gray zone to conflict and escalation in new domains including their nonphysical uses. Figuratively speaking, the question is, “Does the escalation ladder stand in the existing domains, or does it stand in the new domains?” This is a point that requires deepening analyses in light also of the fact that future combat conditions are difficult to forecast.

In particular, with respect to cyber attacks, given that one can imagine that physical attacks against important infrastructure may also be possible, the question of whether physical attacks will be launched using new domains in what way and with what timing during the process in which the situation escalates from a gray zone becomes an important issue in controlling escalation.

When reflecting on the distinctive characteristics of the new domains, we believe the following sort of hypothesis can be made in this point. First, in gray zones, the chances are great that non-physical uses of new domains will be frequent, in a fashion that is joined with attempts to change the status quo in the existing domains with the goal of establishing an advantage in the gray zone. Escalation will easily occur in the context of nonphysical uses in gray zones.

However, even in new domains, it is necessary to be prepared for yet greater risks even for the party disrupting the status quo in the event that a physical attack is carried out. This is because one can imagine in a case where, for example, physical damage is inflicted from a cyber attack, it is interpreted as an armed attack, the party preserving the status quo escalates its response, and a military organization instead of a law enforcement agency attempts to carry out its response on the gray zone concerned. If the likelihood of gaining an advantage in dealing with other law enforcement agencies is high, there will be no need to boldly carry out a physical attack of sort that would induce the opposing side to bring a military organization.

Also, as for malwares, it is very likely for them to be recognized and eliminated in their single usage. For that reason, putting the malware devised into operation at a time when it will have the maximum impact will be effective, and it is expected that timing will likely be the moment for taking decisive action in an existing domain.

Accordingly, it is believed the chances are high that escalation toward physical uses in new domains will be carried out in concert with escalation in the existing domains to maximize its impact. In this case, escalation in existing domains and escalation in new domains will be pursued concurrently. It is believed that in a gray zone, the physical uses of new domains by the party disrupting the status quo will be suppressed. However, it would seem that escalation that includes new domains will suddenly occur at the stage when one party decides to cause escalation from gray zone to conflict. We played a scenario game that hypothesized an “East China Sea gray zone” as part of this project, and we actually observed the phenomenon of escalation rapidly progressing at a certain stage[7].

[7] For an outline and the results of the scenario game, please refer to the materials at the end of the present report.

# Chapter 2

# Sorting Out Concepts in Deterrence and New Domains

Junichi Fukuda

## Introduction

In order to investigate "deterrence in the new domains," it is first necessary to organize concepts with respect to "deterrence" and "new domains." What we will handle in this chapter is that organization. We first offer a definition of deterrence, and then touch on those factors that make deterrence difficult. Next, we touch on escalation, which is a concept that is closely related to deterrence, and furthermore also sort out various concepts that while related to deterrence are distinct from it.

Following this sorting out of conceptions of deterrence, we organize concepts with respect to deterrence in the new domains. First, after offering a definition of "domain," we work out the distinction between the two natures of deterrence in the new domains: "intra-domain" deterrence and "cross-domain" deterrence. Next, we investigate the characteristics of the space domain and the cyber domain, and finally offer four initiatives as countermeasures projected for deterrence in the new domains.

## 1. What Is Deterrence?

### (1) Definitions of Deterrence

Many definitions for deterrence exist. The most classic definition is Thomas Schelling's "to turn aside or discourage through fear" and "to prevent from action by fear of consequences.[1]" For another definition, Alexander L. George and Richard Smoke have offered, "deterrence is simply the persuasion of one's opponent that the costs and/or risks of a given course of action he might take outweigh its benefits.[2]"

Furthermore, Lawrence Freedman defines it as "deliberate attempts to manipulate the behavior of others through conditional threats[3]," while Andrew F. Krepinevich, Jr. offers a more detailed definition: "Deterrence involves efforts to prevent a competitor (the object or "target") from pursuing a proscribed action. Those employing deterrence seek to influence the target's calculation of the costs, benefits, and risks associated with pursuing the proscribed action.[4]"

[1] Thomas C. Schelling, *Arms and Influence*, New Haven and London: Yale University Press, 1966, p. 71.

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

[3] Lawrence Freedman, *Deterrence*, Cambridge: Polity Press, 2004, p. 6.

[4] Andrew F. Krepinevich, Jr., *The Decline of Deterrence*, Hudson Institute, March 2019, p. 16.

Thus, there is great diversity in these definitions, but there seem to be a few fundamentally important elements to the concept of deterrence. First, the rationality of the opponent is presumed. This is because, so long as deterrence depends on the calculation of costs, benefits, and risks, a completely irrational actor is not capable of being deterred. Next, the existence of a deterrent that provides capabilities sufficient for achieving deterrence is also presumed. Theoretically, deterrence based on bluffs is not inconceivable, but if a deterrent is lacking then the possibility of deterrence failing is that much greater.

Furthermore, communication with one's opponent is also essential. Deterrence will not be achieved when the communication of intention, capabilities, and resolve is absent. Credibility of communication is also important. Communication without credibility will not be able to get the other party to change their conduct, leading to the failure of deterrence.

Krepinevich organizes in detail the conditions for realizing deterrence between states[5]. According to his work, (A) state A must communicate to state B that certain actions on the B's part (proscribed actions/actions that cross A's "redline") would trigger a response from A. (B) State B must clearly understand the actions proscribed by A and prospective consequences. (C) State B must believe State A will take the action it has threatened to take if its red line is crossed, and that it will produce the effects threatened by State A (A's threat must be very credible). (D) State B must believe that (due to deterrence by punishment) the prospective costs it will incur by crossing the red line will exceed its anticipated gains, or (due to deterrence by denial) State A's action will preclude State B from achieving its objective. (E) State B must act in a "rational" manner, meaning in such a way that it maximizes its prospective gains and/or minimizes its losses. Deterrence is finally realized when all of the above conditions are satisfied. Thus, generally speaking there are high hurdles when it comes to realizing deterrence. This is why deterrence often fails.

Next, the types of deterrence have been categorized in the following ways[6]. First, there is the distinction between narrow deterrence and broad deterrence. The former means deterring specific military actions during a war, while the latter refers to deterrence of the war in its entirety. Next, there is the distinction between central deterrence and extended deterrence. The former refers to deterring attacks on oneself, while the latter means deterring attacks on others (mainly one's allies). The credibility of the former is seen as high, but the latter often generates credibility problems. Furthermore, there is the distinction between deterrence by denial and deterrence by punishment. The former is deterrence through preventing the deterrence target from achieving their ends, while the latter entails imposing punitive costs on the deterrence target. Finally, there is the distinction between general deterrence and immediate deterrence. The former is deterrence in times of peace, while the latter is deterrence in times of crisis. However, there is the validity problem of whether a situation in

[5] Ibid., pp. 16–17.

[6] Freedman, *Deterrence*, pp. 32–42.

which general deterrence is effectuated should be taken up in the context of deterrence because it is unclear in the first place whether the challenging party has the intention to challenge. Accordingly, most of the discussions around deterrence take place in the context of immediate deterrence.

### (2) Factors That Make Deterrence Difficult

We hope to further delve into the factors that make realizing deterrence difficult. We can list the following five as leading factors.

First, there is the opposite party not being rational. There exists the view that human beings are not rational beings to begin with. There are problems from the start with realizing deterrence premised by rationality owing to cognitive biases, human stress in times of crisis, and the points suggested under the "prospect theory" and so forth. This can be identified as the skeptical theory of deterrence as taken from the perspective of cognitive psychology[7].

Next, there is the possibility that, while the opposite party might be a rational being, there is the possibility of misreading the fact that the premises behind their determinations of costs and risks may differ owing to differences in strategic culture and other areas. Rationality is not necessarily accompanied by universally shared understanding. There may also be cases where an action that appears irrational to one actor is rational to another actor. As a result, the failure of deterrence can occur due to falling into the "mirror-imaging" trap[8] based on the mistaken premise that "the opposite party and we are alike."

Third, one can conceive of the possibility that one might wind up relying on the mistaken premise that is the unified rational actor assumption of state hypothesis. Deterrence theory fundamentally takes the rationality of actors as its premise, but in reality a state is an aggregation of various organizations with many different preferences. Accordingly, the actions of a state do not imply that they exactly reflect the preferences of its decision makers. Therefore, if one is under the illusion that the actions of a state are the result of a rational choice, it will be difficult to present the message of deterrence. This is because in reality that may occur in ways that the decision makers did not intend. It will likely be necessary to keep in mind the perspectives of "Model II (organizational process)" or "Model III (bureaucratic politics)" identified in the *Essence of Decision*[9], a masterwork that analyzed the Cuban Missile Crisis.

Fourth, there is the possibility that credible signaling may become difficult owing to uncertainties in international relations and the motivations of states to mispresent their own

[7] For example, please refer to Robert Jervis, Richard Ned Lebow, and Janice Gross Stein, *Psychology and Deterrence*, Baltimore: Johns Hopkins University Press, 1985.

[8] Don Munton and David A. Welch, *The Cuban Missile Crisis: A Concise History*, 2nd ed., New York: Oxford University Press, 2011.

[9] Graham Allison and Philip Zelikow, *Essence of Decision: Explaining Cuban Missile Crisis*, 2nd ed., New York: Longman, 1999.

preferences. Wiping out uncertainty in international politics—extending to a state's capabilities, intentions, resolves, and actions—is not easy. The possibility of signaling not being delivered clearly to the opposite party cannot be denied[10]. Not only that, it has also been noted that a state that intends to gain the advantage in negotiations over another one has the motivation to misrepresent their own preferences[11]. The possibility that the other party is bluffing despite not being resolved to deter cannot be excluded, and there may be risks that this will result in the failure of deterrence. Whatever the case, the concern exists that highly credible signaling of deterrence will become impaired.

Finally, it is possible that the emergence of new technologies and the involvement of non-state actors will complicate the state of deterrence. There are concerns that the entry of new technologies would expand the dimensions of war and change the balance between offense and defense, and also shorten the time required for making decisions about deterrence[12]. Typical examples of this include the entry of ballistic missiles equipped with strategic nuclear weapons and their development into multiple independently targetable reentry vehicles (MIRV). It can also be pointed out that a state using a non-state actor as its proxy creates an attribution problem where the attacker is difficult to be identified. This is particularly conspicuous in the cyber domain, and it is a problem that is directly related to our investigation of "deterrence in the new domains."

Whatever the case, the realization of deterrence is not an easy task owing to the complex effects of these various factors.

### (3) A Closely Related Concept: Escalation

Next, we touch on escalation as a concept that is closely related to deterrence. Escalation has been defined as "an increase in the intensity or scope of conflict that crosses threshold(s) considered significant by one or more of the participants." At the same, it has also been noted that this kind of escalation occurs "only when at least one of the parties involved believes that there has been a significant qualitative change in the conflict as a result of the new development[13]." Escalation of this sort can arise as the result of a deliberate policy as well as by accident.

To speak of its relationship with deterrence, while deterrence is an effort to prevent an

[10] The foremost example of the consequences of uncertainty in international politics is the "security dilemma," wherein actions taken to increase the security of one's own country are seen as threats by other countries resulting instead in the security of one's own country being harmed. Robert Jervis, "Cooperation under the Security Dilemma," *World Politics*, Vol. 30, No. 2, January 1978, pp. 167–214.

[11] James D. Fearon, "Rationalist Explanation for War," *International Organization*, Vol. 49, No. 3, Summer 1995, pp. 379–414.

[12] To be precise, changes in not only technology but also doctrines and the posture and deployment of armed forces have the same impact. Stephen Van Evera, "Offense, Defense, and the Causes of War," *International Security*, Vol. 22, No. 4, Spring 1998, pp. 66–68.

[13] Forrest E. Morgan, et al., *Dangerous Thresholds: Managing Escalation in the 21st Century*, RAND Corporation, 2008, p. 8.

opposite party from exceeding certain behaviors (redlines/thresholds), there can be multiple redlines/thresholds. Preventing the next line from being breached even after the first one has broken down is important to efforts at deterrence, which is escalation control (or management). It may be said that escalation control sits as an extension of deterrence.

However, escalation control does not simply refer to easing escalation. In order to prevent escalation by an opposite party, a nation would also need to display intentions, capabilities, and resolves capable of implementing escalation to an extent that the opposite party cannot catch up. For this reason, intentional escalation may be pursued in some cases that is meant to achieve escalation dominance. For a recent example, there is the “escalate to de-escalate” strategy[14] that Russia is said to be employing.

Escalation is regarded as comprising the following three types. First is vertical escalation, where the intensity of a conflict increases. Second is horizontal escalation, in which the geographic scope of a conflict expands. Third is compounding escalation, in which new crises and conflicts are added on to existing conflicts due to attacks and the like on allied countries.

The concept of escalation as something that has accumulated particularly in vertical threshold has been referred to as the escalation ladder. The stages sandwiched between each escalation threshold are referred to as “rungs,” and that which groups them together to some degree are referred to as “units.” Herman Kahn, who proposed this concept of escalation, hypothesized in a 1965 work that there would be an escalation ladder for a thermonuclear war between the U.S. and the Soviet Union. He hypothesized it as comprising seven units and forty-four rungs ranging from “ostensible crisis” to “spasm or insensate war (= all-out thermonuclear war)[15].”

Kahn’s concept of an escalation ladder reflected the spirit of the times. It emphasized that controlling escalation was important even in a nuclear war in that twenty-four rungs would still remain after the use of nuclear weapons by the U.S. or the Soviet Union. However, it seems that for the escalation ladder of today, the stage of armed conflict for conventional armed forces and the stage just prior to armed conflict (in a gray zone situation, meaning just below an armed attack as defined by international law) are seen as important. On this point, it may be said that the issue is how to apply the thinking behind an “escalation ladder” to today’s strategic environment[16].

However, the diversification of operational domains noted below is an important challenge to the escalation ladder concept. This is because armed conflict today does not seem likely to take on simple (vertically) layered threshold form hypothesized by the classic escalation ladder. Escalation in the era of the Multi-Domain Operation is thought of as inevitably following a

[14] Nikolai N. Sokov, “Why Russia calls a limited nuclear strike ‘de-escalation’,” *Bulletin of the Atomic Scientists*, March 13, 2014.

[15] Herman Kahn, *On Escalation: Metaphors and Scenarios*, New York: Praeger, 1965, p. 39.

[16] Another important issue in regard to the escalation ladder is whether or not there is a shared understanding between the parties.

meandering course, straddling multiple domains[17]. This is because escalation in one domain is thought to trigger escalation in another domain, and an escalation ladder is built in a form where they have complex interactive effects on one another. Some studies conceptualize such an escalation ladder not as a ladder but rather as a lattice[18]. This view holds that rather than grasping the process of escalation as a vertical ladder, it would be better conceptualized as a lattice where longitudinal intensity escalation and latitudinal cross-domain escalation coexist. Another theorist proposes the concept of wormhole escalation, in which escalation today takes on an accelerated and non-linear form and follows a path that is difficult to predict[19].

While it is hard to say that such theories have established concepts that will replace the existing one of the ladder, it seems that the efforts to revise the escalation ladder concept in ways that make it suited to the age of multi-domain operations will continue.

### (4) Concepts Closely Related to But Distinct from Deterrence

Next, we will sort through concepts that are closely related to deterrence but are distinct from it.

The first to be taken up is compellence. According to Schelling, in contrast to deterrence with its goal of getting the opposite party to not take a specific action, the goal of compellence is to get the opposite party to take a specific action[20]. The hurdles to be crossed in realizing it are seen as higher than those for deterrence in that one is not simply preventing the opposite party's actions but rather compelling them to actively do something. The two concepts tend to be confused, but logically the distinction is necessary.

Next, defense is a military action with an actual opponent that takes place after deterrence fails. In the context of nuclear strategy, it is also called war-fighting. Deterrence and defense are concepts that should be distinguished from one another. However, it is not easy to distinguish between defense and escalation control efforts particularly in the context of deterrence by denial. The difference is nothing more than whether you are simply stopping an opponent from achieving their ends, or you are preventing further escalation by presenting the stance that you will stop them from achieving their ends.

Next is the status quo. Deterrence is the effort to prevent the actions of an opponent trying to change the status quo, but the concept of "status quo" may differ among the parties involved. To give a specific example, the defense of Taiwan by the U.S. prevents a change to the status quo by China but viewed from China the intervention of the U.S. trying to prevent the

[17] King Mallory, "New Challenges in Cross-domain Deterrence," RAND Corporation, 2019, p. 7, Figure 2.

[18] Martin Libicki and Olesya Tkacheva, "Cyber Escalation: Ladder or Lattice?" in Floyd A. Ertan and Stevens T. Pernik, eds., *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, NATO Cooperative Cyber Defense Centre of Excellence, 2020, pp. 60–72.

[19] Rebecca Hersman, "Wormhole Escalation in the New Nuclear Age," Texas National Security Review, Vol. 3, Issue 3, Autumn 2020, pp. 90–109.

[20] Schelling, *Arms and Influence*, p. 69.

unification of China and Taiwan seems to threaten the “status quo.” The concept of status quo can be seen as related to the concept of reference point in “prospect theory[21]” , but when discussing deterrence, the important matter is to grasp what the “status quo” is for who.

Furthermore, there is a concept of dissuasion. This concept was emphasized in 2001 by the U.S. in its Quadrennial Defense Review 2001 (QDR2001). It has been described as, “To discourage others from developing capabilities and/or adopting courses of action that are hostile to the interests of the United States[22].” Initiatives to dissuade are also positioned as pre-deterrence initiatives that come before deterrence. However, this concept is little used today, when the structural outline of strategic competition between great powers has become clear.

Additionally, we have strategic stability. This concept historically has been used in the context of nuclear deterrence between the U.S. and the Soviet Union (the U.S. and Russia). It has been defined as, “[A] situation in which no party has an incentive to use nuclear weapons save for vindication of its vital interests in extreme circumstances[23].” However, this concept has bundled together several concepts, including first-strike stability, crisis stability, and furthermore arms control stability. Its specific mode tends to be interpreted in politically quite varied ways depending on the parties involved. Today, this concept is frequently used in the context of how existing strategic stability is damaged by the impact of missile defense and hypersonic weapons, strategic weapons not restricted by existing arms control treaties, and nuclear multipolarization. Essentially, it is a concept with an affinity to arms control initiatives.

In this connection, another important concept is the stability-instability paradox[24]. This concept presents the paradox that the stability at the level of strategic nuclear forces heightens the possibility of deterrence failure and escalation in the lower levels. That stability exists at the level of strategic nuclear forces means that even if there are actions that bring about deterrence failure or escalation at a lower level, the chances of that developing into a confrontation at the strategic nuclear force level are low. For that reason, stability at the strategic nuclear force level may actually bring about deterrence failure or escalation at a lower level. This paradox is drawing particular attention today in the context of stability at the strategic nuclear force level between the U.S. and Russia, and the U.S. and China, being connected to potential conflicts occurring in Europe and the Indo-Pacific region[25].

[21] Prospect theory is a psychological theory that explains why people fear losing more than winning. A reference point refers to this turning point that separates gains from losses for the actor. Daniel Kahneman and Amos Tversky, “Prospect Theory: An Analysis of Decision under Risk,” *Econometrica*, Vol. 47, No. 2, March 1979, pp. 263–292.

[22] Ryan Henry, “Deterrence and Dissuasion for the 21st Century,” IFPA-Fletcher Conference, December 14, 2005.

[23] Elbridge A. Colby and Michael S. Gerson, eds., *Strategic Stability: Contending Interpretations*, Strategic Studies Institute and U.S. Army War College Press, 2013, p. 55.

[24] Glenn H. Snyder, “The Balance of Power and the Balance of Terror,” in Paul Seabury, ed., *The Balance of Power*, Scranton: Chandler, 1965, pp. 185–201.

[25] The full-scale Russian invasion of Ukraine that began on February 24, 2022, can also be interpreted as having occurred with stability between the U.S. and Russia on the level of strategic nuclear forces forming

Further, there is re-assurance. While deterrence is a concept related to "credible signaling of threat" over crossing a line, in reality sending "credible signaling of cooperation" —i.e., that if the opposite party turns to cooperation, then our side, too, will respond with cooperation—is also important in the context of de-escalation. This can also be interpreted as a pledge that, in keeping with the opposite party turning to cooperation, there will be no taking of aggressive actions on our part. This is re-assurance, which is defined as a "process of building trust," and is a concept related to "convincing the other side that you prefer to reciprocate cooperation, so that it is safe for them to cooperate[26]." However, logically it is difficult to convey credible signaling of deterrence while simultaneously conveying credible signaling of re-assurance.

Finally, we have arms control, confidence building, and the formation of codes of conduct. These can be interpreted as efforts undertaken with the ends of setting up certain restrictions on the capabilities or actions of states so that the aforementioned strategic stability or stability of some form for the parties involved is not damaged. Such efforts may sometimes run counter to deterrence initiatives, but at the same time they can be described as concepts closely related to deterrence since deterrence failure between the parties involved is less likely to occur when there is solid arms control, confidence building, and the formation of codes of conduct.

## 2. What Is Deterrence in the New Domains?

### (1) Definitions of Domain

War traditionally has been seen as being fought in the three domains of land, sea, and air. However today, the domains of war are expanding in a fashion not restricted to these three domains. The domains that have come to be newly regarded as domains for war and operations are referred to in contrast to the traditional domains of land, sea, and air as the "new domains."

However, the definition of "domain" is not always clear. For a broad definition, there is, for example, "any pathway or means for coercion that is different from other means in respect to its utility for political bargaining." According to this, the concept of a domain "describe a discrete territory with clearly delineated boundaries, a legal or bureaucratic jurisdiction, an assertion of ownership, a division of labor, or an area of technical expertise[27]." This is a view that defines domain broadly from the perspective of coercion (which includes both deterrence

part of its background. This is because, so long as the U.S. fears nuclear war with Russia and fixates on maintaining strategic stability, acts of aggression against Ukraine are possible at levels lower than the strategic nuclear one without Russia worrying about nuclear war with the U.S. Junichi Fukuda, "Dai 2 shō: Roshia, Ukuraina sensō—Sono yokushi hatan kara Taiwan kaikyō yūji ni nani o manaberu no ka." In Sugio Takahashi, ed., *Ukuraina sensō wa naze owaranai no ka: Dejitaru jidai no sōryokusen*. Bungeishunju, 2023, pp. 77–81.

[26] Andrew H. Kydd, *Trust and Mistrust in International Relations*, Princeton: Princeton University Press, 2005, p. 184.

[27] Jon R. Lindsay and Erik Gartzke, "Introduction: Cross-domain Deterrence, from Practice to Theory," in Jon R. Lindsay and Erik Gartzke, eds, *Cross-domain Deterrence: Strategy in an Era of Complexity*, Oxford: Oxford University Press, 2019, p. 16.

and compellence[28]) and takes into its field of view not only the field of military affairs but also that of non-military matters.

Specifically, in this view, non-military matters such as politics, economics, diplomacy, finance, the judicature, and so forth are seen as domains where the government broadly exercises coercive power on another party. This view has affinities both with China's "unrestricted warfare" view, in which all the actions of a state regardless of boundaries between military and non-military affairs are means of war[29], and with DIME thinking, which sees it necessary to combine a variety of elements including diplomacy, intelligence, military, and economy when thinking about the security of the state.

On the other hand, there is also a more restricted way of viewing domains that focuses on military affairs. This is the definition that it is the "Critical macro maneuver space whose access or control is vital to the freedom of action and superiority required by the mission[30]." This definition sets its focus more on military multi-domain operations (MDOs) and is one that is close to the interpretation of domain by the world's military organizations. It would seem close to the concept of domain when Japan's Ministry of Defense and SDF talk about "new domains."

Specifically, most military organizations around the world tend to regard the three domains of land, sea, and air as existing or traditional domains, and have a strong tendency to treat the "space" and "cyber" (and "electromagnetic") domains as new domains that have now become of vital importance for gaining advantage in military operations. This is because a loss of superiority in these domains is thought to be fatal owing to the deeper dependence on these domains in the execution of military operations today. For this reason, the execution of military operations today as MDOs that necessarily include the space and cyber (electromagnetic) domains is becoming the basic premise.

The Ministry of Defense and the SDF treat the three domains of "space (uchū)," "cyber (saibā)," and "electromagnetic (denjiha)" as the "new domains[31]," and hence also refer to them as "USADEN." However, there is no need to think in a fixed way about how to classify domains or new domains. This is because the concept of new domains always leaves room for expansion. For example, in recent years, the idea of a "cognitive" domain that overlaps with but is not limited to the cyber domain has also been adopted[32]. It is a way to position the manipulation of

[28] Schelling interprets coercion in this way. Schelling, *Arms and Influence*, p. 71.

[29] Qiao Liang and Wang Xiangsui, *Chogensen 21 seki no "atarashii sensō*, Kadokawa, 2020.

[30] Jeff Reilly, "OTH Video: Beyond the Theory – A Framework for Multi-Domain Operations," *Over the Horizon*, April 13, 2018.
https://overthehorizonmdos.wpcomstaging.com/2018/04/13/oth-video-beyond-the-theory-a-framework-for-multi-domain-operations/

[31] Ministry of Defense and Self-Defense Forces, "Heisei 31-nendo ikō ni kakaru bōei keikaku no taikō ni tsuite," December 18, 2018, pp. 17–19.

