“Complex,” “Full-Spectrum” and “Cross-Domain” Deterrence

Junichi Fukuda

Introduction

The concept of “deterrence” has traditionally been discussed in the context of nuclear deterrence. If the phrase that “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,”[1] is adopted as the definition of deterrence, the origin of deterrence traces back to the birth of human society. However, it was only after World War II that the concept of deterrence came under the spotlight in international relations. It was because the emergence of nuclear weapons, then described as the “absolute weapon,”[2] gave rise to the idea that a nuclear war in which no winner exists can only be avoided by deterring its occurrence. Thus, the concept of deterrence became closely associated with the evolution of nuclear strategies. Of course, the concept of deterrence by conventional forces was not made light of during the Cold War. Still, we can say that the core of the concept of deterrence lay in nuclear deterrence.

Deterrence after the end of the Cold War came to a crossroads as tensions between the superpowers eased and instead the focus of attention shifted to actors hard to deter, such as rogue states and terrorist groups. And thus, the emphasis came to be placed on “tailored deterrence,”[3] designed to flexibly choose the mode of deterrence depending on actors involved and/or situations. In this regard, however, initiatives during this period tended to focus on “pre-emption” or “prevention” rather than deterrence, and it can be argued that for a period of time after the Cold War, including war against terrorism, the attention to the concept of deterrence declined in relative terms.

Today, however, discussions about deterrence are becoming active again. There are at least three reasons behind this renewed interest. First, in today's world, strategic competition between great powers gains growing attention. The rise of China and Russia and their actions to change the status quo as well as the declining relative superiority of the United States are spawning such interest. Second, there are concerns over responses to actions to change the status quo that are less critical than an "armed attack" under international law, or the "gray zone" situation that is neither a peacetime nor a wartime situation. The challenging actions in the East and South China Sea and Ukraine by China and Russia, respectively, gave rise to the need for handling such situations. Third, present-day warfare is being waged beyond the traditional domains. With the importance of new domains, such as outer space and cyberspace, being emphasized, an attempt to gain the superiority though the synergy of various domains is drawing keen interest.

Because of these developments, the concept of deterrence is stimulating renewed interest across the world today. Japan is no exception. Since the 1970s, Japan has adopted the "Basic Defense Force" concept and has relied on that concept even after the end of the Cold War. But this was no more than the concept of considering deterrence in terms of the minimal meaning of Japan not becoming a "power vacuum." However, the National Defense Program Guidelines for FY2011 and beyond, written in 2010, underlined "dynamic deterrence" that focuses on the operation of defense capability in light of China's assertive expansion into the waters.[4] This change was of significance in the sense that Japan has shifted to an approach geared to the enhancement of its deterrence capability in response to specific threats. In the National Defense Program Guidelines for FY2014 and beyond, written in 2013, deterrence was emphasized in the framework of "effective deterrence of and response to various situations.”[5] In light of these changes, it is significant for Japan to review the concept of deterrence again today in view of its plan to further revise the National Defense Program Guidelines in late 2018.

The purpose of this article is to study the relevant nature of the concept of deterrence. In the background of the renewed interest in the concept of deterrence observed today are the three changes, i.e. the renewed interest in strategic competition between great powers, rising concerns over actions to change the status quo that fall short of “armed attack,” and the growing attention being paid to the new domains of warfare. In this article, the author considers the change in deterrence in the future with the use of the three keywords of “complex,” “full-spectrum” and “cross-domain.” “Complex” deterrence shows that the asymmetric nature of the capabilities and motivation of parties involved in deterrence make the deterrence situation diversified and complicated. “Full-spectrum” deterrence shows that there exists no single capability that can deter all sorts of action and it is necessary to deal with the challenges of respective spectrums with respective different capabilities and methods. And finally, “cross-domain” deterrence shows that it is no longer possible to demonstrate the superiority over others in all domains and asymmetric superiority should be pursued by linking the predominance in the particular domain to predominance in other domains. This article argues that what is required in today’s world is the building of the “complex,” “full-spectrum” and “cross-domain” deterrence posture.