[32] Paul Ottewell, "Defining the Cognitive Domain," *Over the Horizon*, December 7, 2020.
https://overthehorizonmdos.wpcomstaging.com/2020/12/07/defining-the-cognitive-domain/

people's cognition through information manipulation and influence operation and the countermeasures to such acts as a new domain of war and strategy.

### (2) "Intra-domain" Deterrence and "Cross-domain" Deterrence

Next, we will sort out the distinction between "intra-domain" deterrence and "cross-domain" deterrence. Even the single phrase "deterrence in the new domains" can have two different meanings. Therefore, it is necessary to distinguish between intra-domain deterrence and cross-domain deterrence.

First, intra-domain deterrence is the issue about how to deter an attack on the inside of that domain. Thinking about the space and cyber domains, the focus becomes how to deter attacks within these domains, and attacks on assets which are essential to maintaining activities and functions in these domains. To give some typical examples, in the space domain the issue is dealing with attacks on satellites in orbit, attacks on space-related facilities on the ground, and attacks on the communications that connect these. In the cyber domain, the issue is dealing with attacks on the crucial infrastructure's SCADA (supervisory control and data acquisition) systems, attacks related to maintaining the functionality of widespread networks, and physical attacks on servers and submarine cable landing stations. While cross-domain deterrence to be discussed below is effective as a countermeasure against these attacks (as means of deterrence), when it comes to intra-domain deterrence, working to improve resilience (discussed below) and working on initiatives for deterrence by denial or defense are also effective. Accordingly, when we think about "deterrence in the new domains", intra-domain deterrence becomes one perspective.

Next, cross-domain deterrence is the issue about how to realize deterrence in a way that crosses other domains. Attacks are not something carried out in a form of being restricted to a specific domain in the first place. Attacks on the space and cyber domains, too, are likely to be carried out in the pursuit of larger political and strategic objectives that go beyond a specific domain. Accordingly, even if there was an attack that might be restricted to a specific domain, it would be natural to think that all domains will be used to deter and defend against it. Looking at the examples of past wars that were carried out only in the traditional domains, countering attacks on land with superiority at sea or pursuing the reverse was common. The important issue here is the pursuit of political and strategic objectives; it may be said that the use of a domain is nothing more than means toward that end. In terms of crossings between traditional domains and new domains, one can offer such possibilities as deterring an attack against a new domain with the suggestion of a counterattack in a traditional domain or deterring an attack against a traditional domain by using capabilities in a new domain. Whatever the case, it would be no exaggeration to say that we should treat all deterrence above all at the strategic level as cross-domain deterrence.

### (3) Characteristics of the New Domains: Space

Next, we want to make a general survey regarding the characteristics of the new domains. In this chapter and throughout the present report, we basically interpret “new domains” with both the space domain and the cyber domain in mind, but first we shall consider the space domain.

Although the space domain has been called a new domain, its military use has actually been going on since the Cold War era. The military use of space is not a new concept. However, the form of the uses of space has greatly changed between then and now. The use of space during the Cold War era was characterized by, the dearth of commercial uses, and the leading actors being limited to the U.S. and the Soviet Union. While we say military uses, generally the uses were related to strategic nuclear deterrence, and the means for attacks in space were limited. With respect to these past uses of space, we can call this, say, “the First Space Age.”

In contrast, the situation today has fundamentally changed. Specifically, (A) uses by the private sector have expanded; (B) many state and non-state actors are mixed together; (C) the dependence of military action on outer space is growing at both the tactical and operational levels; and furthermore (D) various means of attack both kinetic and non-kinetic have emerged. We can call this “the Second Space Age.” It has been pointed out that, as a result, the situation in the space domain has become more diverse, disruptive, disordered, and dangerous[33]. It is an age in which, of necessity, a reinvestigation must take place with regards to deterrence and escalation control in the space domain.

Generally speaking, the space domain is thought to have the following characteristics. First is the difficulty of situational awareness. Outer space is extremely vast and remote, and since human access is not easy, constant situational awareness of what is happening there is often difficult. As a result, grasping whether an attack has actually taken place and determining its cause is difficult. Second, defense is difficult. Outer space assets (satellites, etc.) cannot be equipped with heavy armor due to the launch cost problem, and they are vulnerable to attack. Furthermore, repairing (restoring functionality) after an attack is also difficult, and they are likely to lose functionality. Third, the threshold for attack is low. Due to the difficulties with situational awareness, determining whether or not there has been an attack and who is the attacker is difficult in the space domain. Also, given that there are hardly any humans in orbit, together with the fact that direct loss of human life is unlikely to occur, the threshold for attack is thought to be low.

Fourth is the fact that diverse actors are mixed together. As the active parties grow more and more diverse, both attacks by states and attacks by non-state actors are conceivable. It is the same for the side that is attacked. The possibility of an attack by a state actor in the disguise of a non-state actor is also conceivable. Finally, there is a fact that codes of conduct is

[33] Todd Harrison, et al, *Escalation & Deterrence in the Second Nuclear Age*, Center for Strategic and International Studies, October 3, 2017, p. 5.

absent in the space domain. While there are some controls in space like the Outer Space Treaty, which bans the deployment of weapons of mass destruction in outer space, it is not fully adequate as codes of conduct. We can say that the setting of rules remains insufficient.

As a result, in the Second Space Age of today, the space domain can be said to have the characteristic of being susceptible to becoming offense-dominant, and deterrence failure can easily occur.

### (4) Characteristics of the New Domains: Cyber

It can be pointed out that the cyber domain has characteristics that resemble those of the space domain. The history of the cyber domain (internet) can be traced back to the birth of ARPANET at the end of the 1960s. Back then, there were no problems with its operations that were based on goodwill among a limited number of researchers. However, with public use of the internet progressing from the 1990s onward, problems related to the operation of the cyber domain based on factors as "openness," "decentralized authority," "anonymity," and "credibility" rose to the surface through frequent cyber attacks.

Like the space domain or perhaps even more so, the present state of affairs in the cyber domain is one where (A) the distinction between the private and the military is mixed; (B) a variety of actors including both state and non-state actors are present; (C) the dependence of military operations on the cyber domain is extremely large; and (D) cyber attacks (or cyber intrusions) in various forms are becoming common. For this reason, it may be pointed out that the importance of deterrence and escalation control in the cyber domain is growing. Above all, preventing attacks on military command and control (C2) systems and on critical infrastructure including one in the private sector coming to be of vital importance.

The characteristics of the cyber domain are thought to resemble those of the space domain. First, situational awareness is difficult. Cyber attacks generally go hand in hand with intrusions (Computer Network Exploitation, CNE) as a preliminary step, so that their detection is difficult and assessing damage is also not easy. Additionally, there is the attribution issue, in that the origins of the attacker are difficult to be identified. Second, defense is difficult. Enhancing defenses in advance is difficult because of such developments as network intrusions that go unnoticed and bots (malware) getting planted, or being hit by a zero-day attack in which an unknown vulnerability is abruptly cracked[34]. Third, the threshold of attack is low. The threshold for attack is thought to be low because it is possible for even an individual to carry out an attack if they have knowledge about cyber attacks and an inexpensive system, and because attacks can be made at low cost without requiring large investments. Fourth is that

[34] However, in the case of malware attacks, if the attacker puts the effect into operation once, countermeasures will be taken at an early stage by the defender, rendering it ineffective. Accordingly, in the cyber domain, an attacker will always need to continue probing for vulnerabilities unknown to the defender. Also, since by its nature malware can be expected to produce effects only once, the possibility cannot be denied that when it is used dramatic escalation linked to other domains may occur.

diverse actors are mixed together. Since state actors and non-state actors coexist in the world of the internet, and as noted above it is not easy to resolve the issue of attribution, it is easy for state actors to pose as non-state actors or vice-versa. Fifth is the absence of codes of conduct. Codes of conduct are even more lacking than in the space domain in the non-physical space such as the cyber domain. As a result, institutional checks on infringement activities do not operate well.

Based on the reasons above, we can sum the situation up as, just like the space domain, the cyber domain is susceptible to becoming offense-dominant and deterrence failures are also likely to occur.

## 3. Deterrence in New Domains: Hypothetical Countermeasures

Finally, we would like to summarize the four countermeasures that may be hypothesized in the context of deterrence in the new domains, which have the aforementioned characteristics (= offense-dominant, with deterrence failures likely to occur).

The first hypothetical countermeasure is improvements in situational awareness capabilities. First, if "what is happening" in the domain concerned cannot be assessed, then far from deterrence it will not be possible to even notice that it has failed. Specifically, the need is to improve situational awareness in peace time (surveillance of orbital debris and satellites/monitoring network intrusions, etc.), and to make it possible to identify causes when some malfunction has occurred (was it an accident or a simple breakdown, or a hostile attack). Furthermore, being able to identify an attacker when a hostile attack has been identified (solving the attribution issue) and to make a battle damage assessment (BDA) when carrying out a counterattack would be desirable.

The second is improvements in resilience (as deterrence by denial). What is desired is the guarantee of "mission assurance" in the sense that even if there has been an attack, systems will not reach the point of critical malfunction. This is an initiative that stresses preventing the realization of ends of the opposite party who is attempting to cause a system to malfunction. Specifically, to give examples in the space domain, these would include efforts to try to not allow a partial loss of functionality to lead to a loss of functionality for an entire system (constructing a constellation of small satellites, etc.), or the capability to rapidly restore it when a loss of functionality has occurred (rapid re-launch capabilities, etc.). The countermeasure for the cyber domain is similar to this.

The third is possessing attack (or counterattack) capabilities (as forms of deterrence by denial or deterrence by punishment). The attacking side would be dominant when it comes to the balance between offense and defense in the new domains. If that is the case, then the options for the deterring side are to build up their own attack (or counterattack) capabilities, and find a way of deterrence through demonstrating these capabilities which can put the opponent's means of attack and the values that they attach importance at risk. Specifically, one can conceive of intra-domain attacks or counterattacks that would neutralize the opponent's space assets or network capabilities, or cross-domain attacks or counterattacks using the attack means from other domain (a counterattack using nuclear or conventional armed forces in response to an attack in the space or cyber domain).

Fourth, while they are not deterrence, it is possible to list up initiatives such as arms control, confidence building, and the formation of codes of conduct. While it is not easy to make such attempt among states which need initiatives toward deterrence, ultimately being able to build stable relations through such initiatives among states and between states and non-state actors without depending excessively on deterrence is desirable. However, based on the experience of the U.S.–Soviet Cold War, without the shared experience of a major crisis like the Cuban Missile Crisis, the possibility is great that achieving arms control, confidence building, and the formation of codes of conduct among great powers that are in competitive relationships will be difficult.

## Conclusion

In order to investigate "deterrence in the new domains," in this chapter we have organized concepts with respect to "deterrence" and "new domains." Based on this, we have surveyed the offense-dominant characteristics of the new domains—the space domain and the cyber domain—and presented four hypothetical countermeasures for deterrence in those new domains.

Deterrence by nature is something that often fails due to the difficulty of the conditions for realizing it. If we consider the offense-dominant characteristics of the new domains and the problems with the effectiveness of the escalation ladder concept in the age of the multi-domain operation, there is no mistaking that realizing deterrence in the new domains is further more difficult.

However, as pointed out in Chapter 1, we who are directly confronted with this era of War 3.0 are living in an age in which we have to face up to these difficulties. We would be pleased if the discussion in this chapter and the present report can contribute to overcoming these difficulties.

# Chapter 3

# The Pursuit of Deterrence in Space and the Importance of Resilience and Protection

**Yasuhito Fukushima**

## Introduction

Space deterrence has two aspects[1]. One is "space in deterrence." It refers to the roles played by space systems and offensive counterspace capabilities when deterring attacks on one's own country and the like[2]. The other is "deterrence in space," which refers to deterrence against attacks on space systems[3]. This article considers the relationship between space and deterrence, focusing on "deterrence in space."

Space systems do not necessarily refer only to artificial satellites in orbit. A space system is comprised of three segments: (1) the space segment, which is an artificial object in orbit such as a satellite; (2) the ground segment, including user terminals and the facilities that control the satellite; and (3) the link segment that refers to the signals exchanged between the space segment and the ground segment, etc.[4] Together, these segments function as a space system when they all operate correctly. Understanding this point is the premise for thinking about "deterrence in space."

At present, the primary military functions that space systems provide are (1) intelligence, surveillance, and reconnaissance (ISR); (2) communications; (3) positioning, navigation, and timing (PNT); (4) missile warning; and (5) environmental monitoring (weather observation, etc.)[5]. These functions support the operations of nuclear and conventional forces on Earth[6].

[1] James P. Finch and Shawn Steene, "Finding Space in Deterrence: Toward a General Framework for 'Space Deterrence'," *Strategic Studies Quarterly*, Vol. 5, Issue 4, Winter 2011, pp. 12–13. https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-05_Issue-4/FinchSteene.pdf

[2] Offensive counterspace capabilities of the co-orbital type are also space systems.

[3] These two aspects are closely related. Strengthening deterrence overall is linked to deterrence against attacks on space systems. Deterring attacks against space systems is also vital in enhancing deterrence overall.

[4] Currently, the link segment comprises mainly the downlink (the signal from the space segment to the ground segment) and the uplink (the signal from the ground segment to the space segment). However, the use of the cross-link (the signals exchanged among satellites in the space segment) is beginning to spread.

[5] Aside from these, space systems are being used for space domain awareness and so forth.

[6] Strictly speaking, the functions that space systems offer are also being used for the operation of space systems. For example, space-based PNT services are used to determine the position of satellites. In this case, the user terminals installed on satellites correspond to the space segment rather than the ground segment.

While the concept of space deterrence is not new, thinking about the relationship between space and deterrence is becoming increasingly critical worldwide. This is, first, because the role of space systems in deterrence overall is becoming larger as the value of space systems increases, including for the operations of not only nuclear but also conventional forces. The second context in which the significance of considering the relationship between space and deterrence is growing is the rise in the importance of deterring attacks on space systems, as the military roles of such systems are expanding[7]. The impact on military power and deterrents caused by hindrances in the use of space systems is becoming more acute.

In relation to this, there is a growing number of countries that are researching, developing, and possessing offensive counterspace capabilities, and the risk of space systems actually being attacked is increasing. Offensive counterspace capabilities are mainly classified as (1) direct-ascent, (2) co-orbital, (3) directed energy, (4) electronic warfare, and (5) cyber[8]. (1) is a weapon that destroys a satellite with the direct hit of an interceptor loaded on a missile launched from a land, sea, or air platform. (2) is a weapon that, once put into orbit, draws close to the target satellite and attacks it using destructive or non-destructive means. (3) is a weapon that uses directed energy such as lasers, particles, or microwaves to interfere with or destroy space systems. (4) is a weapon that interferes with communications with satellites using radio frequency energy. (5) is a weapon that uses software and network-related technologies to intrude into computer systems or interfere with and destroy such systems.

It is crucial that Japan gives thought to the relationship between space and deterrence. Not only is Japan expanding its use of space for defense purposes, but the Ministry of Defense now has its own satellites. The ministry launched one X-band defense communications satellite in 2017 and another in 2018, and it planned to launch a third in fiscal year 2023. These are the first satellites possessed by the Ministry of Defense[9]. The ministry also plans to launch a satellite for space domain awareness by fiscal year 2026 and construct a satellite constellation for intelligence, surveillance, reconnaissance, and targeting (ISRT). The situation is such that the role that space systems play in unit operations of Self-Defense Forces is increasing, and Japan has to think about how to deter attacks against these space systems[10]. Above all, the National Security Strategy approved by the Cabinet at the end of 2022 indicated that counter-strike capabilities that employ stand-off defense capabilities and so forth would be the key to

[7] Additionally, the role of space systems in economic and social activities is growing worldwide. Weather forecasts, broadcasts, and PNT, all of which use space systems, are deeply embedded in everyday life. It is also possible that mobile telephone use of satellite transmission will become more common in the future. Based on this, the significance of deterring attacks on space systems used for economic and social activities is increasing.

[8] Secure World Foundation, *Global Counterspace Capabilities: An Open Source Assessment*, April 2023, p. xxxvi. https://swfound.org/counterspace/

[9] Control of these satellites was outsourced to private companies through the private finance initiative.

[10] Setsuko Aoki has pointed out the need for Japan to prepare for deterrence in space and its response if deterrence fails. Research Institute for Peace and Security, "RIPS shūki kōkai seminā 2019: Uchū no anzen hoshō to Nihon no yakuwari," October 7, 2019. https://www.rips.or.jp/symposium/2066/

deterring an invasion against Japan[11]. Deterring attacks on the satellite constellation that provides ISRT essential to operating counter-strike capabilities is likely to be a critical issue.

This paper is organized into the following three sections. The first section will review the historical background from the Cold War period to the present of the relationship between space and deterrence. The second section will examine the relationship between space and deterrence using the example of Russia's full-out invasion of Ukraine that began in February 2022 and Ukraine's resistance to it (referred to below as the Russia–Ukraine war). The third section, focusing on "deterrence in space," considers how to pursue such deterrence and points out the significance of resilience and protection of space systems.

## 1. Historical Background

### (1) Space and Deterrence in the Cold War Period

First, looking back at "space in deterrence" during the Cold War period—that is, the role of space systems in deterrence overall—it can be said that space systems were an essential component of the nuclear deterrent. At the time, many of the military satellites developed and deployed by the U.S. and the Soviet Union were intended for maintaining and improving their nuclear deterrents. Specifically, military space systems were put to use for such things as collecting information about the targets for nuclear attacks; the collection of the weather information needed for the operation of the imaging reconnaissance satellites[12]; early detection of ballistic missiles; communications used for command and control of nuclear forces; positioning that is necessary when launching ballistic missiles from submarines; and the detection of nuclear explosions[13]. Conversely, the contribution of space systems to conventional deterrence was limited. In the latter half of the Cold War, the U.S. and the Soviet Union began integrating space systems into the operations of conventional armed forces. Still, those efforts remained partial.

Next, "deterrence in space" during the Cold War—that is, deterring attacks against space systems—was essentially part and parcel of nuclear deterrence[14]. Given that many of the military space systems operated by the U.S. and the Soviet Union were used to support the operations of nuclear forces, it was understood that attacks on military space systems likely led to nuclear war. Thus, so long as nuclear deterrence was in place, the need to worry about attacks on military space systems was low.

[11] Cabinet Secretariat, "Kokka anzen hoshō senryaku ni tsuite," December 2022, p. 17. https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-j.pdf

[12] Because the imaging reconnaissance satellites that the U.S. and the Soviet Union used during the Cold War period were mainly equipped with optical sensors, they could not take images when a subject area was covered with clouds. For this reason, it was necessary to assess weather conditions for the subject area in advance.

[13] For details, please see below. Yasuhito Fukushima. *Uchū to anzen hoshō: Gunji riyō no chōryū to gabanansu no mosaku. Chikura shobō*, 2020, chap. 2.

[14] Finch and Steene, "Finding Space in Deterrence," p. 10.

### (2) Space and Deterrence in the Post-Cold War Period

Concerning "space in deterrence" in the post-Cold War period, the role of space systems in conventional deterrence for the U.S. had grown remarkably. This is because, with the 1991 Gulf War, the U.S. began to integrate space systems in earnest into the operations of its conventional armed forces[15]. Symbolic examples are using satellite communications to operate long-endurance uncrewed aerial vehicles such as Predator and Global Hawk and Global Positioning System (GPS) for precision strikes using Joint Directed Attack Munitions, etc.

While the military role that space systems played expanded in this fashion, the need for "deterrence in space" —that is, for deterring attacks against space systems—was not urgent in the post-Cold War period. After the collapse of the Soviet Union, Russia stagnated in developing and deploying offensive counterspace capabilities. Nor has there been an increase in the development and deployment of offensive counterspace capabilities by other states. Also, at this stage, the integration of space systems into the operations of conventional forces by countries other than the U.S. had not made much progress. Therefore, deterrence against attacks on space systems was not a priority for the U.S. or other countries.

### (3) Space and Deterrence from Around the Mid-2000s

The post-Cold War period situation began changing around the middle of the first decade of the 21st century, and more full-blown change began to emerge with the start of the 2010s. When considering "space in deterrence," the role of space systems in conventional deterrence has continued to expand from the post-Cold War period. Not only the U.S. but also France, Russia, and China, among others, moved forward with integrating space systems into the operations of their conventional armed forces.

Above all, in 2015, China created the Strategic Support Force responsible for space, cyber, and electronic warfare as a unit under the direct command of the Central Military Commission to strengthen its organizational structure for supporting operations of all sorts. Also, the number of China's operational satellites has surpassed that of Russia (China and Russia operate, respectively, 541 and 172 as of the end of April 2022).[16] The Yaogan satellite constellation, which is believed to be used for maritime reconnaissance, etc., is part of China's so-called anti-access/area-denial (A2/AD) capabilities and, when combined with anti-ship ballistic missiles and so forth, plays a role in deterring military intervention by the U.S. and other countries in the event of a crisis in the Taiwan Strait. Furthermore, China's offensive counterspace weapons are A2/AD capabilities in deterring military intervention by the U.S. and other parties.

Under these circumstances, the necessity of deterring attacks on space systems is growing

[15] For details, please see below. Fukushima, *Uchū to anzen hoshō*, chap. 3.

[16] Union of Concerned Scientists, *UCS Satellite Database*, Updated May 1, 2022. https://www.ucsusa.org/resources/satellite-database

as research and development, testing, deployment, and use of offensive counterspace capabilities have become more notable[17]. During the 2003 Iraq War, Iraq attempted to hinder the U.S. forces' use of GPS with electronic warfare weapons. This was regarded as the first case of the U.S. forces being subjected to interference with GPS use amid combat operations. Moreover, in 2007, China succeeded in its first destructive anti-satellite (ASAT) test using a direct-ascent weapon. The U.S. and the Soviet Union conducted destructive ASAT tests during the Cold War, but such testing ceased after the 1990s. China became the first country in the world since the end of the Cold War to succeed with a destructive ASAT test. According to James Finch and Shawn Steene, who were responsible for space policy and strategy development in the Office of the U.S. Undersecretary of Defense for Policy, China's test provided the impetus for Western scholars to begin to explore how to deter the use of such ASAT capabilities during a conflict[18].

Since then, the intentional destruction of satellites has continued. In 2008, the U.S. used a direct-ascent weapon to destroy its own reconnaissance satellite that had become uncontrollable[19]. The U.S. government did not explain this as an ASAT test. Still, in a paper published in 2009, then-U.S. Under Secretary of Defense for Policy Michele Flournoy and then-strategist in the Office of the Secretary of Defense, Shawn Brimley stated that this demonstrated the U.S. ASAT capability[20]. In 2019, India succeeded with its first destructive ASAT test using a direct-ascent weapon. In 2021, Russia conducted the country's first destructive ASAT test since the end of the Cold War. Furthermore, as will be discussed in the next section, in the Russia–Ukraine war, both sides have been using offensive counterspace capabilities in actual fighting.

## 2. Space Deterrence in the Russia-Ukraine War

### (1) Space in Deterrence

Viewed from the perspective of Ukraine and the countries that support it, it was unable to prevent the start of Russia's full-scale invasion of Ukraine. On the other hand, no nuclear attack by Russia has yet to occur. It can be presumed that this is because the nuclear deterrence against Russia by the U.S. and other countries is functioning. Space systems contribute to nuclear deterrence by offering functions related to nuclear command, control, and communications (NC3)[21].

[17] For details, please see below. Fukushima, *Uchū to anzen hoshō*, chap. 4.

[18] Finch and Steene, "Finding Space in Deterrence," p. 10.

[19] The U.S. government used a specially modified Aegis warship and a Standard Missile 3 to destroy the satellite. Nicholas L. Johnson, "Operation Burnt Frost: A View from Inside," *Space Policy*, Vol. 56, May 2021, p. 4.

[20] Michele Flournoy and Shawn Brimley, "The Contested Commons," *Proceedings*, Vol. 135, No. 7, July 2009. https://www.usni.org/magazines/proceedings/2009/july/contested-commons. Flournoy and Brimley were still private citizens when the U.S. destroyed the satellite.

[21] Please see below for the role of the space systems and the current state of the U.S. NC3 network. Marie

Furthermore, no Russian conventional attacks against the states supporting Ukraine—in particular member states of the North Atlantic Treaty Organization (NATO)—have occurred. This fact suggests the possibility that NATO's deterrence against Russia is working. In this respect, space systems also contribute to deterrence against Russia by enabling nuclear and conventional armed forces to operate more effectively.

Needless to say, deterrence is not achieved through space systems alone. Space systems, together with other military forces, provide a deterrent. U.S. Space Force Chief of Space Operations Chance Saltzman, in an interview from November 2022, emphasized that the Space Force is like eggs for making a cake; eggs have to be mixed with flour to make a cake[22].

### (2) Deterrence in Space

Viewed from the perspective of Ukraine and the countries supporting it, it was not possible to deter Russian cyber and electronic attacks against the space systems that Ukraine uses. It is believed that Russia carried out a cyber attack on the communications system that used the geostationary satellite, KA-SAT, of the U.S. company Viasat immediately prior to its ground-based invasion of February 2022 to present an obstruction to the Ukrainian military's command and control[23]. Also, concerning Ukraine, Russia is believed to have conducted cyber attacks and jamming against Starlink—a satellite communications system operated by the U.S. company SpaceX[24]—and to have jammed against GPS downlink signals[25].