Below, Section 1 attempts to put in order the theoretical basis of the concept of deterrence. Section 2 takes up the three changes that brought the concept of deterrence into the spotlight again and discuss potential changes they may bring to the concept of deterrence in the future. Section 3 considers the respective natures of “complex,” “full-spectrum” and “cross-domain” deterrence. From April 2016 through March 2018, the author was given an opportunity to engage in research activities as the first visiting research fellow at the Air Staff College.

This article represents the result of those research activities. However, the author takes full responsibility for the content of this article.[6]

1. Theoretical Basis of the Concept of Deterrence

First of all, the theoretical basis of the concept of deterrence should be put in order. Deterrence means an act or a process of and an outcome of the persuasion of one's opponent not to take a given course of action from the perspective of costs and/or risks. The realization of deterrence entails the three essentially important requirements: (1) one's opponent is rational, (2) one has the capability to enforce deterrence, or evidence in support of deterrence; and (3) there is a credible way of conveying one's intentions or resolve. Realistically speaking, however, it is not easy to satisfy these requirements, and thus, deterrence often fails.[7]

Firstly, the basic premise of deterrence is that one's opponent is a rational actor. But it is actually not so easy to satisfy this requirement. In the first place, a human being is not perfectly rational actor as one has various thoughts or cognitive biases.[8] In a crisis situation, personal thoughts or biases are further amplified under stress and groupthink.[9] The recognition of rationality may diverge due to differences in strategic cultures of opposing parties.[10] In addition, it is wrong to take the stance that regards a state as a single, rational actor.[11] Because of these reasons, it is difficult to pursue deterrence by simply assuming the opponent to be a rational actor. In particular, it would be difficult to realize deterrence through the mirror imaging that "the opponent must be looking at the world in the same way as oneself."[12]

Secondly, it is essential to have the capability which the opponent believes to be sufficient for deterrence, or evidence in support of deterrence. Theoretically, there is the possibility that deterrence may work even in the absence of the required capability (bluffing), but the lack of the capability basically means little credibility of deterrence. However, modes of deterrent are not uniform. In nuclear deterrence, The common form of deterrence is the deterrence by punishment, designed to increase costs expected by an assumed attacker. On the other hand, in deterrence by conventional forces, the common form of deterrence is the deterrence by denial, designed to lower the probability of an attacker’s expected goal being attained.[13] Which capability is more suitable for deterrence is dependent on one’s opponent and/or actual situation and cannot be determined a priori. The mode of capability suitable for the deterrence depends on the context of situation.

Thirdly, the credible communication of conveying one’s intentions or resolve is essential. The fundamental principle of deterrence is the persuasion of the opponent, and it is crucially important to credibly convey to the opponent what violation (or no violation) would be met by what response (or not invite any response). This is so easy to say, however. Misperception and/or psychological bias could amplify distrust and cause an escalation of the situation (the spiral model).[14] An action designed for self-defense is perceived as offensive by the opponent and could invite an unexpected escalation of the situation (the security dilemma).[15] Furthermore, the party attempting at deterrence has the motive to misrepresent information on its capability or resolve in order to gain an advantage in negotiations.[16] A credible communication of conveying one’s intentions or resolve is essential, but it is far from easy.

Then, how would we overcome the problems of deterrence? Theoretically, there would be the following answers. First, regarding rationality, even if it is impossible to deter the purely irrational opponent, it is still possible to mitigate the problem by various methods. For example, make it clear which action by which opponent is to be deterred. Clearly understand what strategic culture and preferences the opponent has, what organization it has, and what is the intention of the opponent’s challenging action. Then, minimize the possibility of cognitive bias distorting the opponent’s judgment. Specifically, conceivable methods include making the crystal-clear communication, giving enough time to make judgment, and having the point of contact with the center of the opponent's decision making.

What is needed in terms of capability is the deterrent against all sorts of challenge. However, there is no such thing as the single capability that can deter any action by any opponent, that is, there is no "one sizes fits all" for deterrence. For that reason, tailored deterrent is required that corresponds to a particular action by a particular opponent. For example, it is impossible to deter every challenge by simply employing nuclear weapons (deterrence by punishment) alone, because excessive retaliation for a minor challenge lacks credibility. It requires the deterrence structure that combines conventional forces (deterrence by denial) with other capabilities. Deterrence is not necessarily limited to military means. As areas of conflict are spreading widely today, the genuine initiative for deterrent calls a whole-of-government approach that makes use of all capabilities of a state, such as diplomacy, information, military and economics (DIME).