Considering the fact that the jamming of GPS downlink signals had been going on in Ukraine since before the all-out invasion began[26], it is no surprise that such attacks could not be deterred after that invasion was launched. In addition, although GPS is a system operated by the U.S. military, and both KA-SAT and Starlink are owned by U.S. companies, given that the impact of electronic attacks on downlink signals and cyber attacks on users' terminals are relatively localized, the threshold of attacks is not necessarily high[27]. Thus, deterrence on the

Villarreal Dean, "U.S. Space-Based Nuclear Command and Control: A Guide," Center for Strategic and International Studies, January 13, 2023. http://aerospace.csis.org/wp-content/uploads/2023/01/130223_MV_SpaceNuclearFinal. pdf

[22] Tobias Naegele, "Q&A: The New Chief of Space Operations on Empowering the Force," *Air and Space Forces Magazine*, November 27, 2022. https://www.airandspaceforces.com/qa-the-new-chief-of-space-operations-on-empowering-the-force/

[23] Viasat, Inc., "KA-SAT Network Cyber Attack Overview," March 30, 2022. https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview; Antony J. Blinken, "Attribution of Russia's Malicious Cyber Activity Against Ukraine," U.S. Department of State, May 10, 2022. https://www.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/

[24] Tweet dated May 11, 2022, from Elon Musk.

[25] Bryan Clark, "The Fall and Rise of Russian Electronic Warfare," *IEEE Spectrum*, July 30, 2022. https://spectrum.ieee.org/the-fall-and-rise-of-russian-electronic-warfare

[26] Yū Koizumi. *Gendai Roshia no gunji senryaku*. Chikuma shobō, 2021, digital edition; and Joseph Trevithick, "Ukrainian Officer Details Russian Electronic Warfare Tactics Including Radio 'Virus'," *The Drive*, October 30, 2019. https://www.thedrive.com/the-war-zone/30741/ukrainian-officer-details-russian-electronic-warfare-tactics- including-radio-virus

[27] The impact of the cyber attack on the communication networks that use KA-SAT extended beyond

attacks against the ground and link segments was unsuccessful among the three segments of space systems.

Meanwhile, to this point, no Russian attacks on the space segment—that is, destructive or non-destructive attacks on satellites using direct-ascent, co-orbital, directed energy, or cyber weapons—have been confirmed. In an interview from April 2022, U.S. Space Force Vice Chief of Space Operations David Thompson said Russia had not attacked GPS satellites[28]. There have also been no confirmations of Russian attacks on Starlink satellites or commercial earth observation satellites.

This fact could be taken as an indication that the deterrence against Russia is working. One possibility is that deterrence by punishment is having an effect, and Russia is reluctant to attack satellites for fear of receiving some kind of countermeasures from the U.S. and others[29]. Almost all of the satellites that Ukraine uses are owned and operated by governments or companies from other countries[30]. The summary of the Defense Space Strategy released in 2020 by the U.S. Defense Department notes that preparations would be made to protect and defend commercial space capabilities if directed. In other words, the U.S. military could take countermeasures if there were attacks not only against government satellites like GPS but also against commercial satellites[31].

The second possibility is that deterrence by denial is functioning, and Russia has thought that attacks on satellites would have limited results and has not carried them out. Given that the satellite constellations of GPS and Starlink, respectively, comprise dozens and thousands of satellites, even if a portion of them were neutralized, the satellite constellations as a whole could continue providing services.

Of course, it could be that rather than deterrence against Russia having an effect, Russia may simply have no intentions to attack satellites or that attacks against satellites have taken place but are not being made public. Furthermore, it would also be no surprise for Russia to destroy the commercial satellites of other countries in the future. Even though the possibility that such an attack would interrupt services is low, Russia could execute one as a check to

Ukraine to other European countries. Also, the details of the cyber attack on Starlink are not clear in terms of whether it targeted the user terminal portion of the ground segment or the ground stations that control the satellites, or if it was aimed at the space segment, or if it targeted all of those.

[28] Tracy Cozzens, "Russia Interfering with GPS in Ukraine, Pentagon Says," *GPS World*, April 13, 2022. https://www.gpsworld.com/russia-interfering-with-gps-in-ukraine-pentagon-says/

[29] Kazuto Suzuki points out that Russia would hesitate to attack even if it were a commercial satellite so long as it cannot exclude the possibility of the U.S. asserting its right to self-defense and intervening. Cabinet Office, "Uchū bun'ya hōkoku Purojekuto Manējā Suzuki Kazuto, Tōkyō Daigaku Kōkyō Seisaku Daigakuin Kyōju," Reiwa 3, 4 nendo Naikakufu itaku jigyō, "Wagakuni ga senryakuteki ni sodateru beki anzen, anshin no kakuho ni kakaru jūyō gijutsu tō no kentō gyōmu," March 28, 2022. https://www8.cao.go.jp/cstp/stmain/pdf/20230314thinktank/siryo4.pdf

[30] As of the end of April 2022, only two satellites were operated by the Ukrainian public and private sectors. Union of Concerned Scientists, *UCS Satellite Database*.

[31] U.S. Department of Defense, *Defense Space Strategy, Summary*, June 2020, p. 2. https://media.defense.gov/2020/Jun/17/2002317391/-1/-1/1/2020_DEFENSE_SPACE_STRATEGY_ SUMMARY.PDF

hinder companies' support for Ukraine. As noted earlier, Russia conducted a destructive ASAT test in November 2021. It may depend on the altitude at which targeted satellites are orbiting, but it is unlikely for Russia to hesitate to destroy satellites, considering the impact of the space debris generated on the operations of other satellites.

Further, in April 2022, the U.S. government declared that it would not conduct destructive direct-ascent ASAT missile testing and would pursue establishing such a commitment as an international norm for responsible behavior in space[32]. Responding to the U.S. call, by April 2023, 12 other countries have issued similar statements[33]. However, there is no clear way forward for Russia to make such a declaration, and the scope of the declarations by the U.S. and other countries is limited to testing. Such efforts to shape international norms have great significance in maintaining the sustainability of space activities, but the possibility of this functioning as a supplement to a deterrent against Russia is limited.

## 3. Issues for Future Consideration

### (1) How Does One Pursue "Deterrence in Space" ?

As the role of "space in deterrence" —the role played by space systems in deterrence overall—grows globally, the importance of pursuing "deterrence in space" as a premise for space systems to fulfill such a role is increasing. If so, how should one pursue "deterrence in space" ?

The following points need to be considered to bring about deterrence in space. One is the possession and demonstration of one's capabilities. Examples of such capabilities are those related to resilience and protection, retaliation, and space domain awareness (SDA). Possessing capabilities related to the resilience and protection of space systems and demonstrating externally that those capabilities are possessed contribute to deterrence by denial. Also, both possessing retaliatory capabilities and showing others that one has those capabilities lead to deterrence by punishment. SDA provides the basis for resilience, protection, and retaliation capabilities. SDA can also be used for "deterrence by detection" by showing one can be aware of attacks on space systems. However, thought has to be given to the balance between concealment and display. Deterrence is difficult if an adversary is not aware that such capabilities exist. On the other hand, there is the concern that if capabilities are made overly obvious, the adversary will adopt countermeasures in advance.

Also, in pursuing deterrence by punishment, the determination to use retaliatory capabilities must be communicated to the adversary in advance. A 2020 talk delivered by then-U.S. Assistant Secretary of State for International Security and Nonproliferation Christopher Ford

[32] The White House, "FACT SHEET: Vice President Harris Advances National Security Norms in Space," April 18, 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/18/fact-sheet-vice-president-harris-advances-national-security-norms-in-space/

[33] Mike Wall, "3 More Countries Pledge Not to Conduct Destructive Anti-Satellite Tests," *Space.com*, April 11, 2023. https://www.space.com/netherlands-italy-austria-destructive-asat-pledge

was an example of communicating such a determination. He said that the U.S. NC3 architecture was dependent to some degree on space systems and suggested in public that even a non-nuclear attack on related space systems could invite nuclear retaliation by the U.S.[34] In addition, it is significant that NATO declared in 2021 and the U.S. and Japan in 2023 that attacks to, from, or within space could invoke Article 5 of the North Atlantic Treaty and the U.S.–Japan Security Treaty, respectively[35]. Furthermore, it is necessary to consider the balance between ambiguity and specificity to communicate a determination to use retaliatory capabilities. If the content is too ambiguous, there is the possibility of that determination not being fully communicated. On the other hand, if it is overly specific, the adversary could launch an attack in a way that would get around that content.

The third is to pursue cross-domain deterrence[36]. Efforts to deter attacks against space systems are not concluded solely in the space domain. As not only the space segment but also the ground and link segments need to operate normally, it is necessary to pursue deterrence of attacks on these segments as well. In addition, attacks on each space system segment can be cross-domain. For example, an attack on a satellite may be carried out not just from outer space but also from land, sea, air, or cyberspace.

Regarding deterrence by denial, supplementing the military functions provided by space systems（for example, ISR, communications, and PNT）with systems in other domains such as land, sea, or air can improve the deterrent. In the case of deterrence by punishment, it is possible, for example, that not only showing intention to retaliate against an attack on a satellite with a satellite attack but also displaying the determination to retaliate through land,

[34] U.S. Department of State, “Whither Arms Control in Outer Space? Space Threats, Space Hypocrisy, and the Hope of Space Norms,” Remarks by Dr. Christopher Ashley Ford, Assistant Secretary, Bureau of International Security and Nonproliferation, at Center for Strategic and International Studies Webinar on “Threats, Challenges and Opportunities in Space,” Washington, DC, April 6, 2020. https://2017-2021.state.gov/whither-arms-control-in-outer-space-space-threats-space-hypocrisy-and-the-hope-of-space-norms/index.html

[35] The specific content is as follows. “We consider that attacks to, from, or within space present a clear challenge to the security ofthe Alliance, the impact of which could threaten national and Euro-Atlantic prosperity, security, and stability, and could be as harmful to modern societies as a conventional attack. Such attacks could lead to the invocation of Article 5. A decision as to when such attacks would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis,” North Atlantic Treaty Organization, *Brussels Summit Communiqué*, Issued on June 14, 2021, Last updated: July 1, 2022. https://www.nato.int/cps/en/natohq/news_185000.htm; “The Ministers consider that attacks to, from, or within space present a clear challenge to the security of the Alliance, and affirmed such attacks, in certain circumstances, could lead to the invocation of Article V of the Japan–U.S. Security Treaty. The Ministers also affirmed that a decision as to when such an attack would lead to an invocation of 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.” U.S. Department of Defense, “Joint Statement of the 2023 U.S.–Japan Security Consultative Committee（"2+2"）,” January 2023, Section 4. https://www.defense.gov/News/Releases/Release/Article/3265559/joint-statement-of-the-2023-usjapan-security-consultative-committee-22/

[36] Benjamin W. Bahney, Jonathan Pearl, and Michael Markey, “Antisatellite Weapons and the Growing Instability of Deterrence,” Jon R. Lindsay and Erik Gartzke, eds., *Cross-Domain Deterrence: Strategy in an Era of Complexity*, Oxford University Press, 2019, p. 137.

sea, air, or cyberspace will help to improve a deterrent. On this point, through its National Space Policy, the U.S. clearly stated that responses against attacks on space systems would not entirely be symmetrical and would not be limited to the space domain[37].

### (2) The Limits of "Deterrence in Space" and the Significance of Resilience and Protection

Even having pursued deterrence on attacks against space systems, the fact that there are limits to deterrence must be kept in mind. It is crucial to pursue deterrence, but the extent to which deterrence is actually feasible is a different question. As noted above, in the Russia–Ukraine war, electronic attacks against the link segment of space systems and cyber attacks against the ground segment have been confirmed. Such attacks are not limited to times of armed conflicts, and the threshold for making deterrence a success is high. Also, while attacks on satellites (particularly satellite destruction) have not yet been confirmed, since states that possess ASAT capabilities are increasing, it would be no surprise if an attack were to occur at some point. Therefore, improving resilience and protection that would allow space use to continue even if deterrence fails is vital.

In relation to this, the Russia–Ukraine war offers important insights.  Even under Russian attacks on space systems, Ukraine has been able to continue its military use of space. This fact demonstrates the significance of the resilience and protection of space systems.

According to the U.S. Space Force, the measures for securing the resilience of space systems are disaggregation, distribution, diversification, proliferation, and deception[38]. Disaggregation means the separation of capabilities into different platforms, payloads, terrestrial locations, or orbits; distribution means using many nodes that work together to perform the same mission or functions as a single node; diversification means contributing in multiple ways to the same mission by using different platforms or orbits, and leveraging capabilities through partnerships[39]; proliferation means deploying larger numbers of the same platforms, payloads, or systems of the same types to perform the same mission; and deception refers to actions or system implementation designed to confuse or mislead an adversary concerning the location, capability, operational status, mission type, and/or robustness of an asset. Based on the above classification, the fact that the Ukrainian military continued to use satellite communications via Starlink after being unable to use KA-SAT would fall into the category of diversification.

[37] The White House, *National Space Policy of the United States of America*, December 9, 2020, p. 4. https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/12/National-Space-Policy.pdf

[38] U.S. Space Force, *Operations*, Space Doctrine Note, January 2022, p. 14. In the classification for resilience in space systems, which was drawn up in 2015, the U.S. Office of the Assistant Secretary of Defense for Homeland Defense and Global Security situated protection as one means for ensuring resilience. Office of the Assistant Secretary of Defense for Homeland Defense and Global Security, U.S. Department of Defense, *Space Domain Mission Assurance: A Resilience Taxonomy, A White Paper*, September 2015, p. 6.

[39] Diversification also refers to the definition from the U.S. Office of the Secretary of Defense. Office of the Assistant Secretary of Defense for Homeland Defense and Global Security, *Space Domain Mission Assurance*, p. 7.

In addition, according to the U.S. Space Force, measures for protecting space systems include electromagnetic spectrum operations, movement and maneuver, hardening, and cybersecurity[40]. The fact that Starlink continues to provide service to Ukraine even after being subjected to electronic and cyber attacks can be thought of as demonstrating that the protection measures are effective.

## Conclusion

Following a review of the historical background that led from the Cold War period to the present, this article considered the relationship between space and deterrence using the Russia–Ukraine war as an example. In the end, having focused on the deterrence of attacks against space systems, this article enumerated the points to bear in pursuing deterrence and pointed out the importance of coming to grips with resilience and protection, considering the limits of deterrence.

As noted in this article's introduction, the role played by space systems in the defense of Japan is growing, and pursuing the deterrence of attacks on space systems is becoming a crucial issue for the country. At the same time, Japan has to work on the resilience and protection of space systems in case of deterrence failure. The National Defense Strategy, decided by the Cabinet in 2022, clearly stated that efforts would be made to strengthen the resilience of space assets[41]. In pursuing such efforts, it will likely be necessary to bear in mind making effective use of commercial space services, as seen with Ukraine's forces[42].

[40] U.S. Space Force, *Operations*, p. 14.

[41] Ministry of Defense, "Kokka bōei senryaku ni tsuite, December 16, 2022, p. 19. https://www.mod.go.jp/j/policy/agenda/guideline/strategy/pdf/strategy.pdf

[42] The Russia–Ukraine war also shows the risk of depending on specific commercial space services.

# Chapter 4

# Approaches to and Issues in Deterrence in Cyberspace

**Kazuo Tokito**

## Introduction

Cyberspace is evolving constantly due to the development of telecommunications technologies and the global environment. In Russia's invasion of Ukraine that began in earnest in February 2022, there was a real sense that offensive and defensive battles were concretely unfolding in cyberspace, and cyberspace was three-dimensionally expanding its layers. In this chapter, we will consider cyberspace and deterrence, and—using the insights we learned through the discussions at our study meeting and in our scenario games—discuss approaches to and issues of deterrence in cyberspace based on its features and specific examples.

## 1. Cyberspace and Deterrence

Deterrence is defined as "ensuring restraint by convincing the actor that the threat of retaliation is real or that the intended action will not succeed, while restraint will have acceptable consequences[1]." More precisely, the opposite party must understand its rationality, and the defending party must possess those capabilities and have the communication capabilities to credibly convey the message to the opposite party[2]. In cyberspace, deterrence is discussed mainly in terms of deterrence by denial or deterrence by punishment[3], but it is necessary to also focus on a broader concept of deterrence[4] in conjunction with the expansion of cyberspace. Here, we see the ends of deterrence as the deterrence of a conflict; we do not fixate on the thought of deterring a cyber attack itself.

### (1) The Distinguishing Features of Cyberspace

Cyberspace as represented by the internet is a global network connected through the IP protocol. The Internet Corporation for Assigned Names and Numbers (ICANN) is a project commissioned by the U.S. government that is in charge of its assignment and operation[5]. In

[1] Scott Jasper, *Strategic Cyber Deterrence: The Active Cyber Defense Option*, Lanham, Maryland: Rowman & Littlefield, 2017, p. 60.

[2] Joint Chiefs of Staff, "Joint Publication 3-0: Joint Operations" , January 17, 2017, xxii.

[3] Masahiro Kurita, "Saibā kōgeki ni taisuru 'yokushi' no genjō," in National Diet Library Research and Legislative Reference Bureau, *Jōhō tsūshin o meguru shokadai*, March 2015, pp. 158–161.

[4] Frans Osinaga and Tim Sweijs, eds., *Deterrence in the 21st Century: Insights from Theory and Practice*, The Hague, The Netherlands: T.M.C. Asser Press, 2021, pp. 148–150.

[5] Japan Network Information Center (JPNIC), "Intānetto to wa," November 28, 2002. https://www.nic.ad.jp/ja/basics/beginners/internet.html

terms of connected terminals, as of 2018 that number stood at 22 billion, and as of 2023 (as of this writing) it was forecast to have reached 33 billion[6]. The internet is a network that is open to the public. As such, its features are such that a variety of cyber attacks regularly occur owing to the facts that management is decentralized, distinguishing between the private and the military is difficult due to anonymity, and a variety of actors are present. Until now, clear distinctions have been drawn between military networks and the internet. However, as can be seen with the GIS Arta[7] artillery control system that Ukraine has used in response to the invasion, the positions of enemies can be identified based on battlefield data sent from reconnaissance drones and smartphones. The function of assigning weapons that are the most appropriate for a strike in a given region in a short amount of time has been effective, and the uses for the military areas of the internet have also become something that has a touch of the real.

Also, most systems that are not directly connected to the internet are still operated in closed environments based on the IP protocol. It has become a situation where cyber attacks cannot be completely defended against with the conventional recognition that closed systems are safe; considering, for example, that there are chances of input and output of unauthorized data via USB memory sticks, and methods of enabling internet connection using technology that uses the speech functions of computers or mobile devices to attempt data transmissions via voice outside of the audible range[8]. Furthermore, the attribution problem wherein anonymity makes it difficult to identify the source of an attack[9] is also having a significant impact on deterrence by punishment.

### (2) Cyberspace in Deterrence

In considering the roles that cyberspace should play in deterring conflict, a crucial one is to protect one's own systems from cyber attacks and secure against leaks of confidential information while guaranteeing mission assurance of systems including critical infrastructure so that no degradation of defense occurs. Furthermore, in the cognitive domain today, too, the significance is great and role major in protecting against illicit access when attempts are being made to divide society through misinformation and impression management, as well as to disseminate information that will trigger social unrest.

[6] Help Net Security, "Number of connected devices reached 22 billion, where is the revenue?," May 23, 2019. https://www.helpnetsecurity.com/2019/05/23/connected-devices-growth/

[7] 'GIS "ARTA" automated command and control system', https://gisarta.org/en/index.html

[8] Anfractuosity, "Ultrasound Networking" , https://www.anfractuosity.com/projects/ultrasound-networking/

[9] Takahisa Kawaguchi, "Dai-2 shō Saibā kūkan ni okeru anzen hoshō no genjō to kadai: Saibā kūkan no yokushiryoku to NichiBei dōmei," in Japan Institute of International Affairs, *Gurōbaru komonzu (saibā kūkan, uchū, Hokkyokukai)* ni okeru NichiBei dōmei no atarashī kadai. March 2014, pp. 11–26. https://www2.jiia.or.jp/pdf/resarch/H25_Global_Commons/03-kawaguchi.pdf

### (3) Deterrence in Cyberspace

There are a variety of arguments about the effects of deterring against cyber attacks themselves from cyberspace. However, when considering the advance of new attack technologies and the ease with which malware for making such attacks can be obtained from the black market and the like[10], along with a state of affairs in which systems including supply chains are broadly connected, deterrence by denial where systems are completely protected is said to be difficult. In particular, with regard to cyber attacks where a state is the actor, there is also the possibility of zero-day attacks[11] that are not generally disclosed because of the enormous amount of resources spent on the attack. Accordingly, there is a growing need of operation management done on the premise that intrusions will happen, and constant monitoring of cyber attack risks.

## 2. Threats in Cyberspace

Around 2000 when cyber attacks started to become widely recognized, the threat was one of being infected by viruses through email sent indiscriminately that would destroy or falsify data. It was at a level where one could sufficiently protect against it by scanning with anti-virus software.

Since then, attacks gradually became more sophisticated. By around 2020, unobtrusive attacks had become mainstream. What has become noticeable are, for example, improper remittance losses caused by ransomware and illicit access. In 2022, cyber attacks had evolved into ones where breach paths into corporate networks are more complex. Due to the spread of Wi-Fi and the diversification of such IT infrastructure as the cloud and IoT, it is expected that in 2023, there will be a further increase in losses due to the evolution of ransomware, as well as an increase in damage to supply chains and application programming interfaces (API)[12].

### (1) Classes of Attack

Cyber attacks come in many varieties, and they are constantly evolving. They may be classed into attacks against specific targets, attacks on large numbers of random targets, attacks that impose loads, attacks on vulnerabilities and password analysis, and so forth[13]. In particular, when it comes to attacks on specific targets, these include targeted attacks as well as ransomware and supply chain attacks. From information collecting for intrusion to latency, system analysis, and the like, the attacks are sophisticated in many cases; and the intrusion is divided up into stages.

[10] "Jōhō sekyuriti 10 daikyōi 2023," Information-Technology Promotion Agency, March 2023, pp. 52–53. https://www.ipa.go.jp/security/10threats/ps6vr70000009r2f-att/kaisetsu_2023.pdf

[11] "Jissai ni atta zero dei kōgeki no higai jirei matome," CyberSecurityTIMES, June 12, 2020. https://www.shadan-kun.com/blog/measure/6424/

[12] "API no zeijakusei wa dono teido kiken na no ka, dō sureba kōgeki o fusegeru no ka," IT Media, February 5, 2021. https://atmarkit.itmedia.co.jp/ait/articles/2102/05/news104.html

[13] "Saibā kōgeki to wa? sono shurui, jirei, taisaku o haaku shiyō," Cyber Security.com, January 17, 2023. https://cybersecurity-jp.com/column/14651

### (2) The Cyber Kill Chain

There is a model that defines the stages of a cyber intrusion using the example of a kill chain. Devised in 2011 by Lockheed Martin Corporation, it breaks down an attack into seven stages: reconnaissance, weaponization, delivery, exploitation, installation, command & control (C2), and actions on objectives[14]. Breaking down the sequenced attack process into multiple stages makes it easier to think of countermeasures. The concept is that the attacker needs the tools and techniques to be used to move on through each stage of this process, and the entire process will be interrupted if even one link in the chain is broken off.

Various modifications have been made to it referring to this model. For example, Dell breaks cyber attacks down into four basic stages, classifying them as reconnaissance, intrusion, malware injection, and the removal of traces. Its unique feature is that it goes beyond the scope of Lockheed Martin's focus, which focused on the stages of an intrusion in order to include denial of service attacks. For its part, Cybereason breaks down the life cycle of an attack into six stages: external reconnaissance, breach, command and control, spread, lateral movement, and damage. TechTalk added "monetization" as an eighth step to go with the seven from Lockheed Martin[15]. This is the stage in present-day threat analysis of demanding payments of ransom via Bitcoin and so forth.

These cyber kill chain models are used to carry out analyses and detailed diagnoses of malicious cyber activities. They are used effectively not only for making it possible to grasp what systems cyber attackers are intruding, but also for selecting the security countermeasures to be implemented that are optimal for dealing with their respective goals.

## 3. A Comparison of Offense and Defense in Cyberspace

Based on the perspective that Japan—which holds maintaining the status quo as fundamental to its strategy—sees deterring challenges from those states that might possibly try to change the status quo as important, we will compare "the conceivable impacts from the side challenging the status quo" and "the conceivable impacts from the side maintaining the status quo" and consider the advantages of each.

### (1) Comparative Advantages for the Side challenging the Status Quo

#### A. There are few legal or moral restrictions based on democratic control

Because the side seeking to challenge the status quo is an authoritarian state, there are few legal or moral restrictions based on democratic control, and it can collect and use data without giving any consideration to privacy. This could be of considerable significance if we think about the characteristics of the data economy of the future, which it is thought will bring forth major

[14] Lockheed Martin, "THE CYBER KILL CHAIN." https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[15] "Saibā kiru chēn to wa? ," TechTalk, January 17, 2023. https://techtalk.pcmatic.jp/?p=2443

effects with its incorporation of personal data.

### B. There are advantages from information manipulation

This is a matter that is inherent to the political system of an authoritarian state, but through influence operation in the form, for example, of fake news at home and abroad, it is quite possible that it will be able to manipulate public opinion in directions favorable to itself. For example, in its current invasion of Ukraine, Russia has been issuing fake news of various sorts. While this has had hardly any effect on international society, it is succeeding in terms of support at home for Putin's regime.