However, even if one has the capability, deterrence does not function if one's intentions and resolve are called into question. Conveyance of the intentions and resolve has to be made in a credible manner. Theoretically, the threat of deterrence needs to take the form of costly signaling. This means an action to convey one's intentions and resolve by taking an action that entails costs that cannot be borne in the case of bluffing to demonstrate that one's threat is not a bluff.[17] For example, in the case of extended deterrence to assure the security of an ally, such action includes the pre-deployment of troops and military equipment in an allied nation. Another example is to formulate a formal alliance and increase the ex-ante audience cost in the event of failure to fulfill an obligation.[18] There also is a multitude of other credible ways to make the threat of deterrence. They include an announcement of declaration policy regarding deterrence, timely demonstration of deterrent, and the establishment of workable means of communication.

The credibility may be tested beyond the threat of deterrence. When the opponent avoids taking a particular action in response to the persuasion, the credibility is required of the conveyance of “reassurance”[19] that one would not undermine the position of the opponent by taking advantage of that situation. In the absence of the credible reassurance, even if the threat of deterrence is credible, deterrence could fail as the opponent may think the avoidance of the particular action could give rise to a situation worse than facing the retaliatory measures. Thus, if the opponent is persuaded, one needs to make a commitment that one would not cross the line. This includes an attempt to form fundamental norms, including confidence-building, disarmament/arms control, code of conduct, and international rule and law and comply with them. However, the reassurance tends to be less effective when the opponent is an actor seeking to change the status quo.

In sum, the realization of deterrence must meet the three requirements. First, the opponent is a rational actor. Second, one has the capability or evidence in support of deterrence. Finally, the conveyance of one’s intentions and resolve is made in a credible manner. But it is difficult to completely satisfy these requirements. Consequently, deterrence could fall apart quite often. It is necessary to understand the delicate nature of deterrence

2. Renewed Interest in the Concept of Deterrence and Future Transformation

This section discusses the reasons why the concept of deterrence is now coming under the spotlight again by taking up the three changes. After doing that, it discusses potential transformation these changes may bring to the concept of deterrence in the future.

(1) Renewed Interest in Strategic Competition between Great Powers

The first reason the renewed interest has been aroused in the concept of deterrence is the fact that the strategic competition between great powers is drawing growing interest again today. The attention to the concept of deterrence in international relations had its origin in the emergence of nuclear weapons, but this interest declined temporarily after the end of the Cold War as the international community's focus of attention shifted to its responses to regional conflicts and terrorism. The situation changed since the mid-2000s, however. The unipolar world centered around the United States has come to a turning point and the rise of emerging powers, such as China and Russia, drew attention. In addition, the occurrence of the global financial crisis impressed the world with the decline in the leadership of advanced democracies, including the United States and European countries. Thus, China and Russia seized this change as a strategic opportunity to expand their influence, putting up the proactive challenges against the existing international order.

More specifically, Russia's invasion of Georgia in 2008 and China's shift in its foreign policy the following year marked a turning point.[20] Since then, China and Russia increasingly took actions seeking to change the status quo. In 2014, Russia intervened in the Ukrainian conflict, annexed the Crimean Peninsula and destabilized the eastern region of Ukraine. In 2015, Russia intervened in the civil war in Syria, and in 2016, Russia interfered with the U.S. presidential election by way of cyber and information maneuvering. China, meanwhile, increased the tendency of seeking coercive maritime expansions since 2010. In 2012, China and Japan were in a state of sharp confrontation over the ownership of the Senkaku Islands, and China seized the Scarborough Shoal from the Philippines. In the South China Sea, China threatened the "freedom of navigation" of U.S. military vessels. China started building artificial islands on the Spratly Islands, and proceeded to militarize the facilities on these islands in disregard of the ruling by the Permanent Court of Arbitration that determined China's actions were unlawful. [21]

In the wake of these changes in the postures of China and Russia and their challenges to change the status quo, the Obama administration of the United

States first took an appeasing policy such as “Reset” and “Strategic Reassurance (later the “New Model of Major-country Relationship”),” but later shifted to a more hardline stance. This shift in the U.S. policy became definitive with the “National Security Strategy” and the “National Defense Strategy” under the Trump administration, as both documents identify China and Russia as “revisionist powers” and made clear the policy to seek U.S. superiority through “long-term, strategic competition” with them.[22] These changed recognition of threats by the United States were shared by allied nations. European countries grew more alert to Russia, and Indo-Pacific countries, including Japan, strengthened their stances to hold China in check. The renewed interest in the concept of deterrence observed today cannot be separated from the interest in strategic competition between great powers as discussed above.

(2) Rising Concern over Actions to Change the Status-Quo Short of “Armed Attack”

The second reason behind the renewed interest in the concept of deterrence is the fact that concerns have deepened over actions to change the status quo that fall short of an “armed attack” under international law. Under international law, the legitimation of the exercise of the right of self-defense (consequently, the invocation of the collective defense clause of an alliance) requires the evidence of an “armed attack” from other country or countries. In recent years, however, China and Russia increasingly took the stance of seeking to incrementally change the status quo by containing situations just short of an “armed attack.”

For example, China’s maritime challenges were undertaken by making use of the maritime law-enforcement authority, the China Coast Guard, and maritime militias. China’s actions like the intrusions into Japan’s territorial waters and contiguous zones around the Senkaku Islands and the seizure of the Scarborough Shoal were designed to seek to change the status quo by making use of government (or public) vessels. China also displayed the stance of using economic means as a tool of coercion. An embargo on rare earth to Japan, curbs on imports of bananas from the Philippines and economic harassment of South Korea for the deployment of Terminal High Altitude Area Defense (THAAD) missiles in the country were actions to wrench concessions from the countries involved by leveraging potential economic damage. China has been seeking to change the status quo by making such challenges short of an “armed attack” and without advancing the situations beyond an “armed attack.”

Russia has also made use of actions to change the status quo that fall short of an “armed attack.” In the case of a cyber-attack on Estonia, Russia avoided an escalation of the situation by disguising the perpetrator as “patriotic hackers.” In the Ukrainian conflict in 2014, Russia sent in a paramilitary armed group, called “Little green men,” concealing the involvement of the Russian government.[23] In the alleged interference in the 2016 U.S. presidential election, Russia used non-state actors to undertake information maneuvering designed to agitate the division of the United States, again categorically ruling out the Russian government’s involvement.[24]

Russia tended to make these challenges in combination with the challenges that go beyond an “armed attack” by the regular military forces, hence they are often called “hybrid warfare.”[25] That said, Russia, like China, has adopted the stance of seeking to incrementally change the status quo by controlling an escalation of situations by using challenges short of an “armed attack.” These challenges are sometimes called “probing” or “salami tactics” to mean the groping for the lower limit of the opponent’s resolve. They are difficult to deal with by the conventional military capability, but overlooking them entails the risk of just sitting still and watching the changes to the status quo, thus requiring countries subject to such challenges to explore a new means of deterrence.

(3) Growing Attention Paid to the New Domains of Warfare

The final reason behind the renewed interest in the concept of deterrence is the fact that today’s warfare has come to be waged on the dimensions beyond the traditional domains. Warfare that were previously fought in the three domains of land, sea and airspace have now extended into the broader domains. The typical examples are the extensions of warfare into outer space and cyberspace. Furthermore, efforts are under way to conceptualize the fighting in the information and psychological domains as “political warfare”[26] and fighting in the “human domain.”[27]

These changes stem largely from the tendency of activities of the armed forces to depend on access to non-conventional domains such as outer space and cyberspace because of the advancement of technology and science. They also arise from the fact the concept of warfare itself has undergone change and the position has emerged to view all aspects of human activities from the perspectives of conflicts and competition.