### C. The distinctive characteristics of a cyber attack are easily used

Most cyber attacks have the characteristic of paralyzing or slowing down the actions of the party on the receiving end. These characteristics have great affinity with the actions of the side challenging the status quo such as working to make such change a fait accompli through quick action. If they can implement one that paralyzes or slows the opposite party's actions at a crucial moment, acting to change the status quo will be extremely easy.

## (2) Comparative Advantages for the Side maintaining the Status Quo

### A. Disclosing the truth

Disclosing the "truth" appropriately makes it easy to get the support of international society. It may be said that Ukraine is making full use of this with respect to Russia's invasion. With being able to appropriately disclose "truths" that have great credibility being the premise, this is an important comparative advantage for democratic states.

### B. The Development of Traceback Technology

Traceback technology has a crucial role to play in the attribution of cyber attacks[16]. If it becomes possible to rapidly determine where a cyber attack is coming from, this will be of crucial significance to deterring and responding to cyber attacks. With existing traceback schemes, the success rates have been low and the overhead on communication traffic has been high. Given this, there have been problems such as that traceback functions to the contrary become targets of cyber attacks themselves. Of late, research is also being done on technologies to improve this[17]. Also, for example, the automation of cyber attack detection employing AI that makes full use of the cloud environment and draws on large volumes of data[18] is also being

[16] Traceback Research Portal https://www.telecom-isac.jp/tb/

[17] Jie Ma, Wei Su, Yikun Li, and Fangtao Yao, "A Low-Overhead and High-Precision Attack Traceback Scheme with Combination Bloom Filters," *Hindawi Security and Communication Networks*, Volume 2022, October 13, 2022, pp. 1–13.

[18] Rob Mead, "How Azure Security Center automates the detection of cyber attack," Microsoft Threat Intelligence Center, October 24, 2017.

used effectively for traceback.

### C. Monopoly over crucial internet functions

The side maintaining the status quo has a monopoly over the internet's basic functions including domain name system (DNS) servers and its administrative and operational organizations. In the past, it has been pointed out that the DNS, the border gateway protocol (BGP), and so forth, which plays an important role on the internet, are vulnerable. However, with regard to DNS, the risk of falsifications and outages has been reduced thanks, for example, to the implementation of standards such as DNSSec[19] (DNS Security Extensions) that ensure reliability, and to the proper setup by internet service providers (ISP)[20]. Even the distributed denial of service (DDoS) attack on DNS root servers in 2015 had hardly any impact owing to overwhelming resources from a redundancy of DNS root servers[21]. As to BGP, thanks to the introduction of the standard of Resource Public Key Infrastructure (RPKI) that blocks errant or false routing information[22], the vulnerabilities are on track to gradually being resolved, contributing to the stable operation of the internet.

## (3) Matters of Great Uncertainty

### A. Use of Artificial Intelligence (AI) Technology

While the U.S. had long been the front runner in AI technology, the sudden rise of China in recent years has been eye-opening. For this reason, at the moment it is difficult to determine which country will seize the technological advantage. In particular, the language-model Generative Pre-trained Transformer (GPT), which uses a Transformer[23] method developed in 2017 by researchers at Google and Toronto University, has for several years now demonstrated surprising performance, while Chat GPT released in 2020 by Open AI has been made broadly available as a chat-capable service and has become a sort of phenomenon. These are drawing the attention of China[24] as well, and while there are still obstacles to overcome on the way to their full-out implementation, conditions could change considerably by adopting these technologies and giving them military capabilities in the future.

[19] Takeshi Mitamura and Arata Satō, "DNSSEC kaisetsu," *Jōhō shori*, Vol. 52, No. 9, September 2011, pp. 1158–1165.

[20] Japan Registry Services, "Bot keiyu de DNS sāba o hiroku usuku kōgeki: DNS mizuzeme kōgeki no gaiyō to taisaku." https://jprs.jp/related-info/guide/021.pdf

[21] ZDNET, "Rūto nēmu sāba ni kōgeki: Kōgekisha no shōtai wa fumei." https://japan.zdnet.com/article/35074787

[22] R. Bush, "The Resource Public Key Infrastructure (RPKI) to Router Protocol," RFC 6810, January 2013. https://www.rfc-editor.org/rfc/rfc6810.html

[23] Ashish Vaswani, et al, "Attention Is All You Need," 31st Conference on Neural Information Processing Systems, NIPS 2017, Long Beach. CA. USA.

[24] "Chūgoku ga chatto GPT ni keikaikan o takameru 'binkan na yōgo' ni tsuite seifu to kotonaru kaitō renpatsu," *NEWS Post Seven,*
March 19, 2023. https://www.news-postseven.com/archives/20230319_1851569.html?DETAIL

There are a variety of arguments about guaranteeing credibility when it comes to AI, but the risk management frameworks and so forth for AI[25] may also be of some use.

### B. Rebuilding the Supply Chain

When it comes to hardware and to software—including platforms—at present it is difficult to forecast how power will be distributed when it comes to the degree to which not just the states maintaining the status quo but all of international society depend on China. This will have a significant impact on the international political environment going forward.

## 4. Considerations about Cyber Warfare in the Ukraine Invasion

Russia brought its military power to cross the border and invade Ukraine. However, the first act of encroachment is said to have taken place several hours earlier on the preceding day[26]. It was a cyber weapon sent to Ukraine's computers, an attack that had already been observed by other countries[27]. This battle appears different from what had come before, and even more than one year after the invasion it has yet to come to an end. Here, we will consider below this invasion from the perspective of cyber warfare.

### (1) Asymmetric Forces

It can be said that cyber warfare is suited to an asymmetrical approach, since it is low-cost, has technological advantages, and its effects can continue over time. When an asymmetrical approach is adopted by a hostile force that has a strong will to try to protect its own country's existence and its vital interests, that force will not balk at taking actions that may be described as irresponsible, even if they are subjected to various criticisms related to ethics and laws. Asymmetry in cyberspace also contains the perspective that "attacking has advantages over defending."

Generally speaking, while it is good enough for an attacker if they succeed one time at intruding a system, the defending side must build layers of defense prepared for attacks from any direction. In short, "offensive operations are low cost and yield great returns, while defensive operations are high cost and very inefficient." They are also used for attempts to make the opposite party aware of the power to do damage in the digital realm and, by exacting costs, try to forcibly secure concessions.

In response to a large-scale cyber attack against Estonia in 2007 that appeared to have come from Russia and had major impacts that led to government and private websites being shut

[25] NIST "Artificial Intelligence Risk Management Framework (AI RMF 1.0)," NIST AI 100-1, January 2023.

[26] Scott Jasper, *Russian Cyber Operations: Coding the Boundaries of Conflict*. Translated by Kōki Kawamura as *Roshia saibā shinryaku: Sono keikō to taisaku*, Sakuhinsha, March 1, 2023.

[27] Brad Smith, "Defending Ukraine: Early Lessons from the Cyber War." Translated as "Ukuraina no bōei: Saibā sensō no shoki no kyōkun," Microsoft Japan News Center, July 4, 2022. https://news.microsoft.com/ja-jp/2022/07/04/220704-defending-ukraine-early-lessons-from-the-cyber-war/

down, the chaos on networks was constrained and Russia was unable to extract concessions from Estonia[28]. On the other hand, Estonia is a member of NATO, and it wished to invoke Article 5 of the NATO charter and requested the right of collective self-defense. However, since no conclusive proof could be found that the cyber attack was from Russia, it did not reach the threshold of an armed attack.

In regard to the Ukraine invasion, while a cyber attack from Russia did take place prior to the invasion, Ukraine had already forecast the attack and shut down the sites that would attack Ukraine before the attack occurred. As to the attacks on networks, it was able to avoid malfunctions due to the destruction of data thanks to securing alternate means through Starlink and evacuating national data in advance to the cloud. In any case, it would be hard to say that Russia was able to demonstrate the maximum asymmetric effects of cyber warfare.

### (2) Hybrid Warfare

In hybrid warfare, an adversary will combine in their own way a variety of approaches and direct them toward the opposite party's weaknesses. They select the optimal means from a variety of tactics and technologies and fuse the various means together in novel ways suited to their own strategic culture, geographical characteristics, and ends. However, each and every element that comprises hybrid warfare does not always rise to the level of armed conflict. For Russia, there is the Gerasimov Doctrine concerning the essential changes to wars, which in 2013 stressed the important of non-military tools in conflicts. After the annexation of Crimea in 2014, it has been recognized by scholars as a hybrid warfare doctrine. According to this model of modern warfare, non-military and military means are to be executed at a roughly 4:1 ratio. It is a useful concept in terms of analyzing the cyber operations that were used as a tool for the annexation of Crimea.

### (3) Information Warfare

Keir Giles points out that what has become clear from the Ukraine invasion is that Russia has been using cyber activities as a subset of the broader domain that is information warfare and occasionally used them as a catalyst[29]. The sabotage directed against the mobile telephones of Ukraine's parliamentarians and the National Security and Defense Council of Ukraine's internet that took place immediately after combat began was an attempt to impact Ukrainian government's decision-making. This took place when Russia was in the middle of pursuing an immense information operation to spread propaganda through its television programs and various media organizations by using false news and fabricated narratives with strongly ideological coloring in order to manipulate the masses. Cyber operations are playing a crucial

[28] Jasper, *Roshia saibā shinryaku*, p. 75.

[29] Keir Giles, "The Next Phase of Russian Information Warfare," NATO Strategic Communications Centre of Excellence, May 20, 2016.
https://stratcomcoe.org/publications/the-next-phase-of-russian-information-warfare/176

role in the theft of valuable information essential to influence operations.

Cyber warfare becomes a tool for skillfully contriving a strategic and operational environment that falls just short of an armed invasion, and for manipulating the threshold for conflict that evades countermeasures from the victimized country and measures from international society. However, in times of conflict it can be changed into a tool that adds to military capabilities, such as operational support and escalation control. In short, a strategy devised based on the legal ambiguities and technological complexities in gray zones will in the end fail at the time of an armed invasion. Russia on its own closed off the opportunity to achieve its operational goals without any counterattacks or sanctions by explicitly launching an armed invasion of its own accord. Its cyber activities thenceforth would be regarded as part of an armed attack, and economic and financial sanctions would be imposed by international society, including the West.

## 5. Strengthening of Cyber Warfare Capabilities

Japan to date has primarily implemented protection against cyber attacks[30]. However, with passive protection, because it can only deal with an attack after it has occurred and is also limited to dealing with one in the early stages, the need for active defense has been growing[31]. In the face of attacks by cyber attack technologies that are evolving every day, the limits on absoluteness of multiple defenses based on conventional perimeter security are starting to become apparent[32], and the introduction of security countermeasures premised by intrusions based on cyber attacks has already begun in part.

Backgrounded by such an age, at the end of 2022 the Cabinet approved three strategic documents, including one on national defense strategy[33]. Particularly in regard to cyber warfare capabilities in cross-domain operations, the strategy called for establishing a posture by fiscal 2027 that would be able to preserve command and control capabilities and high-priority component systems even while under cyber attack, and establishing a posture that would enable underlying support for defense industry cyber defenses. In roughly ten years, while establishing a posture that would preserve command and control capabilities, the capabilities to display war potential, and operational infrastructure to enable executing missions even while under cyber attack, it would strengthen a posture that makes it possible to support cyber security for areas other than the SDF[34].

In short, it is going to ensure resilience against cyber attacks across a broad area. It shows

[30] Cabinet Decision, “Saibā sekyuriti senryaku,” September 28, 2021.

[31] The White House, “National Cybersecurity Strategy,” March 2023, pp. 14–15.

[32] “Zero torasuto sekyuriti o manabu: Jūrai no kyōkaigata bōgyo dake de wa mamorenai kigyō shisutemu,” CYBERNET. https://www.cybernet.co.jp/zerotrust/learning/01.html

[33] Decision by the National Security Council and the Cabinet, “Kokka anzen hoshō senryaku ni tsuite,” December 16, 2022. (Provisional English translation: “Regarding the National Security Strategy of Japan.”)

[34] Decision by the National Security Council and the Cabinet, “Kokka bōei senryaku ni tsuite,” December 16, 2022.

that, even if a system has been intruded by a cyber attack, the system will continue to operate in order to achieve its original goals even if some of its functions are degraded. The following functions presented in the Defense Buildup Program[35] must be enhanced in order to make those functions a reality.

### (1) Promotion of Information Sharing

It is said that 39% of cyber attacks are prevented by the sharing of cyber threat intelligence[36]. As to the necessity of information sharing in cyberspace, the sharing of information across all fields, domestically and internationally, is crucial both in confirming the circumstances of a cyber attack and for identifying the attack's source. However, solid management of information is essential in the sharing of that information, and establishing a security clearance regime for that purpose[37] is crucial. In particular, it will also be necessary to keep down to a minimum the time required from that regime being established to actually implementing it in systems; applying it to related systems and linking it with authentication and authorization systems will also be crucial.

### (2) Active Cyber Defense

With respect to active cyber defense[38], the range of definitions is broad and there is room for discussion about specifically how far they apply[39]. When it comes to the combinations of elements including an attacker's intentions, the attack opportunities, and an attacker's capabilities, there is a need to investigate the effectiveness as an active countermeasure against each. By collecting these information accurately, one course will be to create attacker profiles, engage in information sharing between the public and private sectors in a timely fashion, and take active efforts to prevent harm before it happens based on forecasts of where it might occur. Toward that end, all-source information analysis that includes cyber threat information is crucial.

At the start of 2018, the U.S. Cyber Command was given authorization to adopt a more aggressive approach. It worked out a "defend forward" posture, where it would track down attackers on the other side of the network or system and counter them before large-scale damage results from the adversary's activities. This concept will also be useful for clarifying the enemy's tools and weapons based on observation of their technologies, procedures, and

[35] Decision by the National Security Council and the Cabinet, "Bōeiryoku seibi keikaku ni tsuite," December 16, 2022. Provisional English translation: "Defense Buildup Program," https://www.mod.go.jp/j/policy/agenda/guideline/plan/pdf/program_en.pdf.

[36] Jasper, *Roshia saibā shinryaku*, p. 222.

[37] "Kokka anzen hoshō senryaku ni tsuite," p. 24.

[38] "National Security Strategy of Japan," December 16, 2022, pp. 23–24.

[39] Hayato Sasaki, "'Sekkyokuteki saibā bōgyo' (active cyber defense) to wa nani ka: Yori gutaiteki na giron ni mukete hitsuyō na kanten ni tsuite," JPCERT/CC, September 21, 2022. https://blogs.jpcert.or.jp/ja/2022/09/active-cyber-defense.html

tactics[40]. Partnering with units that have such functions will also be crucial.

### (3) Strengthening Capabilities in Cyberspace

Cyberspace consists of a variety of telecommunications technologies, and as measures for countering new threats it will be necessary to adopt the following environments to give it military capabilities.

### A. Adoption of Zero Trust

Conventional perimeter security measures are premised by the data and systems to be protected being within the network. However, with the spread of the cloud, there is data that needs to be protected on the network. Zero trust involves devising security measures based on the premise that no communications are to be trusted. For that reason, it is necessary in particular to develop a good balance while steadily transitioning from the conventional measures with doing so incrementally with reference to the zero trust maturity model[41] and the like so that no security holes arise.

### B. Adoption of a Risk Management Framework

A risk management framework deals with risks from the two perspectives of information systems and shared management measures. As regards information systems, the authority is granted that is necessary for the operation or use of those systems; this is to address security risks and privacy risks. With regard to shared management measures, the authority is granted to carry out the specific management strategies necessary to operating the systems of the designated organization. Security management measures include measures for protecting the confidentiality, integrity, and availability of a system. They comprise seven basic steps[42]. These are compatible with a variety of system types and can be applied with no conversion even when the system changes, so they do not necessarily individually require new risk management processes. They will be useful to management approaches for dealing with most systems in the future.

### C. Cyber Threat Hunting

As to the efforts to detect and remove sophisticated malware that has invaded a system, instances where it is difficult to detect them with conventional anti-virus software are on the rise. Threat hunting entails doing investigations premised by being infected with malware. Adopting it is effective for preventing cyber attacks as it makes even better analyses and forecasts possible due to raising the level in partnership with specialized departments based on

[40] Jasper, *Roshia saibā shinryaku*, p. 298.

[41] “Zero Trust Maturity Model Version 2.0,” CISA, April 2023.

[42] “Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,” NIST Special Publication 800-37 Revision 1, December 2018, pp. 8–12.

the five-step maturity model[43] and providing feedback for threat intelligence.

### (4) Securing the Capabilities to Obstruct the Use of Cyberspace

With regard to capabilities for obstructing an opposite party's use of cyberspace[44], because they have a direct impact on that party's cyber attack activities, they are effective of course for deterring cyber attacks and also as a capability for obstructing that party's command & control and telecommunications. For that reason, it is necessary to select objectives based on situational awareness in cyberspace, attribution, and the like, and direct all capabilities including active cyber defense capabilities. Furthermore, exposing an opposite party's attack in advance can also be expected to have certain effects. Since these require sophisticated and practical capabilities, it will be necessary to partner with a variety of units on timing, degree and scope of implementation and so forth to wield the means effective for the situation. It will also be necessary both to deepen the discussions over roles, missions, and capabilities, and to implement practical training.

### (5) Promoting Legislative Preparations in Cyberspace

While international cyber law does not clearly exist, the discussions are ongoing[45]. Interpretations of the Tallinn Manual 2.0 that serves as a reference for norms are complex, and its ambiguities are the subject of debate. However, in eliminating and clarifying the ambiguities, finding a balance is also important since cases are also occurring where in a turn around they are being used to launch cyber attacks[46]. Also, with regard to cyber-related legislative preparations in Japan, these need to be developed quickly so capabilities such as active defense can be demonstrated[47], and also need to hasten improvements in practical capabilities.

### (6) Cultivating Human Resources

In order to strengthen the human resource base, measures such as raising the retirement age for SDF officials, expanding reappointment, and securing human resources including civilians who possess specialized knowledge and skills are being taken, along with a significant expansion in regard to SDF reservists including the cyber domain[48]. That initiative has already begun, with fiscal 2027 being the target for expanding the cyber-related units to approximately 4,000 persons and having 20,000 cyber personnel[49]. Support efforts for private businesses including in critical infrastructure fields will be needed, as will the cultivation of a broad range

[43] "A Framework for Cyber Threat Hunting," sqrrl, White Paper, pp. 3–10.

[44] "Bōeiryoku seibi keikaku ni tsuite," p. 11.

[45] Jasper, *Roshia saibā shinryaku*, pp. 153–157.

[46] Ibid., pp. 270–273.

[47] "Kokka anzen hoshō senryaku ni tsuite," pp. 21–22.

[48] "Kokka bōei senryaku ni tsuite," pp. 27–28.

[49] Ministry of Defense, "Wagakuni no bōei to yosan: Bōeiryoku bapponteki kyōka 'gannen' yosan," March 28, 2023, p. 21.

of human resources including in related legal fields.

## 6. Course of Action for Demonstrating a Deterrent in Cyberspace

We have considered elements to be developed essential for strengthening cyber warfare capabilities from a defensive force buildup perspective. By giving military potential to these elements, cyber attacks can be detected and prevented through countermeasures. Recovery can also be achieved through early detection and countermeasures even in an occurrence of a cyber attack. Obtaining resilience in the system such that it can still function regardless of a breach will lead to deterrence by denial. From the perspective of conflict deterrence, it is important to appropriately select an order of priority that guarantees crucial functions even if some functionality is lost so as to maintain compatibility with operations, maintain command and control functions and information collection and analysis functions, and minimize the impacts on these functions.

Constant surveillance and swiftness in responding to new threat information that allows for dealing with cyber attacks that changes day to day is also important here; analysis of various information and information obtained will also lead to identifying the source of the attack. With regard to counterattacks, imposing costs on the opposite party is effective. This is done by naming and shaming the opposite party by exposing a state of attack, and by working not just in cyberspace but in close concert with other domains including the kinetic, as well as various other domains such as the diplomatic and the economic. Meanwhile, in a conflict situation, before, after, or timed to coincide with an armed attack, cyber attacks using a variety of techniques will take place against systems and equipment connected to Japan's use of its defense capabilities as well as against critical infrastructure. In the application of Article 5 of the U.S.–Japan Security Treaty, because Japan will work in partnership with U.S. forces that have cyber counterattack capabilities, there is a need to continually increase proficiency through joint exercises and so forth to enable smooth operation with the Cyber Mission Force (CMF) composed of units connected with U.S. Cyber Command. Classifying the situation based on the scale and severity of the cyber attacks in peace time and gray zone situations[50] and making preparations to address an expansion of the situation is important. This sort of activity leads to deterrence by punishment.

Based on considerations of the Ukraine invasion, powers of recovery are also important to suppress the effects of a cyber attack, and attribution is essential to situational awareness and dealing with what comes after. It is important to not show the weaknesses to the opponent and take care not to be drawn into asymmetrical warfare by strengthening cyber warfare capabilities. As from the perspective of hybrid warfare, it is also important to make the most

[50] Masahiro Matsumura, "Wagakuni no saibā sekyuriti senryaku no ketten to tenbō: 'Heiwa Kokka' taisei no shikkoku e no taiō o kangaeru," *Journal of Information and Communications Policy*, vol. 5, no. 2. 2022, III-1-III-22. https://www.soumu.go.jp/main_content/000787278.pdf

of the comparative advantages to the side maintaining the status quo by quickly responding in close cooperation with other domains, such as steadfastly maintaining networks to defend against attacks and proactively disclosing the truth, since cyber attacks take place using a combination of various methods in multiple simultaneous, time-sequenced, and wavelike ways. These will result in integrated deterrence.

In terms of the means for communicating these capabilities to an opposite party, while bearing in mind the need to not show its hand, Japan needs to carry out such measures as formulating and publicizing its cyber strategy with regard to security, publicizing joint cyber exercises with the U.S. and other countries, achieving results such as winning high marks in cyber offense and defense (Capture the Flag, CTF) contests, and retaining personnel qualified in connection with advanced security. Getting an accurate grasp of the state of a cyber attack is also important. When managing actions in gray zones and in contingencies, it is necessary for Japan to promptly enhance its preparedness to better demonstrate its organizational strength in cyber command and control functions and blend them organically with other domains, and—based on their synergistic effects—link them closely as part of its cross-domain operations capability that amplifies the capability of the entire organization[51]. It goes without saying that partnering with other countries including the U.S.[52] is also important here.

## 7. The Evolution of Cyberspace

Ever since the enhancement of remote environments occasioned by the Covid-19 pandemic,

dramatic changes to cyberspace in forms visible to the eye have been acknowledged. Based on the premise that the new domains are having an impact on how battles are waged, further technological developments will be a game changer. They will become factors that further develop previous arguments, or contain uncertainties to such a degree that those are overturned. Accordingly, we want to touch on the main changes.

### (1) Cloud Computing

The cloud is a form that has accompanied the enhancement of the network environment, where it uses the resources in a data center without physically possessing the computing resources necessary to it[53]. The Ministry of Defense, too, is already moving toward its development as a shared infrastructure[54]. Services that use this environment to protect the cloud environment itself are also being provided[55]. Considering that the environment is

[51] “Kokka anzen hoshō senryaku ni tsuite,” p. 22.

[52] Ministry of Foreign Affairs, “Nihon no saibā bun’ya de no gaikō: Nikokukan kyōgi, taiwa tō,” February 7, 2023. https://www.mofa.go.jp/mofaj/fp/nsp/page24_000687.html

[53] Japan Business Federation, “Bōei dejitaru toransufōmēshon (DX) no genjō to dōkō,” *Bōei gijutsu hōkokusho*, March 2023, pp. 261–265.

[54] “Bōeiryoku seibi keikaku ni tsuite,” p. 7.

[55] Microsoft Corp., “Microsoft Defender for Office 365.” https://www.microsoft.com/ja-jp/security/business/siem-and-xdr/microsoft-defender-office-365

constructed in a way that integrates the conditions of the server that provides services from an endpoint with data correlation technologies, it is assumed that the precision of capabilities to identify the sources of cyber attacks is greatly improving. The use of cloud environments needs to be considered from a cyber warfare perspective.

### (2) Diverse Network Environments

In Russia's invasion of Ukraine, internet use based on the Starlink system comprised of small satellites in low Earth orbit has attracted much attention. This service has also been launched in Japan, making it possible to use high-speed internet throughout the country. There is no need to use communications facilities spread out around the ground, and resilience in combination with the ground-based network is improved. Furthermore, when it comes to transmission methods, the 5G service[56] has already been launched, and the network environment going forward will further evolve. Also, studies are underway on a new QUIC protocol that would replace TCP for the fast encryption internet transmission protocols (TCP/IP). The Internet Engineering Task Force (IETF) has recommended it as "RFC9000[57]," and it is now at the stage of practical implementation. Still further, there are also moves toward new services that would make it possible to deliver high-speed, high-capacity transmissions that exceed the limits of the internet so far, along with enormous amounts of computational resources and the like[58]. New fields have the potential to be used in various ways for both attacks in cyberspace and activities for defense. It will be necessary to pay attention to trends.

### (3) Practical Applications of Quantum Technology

The first domestically manufactured quantum computer has begun operating in Japan[59]. Its performance that even surpasses that of super computers has also attracted notice especially in the field of cryptography. Because today's security technologies are based on encryption technology, the practical implementation of quantum computers presents a new threat and a variety of countermeasures will need to be created as soon as possible. The adoption of physical cryptography and post-quantum cryptography will likely be the realistic initiative at the present stage[60].

[56] Ministry of Internal Affairs and Communications, "Heisei 30-nenban Jōhō tsūshin hakusho." https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/html/nd133420.html

[57] J. Iyengar and M.Thomson, eds., "QUIC: A UDP-Based Multiplexed and Secure Transport," IETF, May 2021.

[58] NTT, "IOWN." https://group.ntt/jp/group/projects/iown.html

[59] "Riken, kokusan ryōshi keisanki o kadō: Bei-Chū kyōsō ni Nihon mo nanori," *Nihon Keizai Shimbun*, March 27, 2023. https://www.nikkei.com/article/DGXZQOUC234XF0T20C23A3000000/

[60] Katsuyoshi Harasawa and Kazuo Tokito, "Tsūshin sekyuriti to ryōshi angō," *Bōei gijutsu jānaru* [Defense technology journal], no. 41, May 2021, pp. 4–14.

### (4) Connections with the Cognitive Domain

While cyberspace does not encompass all layers of the cognitive domain, it is closely related to digital influence operations[61]. Since there is a necessity of also strengthening responses to information warfare in the cognitive domain[62], the strengthening of capabilities in cyberspace is also a function directly related to digital influence operations. Therefore, interconnectedness with information warfare is required[63].

### (5) Practical Application of AI Technology

AI technology is attracting attention in a variety of fields. The aforementioned language-model GPT has the potential to change the world. The possibilities that automation and analysis in cyberspace will contribute to a surprising acceleration of decision-making can be imagined to be incredibly huge. Accordingly, it will be necessary to pay attention to trends going forward while investigating practical implementation beginning with what is feasible.

## 8. The Issues of Deterrence in Cyberspace

In regard to deterrence in cyberspace by Japan, while this will be dramatically strengthened by the three security documents, this needs to be steadily developed and given military potential. In addition to that, the issues are as follows:

(1) In regards to cyber attacks, secure the functions that are a system's purpose and strengthen its power to execute them by strengthening deterrence by denial and maintaining resilience.
(2) With respect to deterrence by punishment, from the perspective of active cyber defenses, build up offensive capabilities and prepare their legal basis, and guarantee effective capabilities with good governance
(3) With respect to developing the systems for strengthening cyberspace capabilities including training personnel, it is necessary to conceptualize and disseminate the strengthening of cyber warfare capabilities.
(4) Guaranteeing superiority in cyberspace including public-private partnerships is crucial.
(5) In regards to cyber attacks, building an integrated response system that includes diplomatic inquiries, sanctions, and litigation is necessary.

[61] Kazuki Ichida, et al., *Netto seron sōsa to dejitaru eikyō kōsaku: 'Miezaru te' o kashika suru*, Hara shobō, March 2023, p. 10.

[62] "Kokka anzen hoshō senryaku ni tsuite," p. 24.

[63] Takamichi Saitō, "Dejitaru eikyō kōsaku no pureibukku,' in Kazuki Ichida, et al., *Netto seron sōsa to dejitaru eikyō Kosaka*, pp. 49–78.

## Conclusion

The situation with respect to deterrence in cyberspace is steadily changing in conjunction with the evolution in the latest technologies and usage patterns, where the source of an attack is identified by rapidly collecting and analyzing large volumes of data, and response to a cyber attack is automated using AI. However, the scope impacted is expanding rapidly. What is important is to deter conflicts by alertly grasping technology trends in IT, quickly adopting those that are necessary, and partnering with many other organizations. Innovative concepts from the whole country about how cyberspace is to be used as a means toward that end and their continued implementation will likely function effectively as a deterrent against wars that are drastically changing (War 3.0). It has become an age where such actions are necessary.

# Chapter 5

# Issues for Japan and U.S. Cyber Operations in a Taiwan Contingency

**Satoru Mori**

## Introduction

What missions in the area of cyber operations would Japan and the U.S. have to undertake in the event a Taiwan contingency broke out? What capabilities does Japan require for the mission it would have to carry out in the cyber domain, and what are the issues in terms of their development? The goal of this article is to consider these questions and conduct a preliminary investigation of Japan's initiatives going forward. Accordingly, this article is a thought exercise that will deductively lay out the issues in Japan–U.S. cyber operations. We wish to set down in advance that it is not the sort of report that describes or assesses existing policies.

To begin with, in proceeding with this investigation, we would like to affirm the three basic conditions upon which it is premised. First is the premise that China has as its strategic objective changing the status quo by having control over Taiwan or the Senkaku Islands, and that Japan and the U.S. will adopt defensive strategy whose objective is to deny changes in the status quo by armed force. Second is that while they have to deny a showdown with China in the short term, if the war lengthens, the possibilities will increase that Japan and the U.S.' will to continue the war will wane. Third is that, for Japan and the U.S., the fundamental objective is to deter a change in the status quo by armed force. Should this deterrence break down, it will result in the conducting of a Japan–U.S. joint operation, and such an operation would have a double-sided nature. That is, it would require carrying out (1) offensive operations to diminish the capabilities and will that China needs for its "Theory of Victory" (TOV) in order to achieve its strategic objectives, and (2) defensive operations to protect the capabilities and will that the U.S. and Japan need for TOV in order to accomplish their strategic objective (the denial of China's strategic objectives). When Japan and the U.S. had an advantage in capabilities over China, they were able to deny China's strategic objectives mainly through a defense strategy centered on defensive operations. However, with the deterioration in the regional balance of conventional armed forces, it has become necessary to combine not only defensive operations but also offensive operations and increase the latter's relative importance appropriately.

Based on the foregoing basic presumed conditions, with regard to offensive operations to diminish the capabilities and will that China needs to achieve its strategic objectives and the defensive operations to protect the capabilities and will needed for the strategic objective of denying a change in the status quo by China, we will lay out what roles Japan and the U.S. could conceivably play in cyber operations (Sections 1 and 2), and investigate the capabilities needed for the missions that correspond to each role and the main issues in regard to developing those capabilities (Section 3).

## 1. Roles in Cyber Operations, 1: Offensive Operations (Primarily U.S.)

First, we would like to lay out what missions will be necessary in cyber operations in order to diminish the "capabilities" and "will" that China needs for its TOV (the issue of cyber attacks by the U.S. or China on nuclear command, control, and communications [NC3] falls out of the scope of this article's investigations).

### (1) Cyber Operations to Diminish the "Capabilities" Necessary to China Realizing Its TOV

The "capabilities" needed for China's TOV can be thought of as comprising military capabilities and the private and social infrastructure that supports those military capabilities. We will investigate these separately.

First, China's TOV comprises as its most fundamental elements (1) missile attacks, (2) gaining air superiority, (3) gaining command of the sea, and (4) landing operations. According to the "integrated maritime defense-in-depth strategy" that Sugio Takahashi mentions in his book, while (1) and (2) are regarded as difficult to stop, (3) and (4) can be prevented, so anti-ship missile saturation attacks are seen as being effective. In light of this, the question of how much that effectiveness can be improved depends on how far China and the U.S. or Japan can detect the targets of those attacks—that is to say, it depends on intelligence, surveillance, and reconnaissance (ISR) capabilities[1]. If the People's Liberation Army (PLA) were to carry out various attacks based on the integrated operation of units that would draw upon ground-launched missiles, aircraft, and ships, cyber attack missions are conceivable targeting the various functional phases of the Observe-Orient-Decide-Act (OODA) loop from detecting targets to carrying out attacks. These would be "counterforce cyber attack missions" targeting military organizations. At that point, the question becomes wielding what sorts of cyber capabilities against what part of the PLA's OODA loop would be effective.

Furthermore, given that there is also private and social infrastructure that directly supports PLA units (for example, telecommunications infrastructure, ships, aircraft, etc.), if as a result of China's wielding of information warfare against Japan and the U.S. the "fog of war" around the two countries thickens, then it is possible they be forced to escalate the scope of their attack targets from counterforce to countervalue. Should the situation lead to this point, while

[1] Sugio Takahashi, *Gendai senryakuron: Taikokukan kyōsō jidai no anzen hoshō*, Namiki shobō, 2022, pp. 201–209.

it would depend on the war conditions, fundamentally non-kinetic “countervalue cyber attack missions” would play a major role operationally.

### (2) Cyber Operations to Diminish the “Will” Necessary to China Realizing Its TOV

In the event that deterrence fails and there is an attack from China and it ends up embarking on a so-called contingency, for Japan and the U.S.—which take a defense strategy aimed at maintaining or restoring the status quo—the strategic objective would be to persuade China’s supreme decision-makers to abandon changing the status quo through armed force or at least get them to temporarily halt (postpone) it. We will not know whether China’s supreme decision-makers will choose the option of escalating or that of pausing, working out how to regroup, and resuming the attack at a later date until that moment when, after having decided to change the status quo through armed force and begun their effort, they are confronted with a situation where achieving such is difficult.

The question is which indicators China’s decision-makers will focus on to decide on their response. If conditions in China are stable, does that make it easier to choose escalation or to pause and regroup? Or, if criticism against the establishment erupts domestically in China, will decision-makers see their legitimacy as being at question and that lead more easily to escalation, or will they worry that the situation will get even worse and decide to pause external military actions and prioritize restoring public order at home? General forecasts are probably impossible, and ultimately the issue will likely be one of intelligence under each specific situation. If criticism against the establishment were to erupt domestically in China, information operations using cyber means would likely carry great significance since China would need to focus more on stopping rather than continuing a military action with no visible exit and restore public order at home. Information operations of this sort would fall under the category of “countervalue cyber attack missions” whose goal is to influence and divide public opinion.

## 2. Roles in Cyber Operations, 2: Defensive Operations (Primarily Japan)

Given that China—based on the expectation that Japan and the U.S. will prevent China from achieving its strategic objectives—will execute attacks meant to diminish the “capabilities” and “will” of Japan and the U.S. that create such a threat, we want to now lay out the defense missions that Japan and the U.S. must carry out in cyber operations in response to an attack from China.

### (1) Defense Against Attacks by China on Japanese and U.S. “Capabilities”

Assuming that the warships, vessels, and ground forces used in a transoceanic landing operation are of vital importance to China, the PLA will come to hinder the anti-ship attack capabilities of the U.S. military and the SDF. Namely, conceivable are (1) attacks on and interference with Japan and U.S. ISR assets; (2) attacks by unmanned systems on Japan and U.S. platforms for anti-ship purposes; (3) attacks by ballistic and guided missiles on the staging points (bases, etc.) of Japan and U.S. anti-ship attack platforms; and (4) cyber attacks on national defense networks meant to hinder the integrated operations capabilities of the U.S. military and the SDF. Additionally, assuming that China attempts to deprive Japan of its capabilities to deal with gray zone situations, one may also assume cyber attacks on Japan's law enforcement agencies. The cyber operations focused on the PLA meant to counter these attacks will be items included exclusively under the "counterforce cyber attack missions" taken up in 1 (1).

Chinese cyber attacks can also be expected on the private networks that support Japanese and U.S. operations in various ways. One can presume, for example, cyber attacks on the networks of the private shipping companies that handle transport; cyber attacks on defense industry networks with the goal of disrupting Japanese and U.S. munitions production systems; and cyber attacks on the networks of critical infrastructure such as the systems that supply the electricity necessary to the operations of the defense and other industries. With the active cyber defenses whose introduction was announced in the National Security Strategy of Japan, notifications of cyber attacks from private companies and the monitoring of data flows on telecommunications company networks will lead to improving situational awareness in cyberspace and plotting the necessary responses. With regard to grave cyber attacks on the government and critical infrastructure, Japan and the U.S. will adopt active defense strategies to intrude the attackers' servers and render them harmless beforehand.

### (2) Defense Against Attacks by China to Diminish Japanese and U.S. "Will"

The possibility of China working to mold public opinion in Japan and the U.S. through an information operation to oppose intervention in a Taiwan contingency is conceivable. In the U.S., there is the possibility of China whipping up opinion opposed to intervention out of fears of escalation in the conflict. In Japan, the counterargument could be stirred up that cooperating with the U.S. in an attempt to intervene in the defense of Taiwan would result in a retaliatory strike from China and people's lives would be at risk. The issue is how to deal with information operations in the so-called cognitive domain.

## 3. Missions in Cyber Operations

The various types of operational missions and issues laid out in Sections 1 and 2 will be broadly laid out as follows. In view of the capabilities that Japan and the U.S. currently have, it would likely be reasonable for the roles to basically be divided, with the U.S. military in charge of offensive operations in cyberspace and the SDF in charge of defensive operations.

### (1) Missions in Offensive Operations by the U.S.

#### A) Counterforce Cyber Attack Missions

The question here is implementing what sorts of cyber attacks against what part of the PLA's OODA loop will be effective. In terms of hindering the PLA's ISR capabilities, cyber attacks can be conceived of against satellite systems and sensor-equipped manned or unmanned vehicles. When it comes to hindering PLA command and control (C2), conceivable measures would include interrupting the functions of communications networks and contaminating and deceiving data meant for the cloud where sensor data is collected.

#### B) Countervalue Cyber Attack Missions

The question here is against which parts of China's private and social infrastructure carrying out what sort of cyber attack would be effective. In the case of targeting the private systems that support PLA logistics, for example, one could conceive of cyber attacks against those actors that operate railroads and shipping along China's coastal regions and primarily in Fujian Province, or critical infrastructure such as the power supply networks in major coastal cities that support the social and economic system. If pressured by the need for escalation, and pressured by the need to carry out cyber attacks of a scale and standard that would force the degradation of infrastructure intended for the general public, attacks on financial system and media organization servers along with the networks of water and gas grids could also be included among the options.

#### C) Cyber Attack Missions on the Cognitive Domain

The question here is what sorts of information operations should be attempted against the PRC citizens' cognitive domain, and what results they should aim to produce. One could conceive of the large-scale circulation of narratives and messages using such means as social media that would cause popular support for the option of unification with Taiwan by armed force to recede. While investigations based on a more specialized analysis would be needed to determine specific narratives, generally speaking, one could imagine spreading messages in forms that embedded more specific information of varied purport. For example, such messages could say, " Bringing Taiwan under control through armed force at great cast will be of little benefit to the Chinese people, so changing the status quo by force is a failed strategy and should be abandoned at once," or "If Taiwan is unified by force, China's relations with major powers will worsen over the long term afterward, and the considerable costs to be paid will more than offset the benefits won by unifying with Taiwan, so the attempt should be abandoned at once."

### (2) Missions and Capabilities in Defensive Operations by Japan

The Japanese government should focus its protections on the national defense-related networks of the Ministry of Defense and the SDF; public networks such as those of government ministries, law enforcement agencies and critical infrastructure; and the networks of private sector enterprises, along with the cognitive domain of the general public that is contiguous with the digital space.

### A) National defense network defense missions/Government ministry and law enforcement agency network defense missions/Private network defense missions

The nature and security standards of networks differ when it comes to national defense, government ministries, law enforcement agencies, and private sector enterprises. However, when defending networks as a state, the question becomes one of what capabilities to acquire. The capabilities to be acquired conceivably would be those of cyber situational awareness and cyber resilience. In the future, one could also imagine the acquisition of precision cyber counterattack capabilities[2].

With regard to cyber situational awareness, in the National Security Strategy, measures were taken to enable private businesses to share information with the government when a cyber attack occurs, and to enable the utilization of information related to the transmissions that domestic telecommunications carriers provide as a service to detect servers suspected of being misused by attackers[3]. After putting existing and new measures into effect, it will be necessary to realize comprehensive capabilities that can detect situations where severe cyber attacks are occurring, including at the stage immediately prior to a contingency occurring. For example, if a multitude of activities in cyberspace take on the appearance of activities that, while ostensibly legitimate, on the whole would create harm and risks in terms of security when they progress and develop in conjunction with one another, it will be necessary to acquire the capabilities to detect automatically or semi-automatically a skillful and sophisticated cyber attack that is not obvious at first glance by "connecting the dots" of those activities. To achieve this, advanced cyber attack detection systems using AI must be developed[4].

With regard to cyber resilience, what is needed is to develop a program that automates patching vulnerabilities and a mechanism that automatically builds, improves, and repairs complex software. The following three approaches may be possible. (1) Defend through preemptive patching (getting rid of vulnerabilities). (2) Develop systems that are sufficiently reliable and deal with bots and so forth using AI. (3) Use AI to assess the structure of a system and reduce vulnerabilities by making changes to that structure[5]. Since completely

[2] The various initiatives of the Information Innovation Office (I2O)—which is the cyber and AI unit of the U.S. Defense Advanced Research Projects Agency (DARPA)—are instructive. The issues raised in this section of cyber situational awareness, resilience, and precision counterattacks are future issues in the cyber area that the I2O's director brought up at an event celebrating the 60th anniversary of DARPA's founding.

[3] Decision by the National Security Council and the Cabinet, "Kokka anzen hoshō senryaku ni tsuite," December 16, 2022., p. 21.

[4] For example, DARPA's Cyber-Hunting at Scale (CHASE) project aims at developing such capabilities.

[5] For example, DARPA's Assured Micropatching (AMP), Cyber Assured Systems Engineering (CASE), Configuration Security (ConSec), and Symbiotic Design for Cyber Physical Systems (SDCPS) projects are

preventing intrusions is impossible, the issue becomes one of quickly making up for vulnerabilities when an attack has occurred and guaranteeing security at as high a level as possible, while restoring and restarting systems after the incident.

Furthermore, as laid out in the National Security Strategy, when it comes to attacks on the state and critical infrastructure, measures for infiltrating an attacker's server and nullifying it in advance will also be adopted going forward as part of active cyber defense. In addition, looking forward, it is likely that the option of carrying out a precision cyber counterattack in the face of a cyber attack having taken place will also be given consideration. One conceivable option would be to develop collaborative systems between man and machine, detect cyber attacks by making use of machine learning and pattern detection and, based on appropriate human decisions, develop the capabilities to carry out precision cyber counterattacks. One imagines that these machines would detect attacks based on the analysis of large amounts of data, and humans would determine the appropriate ways to counterattack based on the context. In such a case, it is conceivable that—among the red space (the domain of the enemy), gray space (a neutral domain), and the blue space (one's own domain)—so-called bot nets in the gray space may be identified and nullified. Developing technological solutions and policies toward that end is called for[6].

### B) Cognitive Domain Defense Missions

If conditions revolving around Taiwan become tense and a situation where the crisis is growing arises, it is possible that China—targeting the cognitive domain of the general publics of the U.S. and Japan—would pursue information operations in cyberspace to stir up an environment advantageous to itself by circulating text and images across social media[7]. It is possible that it would try to interfere with Japan–U.S. cooperation using a variety of information. For example, it might stir up discourse critical of the strategies and policies of the Japanese government cooperating with U.S. responses to crises and contingencies. Or, if an armed conflict were to develop between the U.S. and China over Taiwan, it might spread false information such as a discourse about how Japan cooperating with the U.S. would become the object of Chinese attack and how there would be many victims in Japan, or about U.S. forces being involved in incidents inflicting bodily harm in Japan[8].

in the middle of developing technologies for implementing these three approaches.

[6] DARPA's Harnessing Autonomy for Countering Cyberadversary Systems (HACCS) project and so forth are moving forward on development of such capabilities.

[7] With regard to Chinese influence operations and conflicts over the psychological and cognitive domains, refer to the following. Shinji Yamaguchi, Masaaki Yatsuzuka, and Rira Monma, *Chūgoku anzen hoshō repōto 2023: Ninchi ryōiki to gurēzōn jitai no shōaku o mezasu Chūgoku,* National Institute of Defense Studies, 2023, pp. 26–47; and Yū Koizumi, Kyōko Kuwahara, and Kōichirō Komiyama, *Nisejōhō sensō: Anata no atama no naka de okoru tatakai*, Wedge, 2023, pp. 52–87.

[8] Kyōko Kuwahara, "Taiwan yūji ni okeru disuinfomēshon no kyōi to taisaku no arikata," Japan Institute of International Affairs Research Report, March 1, 2022. https://www.jiia.or.jp/research-report/security-fy2021-01.html; and Jun Ōsawa, "Hybrid warfare in a Taiwan contingency," Sasakawa Peace Foundation

Discourse that, for example, expresses criticisms of government strategies and policies along with appealing to feelings of fear about a war breaking out can arise within Japan or be injected by an adversary into Japan's discourse space. There also is the possibility that the two will combine and the arguments in Japan opposing cooperation with the U.S. and antiwar voices will grow louder. This type of information warfare that works to amplify certain opinions at home is a "battle over opinions." As such, the government has no choice but to explain its strategies to the public. The question of whether those explanations will be accepted by the public hinges on the degree of confidence that the public has in the government. This is not a situation that can be handled on the spot when such conditions develop. Rather, it will depend on whether the government can regularly win the trust of the people[9].

On the other hand, with regard to disinformation, various efforts are underway in other countries[10]. Japan, too, will need to devise various sorts of countermeasures based on the efforts of those other countries. The circulation of disinformation will likely take place through various media. However, it is conceivable that the disinformation that circulates through image (moving and still) media fabricated using high-quality generative AI will lead to serious problems. It is said that every day more than two billion images are uploaded to social media around the world, and the number of fabrications is only expanding. Should a Taiwan contingency occur and the submarine cables connecting Taiwan with the Chinese mainland were cut and satellite communications were also interfered with, the resulting situation would be an information blackout. That is, it is possible that other countries would find it difficult to get a sense of the situation in Taiwan, and in Taiwan it would be difficult to assess developments in other countries. With information starvation resulting from a de facto information blockade, if extremely fabricated images of a quality so high that one could not easily recognize that they are fabrications were circulated, it could have a major impact. Moreover, if such kinds of fabricated images are distributed as ones that were obtained from wide-ranging and, at first glance, unrelated routes, they may be accepted as "well-supported items." If various images circulate with plausibility in Taiwan that deliver a de facto message whose thrust is that support from other countries cannot be anticipated and also other images circulate in foreign countries that deliver a de facto message that Taiwan's citizens have lost their will to fight, public opinion in Japan, the U.S., Taiwan, and third-party countries, as well as the government's decisions in politics, diplomacy, and strategy may become confused. Limiting such risks will call for a platform to engage in a comprehensive and automated analysis of data forensics. If data forensics can be performed on a large scale, it would become a counter-

International Information Network Analysis (IINA), August 24, 2022.

[9] The author is grateful for comments by Sugio Takahashi on this point.

[10] The "Indo-Pacific Regional Disinformation Research Series" that the Sasakawa Peace Foundation publishes at its International Information Network Analysis (IINA) introduces examples of initiatives from Australia (Tomoko Nagasako), the U.S. (Satoshi Narihara), and Singapore (Kei Koga), and an article on the effectiveness and limitations of fact-checking as a disinformation countermeasure (Masato Kajimoto).

disinformation measure that would disclose the facts of fabrications. It is conceivable that the technologies for discerning the real and the fake of such image data will perhaps interact recurrently with technologies meant for deception. Investments for ongoing development will be necessary.

## 4. Conclusion

The cyber domain is becoming more and more complex and difficult due to at least the following three factors. First, the potential attack targets are rapidly expanding. While the reliance of Japan and the U.S. on information technology and the cyber domain is growing rapidly in terms of both scale and the complexity of applications, that does not mean that systems sturdy enough to withstand cyber attacks from the PLA and related organizations are spreading. Second, conditions will continue such that the actors who perform cyber attacks will be able to do so since they will be immune to a considerable degree going forward, too, from punishment and retaliation. It will be possible to substantially improve the effectiveness of attacks by enabling the use of vast amounts of resources on computers in both legal (commercial cloud) and illegal (botnets) forms, as well as concealing one's various offensive activities amid the enormous data transmissions over the internet. Also, the situation is further complicated by the fact that it is possible for not only a military's cyber forces but third-party organizations to arbitrarily help with attacks. Third, the cyber battlefield will continue to be enveloped in a deep "fog." While cyber technologies for defense uses are developed for civilian uses, cyber technologies for offensive uses are developed by state and non-state actors in secret. Accordingly, getting an accurate grasp of the cyber warfare capabilities of an adversary power will continue to be impossible or extremely difficult. The possibility of being confronted with a technological surprise cannot be denied, and it will be necessary to improve capabilities for grasping the activities of an adversary power[11].

Should a Taiwan crisis or contingency occur, the missions in terms of cyber operations presented in Section 3 above would be implemented in the context of the trends in cyber domains as mentioned above. With the U.S. playing the main role in cyber offensive operations, Japan must prioritize handling cyber attacks directed toward itself; make effective the network defenses for national defense, government ministries and law enforcement agencies, and private sector companies through various measures for active cyber defenses, while also responding to information operations aimed at the cognitive domain of the Japanese public. When such cyber defense operations are carried out, the capabilities in cyber situational awareness, cyber resiliency, and disinformation strategies will come into question. There seem to be numerous specific issues in pursuing these grand initiatives. From the perspective of developing the fundamental capabilities that will be needed based on a division of roles and

[11] These comprise the principal trend in the cyber domain as pointed out by the director of the I2O at an event celebrating DARPA's 60th anniversary.

missions in Japan–U.S. cyber operations, the important issues and urgent tasks will be divided up as follows: (1) with regard to cyber situational awareness, adopt AI and machine learning in order to detect attacks by analyzing the vast amounts of data that varied sensors have been collecting; (2) with regard to cyber resiliency, transition to a zero-trust architecture in order to mitigate the risks that come with an expansion of potential attack targets; and, (3) with regard to disinformation strategies, adopt a large-scale data forensic platform in order to determine the authenticity of vast amounts of image data.