For example, the importance of outer space has not fundamentally changed from the Cold War era. However, the arms race in outer space was limited during the Cold War era, causing no serious impediments to access to outer space. But in the “Second Space Age”[28] of today, the situation is entirely different. Many countries other than the United States and Russia now have their own satellites and the number of commercial satellites has also increased. The advancement of information and communication technology (ICT) heightened the dependence of all military activities on outer space, and together with it, the possibility is increasing of access to outer space being hampered by the development of anti-satellite weapons. Today, outer space has changed into the more diversified and disrupting place, and this change is inevitably giving rise to the issue of how to realize deterrence in outer space.[29]

The same can be said of cyberspace. The advancement of ICT has brought forth the situation where military operations rely on the networks in all aspects. It was the important change in military history that this has led to the development of “network-centric warfare.”[30] At the same time, however, the threats of cyber intrusions and attacks have become apparent to compromise the availability and integrity of the networks through their weaknesses. This is recognized as the main weakness in today's military activities. Furthermore, the threat of cyber-attacks is likely to cause wide-ranging damage to society via the failure of critical infrastructures and thus it has now come to be recognized as a threat on the national scale. For that reason, the realization of deterrence in cyberspace is now being vigorously explored.[31]

Also attracting attention are responses to the challenges in the information and psychological domains. As society has now become diversified and complicated in the wake of the global interdependence and technological advancement, warfare increasingly tends to be fought in an unrestricted manner by using every means.[32] Under these circumstances, actions to seek the superiority over an opponent through manipulation of information and psychology have become visible, including China's "three warfares (public opinion warfare, psychological warfare, and legal warfare) and Russia's espionage operations in other countries. An attempt to position this as a new domain of conflict may still has a long way to go. But there is no doubt that there is the growing awareness of the need for deterrence in information and psychological warfare beyond the existing domains.

(4) Changes in the Future Concept of Deterrence

Then, what sorts of transformation will these changes bring to the concept of deterrence in the future? The following three points may be noted.

First, the renewed interest in strategic competition between great powers mean that the interest is shifting from deterrence mostly of rogue states and non-state actors in the post-Cold War to deterrence of such powers as China and Russia. However, the interest in the latter did previously exist during the Cold War period and thus it would be more appropriate to describe it as the resurgence of interest. On the other hand, the importance of deterrence against rogue states or non-state actors has not vanished and is still there. Therefore, in the future, efforts toward more "complex" deterrence will come onto the agenda. More specifically, what can be assumed include not only "deterrence against challenging acts by great powers” but also “deterrence against rogue states in the context of strategic competition with great powers” and “deterrence against non-state actors behind whom great powers are involved in.” It is necessary to consider the element of “complex” deterrence within the framework of the contemporary competition between great powers.

Next, concerns over revisionist actions to change the status quo that fall short of an “armed attack” under international law have provided depth to discussions that tended to give a disproportionate emphasis on responses to situations beyond an “armed attack.” The challenges short of an “armed attack” gave rise to growing concerns over potential changes to the status quo, introducing efforts to restrain challenges at this stage into the discussions about deterrence.[33] At the same time, however, it is also true that responses to the challenges short of an “armed attack” cannot be separated from responses to the challenges of an “armed attack” or beyond, because if the credibility of deterrence against the challenges of an “armed attack” or beyond is undermined, a situation could easily escalate to an upper stage. On the other hand, there could be the possibility of the fact that deterrence against an “armed attack” or beyond is working, which makes a challenge short of an “armed attack” more likely (the paradox of stability and instability).[34] Going forward, therefore, it is deemed that deterrence at multiple different stages should be consolidated into the framework of integrated deterrence. “Full-spectrum” deterrence that bears every stage in mind becomes essential.

Finally, the attention paid to the dimension of warfare beyond the traditional domains also plays an important role in extending the concept of deterrence. It is no longer possible to wage warfare today in the domains of land, sea and airspace alone. It is crucially important to focus on the achievement of superiority in the new domains like outer space and cyberspace, information and psychology (or, at least keeping the opponent from acquiring that superiority). Under these circumstances, it has been pointed out that the key to a victory in contemporary war is the “cross-domain” synergy that links the superiority in a particular domain to the superiority in other domains.[35] In particular, it should be deemed difficult to demonstrate one’s superiority over others in every domain now because the era of U.S.-centered unipolar world has ceased and the transition and diffusion of power is expected. The only way to maintain the effectiveness of deterrence amid such situation is to pursue the asymmetric superiority by leveraging the superiority in a particular domain and linking it to the superiority in other domains. It is assumed that for deterrence in the future, an emphasis is expected to be placed on the pursuit of superiority that straddle multiple domains on the assumption that “there can be no overall domain superiority over others.”