# Chapter 6

# The Evolution of Air & Space Power and Deterrence

**Kimitoshi Sugiyama and Hiroshi Nakatani**

## Introduction

Since the dawn of time, human beings have long dreamed about flying in the skies, as symbolized by the flying machines depicted by that great Renaissance period artist Leonardo da Vinci. Humanity—having achieved this long-held dream and stepping out into space—has moved beyond the skies to reach space, and is now even considering activities on planets other than theEarth. In sum, the space and domains into which humans are stepping into have tremendously expanded. Accompanying this, humanity's conflicts in these domains are also intensifying, and the question of how to use these domains strategically will be a factor that will have considerable sway over international politics going forward. The air domain where air power is demonstrated is a vast space that covers the skies over land and sea and connects them to space. From the perspective of effectively demonstrating air power, given that making good use of information collection, of such space assets as telecommunication and positioning satellites, of a wide variety of computer networks, and of a wide band of electromagnetic waves is essential, it could be said to be one of the combat domains to be most impacted by fights in the so-called new domains of space, cyber, and electromagnetic. And, in keeping with the rise of space that sits beyond air as a strategic domain these days as can be seen in the creation of space forces, the combination of air and space as air and space power is essential when talking about strategy in the modern era.[1]

From these perspectives, in the present chapter we take up air and space power as an example. Based on their characteristics and evolution, we will discuss how superiority in the new domains contributes to aerial warfare and deterrence. What, then, is air and space power? In this paper, to borrow from the definition of "air power" offered by William (Billy) Mitchell[2]—the progenitor of a strategy for aerial warfare who, from an early era, with his foresight, called

[1] As one example, responding to the changed strategic environment, at the end of 2020 the Royal Australian Air Force changed the name of its research institute from the Air Power Development Centre to the Air and Space Power Centre. For the primary factors and background behind the name change, refer to the following. Air and Space Power Centre, "Chief of Air Force- Launch of Air and Space Power Centre," December 2, 2020.
https://airpower.airforce.gov.au/videos/chief-air-force-launch-air-and-space-power-centre

[2] For Mitchell's definition of air power, see the following. William Mitchell, *Winged Defense: The Development and Possibilities of Modern Air Power Economic and Military*. 1925. Reprint, Dover Publications, 1988, pp. 3–4. See also the following. Colin S. Gray, *Air Power for Strategic Effect*, Air University Press, 2012, pp. 8–9, 305.

for the establishment of an air force as an independent military service—we define "air and space power" as "the ability to achieve objectives in or through the air or outer space." Accordingly, this means that air and space power is not solely comprised of such weapons as fighters or anti-satellite weapons. These are nothing more than the constituent parts of air and space power. The fact is, there are numerous factors that operate in air and space, and support the achievement of objectives through their activities. In short, when thinking about air and space power, we need to think of air and space as an integrated system.[3]

Also, today in the 21st century, the illusion of a "unipolar" world led by the U.S. that had become widespread after the Cold War has come to an end, and the return of great power competition has been declared.[4] The frontline of great power competition in the 21st century is the Indo-Pacific, and the stability of this vast region is more crucial than ever.[5] As the core concept with regard to this great power competition, the U.S. Biden administration in its National Security Strategy has come out with "integrated deterrence." One of the major features in this concept signifies that deterrence cooperation with allied countries is greater than before.[6] Meanwhile, Japan's own National Security Strategy announced in December 2022 stressed to the effect that Japan shall defend itself on its own by fundamentally strengthening of its defensive capabilities[7]. Both documents suggest that Japan's efforts on deterrence be all the more vital, and based on the recognition that it is all the more timely to be thinking about what deterrence using air and space power actually might be, in this chapter we will talk about deterrence that draws fully upon air power.

## 1. The Evolution of and Transitions in Air and Space Power

The air and space power—which function primarily in air and outer space—are global in nature. If one were to draw fully upon air and space power, it would be theoretically possible to swiftly access any location that is above ground without regard to such topographic restrictions as mountains and rivers. Accordingly, it did not take long for air and outer space to be used for military purposes, including everything from operational support in the forms of

[3] In fact, Mitchell saw air power as an integrated system that involved the relationship among, for example, personnel, aircraft, industry, production capabilities, maintenance personnel, aerial routes, fueling stations, civil aviation, and relationship among air and other domains. On this point, please see the following. Mitchell, *Winged Defense*, pp. 31–33.

[4] The White House, *National Security Strategy of the United States of America*, December 2017, p. 27. https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf. Refer also to the following. Elbridge A. Colby, *The Strategy of Denial: American Defense in An Age of Great Power Conflict*, Princeton University Press, 2021, pp. ix–xii.

[5] The White House, *The National Security Strategy of the United States of America*, October 2022, pp. 11, 37. https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

[6] Ibid., p. 22.

[7] National Security Council, "Kokka anzen hoshō senryaku" [National Security Strategy], December 2022, pp. 17–20. https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-j.pdf

reconnaissance, observation, supply, and telecommunications, to direct attacks on the mainland of a hostile country.[8] What, then, are the characteristics of this air and space power that has come to be seen today as indispensable when thinking about strategy and how has it evolved? We will consider the characteristics of air and space power and discuss their military applications below.

### (1) The Characteristics of Air Power

Since the Wright brothers made their first successful powered flight at the start of the 20th century, aviation-related technologies have developed rapidly. Air forces as a branch of the armed forces were birthed around 100 years ago. Compared to armies or navies, their history is quite slight. However, air power in war today is recognized as the indispensable element that will have a significant impact on the outcome of a war.[9]

The most outstanding characteristics of air power are responsiveness and mobility. The surface of the earth is covered by the atmosphere, and the vast aerial space that extends to outer space exists as the air domain. Flying objects such as aircraft and missiles that move through the air domain are not restrained by topography. Given how little friction there is in the air as compared with on land or at sea, supersonic flight is also possible, and they can travel across expanses at extremely high speeds. That is, air power can make rapid force projection possible against any objective not just in the air but also on the land or at sea. It is, fundamentally, a cross-domain military force.[10] Aside from this, the advantages of air power include its superb intelligence, surveillance, and reconnaissance (ISR) capabilities based on its high altitude and wide mobility range, along with its long-range strike abilities.[11]

On the other hand, when it comes to air power as represented by fighters and the like, they are vulnerable on land and their activities are easily restricted by climate conditions. There is also the need to organically partner with a variety of functions in order to manifest their military capabilities. Accordingly, it also has a vulnerability in that the loss of some functions may dramatically deteriorate the demonstration of its military capabilities.[12] For example, the F-15 fighter aircraft is built from around 100,000 parts,[13] but if all those parts are not in a state where they have been appropriately combined and properly function together it will not be possible to operate it as a functioning aircraft. Furthermore, it is also necessary to have the air bases with, for example, runways from which fighters will land and take off, the radar facilities that handle control support, and the command and communications networks to all be

[8] Tami David Biddle, *Air Power and Warfare: A Century of Theory and History*, U.S. Army War College Press, 2019, pp. 4–5.

[9] Kimitoshi Sugiyama, '21-seiki no ea & supēsu pawā.' Lecture, *Senryaku kenkyū*, no. 32, March 2023, p. 94.

[10] Biddle, *Air Power and Warfare*, pp. 4–5.

[11] JASDF Air Staff Office, "Kōkū Jieitai no gaiyō," 2022 ed., p. 14.

[12] Ibid.

[13] Tetsuyoshi Chagi, "Kōkūki iji buhin no hokyū kanri ni tsuite," *Bōei shutoku kenkyū*, vol. 3, no. 4, March 2010, section 3.

functioning properly. Still further, in order to operate the wide variety of equipment based on scientifically advanced technologies, the training of personnel will likely call for vast amounts of money and a long period of time.[14]

To summarize, when all of the aforementioned conditions come together, air power is characterized by being able to demonstrate extremely great military capabilities on the one hand, but also by the possibility of those military capabilities being dramatically reduced owning to various restrictions and the loss of certain functions. The outcome is an extremely important variable that will have an impact on the entire phase of the conflict.

### (2) The Fluctuating Concept of Air Superiority

Battles in the sky may also be described, in the most straightforward sense, as battles over air superiority.[15] Air superiority means that our air power is superior, and that the situation is such that we can execute various operations without serious interference from our enemies. Since the emergence of air power, there have been countless examples of battles where the side that has attained air superiority has achieved victory. If the enemy maintains air superiority, the fact that we will be threatened by the enemy's air power will make carrying out all of our operations difficult, including both those over land and sea. To control the skies means it is possible to look down on an enemy from a higher location, and use that potential energy to advantageously attack. On the other hand, the side that lacks air superiority will be at an extreme disadvantage since they will be in a position where it is difficult to accomplish such basic activities as transport and movement. This is why attaining air superiority has been thought to be of vital importance.

Pursuing the development of the fighter jets that are the main weapons for achieving such air superiority has been central, but the work has been constant on the evolution of such equipment as radars and surface-to-air missiles to counter them. These weapons may be broadly classified into sensors for searching and detecting (radars, etc.) and shooters as a means of attack (platforms for discharging missiles, bombs, and the like), along with networks that combine the two. The general trend is that sensors have expanded their search range and improved detection precision, shooters have extended the range of their shots and improved their target precision, and networks have accelerated and expanded the capacity on their communications. Thus, the system ceaselessly continues to evolve into something that is even more sophisticated, the combat domain is also expanding, and the aspect of combat continues to change into something that is ever more complex.

As the technologies advance, the degree to which space, cyber, and electromagnetic domains

[14] Sugiyama, "21-seiki no ea & supēsu pawā," pp. 85–86.

[15] Ibid., p. 86.

are being used is increasing more and more. GPS satellites provide precise positioning information. This means they are not only useful for navigation, but they also make possible precision guided attacks for pinpoint strikes and further enable the time synchronization needed by communications systems of all sorts. Satellite communications enable long-distance communications over the horizon, while the imaging information collected by reconnaissance satellites and missile launch detection from early-warning satellites provide extremely important timely information about enemy movements. In addition, the cyber domain is also closely connected to all military activities. Above all, wielding the highly systematized military force that is air power depends heavily on a variety of computer networks. These network systems bind together command communications, radar, weather forecasting, logistics, flight plans, air-traffic control, and power control. If they should malfunction due to, for example, a cyber attack, it could be a hindrance to the demonstration of military capabilities. It is the same with electromagnetic waves. As a means for aircraft moving through the air at high speed to communicate with headquarters and so forth on the ground, whether it be wireless voice communications or data links they are premised by the use of radio waves. Interfering with these would greatly hamper the demonstration of military capabilities.

The sequence of links known as the so-called kill chain or F2T2EA[16] comprises Find, Fix, Track, Targeting, Engage, and Assess. It is basically the same regardless of whether the means are kinetic or non-kinetic. For the attacker, it is crucial that this chain be made to function promptly and effectively, while conversely for the defender interfering with one part of this chain could deny the opposite party from achieving their objectives. Space assets like manmade satellites, computer systems of all types, and the networks that link these things together play extremely important roles in the kill chain, so they could be impacted severely by cyber attacks or electromagnetic interference.[17] Accordingly, ensuring superiority in the space, cyber, and electromagnetic domains continues to grow more and more important.

However, in reality, when it comes to the battle for air superiority, given that air power has little capacity to achieve a temporal or spatial monopoly, gaining complete air superiority is unrealistic and fluid. Even so, there is great value to gaining superiority at critical moments and over critical air space, and it will make it possible to pursue the advantage in operations overall.

In sum, the space, cyber, and electromagnetic domains are closely connected to the battles in the existing domains, and play a role as devices for greatly increasing military capabilities (force multipliers). Conversely, by interfering with these capabilities, it is also possible to vastly diminish the opposite party's demonstration of their military capabilities, and if successful can result in an extremely cost-effective attack. That is, for superiority in the space

[16] U.S. Air Force, Air Force Doctrine Publication 3-60, *Targeting*, Lemay Center, November 12, 2021, p. 27. https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-60/3-60-AFDP-TARGETING.pdf

[17] Biddle, *Air Power and Warfare*, pp. 4–5, 67–68; Krista Langeland and Derek Grossman, *Tailoring Deterrence for China in Space*, RAND Corporation, 2021, pp. 1–5.

and cyber domains to have a major impact on the battle in the air over air superiority in existing domains is becoming a reality. In a high-end battle between nations, both may make effective use of the space, cyber, and electromagnetic domains, and it is possible that superiority or inferiority in those domains will result in an overwhelming gap. Accordingly, we can no longer say that gaining air superiority is a sufficient condition for gaining victory; it is shifting way from something that assures one's superiority. Taking into account that having superiority in the space, cyber, and electromagnetic domains is also useful to gaining air superiority, it would seem necessary that we take a fresh look at the conventional concept of "gaining air superiority" to also include superiority in the new domains.

### (3) The Evolution of Air Power: Trends in Fighter Development, and Unmanned Aerial Vehicles as Game Changers

Unmanned aerial vehicles (UAVs, or drones) have developed to an eye-opening degree in recent years. They can be seen to have contributed greatly to Azerbaijan's victory in 2020 in the Nagorno-Karabakh conflict, and they are being used regardless of air superiority in the Ukraine war. Drones are demonstrating the functions of "air power." As a matter of fact, in the vast air domain, there are certain restrictions on the altitudes at which fighter planes and other aircraft can demonstrate their capabilities. For example, lower altitudes where there is a risk of an impact with the ground and high buildings are a domain where operations are difficult for manned aircraft. On the other hand, these low-altitude zones—the "aeriallittoral" between the sky and the earth's surface[18]—are the domain where small drones can be most active. Coupled with the development of artificial intelligence (AI) and 5G and other high-speed, high-volume communications technologies, it is quite possible that the variety of autonomous weapons will evolve still further in the future. We can see this from the conspicuous battlefield service of drones in the Ukraine war that began in 2022.[19]

Furthermore, as can be seen from the case of a U.S. Air Force F-22 fighter jet shooting down a Chinese balloon over the U.S. East Coast in February 2023, responding to objects flying at the high altitudes of the stratosphere is also being brought to the fore as a real issue. In fact, the borders of space and a country's airspace have not been clearly defined, and neither regulations nor a consensus under international law have been established. The record for the lowest altitude at which a manmade satellite can maintain earth orbit is approximately 167 kilometers above ground, set by the Japan Aerospace Exploration Agency's (JAXA) technology test satellite TSUBAME. Considering that the record for the highest altitude at which a jet can fly was 26 kilometers above ground—set by a U.S. Air Force SR-71 reconnaissance aircraft—there

[18] George M. Dougherty, "Ground Combat Overmatch Through Control of the Atmospheric Littoral," National Defense University Press NEWS, July 24, 2019, *Joint Force Quarterly*, Vol. 94. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1913099/ground-combat-overmatch-through-control-of-the-atmospheric-littoral/

[19] Sugiyama, "21-seiki no ea & supēsu pawā," p. 94.

is a gap between them of more than 100 kilometers. China's sending a balloon to fly at a high altitude in the air over the U.S. mainland gave visible form to the problems of responding in a domain that had not drawn much attention previously. It may be expected that there will be pressure to revisit legal norms and air defense postures going forward. Aircraft—which have been designed thus far based on the premise that humans will occupy them—have restrictions in terms of the scope that humans can tolerate such as in their size, shape, rate of acceleration, and time in the air. However, UAVs are freed from the restrictions of such human factors. A myriad of unmanned systems quite removed from the conventional concept of an aircraft are being developed, and without a doubt we are now entering an era of explosive evolution.

### (4) Space Power: Security in the Space Domain, SDA, and the Evolution into an Air and Space SDF

Outer space is a global space where dominion over a physical space and the concept of national borders do not apply. Accordingly, the main purpose of security-related activities in the space domain is not to maintain national sovereignty but rather to ensure the stable use of that domain. Outer space provides essential functions for modern life as well, and the importance of the stable use of space continues to rise. In space, many actors—whether nations, militaries, or private enterprise—are active, and the boundaries between military and non-military are also indistinct.

Accompanying this increased activity in the use of space, in earth orbit there are a large number of objects referred to as space debris. These include satellites that are no longer in use, destroyed fragments, and so forth. These objects—even the small fragments—travel at extremely high speeds on the order of several kilometers per second and have a great amount of kinetic energy. Because of this, they could cause significant damage if they were to collide with manmade satellites and the like. In addition, the development of various anti-satellite weapons is also surfacing, and the risks and threats to space systems are growing with every passing year. Also, even if an attack were to be carried out, attribution of the attacking actor is difficult. This is because space assets as represented by satellites are vulnerable, and it is conceivable that there would be cases where it is difficult to determine whether something was a deliberate attack by some opposite party or if it was a naturally occurring accident in outer space.

In light of this situation, the importance of space domain awareness (SDA) is on the rise. One after another, countries are creating space operations units. For example, in 2019 the U.S. established an independent Space Force as its sixth armed service, while France has renamed its air force the Air and Space Force (Armée de l'air et de l'espace).

In Japan, too, the so-called three strategic documents that were developed in December 2022 clearly stipulated that a specialized unit for the space domain with the Air Self-Defense Forces (SDF) under the command of a general officer would be created, and that the Air SDF would be renamed the Air and Space SDF[20]. It is extremely worthwhile for Japan to cooperate closely with the U.S. and other allied and like-minded countries, regularly monitor the status of our space systems and avoid collisions with space debris and so forth for the stable use of space, while also working to detect and deter in advance acts such as ones that would intentionally obstruct our satellites.

For Japan, there was a long period of time where "the peaceful use of space" meant the space domain was not used for security ends. However, the space-related technologies that Japan possesses are among the best in the world, and in the future Japan will be able to demonstrate its strengths in the space domain. One could say that it would be logical to maintain a relative advantage and strengthen the deterrent against aggression toward our country by strengthening these areas. Above all, acts in the space domain where it is difficult to identify the actor behind an attack may be said to be an option with a relatively low hurdle to choose in a gray zone situation. For that reason, by cooperating closely with the U.S. and other like-minded countries during peacetime and creating an excellent space situation surveillance posture where any act in space does not go unnoticed, such acts will be deterred and by extension it will lead to the shaping of an international security environment favorable to our country.

## 2. Deterrence Using Air and Space Power

Based on the characteristics of air and space power, what sorts of contributions can Japan's own air and space power make to deterrence? In considering the forms of deterrence for which Japan—with its exclusively defense-oriented policy as its basic one for national defense—would wield its air and space power, rather than deterrence by punishment where enormous damage is inflicted on the opposite party, the more crucial perspective is like that of deterrence by denial, in which resilience, perseverance, and the like make it difficult for the opposite party to achieve their objectives. At the same time, this suggests that the initiatives and efforts that Japan undertakes would only be ones of indirect support for deterrence. Furthermore, looking at Japan on its own, there are limits on deterrence with air and space power alone. In practice, a combination of land, sea, and air assets (cross-domain), and in particular collaborating with its ally the U.S. are essential to deterrence.

In short, it would be appropriate to see air and space power only as one of the elements (part of the whole) that comprise deterrence.[21] Also, multilateral cooperation that includes working together with like-minded countries and whose progress is expected to accelerate in

[20] Decision by the National Security Council and the Cabinet, "Bōeiryoku seibi keikaku ni tsuite," December 16, 2022, p. 15. https://www.mod.go.jp/j/policy/agenda/guideline/plan/pdf/plan.pdf;
Decision by the National Security Council and the Cabinet, "Kokka bōei senryaku ni tsuite," December 16, 2022, p. 24. https://www.mod.go.jp/j/policy/agenda/guideline/strategy/pdf/strategy.pdf

[21] Regarding this point, see the following. Colin S. Gray, *Modern Strategy*, Oxford University Press, 1999, pp. 239–240; Gray, *Air Power for Strategic Effect*, pp. 304–305.

the future is also essential to deterrence.[22] Below, bearing in mind that the demonstration of military power is supported by the capabilities of the new domains, based on the characteristics of air and space power as laid out above we will discuss the potential deterrence effects that such power has.

### (1) Japan as a Strategic Strongpoint

When it comes to Japan's geographic features, it is generally pointed out that it is an island nation with seas in all four directions and that its territory is relatively confined. Also, in terms of its defense system, it possesses the minimum defensive capabilities needed to specialize in its exclusively defense-oriented policy. Its so-called power projection capabilities as just one country are extremely limited.[23] Although it was expressly written in the recent three strategic documents that Japan will possess a counter strike capability, it is Japan's ally the U.S. that can demonstrate strong power projection capabilities against other countries.

In practice, it has been observed that the U.S. military stationed in Japan uses Japan as a strategic strongpoint in a way that perhaps makes up for Japan's power projection capabilities.[24] This, it is said, has not changed since the early years of the Cold War (particularly after the outbreak of the Korean War).[25] While the U.S. is an Indo-Pacific country, the hot spots of the Korean Peninsula and the Taiwan Straits are far from the U.S. mainland; without Japan as a strongpoint, its power projection capabilities would be limited.[26] Taking this into account, for Japan, maintaining a posture in which the U.S. can stably use Japan contributes indirectly to deterrence.[27]

Now, then, we will narrow our focus to the air and space power that is the title of this chapter, and here on air power in particular, as we consider how they can specifically contribute to Japan's defense and deterrence. First, there is surveillance of the airspace

[22] Decision by the National Security Council and the Cabinet, "Kokka anzen hoshō senryaku ni tsuite," December 16, 2022., pp. 5–6. https://www.mod.go.jp/j/policy/agenda/guideline/pdf/security_strategy.pdf. For the relationship between multilateral cooperation and deterrence, please see the following. Rory Medcalf, Indo-Pacific Empire: China, America and the Contest for the World's Pivotal Region. Translation supervised by Masashi Okuyama and Shigetoshi Hirayama as Indo Taiheiyō senryaku no chiseigaku: Chūgoku wa naze haken o torenai no ka, Fuyō shobō, 2022, pp. 394–397.

[23] Narushige Michishita, et al., *Gendai senryakuron: Sensō wa seiji no shudan ka*, Keisō shobō, 2000, p. 167.

[24] Kazuhisa Ogawa, *NichiBei dōmei no riarizumu*, Bungeishunjū, 2017, pp. 18–24; Michael Lostumbo, et al, *Overseas Basing of U.S. Military Forces: An Assessment of Relative Costs and Strategic Benefits*, RAND Corporation, 2013.

[25] U.S. Department of State, *Foreign Relations of United States, 1958-1960, Japan; Korea*, Vol. XVIII, U.S. Government Printing Office, 1994, Document 23, p. 60.

[26] Thomas B. Mahnken, et al., *Tightening the Chain: Implementing a Strategy of Maritime Pressure in the Western Pacific*, Center for Strategic Budgetary Assessment, May 2019, p. 1, 14. Please also see the following. Colby, *The Strategy of Denial*.

[27] Mike M. Mochizuki, "Japan's Search for Strategy," *International Security*, Vol. 8, No. 3, Winter 1983/84, p. 156; Col. Kimitoshi Sugiyama, "Japan's Approach to Deterrence in the Age of Great Power Competition in the Indo-Pacific," CASI Conference 2022-Great Power Competition and Deterrence, May 17 2022, National Defense University, Washington, D.C.

surrounding Japan and, in response to unidentified aircraft that may encroach on Japan's territorial airspace, keeping the opposite party away from Japan through countermeasures against intrusions into Japan's airspace in the form of scrambling fighter jets. Second, if the situation escalates and Japan's territory is directly threatened, as far away as possible from Japanese territory, Japan would implement an air defense operation involving not only fighter jets but also Airborne Warning and Control Systems (AWACS) and tanker aircraft to minimize any damage to national territory.

Third, Japan should do as much as possible to neutralize missiles flying to Japan with its missile defense capabilities (active defenses). Fourth, SDF bases need to be hardened and their survivability improved to limit the damage from an attack on Japan. Fifth are measures to improve the possibility of air power on the ground surviving an opposite party's attack through reciprocal use of Japanese and U.S. bases located in Japan.

Thinking about deterrence effects, the hardening and the stable use of existing bases in Japan (including not only Air SDF but also Maritime SDF bases) must be ensured. For this, one can first imagine improving the survivability of bases (passive defense) by building new facilities at existing bases. However, as was also touched upon in the January 2023 joint statement of the U.S.–Japan Security Consultative Committee ("2+2")[28], removing the obstacles to building up the sharing or near sharing in peacetime of Japanese and U.S. bases in Japan would contribute to increasing the stable operational infrastructure for both Japan and the U.S. Viewed in practical terms, with respect to existing bases, the time needed for strengthening that infrastructure would be less than that needed to build new bases.

Also, ultimately defending Japanese national territory means denying an opposite party from invading Japanese territory—or more precisely, denying that opposite party from crossing the sea—and therefore the capability to strike at an opposite party at sea is crucial.[29] Of course, it will be necessary to respond with a combination of land and sea assets. However, if in addition to mobile ground-based launch systems, aircraft were equipped with long-range missiles, it would be possible to strike at sea at the opposite party from multiple Japanese and U.S. bases as mentioned above. This, in turn, might make that party's calculations more complex.[30] In addition to long-range missiles, by using so-called self-destructing drones in the future, even if part of an attack is neutralized by the opposite party's air defense capabilities it would still be possible to continue causing a certain amount of attrition.

What's important from a deterrence perspective is that by indicating to an opposite party

[28] U.S. Department of Defense, "Joint Statement of the 2023 U.S.–Japan Security Consultative Committee ("2+2")." Provisional translation by the Ministry of Defense as, "NichiBei anzen hoshō kyōgi iinkai (2+2) kyōdō happyō," January 11, 2023. https://www.mod.go.jp/j/approach/anpo/2023/0112a_usa-j.html

[29] Sugio Takahashi, *Gendai senryakuron: Taikokukan kyōsō jidai no anzen hoshō*, Namiki shobō, 2023, pp. 216–219.