Summarizing the above discussions, what is called for today is the building of the “complex,” “full-spectrum” and “cross-domain” posture of deterrence.

3. Concept of “Complex,” “Full-Spectrum” and “Cross-Domain” Deterrence

In the preceding section, the author pointed out that the building of the “complex,” “full-spectrum” and “cross-domain” posture of deterrence is required today. This section looks at the nature of each deterrence.

(1) “Complex” Deterrence

It has been often described that deterrence in the 21st century has become “complex” in light of the structural features, such as the diversification of actors involved in deterrence, the complicated power relationships among them and opaque motives. For example, T. V. Paul in 2009 defined “complex deterrence” in the following way: “An ambiguous deterrence relationship, which is caused by fluid structural elements of the international system to the extent that the nature and type of actors, their power relationships, and their motives become unclear, making it difficult to mount and signal credible deterrence threats in accordance with the established precepts of deterrence theory.” Paul then presented the five ideal types of relationship between the actors in a complex deterrence situation: (1) deterrence among great powers; (2) deterrence among new nuclear states; (3) deterrence involving nuclear great powers and regional powers armed with chemical, biological and nuclear weapons; (4) deterrence between nuclear states and non-state actors; and (5) deterrence by collective actors (such as international organizations).[36] Even in light of the recent resurgence of the security interest to strategic competition between great powers, it still cannot be denied that the deterrence situation today is diversified and complicated.

Thus, the deterrence posture being sought today is also required to continue to respond to the “complex” situation of deterrence. The essential crux here is how to overcome problems associated with the asymmetric nature of the powers and motives of actors involved in deterrence. Such asymmetric situation of deterrence can take various forms. The most notable form is the relationship of deterrence (and extended deterrence) of great powers, such as increasingly expansionist China and Russia and countries surrounding them. Since there usually exists the asymmetry of capability between them, it is difficult for surrounding countries to conduct deterrence on their own. Thus, the basic prerequisite is extended deterrence by extra-regional countries (typically, the United States). However, there is the asymmetry of motives for conflict intervention between surrounding countries and extra-regional countries in the event of failure of extended deterrence, making it serious for the concern over the credibility of extended deterrence, i.e. the problem of “de-coupling.” Therefore, in deterrence against great powers seeking to change the status quo with their expansionist actions, the challenge boils down to how surrounding countries can exert efforts to fill the gap of the asymmetric power (capability) relationships with the challengers (basic deterrence) or how surrounding and extra-regional countries can eliminate the asymmetry of deterrence-related motives (extended deterrence).

Moreover, there is the problem of how surrounding and extra-regional countries can deter rogue states that develop and own weapons of mass destruction, including nuclear weapons. Countries like Iran and North Korea are deemed to be pursuing strategic deterrence through the development and deployment of nuclear and other weapons of mass destruction and aspiring after asymmetric acts of challenge against surrounding countries while excluding the intervention by extra-regional countries. If Iran and North Korea become confident of strategic deterrence with nuclear and other weapons of mass destruction in the future, it would give rise to a "paradox of stability and instability," giving rise to the concern that they could increasingly activate their asymmetric acts of challenge against surrounding countries. How to deter such challenges by rogue states will remain as the important issue in the future.

Deterrence against non-state actors is also taking on importance. As the diffusion of technologies is increasingly empowering individuals and groups today, the challenges by non-state actors, such as terrorists, organized crime groups and threat actors in cyberspace are escalating.[37] Since the challenges by non-state actors are usually less intense than those by state actors, importance tends to be attached to defense or hygiene instead of deterrence. However, it should be noted here that state actors may sometimes make the challenges by disguised as non-state actors. For example, there is the concern these days that state actors conduct cyber-attacks by disguising themselves as non-state actors. This is because it is relatively easy for a state actor to conduct an act of challenge against other countries in cyberspace under the guise of a non-state actor because of the attribution issue that makes it difficult to identify the attacker. Such concerns were already turned into reality in the Estonian case in 2007 and the alleged interference with the U.S. presidential election in 2016. This problem will likely grow increasingly serious in the future.