[30] Thomas Mahnken, "Air and Space Power Strategy for Great Power Competition," *Ea andō supēsu pawā kenkyū*, no. 10, January 2023, pp. 7–8.

that not only are Japanese and U.S. operational bases hardened but there is also the possibility of an attack from multiple moving targets, they would not be able to neutralize Japanese and U.S. military capabilities with only unilateral missile attacks against the two. Japan and the U.S. must be dedicated to a persistent defense. By doing so, the attacker's attempt to achieve their objectives quickly will be rejected, and they will be made to realize that the conflict will fall into a state of deadlock.[31]

### (2) The Strategic High Ground: "Eyes" from a High Place

While in the foregoing we focused on activities on the ground above all else, naturally when thinking about the features of air and space power we cannot ignore making use of the physical domains that are air and space. Notably, there is the notion of wiping out an opposite party through air power, which developed alongside the birth of the aircraft. However, it took time until it actually became possible to strike directly at an enemy's air power and an enemy country's home territory.[32]

The primary mission of aircraft at their dawn was not bombing, which would later predominate, but rather reconnaissance and surveillance from the air.[33] This means that, just as a highland with a commanding view in the past provided a strategic high ground for viewing an entire tactical situation, air and space play the role of strategic high grounds. Having superior reconnaissance and surveillance capabilities is one of the strengths of air and space power. Thanks to scientific and technological progress, getting an unobstructed "over the hill" view of things not visible to the naked eye has become possible through the use of air and outer space.[34] While the air and space are both impacted by astronomical and weather conditions, from both spaces it is possible to get unobstructed views across vast distances, and activities in them cover the globe.[35]

Consequently, humanity as a matter of course has worked at evolving and wielding the act of standing watch over and reconnoitering the movement of an opposite party from the high ground. This began with reconnaissance and surveillance from the high ground that made the most of topography, to grasping enemy movements from the high ground offered by balloons, to the birth of fixed-wing aircraft that went on to the U-2 high-altitude reconnaissance aircraft, AWACS), UAVs like the Global Hawk, and (warning) surveillance above the earth from

[31] Takahashi, *Gendai senryakuron*, pp. 209–219.

[32] Giulio Douhet, trans. and eds. Joseph Patrick Harahan and Richard H. Kohn, *The Command of the Air*, The University of Alabama Press, 2009; Phillip S. Meilinger, "Giulio Douhet and the Origins of Airpower Theory," in Phillip S. Meilinger, ed. *The Paths of Heaven: The Evolution of Airpower Theory*, Air University Press, 1997, pp. 1–40; Robert Pape, *Bombing to Win: Air Power and Coercion in War*, Cornell University Press, 1996.

[33] Martin Van Creveld, *The Age of Airpower*, Public Affairs, 2011, ppb. 2012, pp. 6–23.

[34] Gray, *Modern Strategy*, pp. 261–262; Sugiyama, "21-seiki no ea & supēsu pawā," p. 85.

[35] Yasuhito Fukushima, *Uchū to anzen hoshō: Gunji riyō no chōryū to gabanansu no mosaku*, Chikura shobō, 2020, pp. 29–32; Mitchell, *Winged Defense*, pp. 3–4.

satellites that are active in the outer space that lays beyond the sky.

However, even if air and space are the strategic high grounds of today, in the vast region of the Indo-Pacific which stretches across two oceans, getting an accurate grasp in real time of the actual conditions on the land, at sea, and in the air is not easy.[36] Especially, there are limits to the surveillance capabilities of a single country. To grasp the situation in the vast Indo-Pacific where Japan is located, it is necessary to work together with countries in the region to share and combine the latest local information that each has and create a Common Operational Picture (COP) for the Indo-Pacific.[37] Of course, there is the problem that there is a lack of shared assets to form official information-sharing mechanisms and infrastructure among the countries in the region. However, the important thing is that an opposite party can be made to feel insecure and suspicious by making them aware that their own unlawful acts and military actions are constantly being watched by someone. Depending on the situation, by jointly revealing their actions and wrongdoings to the international community, the actions of the opposite party may be checked in advance.[38] One example of this is the "Free and Open Indo-Pacific" concept proposed by the Japanese government that has been well-received by numerous countries in the region. Each country could fully have the incentive to cooperate toward regional transparency and openness. Ideally, one could imagine countries in the region building radar networks, sharing satellites, and creating multinational information centers, but we are not at the stage yet where this is a reality.[39]

Even with no information-sharing mechanism in place among regional countries, joint patrol activities and the like through combined training activities with some regional countries even today could be possible. Accompanying this, grounded in United Nations Status of Forces agreements, countries from outside the region including the United Kingdom, France, and Canada are using U.S. bases in Japan for watching and surveillance activities with respect to illegal maritime activities including ship-to-ship cargo transfers by North Korean vessels.[40] These are countries that not only highly value but also are receptive to the "Free and Open Indo-Pacific" concept. Joint patrols meant to realize that concept are equally feasible.

[36] Thomas G. Mahnken, Travis Sharp, and Grace B. Kim, *Deterrence by Detection: A Key Role for Unmanned Aircraft Systems in Great Power Competition*, Center for Strategic Budgetary Assessment, 2020, pp. ii-iii, 22–26.
https://csbaonline.org/research/publications/deterrence-by-detection-a-key-role-for-unmanned-aircraft-systems-in-great-power-competition

[37] Thomas Mahnken, "Air and Space Power Strategy for Great Power Competition," p. 6.

[38] Mahnken, Sharp, and Kim, Deterrence by Detection, p. 6, 41; Thomas G. Mahnken, et al, *Implementing Deterrence by Detection: Innovative Capabilities, Processes, and Organizations for Situational Awareness in the Indo-Pacific Region*, Center for Strategic Budgetary Assessment, 2021, pp. 6, 11–15, 31–39. https://csbaonline.org/research/publications/implementing-deterrence-by-detection-innovative-capabilities-processes-and-organizations-for-situational-awareness-in-the-indo-pacific-region; Mahnken, "Air and Space Power Strategy for Great Power Competition," p. 6.

[39] Mahnken, et al, *Implementing Deterrence by Detection*, pp. 31–39.

[40] Ministry of Defense, "'Sedori' ni taisuru kankeikoku ni yoru keikai kanshi katsudō," October 31, 2022. https://www.mod.go.jp/j/approach/defense/sedori/2022.html

Ultimately, by multiple regional countries establishing surveillance activities and developing a collective surveillance posture, an opposite party would be made to realize that they are regularly being monitored by a group and further checks can be imposed.[41] In short, to reiterate the key is the uneven distribution of the surveilling eye. It gives rise to a feeling akin to the fear that eyes are directed toward the opposite party from everywhere.[42]

However, this does not mean that in the U.K.—which is notorious for its surveillance society—crime does not occur at all.[43] Furthermore, it should be noted that the U.K. is not one of the countries in Europe of the sort noted for law and order. That is to say, just having a watchful eye does not necessarily mean that unlawful acts will not occur. Its deterrence effects are insufficient. What is needed are actions to quickly discover and detect abnormalities and then punish unlawful acts.

Although one cannot categorically state that surveillance from air and space itself functions as a deterrent, there is no mistaking that information collection through multilateral cooperation is an important initiative in that it supports the accuracy of the information of oneself and leads to improving the accuracy of awareness of the current situation. This would ultimately be of mutual benefit to the countries in the region. Also, as a vital point, there are limits to the information that can be collected by one country alone. By having regional countries work with one another, not only is it possible to obtain an even more broad range of information, but these actions can also serve as peer pressure against an illegitimate state.[44] Furthermore, by monitoring the region in peacetime, it may be possible to not only quickly detect abnormalities, but also in a contingency become an important source of information essential to constructing a kill chain.

### (3) Multilateral Cooperation and Collective Security

As mentioned earlier, the “Free and Open Indo-Pacific” concept heralded by the Japanese government has been broadly accepted by countries around the region. Multilateral exercises and training among those nations that endorse this concept have been held around Japan and its environs. Coincidentally, multilateral exercises on Japanese territory are also taking place more often. To give one example, the Australian “Pitch Black 22” exercise that was held around the summer of 2022 was a large-scale event in which 17 countries participated,

[41] Mahnken, et al, *Implementing Deterrence by Detection*, pp. 6, 31–39. Please also see the following. Iris van Sintemaartensdijk, et al, “Assessing the deterrent effect of symbolic guardianship through neighborhood watch signs and police signs: a virtual reality study,” *Psychology, Crime & Law*, May 2022, pp. 1–21.

[42] Mahnken, Sharp, and Kim, *Deterrence by Detection*, p. 6,41; Mahnken, et al, *Implementing Deterrence by Detection*, p. 9, 37.

[43] “Britain is ‘surveillance society’,” *BBC*, November 2, 2006. http://news.bbc.co.uk/2/hi/uk_news/6108496.stm; Patrick Wintour, “Only ‘tiny handful’ of ministers knew of mass surveillance,” *The Guardian*, November 5, 2015. https://www.theguardian.com/world/2015/nov/05/nick-clegg-cabinet-mass-surveillance-british-spying

[44] Mahnken, Sharp, and Kim, *Deterrence by Detection*.

including Japan's debut participation. It may be gathered from it that the importance of multilateral cooperation in the Indo-Pacific is growing. Speaking in terms of these exercises, there are also analyses that say historically, exercises that have had the goal of improving joint operational capabilities not only demonstrate the closeness of the countries participating in the exercises, but also have a deterrence effect based on their potential to offset the advantages in capabilities of the other.[45]

Japan traditionally has emphasized joint exercises with its ally the U.S., but today exercises with countries other than the U.S. are not uncommon. Australia in particular has lately been becoming closer to Japan. In January 2022, the two countries concluded a reciprocal access agreement (RAA) that facilitates mutual access for both countries when conducting exercises. The advantage to this is that exercises whose content would be difficult to implement in Japan where the exercise airspace is limited can be attempted in Australia.

Furthermore, the Quadrilateral Security Dialogue (QUAD) between Japan, the U.S., Australia, and India that lately has been a topic of interest is limited at the moment to that strategic dialogue. However, the four participants are like-minded countries that place the same value on achieving a "Free and Open Indo-Pacific" based on the rule of law.[46] While QUAD is a strategic dialogue, in the Indo-Pacific AUKUS is a security partnership more specialized on security matters. Its primary goal is for Australia, the U.K., and the U.S. to work together for Australia to acquire nuclear submarines.[47] While there are arguments for and against Australia having nuclear submarines, the point here is like-minded countries as one part of multilateral cooperation possessing an asset in common. However, possessing the exact same asset in common realistically brings with it great difficulties. On the other hand, if fuel and munitions could be made mutually interchangeable, this would also lead to improvements in the ability to sustain a war.

In short, it is operational support. As seen with Ukraine having been able to fight resiliently on against Russia for a long time, munition and fuel support from other countries is an essential factor behind the ability to sustain a war. From the perspectives of mutual assistance and deterrence, too, one imagines that it will be crucial going forward for Japan, the U.S., and Australia ideally to build joint munitions depots and fuel facilities in their respective countries

[45] Beatrice Heuser and Harold Simpson, "The Missing Political Dimension of Military Exercises," *The RUSI Journal*, Vol. 162, No. 3, July 2017, p. 22, 24; Raymond Kuo and Brian Dylan Blankenship, "Deterrence and Restraint: Do Joint Military Exercises Escalate Conflict?" *Journal of Conflict Resolution*, Vol. 66, No. 1, July 2021, pp. 3–31.

[46] U.S. Department of State, "Joint Statement on Quad Cooperation in the Indo-Pacific," February 11, 2022. https://www.state.gov/joint-statement-on-quad-cooperation-in-the-indo-pacific/

[47] The White House, "Remarks by President Biden, Prime Minister Morrison of Australia, and Prime Minister Johnson of the United Kingdom Announcing the Creation of AUKUS," September 15, 2021. https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/09/15/remarks-by-president-biden-prime-minister-morrison-of-australia-and-prime-minister-johnson-of-the-united-kingdom-announcing-the-creation-of-aukus/; The White House, "Joint Leaders Statement on AUKUS," March 13, 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/13/joint-leaders-statement-on-aukus-2/

(that said, there are U.S. military fuel and munitions depots in Japan already).[48] In that circumstance, hardening and improving the survivability of facilities even more by setting them up underground will be crucial.

Furthermore, with regard to the space domain, hosted payloads—which refers to the multiple equipment of mission equipment and materials such as space situational awareness (SSA) sensors for manmade satellites—are becoming widespread. If such cooperation is pursued not only by Japan and the U.S., which have already agreed to cooperating on hosted payloads,[49] but also with other regional countries or in a form where certain European countries that approve of the "Free and Open Indo-Pacific" concept were also involved, then an attack or actions taken to interfere with the satellites that Japan operates could also be regarded as an attack against or interference with multiple countries. This at the very least could make the decision-making and calculations of an opposite party uncertain.

The important thing is that information sharing and across-the-board operational support would be part of each country's strategy. Working together from the strategic planning stage with allies and, if possible, like-minded countries would itself not only be a strong expression of resolve that each would try to contribute to regional security, but it would also be pragmatic deterrence partnership against an opposite party. This would mean, regardless of whether the domain is ground, air, or space, a confrontation would not be with one country alone but rather with multiple countries, which would both make a situation more complex and  the opponent's strategic calculation more complex.

An essential perspective for thinking about deterrence using Japan's air and space power is that, while its contribution to deterrence itself may be indirect, Japan has to be recognized as a formidable opponent. That means an opposite party would have to recognize that not only might a situation spread in unexpected directions, but it could also worsen terribly and so ultimately bring out self-restraint by that party. This, as described above, is not something that Japan can accomplish on its own. It is a combined effort. Rather than something that is restricted to one or another initiative, it is a matter of various braking effects overlapping to function as deterrence.

[48] Ministry of Defense, *Reiwa 4-nenban Bōei hakusho, shiryōhen*, 2022, pp. 165–169; and Ministry of Defense, "ZaiNichi Beigun no taishō bōei kankei shisetsu no ichiran." https://www.mod.go.jp/j/presiding/law/drone/list_zaibeigun.html

[49] Ministry of Foreign Affairs, "Nihonkoku to Amerika gasshūkoku to no aida no sōgo bōei enjo kyōtei ni motozuku hosuteddo peirōdo kyōtei ni kansuru shokan no kōkan," December 15, 2020. https://www.mofa.go.jp/mofaj/press/release/press3_000392.html

## Conclusion

When it comes to strategy and deterrence, it is necessary to consider air and space—and the same is true for the domains of land and sea—not just on their own but also based on their connection with the other domains[50]. Since the dawn of time, humans have had their lives based on the ground, and as ever activities on the ground have a great impact on international politics. On this point, as the eminent U.S. strategic thinker Rear Admiral Joseph C. Wylie had it in pointing out the importance of activities on the ground, the idea that "The ultimate determinant in war is the man on the scene with a gun" is still valid. Of course, in light of the aspect the Ukraine war has taken on, it is greatly expected that the move to unmanned operations in future wars will proceed, but that is not to say that UAVs alone will be the ultimate deciders. In the end, it is the will of the humans who started a war that will rule.

As pointed out earlier, deterrence that wields only air and space power plays an indirect role rather than a direct one. Of course, some pundits may believe that air and space power will play an overarching role in deterrence thanks to the conspicuous work of UAVs and spacecraft. However, in this chapter we see that air and space power in the current context largely comes down to activities on the ground. That is to say, deterrence using the global airspace and domains that are the air and space will first come into effect by means of its relationship with the ground. Air and space power is an element that cannot be missing when thinking about strategy, but it definitely is nothing more than one element. Put another way, while it is essential, it is still only one part of the broad picture.

On the other hand, air and space power, with its scope of activities that spans the globe, is a space and a domain that no one possesses. Needless to say, it is essential for Japan to preserve the stability and use of the airspace and domain around the nation. This said space that is a strategic high ground is without a doubt a great "eye" for viewing everything on the ground. In the past, at present, and for the foreseeable future, it is a constituent element so indispensable that without this eye it would not be possible to put strategies together. Additionally, an eye that is constantly looking down from the skies will be a primary factor constraining an opposite party. Furthermore, because of their feature of being global, international partnerships using air and space power are also brisk. Should the orientation of international partnerships become more mutually complementary going forward, the hurdles to acts of aggression by an opposite party will become that much higher. For Japan, making full use of air and space power and check countries that threaten regional stability not only with Japan's own powers but also together with allies and like-minded countries is growing in importance with each passing day. Fulfilling that obligation will likely indirectly lead to regional stability.

[50] Biddle, *Air Power and Warfare*, pp. 4–5; Karl Mueller, "Strategies of coercion: Denial, punishment, and the future of air power," *Security Studies*, Vol. 7, No. 3, 1998, p. 203.; J. C. Wylie, *Military Strategy: A General Theory of Power Control*. 1967. Reprint, Naval Institute Press, ppb. 2014, p. 72.

# Appendix

# Summary and Results of the Scenario Games

In this research project, we conducted two scenario games (wargames) with the Study Group members as its players to identify issues of deterrence in the new domains. The first game was conducted in July 2022 hypothesizing a "**Taiwan Straits contingency.**" The second game was conducted in November 2022 hypothesizing an "**East China Sea gray zone.**" Recorded below are summary of each and the results.

The games were conducted as interactive matrix games, using a format with the researchers divided up into teams representing China, the U.S., and Japan. Each team made their decisions after having set their respective strategic objectives, and set forth their actions by placing a force card distributed beforehand on the designated matrix. The results of the interactions between the teams were determined by the game master based on the rules and, when necessary, using dice.

The games were played over multiple turns. Each turn saw separate phases played out, including a new domains action phase, missile attack phase, and operational actions phase. Diplomatic phases were inserted after the end of the second turn and after all turns had ended, with position statements presented by each team. Then, after the end of the game, there was a comprehensive review conducted by all of the players.

## Scenario Game No. 1 : Taiwan Straits Contingency

China, the U.S., and Japan were set as the players, and **the game started based on a situation where China had launched an armed attack on Taiwan** (in this game, a gray zone stage was not set as a stage preliminary to armed conflict).

### 0. Setting Strategic Objectives

First, each team set their **strategic objectives**. The overriding goal of the China team was to occupy and annex Taiwan. Its secondary goal was to establish dominance over the so-called "first island chain" (including the seas east of Taiwan). The overriding goal of the U.S. team was to maintain a pro-U.S. administration in Taiwan (and maintain U.S. supremacy in the Asia-Pacific, as well as freedom of navigation and lines of communication with Guam). Its secondary goal was to prevent an invasion of Taiwan by China. The overriding goal of the Japan team was to preserve Japanese territory and its territorial waters (particularly the Southwest [Ryūkyū] Islands), while its secondary goal was to maintain the status quo in the East China Sea.

### 1. **Turn 1**

In the new domains action phase of Turn 1, the China team used means from the new domains (space and cyber domains) to attack cities in Japan and Taiwan. The Japan and U.S. teams defended Japan with the same means from the new domains. The decision result was that this attack had no effect (it did not lower morale in either Japan or Taiwan). During the missile attack phase, the China team used missile attacks to broadly destroy air bases in Guam, Taiwan, Okinawa, western Japan, and eastern Japan. The Japan and U.S. teams also destroyed one of the four air bases in China's coastal region.

In the operational actions phase, the China team gained control broadly over the northern East China Sea, the southern East China Sea, the Taiwan Straits, the northern South China Sea, and the seas east of Taiwan. The Japan and U.S. teams gained control over the Philippine Sea and also attempted to gain control over the seas east of Taiwan in order to maintain lines of communication between Taiwan and Guam, but after losing a battle with China in the same waters it was not able to achieve its objective.

### 2 . **Turn 2**

In the new domains action phase of Turn 2, the Japan and U.S. teams continued trying to protect Japanese cities with the means of the new domains, while the China team did not attack Japan and Taiwan with the means of the new domains. However, in the missile attack phase China continued over a broad range with the goal of complete destruction of Japanese and U.S. air bases. The bases in Guam, Taiwan, and western Japan were completely destroyed, and thereafter were unusable. Bases in the Philippines were also destroyed. Okinawa was attacked but escaped damage, while bases in eastern Japan were not attacked. Japan and the U.S. destroyed one air base in China's coastal region different from the base in Turn 1. However, the Chinese air base destroyed in the previous turn was restored functionally.

In the operational actions phase, the China team continued to control the northern East China Sea, the southern East China Sea, the Taiwan Straits, the northern South China Sea, and the seas east of Taiwan. The U.S. team announced the forward deployment of B-61 tactical nuclear weapons to the theater of operations in a situation where it was numerically disadvantaged in terms of conventional armed forces. The China team responded to this development by declaring it would withdraw its unconditional pledge of no first-use of nuclear weapons and its negative security assurances. The Japan team abandoned recapturing domination over the East China Sea, and shifted to a posture of prioritizing defense of the home territories. However, since there were no attacks on Japan from China other than missiles, the team adopted the policy of redirecting SDF capabilities to U.S. operations aimed at preserving lines of communication between Taiwan and Guam.

**In the diplomatic phase that followed Turn 2**, the China team asked for the U.S. and Japan to suspend their intervention in the Taiwan Straits conflict, and sought to gain acceptance for not allowing the entry of Japanese and U.S. warships and aircrafts to the first island chain. The

Japan and U.S. teams sought to stop China's invasion of Taiwan, and by showing a strong determination with willingness to even use nuclear weapons to defend Taiwan sought to get China to give up on its invasion. The diplomatic phase failed to achieve a ceasefire and the game continued.

### 3. Turn 3

In the new domains action phase of Turn 3, the Japan and U.S. teams again used the means of the new domains to try to protect Japan's cities, but the China team did not attack either Japan or Taiwan. In the missile attack phase, the China team did not attack, but the Japan and U.S. teams completely destroyed four air bases in China's coastal region using B-2 stealth bombers carrying B-61 tactical nuclear weapons (based on a decision, the collateral damage from this was slight). As a result, China could no longer deploy bombers or fighter aircraft to the seas east of Taiwan.

In the operational actions phase, the China team continued to control the northern East China Sea, the southern East China Sea, the Taiwan Straits, and the northern South China Sea, and announced that the People's Liberation Army (PLA) was landing in Taiwan. Furthermore, by controlling the southern South China Sea, the Philippines air base that had recovered functionality after having been destroyed in the previous turn was rendered unusable. Specifically, China applied pressure on the Philippine government to reject its use by Japan and the U.S. However, as a result of the Japan–U.S. nuclear attack, it was not able to deploy bombers or fighter aircrafts, and having dispersed its military force in the waters around Taiwan it lost the naval battle with Japan and the U.S. in the seas east of Taiwan. Having continued their control of the Philippine Sea, the Japan and U.S. teams concentrated its military forces in the seas east of Taiwan. As a result of their nuclear attack that neutralized the air bases in China's coastal region, they succeeded at greatly reducing Chinese air power and won the naval battle with China in those seas. However, they did not announce a landing in Taiwan.

### 4. Turn 4

In the new domains action phase of Turn 4, the China team used the means of the new domains to attack Taiwan only, but by decision they had no effect. The Japan and U.S. teams defended Japan, but no attack was carried out by China. In the missile attack phase, the China team launched a nuclear attack on the air base in Okinawa and completely destroyed it (by decision, the collateral damage was slight). Japan and the U.S. did not launch a missile attack on China. At this point, the only usable air bases for Japan and the U.S. were two in eastern Japan.

In the operational actions phase, the China team continued to control the northern East China Sea, the southern East China Sea, the Taiwan Straits, the northern South China Sea, and the southern South China Sea. The PLA also continued its Taiwan landing operation. In the seas east of Taiwan China challenged Japan and the U.S. to another battle, but it continued its inability to deploy bombers and fighter aircrafts to those seas, and with its military capabilities dispersed to the seas around Taiwan, it was again defeated. With their continued control of the Philippine Sea, the Japan and U.S. teams won the battle with China by concentrating their military capabilities in the seas east of Taiwan. As a result, they maintained lines of communication from Guam to Taiwan, and announced that U.S. forces were landing on Taiwan.

**In the diplomatic phase after the end of Turn 4,** the China team called for the withdrawal of the U.S. forces that had landed on Taiwan as a ceasefire condition. China asserted that, although its coastal region had been damaged by a nuclear attack and lost the battle in the seas east of Taiwan, it still had residual military capabilities, and given enough time restoration of the air bases that had been destroyed by that attack was possible, enabling it to once again deploy bombers and fighter aircrafts to those seas. The team made the argument that it had not lost the conflict, and when considering the possibility of further escalation (including nuclear), there was reason for the U.S. forces to withdraw from Taiwan.

The Japan and U.S. teams called for the withdrawal of the PLA forces that had landed on Taiwan as a ceasefire condition. Since the sea line of communication from Guam to Taiwan had been maintained, the U.S. position was that it did not believe they had lost the conflict. When considering the possibility of the U.S. changing its objective to toppling the Chinese Communist Party government in the event of further escalation (including nuclear), the team argued that China, too, had reason to halt the conflict. The position of the Japan team was slightly different from that of the U.S. team. It agreed with the ceasefire conditions demanded by the U.S., but presented their view that the possibility of these being realized was low. Furthermore, with Okinawa having been attacked by nuclear weapon, they presented their stance that Japan had no choice but to seek after its own nuclear weapons and requested U.S. support for this.

## 5. Evaluation

The diplomatic phase again failed to achieve a ceasefire, but with this the game was over. The **overall victory decision based on the rules** was that the China team had 5 points while the Japan and U.S. teams had 4 points, giving China a narrow victory. However, the game ended with the sea line of communication from Guam to Taiwan having been maintained and ground combat between the U.S. and China continuing on Taiwan itself.

As for **overall comments** from the players, they pointed out that the developments were noticeably disadvantageous to the Japan and U.S. side throughout the game, impacted by the roll of the dice.

In the face of the China team's overwhelming quantitative advantage, the Japan and U.S. teams were forced to concentrate their military capabilities without dispersing them. Also, there was the aspect that they were able to barely counter the China teams' advantage thanks to the first-use of nuclear weapons. As for the China team, it was forced to disperse its military capabilities to the southern East China Sea, the northern South China Sea, and the seas east of Taiwan in order to prevent Japan and the U.S. from entering the Taiwan Straits. As a result, they were defeated twice in the battles in the seas east of Taiwan where the Japan and U.S. teams had concentrated on inserting their military capabilities, and they were unable to cut the line of communications from Guam to Taiwan. This led to the game's result of ground combat between the U.S. and China on Taiwan itself.

**The nuclear attack unsurprisingly was the game changer.** With the air bases in the coastal region destroyed by the nuclear attack, China was unable to deploy bomber and fighter units to the seas east of Taiwan, which worked to the advantage of Japan and U.S. teams. It was an example that proved the view that escalation (including nuclear) is always done by the side in the inferior position. On the other hand, the nuclear attack on the air base in Okinawa by the China team was a chance outcome, arising from that base having escaped destruction before that in the missile attack using conventional warheads. If it had already been destroyed, there would have been little reason to launch a nuclear attack. The purpose of the attack was a purely military one, and the long-term political implications were not considered.

**The element of the new domains (space and cyber domains) did not become a decisive factor in this game.** Their effect on (lowering morale as a result of) the attacks on cities was limited, and the use of the new domains for operational support was also limited to only the support element of being a force multiplier. Even in the context of deterrence, **attacks (or counterattacks) based on the new domains had the aspect of lacking a crystal ball effect (the effect such that it is obvious to an opposite party what will occur if they are used) like that of nuclear attacks, which makes them difficult to use as a means of deterrence.** **The background in which the game's development had a composition wherein it began right away with armed conflict and it did not lead to antagonisms at the gray zone level was also thought to be major**. Nevertheless, the new domains are of great significance in contexts such as cognitive warfare. If attention is given to such contexts, it was conjectured that **the impact of elements of the new domains would be greater by having a game structure that takes into consideration escalation from the gray zone level.**

## Scenario Game No. 2 : East China Sea Gray Zone

With the results of the first game in, the East China Sea Gray Zone game was conducted to investigate the issue of deterrence in new domains on the context of gray zone situation. The game had the same three players of China, the U.S., and Japan, hypothesizing a confrontation at the gray zone level in East China Sea waters "neighboring the Senkaku Islands" and "adjacent to the gas fields" (in the vicinity of the median line between Japan and China).

### 0. Setting Strategic Objectives

First, each team set their strategic objectives. These were shared only within each team itself and were not revealed to the other teams until the end. The China team was given instructions by the president: "The problems with Japan over the Senkaku Islands and the exclusive economic zone (EEZ) in the East China Sea should be wrapped up in China's favor in order to achieve Chinese unification of Taiwan. Through the actions in question, if possible weaken the Japan–U.S. alliance before taking actions on Chinese unification." Based on this, the team set as its strategic objectives "establish maritime and air superiority in the East China Sea" and "establish effective control over the Senkaku Islands." Also decided on as items for consideration were: avoid armed conflict prior to Chinese unification, search out gray zone situations of a scope that does not lead to U.S. intervention, and land "fishermen" on the Senkaku Islands.

The U.S. team set as its strategic objectives, "Maintain order in the East China Sea and do not allow changes to the status quo through force," "With the goal of stability in the East China Sea, prevent actions to cross the median line between Japan and China," and "Prevent decoupling between Japan and the U.S." Items for consideration included: do not allow the Chinese side to make physical attacks, and engage in creating a base in the cognitive domain for an operational posture buildup, information disclosure, non-kinetic attacks, and information collection. Similarly, Japan set as its strategic objectives, "Prevent China as much as possible from changing the status quo, and work to restore the status quo," "Avoid conventional war as much as possible," and "Do not allow any decoupling between Japan and the U.S." Its items for consideration included deeming it to be an armed attack situation when space and cyber attacks are carried out that interfere with the capabilities for situational awareness in "the remote islands."

### 1. <u>Turn 1</u>

In the new domains action phase of Turn 1, the China team took the following actions. First, in the space domain, it carried out attempts at downlink jamming against Japan's positioning, navigation, and timing (PNT) capabilities; uplink jamming and dazzling and blinding against its information, surveillance, and reconnaissance (ISR) satellites. In the cyber domain, it hacked the account information of the Okinawa Prefectural Police chief and transmitted disinformation. It also carried out malware attacks against the Coast Guard's image transmission systems (private communication satellites), the fueling control PCs of the private companies that carry out the refueling of Coast Guard patrol boats at Ishigaki Island, and the East Japan Railway systems that handle operation and control in the Kanto area. As a result, the Okinawa Prefectural Police were at the mercy of dealing with anti-base demonstrations on the main island and were unable to respond in the Senkakus; the Coast Guard's activities in the East China Sea including the Senkaku Islands were hindered; and damage resulted to the Japan team as a result of transportation chaos in the East Japan region such as the impact it had on the response of staff at the Ministry of Defense.

The Japan and U.S. teams responded in the space domain by carrying out downlink jamming against China's PNT capabilities, and also made attempts of dazzling and blinding directed against its ISR satellites. In the cyber domain, they launched malware attacks against the servers for satellite measurement and control use directly under the Equipment Development Department of China's Central Military Commission.

In the operational actions phase, the China team built two new oil rigs in a gas field area of a scope able to cover the Senkaku Islands, and used this as a base for establishing maritime and air superiority. It also dispatched 200 fishing vessels and four government ships to the vicinity of the Senkaku Islands. Furthermore, it also deployed two destroyers, 10 fighter aircrafts, and one drone to the vicinity of the oil rigs north of the Senkaku Islands.

In response, the Japan team attempted to deploy all deployable patrol boats to the vicinity of the Senkaku Islands, but with the Coast Guard's systems having been subjected to a cyber attack as noted above, only two patrol boats were deployed. Two Maritime SDF destroyers were also deployed. At the same time, the team also tried to deploy an Air SDF unit to Naha, but they were not able to do so because the latter's activities in the air were hampered by the attack on the satellites. Beyond this, a Ground SDF Amphibious Rapid Deployment Brigade was placed on standby at Camp Ainoura in Nagasaki Prefecture. The U.S. team attempted information collection and deterrence activities with 20 Marine Corps aircrafts, and also forward deployed strategic bombers (B-2s/B-52s) to Guam. In this situation, the Japan team's situational awareness capabilities in the seas neighboring the Senkakus were markedly restricted, but the team had not reached the point of identifying this as an armed attack situation.

### 2. Turn 2

In the new domains action phase of Turn 2, for its actions in the space domain, the China team carried out uplink jamming against Japan's space situational awareness (SSA) capabilities; downlink jamming against communications capabilities; dazzling and blinding of ISR satellites; and a co-orbital ASAT attack (using robot arms) against communications satellites in geostationary orbit. As a result, not only the Coast Guard but also the SDF had lost satellite communications, yielding a situation in which they had only shortwave communications. Communications services using Starlink were also disabled. In the cyber domain, malware attacks were launched against communications between Ground SDF coastal surveillance unit on Yonaguni Island and its superior organization, Western Army Military Intelligence; the PCs for communications in the Defense Attaché office at the U.S. Embassy in Japan; and the U.S. Space Force's SSA systems. As a result, Japan could no longer get information from Yonaguni Island, and the SSA capabilities of the U.S. were also hindered.

The Japan and U.S. teams responded to this by carrying out malware attacks to interfere with data transmissions on communications servers at the People's Armed Police (PAP), the umbrella organization over the China Coast Guard (CCG). This resulted in a situation where communications between CCG headquarters and government ships were delayed.

In the operational actions phase, the China team deployed 500 fishing vessels and six government ships to waters adjacent to the vicinity of the Senkaku Islands, and sent one submarine through those same adjacent waters. Also, after having stationed another submarine in the vicinity of the oil rigs, the team stationed six destroyers and two drones in the vicinity of the Senkaku Islands and the oil rigs. Furthermore, 300 PLA ground troops were split up to be stationed at two oil rigs, and 40 fourth-generation fighter aircrafts were deployed to the Senkaku Islands and the vicinity of the oil rigs.

The Japan team dispatched an escort fleet (five destroyers, two submarines) between China and the Senkaku Islands, and attempted to block China's sea line of communications. They also issued a warning that Japan and the U.S. would be conducting joint exercises in the vicinity of Taishō Island, and urged that Chinese government ships and fishing vessels withdraw. However, in order not to obstruct Chinese moves to evacuate, they intentionally did not block communications to Chinese government ships and fishing vessels. They also disclosed to the world that it was possible that China would illegally make a landing on and occupy the Senkaku Islands. They also specified attribution for the cyber attack on East Japan Railway that had been carried out in the previous turn, and made it plain that the cyber attack was from either China or North Korea. The U.S. team deployed amphibious assault ships and aircrafts for the holding of the Japan–U.S. joint exercises in the vicinity of Taishō Island, and the U.S. Cyber Command identified and announced that the cyber attack on East Japan Railway was from China. It also requested that the Japan team increase its precautions against possible attacks by China on critical infrastructure.

**In the diplomatic phase that followed the end of Turn 2**, each team made arguments as noted below. First, the China team protested the Japan and U.S. teams' dispatch of warships against the Chinese fishing vessels in the vicinity of the Senkaku Islands. The team also denounced the holding of Japan–U.S. joint exercises at the Senkaku Islands as a situation that would stir up fears of a military threat. The Japan team in response rebutted the argument. It pointed out that given circumstances of Japan being under cyber attack and the difficulty gaining situational awareness on the ground by satellite, it was forced to believe that the Chinese side was deploying the fishing vessels with ambition of seizing territory. The U.S. team presented its understanding that the joint exercises were being carried out under the Japan–U.S. alliance, and the current status quo was close to that of a quasi-contingency. Based on an understanding that it was possible that the Chinese side was commencing hybrid warfare, the U.S. team argued that it would conduct the joint exercises in order to exclude that possibility and there was no problem with exercises having given advance notice. The Japan team also argued that the military exercises were in the pursuit of legitimate national interest, and again urged that the Chinese fishing vessels be withdrawn. In response, the China team reproached that any damage to the fishing vessels would be Japanese and U.S. responsibility, and questioned whether Japan and the U.S. would be able to notify all of the fishing vessels that the exercises were being conducted. The situation did not end with the diplomatic phase and moved on to Turn 3.

### 3. Turn 3

In the new domains action phase of Turn 3, for actions in the space domain the China team conducted a co-orbital ASAT attack on Japan's geostationary communications satellites; uplink jamming against SSA capabilities; downlink jamming against PNT and communications capabilities; and dazzling and blinding attacks against ISR satellites. Also, in the cyber domain, the team launched malware attacks against fuel system PCs at the U.S. Navy's base at Sasebo in Japan; the private power transmission control systems for Camp Ainoura, where the Ground SDF Amphibious Rapid Deployment Brigade is stationed; control systems at the U.S. military's base at Iwakuni in Japan; the integrated control information processing system at the Kobe Air Traffic Control Center that handles air traffic control in the Okinawa area; and NTT East's secured email servers for government offices use. As a result, the damages were as follows: U.S. military units at the Sasebo base could not be deployed to the Senkaku Islands; the Amphibious Rapid Deployment Brigade could not operate; air traffic control at the Iwakuni base became impossible; the air traffic control system for the Okinawa area ceased to function; and the government offices' closed system became inoperable.

The Japan and U.S. teams responded in the space domain by conducting uplink jamming against China's communications satellites; downlink jamming against its communications capabilities; downlink jamming against PNT capabilities; uplink jamming against ISR satellites; dazzling and blinding attacks against ISR satellites; uplink jamming against SSA capabilities; and co-orbital ASAT attacks against communications satellites in geostationary orbit. In addition, in the cyber domain they launched malware attacks against the flight plan inputting systems of the PLA Air Force's UAV units. As a result, both Japan and China saw their satellite capabilities go down, and PNT, ISR, and communications capabilities were all obstructed.

In the operational actions phase, the China team stationed 800 fishing vessels and eight government ships in the vicinity of the Senkaku Islands, and adopted a posture of ignoring the Japan–U.S. joint exercises. The team also stationed an aircraft carrier with 50 fighter aircrafts, two landing ships, and one submarine in the vicinity of the oil rigs. Furthermore, it also deployed 80 fourth-generation fighter aircrafts and three drones to the vicinity of the Senkaku Islands.

The Japan team wanted a U.S. aircraft carrier deployed to the Senkaku Islands on the pretext of the joint Japan–U.S. exercises to counter China's moves, but as a result of the cyber attack on the Sasebo base the U.S. team could not deploy the aircraft carrier and deployed only a portion of its fighter aircrafts. However, by decision, the functions of the Sasebo base were to be restored with Turn 4. The Japan and U.S. teams also worked to clarify the zone for the exercises and the safe zone.

### 4. Turn 4

In the new domains action phase of Turn 4, as its actions in the space domain the China team conducted its continued co-orbital ASAT attack on geostationary communications satellites; uplink jamming against SSA capabilities and ISR and communications satellites; downlink jamming against PNT and communications capabilities; and dazzling and blinding attacks against ISR satellites. In the cyber domain, the team launched malware attacks on the PC used for dedicated email lines between SDF and U.S. forces under U.S. Forces Japan headquarters; the Maritime SDF's backup logistical support systems for the SDF fleet; the Ground SDF's backup logistical support systems for the Kyushu Logistics Depot; the Joint Staff central command's systems; and the power supply systems of the power company (Tokyo Electric) that handles the Ichigaya, Yokota, and Yokosuka areas. The resulting damage was that the Maritime SDF fleet could not be deployed and there were power outages in the Kanto region.

The Japan team responded to this in the space domain by conducting co-orbital ASAT attacks on geostationary communications satellites; uplink jamming against SSA capabilities, ISR satellites, and communications satellites; and downlink jamming against PNT and communications capabilities. In the cyber domain, the team launched malware attacks against the smart grid for the Chinese city of Shenzhen and against the communications systems of the mobile phone company that controls the city of Tianjin. The resulting damage was power outages in Shenzhen and communications systems in Tianjin becoming inoperable.

The U.S. team in the space domain likewise conducted co-orbital ASAT attacks against geostationary communications satellites; uplink jamming against SSA capabilities, ISR and communications satellites; downlink jamming against PNT and communications capabilities; and dazzling and blinding attacks against ISR satellites. In the cyber domain, the team launched malware attacks against PCs for the communications systems of the satellite telephone company that controls Beijing; Shanghai's smart grid; the traffic systems for Xiong'an New Area (Smart City) in Hebei Province; the general broadcasting server for China Central Television (CCTV); and the water-level management systems for Three Gorges Dam. The damage that resulted was the mobile network for Beijing became inoperable; Shanghai experienced power outages; Hebei Province's smart system was paralyzed; CCTV was put out of commission; and water levels at Three Gorges Dam rose.

Also, aside from Japanese, U.S., and Chinese geostationary satellites being destroyed, all satellites stopped functioning.

In the operational actions phase, the China team landed fishermen on the Senkaku Islands due to bad weather. Some 1,500 persons from 300 vessels landed on the islands, with 1,000 landing on Uotsuri Island and 500 on Taishō Island. They then had Chinese government ships intrude into territorial waters purportedly on a rescue mission. Furthermore, they stationed one aircraft carrier, four destroyers, and two submarines in the vicinity of the Senkaku Islands, and one aircraft carrier, three landing ships, and one submarine were stationed outside that area just short of Senkaku waters. Additionally, they also deployed 90 fighter aircrafts (80 fourth-generation aircrafts and 10 fifth-generation aircrafts).

The Japan team in response attempted to commit all of the deployable Maritime SDF forces to the exercises zone at the Senkaku Islands, but it was unable to deploy them because the backup logistical support systems were down due to Chinese cyber attack.

With the restoration of functions at the Sasebo base, the U.S. team attempted to commit all of the maritime assets it had planned to commit in Turn 3 to Senkaku waters, but it was unable to deploy them due to impact of satellites ceasing to function and the breakdown in communications with the SDF. However, it also forward deployed B-2 and B-52 bombers to Guam, deployed U.S. Air Forces fighter aircraft from Kadena to the Ryukyu Islands, and publicly announced its attribution finding that “the cyber attacks against Japan were launched by China.”

With regard to the restoration, based on a decision made using the dice, of the eight systems that went down between Japan and the U.S., the U.S. Space Force’s SSA capabilities were recovered. Of the seven systems that went down in China, functions recovered for CCTV, Beijing, Shanghai, and Three Gorges Dam.

### 5. Turn 5

In the new domains action phase of Turn 5, as its actions in the space domain the China team conducted the same sort of co-orbital ASAT, jamming, and dazzling and blinding attacks as in Turn 4. In the cyber domain, it launched a malware attack against the systems that manage flight plans for the U.S. Air Forces’ base at Kadena. The damage that resulted was the withdrawal of U.S. fighter aircrafts due to the Kadena base experiencing dysfunction.

The Japan team, too, for its actions in the space domain, launched the same sort of attacks as in Turn 4. No cyber attacks were carried out.

The U.S. team did not carry out attacks in the space domain, but as its actions in the cyber domain it launched cyber attacks against over-the-horizon (OTH) radar in Zhejiang Province, and against PCs used for communications by anti-ship ballistic missile (ASBM) units. The resulting damage was that ASBM unit communications were cut and ASBMs could not be used.

In the operational actions phase, the China team stationed one aircraft carrier, three landing ships, and three submarines in the waters adjacent to the Senkaku Islands, and continued its deployment of 90 fighter aircrafts.

The Japan team recognized the situation as an armed attack, and asked the U.S. that Article 5 of the U.S.–Japan Security Treaty be invoked. The team also said it would seek to remove the fishermen by armed force, and asked the U.S. to reconfirm its extended nuclear deterrence commitment. However, Japan on its own had no countermeasures available aside from attacks in the space domain.

The U.S. team, with its recovery from the cyber attacks, deployed aircraft carriers and other warships to the vicinity of the Senkaku Islands. The team also declared as its commitment to Senkaku 's defense, “We are prepared to use all means necessary, including nuclear.”

It also reiterated its criticism that “the cyber attacks against Japan and the U.S. were launched by China.” The U.S. also raised the issue with the U.N. Security Council as “a reckless act that surpasses Russia's invasion of Ukraine,” and issued a joint Japan–U.S. statement.

**In the diplomatic phase after the end of Turn 5**, the arguments of each team were as follows. First, the China team furiously criticized Japan, stating it was unacceptable of Japan recognizing an armed attack situation when China had not launched any armed attack. According to the China team's argument, under the current status quo, China's forces were only on the high seas to rescue fishermen who had taken refuge on the Senkaku Islands. On the other hand, 100,000 people had died due to the U.S. cyber attack on Shanghai. They harshly criticized Japan and the U.S., saying this was already an act of war and China had no choice but to act in self-defense.

The Japan team argued, with functional outages all around Japan, in light of the U.S. having shared its attribution findings that the cyber attacks on Japan came from China, and based on the situation of China having deployed fishermen to the Senkaku Islands, it had no choice but to recognize that an armed attack had clearly been made. It then sent notice to China to the effect that it was calling for the withdrawal of all Chinese fishermen, warships, and the like; that if this was not accomplished it would be forced to prepare for all-out war; and that this was an ultimatum.

The U.S. team made the criticism that the attacks on U.S. bases and satellites were done by China. They also presented their understanding that the present situation was one in which China had carried out hybrid warfare and the so-called “Three warfares” (public opinion warfare, psychological warfare, and legal warfare). Based on this, the U.S. team presented their plan that they would apply Article 5 of the U.S.–Japan Security Treaty to the situation, and demanded that Chinese forces withdraw from the waters in the vicinity of the Senkaku Islands. The U.S. also set forth its stance that if the situation were to continue as is, it was prepared to respond using all means available. It also gave notice that it had deployed the forces needed not only to Japan but also to Guam (hinting at the presence of nuclear forces).

In response, the China team made a rebuttal saying that while it had no intention whatsoever of going to war, if attacked it had no choice but to respond based on the right of self-defense; whether Japan and the U.S. would do battle in the current situation where China's naval forces had the advantage; and that it was unreasonable for Japan to recognize this as an armed attack situation despite Japan had suffered zero casualties.

The Japan team made a rebuttal saying that an illegal seizure of territory was being made at the Senkaku Islands, which are Japanese territory; they believed the purported fishermen to be a maritime militia; the recognizing of the situation as an armed attack was due to the stacking up of all of the circumstances including the fishermen, the militia on the oil rigs, and the attacks in the space and cyber domains; and that regarding the fishermen, it had enforced a naval blockade and waited for a fixed period of time for their withdrawals, but since they had not complied with the final notification, going forward Japan would consider their removal using a ground operation.

The China team in response argued further that under current conditions China had an overwhelming advantage; whether Japan and the U.S. would really do battle; Chinese ground troops would also enter before the Amphibious Rapid Deployment Brigade landed, so the removal seemed to be impossible; and that the Chinese side also had anti-aircraft sites and radar sites on the oil rigs, so Japan and the U.S. should reconsider.

With this, the game ended.

As to the **comprehensive review** conducted after the game's conclusion, first the **China team** pointed out in its comments that **they had managed to accomplish the plan to obey the instructions from the president that they should avoid armed conflict before Chinese unification of Taiwan while landing fishermen on the Senkaku Islands,** and that having ground troops stationed on mobile rigs on the high seas was an effective means.

**The Japan team** commented that while they were able to avoid a decoupling per se between Japan and the U.S., **they were unable to prevent Chinese actions to change the status quo**. However, no matter what they did, they would not have been able to stop it. **At the start, Japan attempted to respond with the plan to forward deploy as many forces as possible,** but it was regrettable that this strategy had collapsed under China's cyber attacks.

**The U.S. team** commented that while they thought they had achieved maintaining order in East Asia and preventing a decoupling between Japan and the U.S., **they were not able to respond well to information warfare in the cognitive domain.** The U.S. had planned to buy time and deter the Chinese side through non-kinetic means where attribution is difficult, but **they did not imagine that moves by Japan and the U.S. would halt due to China's cyber attack.**

In the entire exchange of views, the following items were pointed out with regard to **escalation in the new domains**. First, **the fact that Japan (the SDF) did not have the option of cyber attacks to halt the PLA's moves** drew attention. There was a premise that in light of the SDF's cyber capabilities such an attack would not be possible, **though the problem was that, when China moved in the physical domains in Turns 3 and 4, Japan lacked the option (of denying them) through an effective cyber attack.**

Also, it was pointed out, while the U.S. launched cyber attacks against China in the context not of counterforce but rather countervalue, if the U.S. had gone into it further the outcomes might also have changed, and under the assumptions of an all-out war it might have led to nuclear escalation. However, the aspect of **not being able to figure out escalation in the new domains** was also significant. Unlike kinetic missile attacks and the like, with **a cyber attack, capability assumptions were difficult.**

Furthermore, given that Japan and the U.S. wanted the fishermen to withdraw from the Senkaku Islands, they initially avoided jamming directed at China's PNT capabilities. In actual fact, the possibility of hesitation working was high with regard to hindering communications with the maritime militia.

As a result, the following **summary of the game** was made. First, it was learned that **once it has been analyzed and addressed, malware cannot be reused. By its nature, it can be used only once, and so as a result it is used all at once in many locations and drastic escalation occurs.**

Next, in a gray zone situation, **so long as the situation is gray, the advantage goes to the first move and to the attacker. The situation would no longer have been gray had the Japanese side, with the approval of the U.S. side, landed some personnel on the Senkaku Islands first. It is possible that this would have, in the end, lead to deterrence, since the costs of the Chinese side attempting to seize them would have risen.** However, in this game, since moves by the Okinawa Prefectural Police had been shut down in its opening stages, even if the option had been selected it would not have been possible to effectively carry it out. This point demonstrates **the importance of improving resilience to deal with attacks using the new domains against law enforcement agencies.**

In order to protect the Senkaku Islands, **raising the ladder of escalation from both Japan and the U.S. will be crucial as a response.** However, **the fact that such options were thwarted by the Chinese cyber attack** was of deep significance to the game.

When it comes to Japan's **armed attack situation recognition,** the game demonstrated that **there is the need to deepen discussions in the future regarding how to go about such recognition when each element is lacking when it comes to going over the hurdle for recognition (including in the new domains) but on the whole they cross it.**

“Deterrence in the New Domains” Project, Secretariat

Junichi Fukuda, Senior Research Fellow, Security Studies Program, Sasakawa Peace Foundation
Yayoi Watabe, Assistant, Security Studies Program, Sasakawa Peace Foundation

War 3.0: the Rapid Change of Warfare
– Deepening Deterrence in the New（Space and Cyber）Domains –

Published March 2024
Publisher: The Sasakawa Peace Foundation
The Sasakawa Peace Foundation Bldg.
1-15-16 Toranomon, Minato-ku, Tokyo 105-8524, Japan
Phone: +81-3-5157-5430; URL <https://www.spf.org/>

SPF 笹川平和財団