As seen above, in today's world, the asymmetric relationships of deterrence, such as deterrence between expansionist great powers and surrounding countries, deterrence against rogue states that own weapons of mass destruction, and deterrence against non-state actors, are increasingly important. In addition, it has become necessary to re-position the already complicated situation of deterrence within the framework of competition between great powers in recent years. Going forward, we are expected to see an increasing number of cases where we simultaneously face the multiple deterrence situations as well as an increasing number of situations that are essentially recognized as part of deterrence between great powers where deterrence on the surface appears to be deterrence against rogue states or non-state actors. The deterrence structure needs to deal with such “complex” situations.

(2) “Full-Spectrum” Deterrence

In the past, the United States was confronted with the limitations that there exists no single capability that deters every challenge. As the United States lagged behind the Soviet Union in conventional forces in Europe in the 1950s, the United States came out with the “massive retaliation” strategy to complement conventional forces with nuclear forces. But this strategy had a major problem. If the challenge at a lower stage was met with massive nuclear retaliation, every conflict would develop into an all-out nuclear war. Such deterrence strategy lacked the credibility of deterrence. Because of this, the United States made a shift to the strategy of “flexible response” that attached importance to responses by conventional forces.

This indicates that even nuclear weapons cannot deter every sort of challenge. Since a challenge involves numerous rungs or steps, it is impossible to maintain the credibility of deterrence unless one responds to a challenge in each rung by adopting respective responses of tailored capabilities and methods. Herman Kahn, who studied the ladders of escalation between the United States and the Soviet Union, pointed to the existence of as many as 44 escalation ladders.[38] His book made the striking point that there are as many as 24 escalation ladders even after the first use of nuclear weapons. Though the threat of thermonuclear war has dwindled today, modes of conventional wars and the challenges short of an “armed attack” have become diversified.[39] This was accompanied with the changes in the ladders of escalation. While this article cannot make a precise study of ladders, it can still refer to the major stages of a conflict. Khan reorganized the 44 escalation ladders into seven units. In accordance with this, this article assumes the five stages of “nuclear war,” “regional conflict,” “localized conflict,” “gray zone” situation and “peacetime” as the stages of escalation today.[40] Below, we discuss the nature of respective challenges and deterrence responses that should be taken for the four stages other than “peacetime.”

First, the deterrence against “nuclear war” (or the use of nuclear weapons), the highest stage of conflict, represents the fundamental basis of deterrence. At present, the existence of nuclear weapons still influences the basic strategic stability among states. Even when a conflict occurs, a state has a strong incentive to avoid its excessive escalation because of its awareness of the possibility of nuclear war. This means that even today, just as during the Cold War era, the thought of “limited war” to avoid an all-out nuclear war is still valid. Maintaining the credibility of nuclear deterrence, holding back an escalation into nuclear war and containing a conflict at a manageable level if it cannot be prevented remain as one of the essential purposes of deterrence.

However, it is problematic to assert the role of nuclear weapons only as deterrence against the use of nuclear weapons by a challenger, because nuclear weapons also have the role of deterring attacks other than nuclear attacks (attacks using biological and/or chemical weapons as well as conventional forces).[41] As long as nuclear weapons have the role of deterring non-nuclear attacks, deterrence against an escalation into a nuclear war cannot be made as the definite purpose, because it is possible to assume a situation where one has no choice but to make the first use of nuclear weapons before one’s opponent. While it depends on the situation whether one will make a nuclear counterattack against any non-nuclear attack, one needs to have the option of escalating the situation to the stage of “nuclear war” for the sake of the highly credible deterrence. In this sense, making a declaration of “no first use” policy is greatly problematic.

Similarly, overly pursuing strategic stability with a challenger is also problematic.[42] In particular, the measure to avoid an escalation into the stage of “nuclear war” by mutually recognizing the vulnerability to a nuclear attack may invite a failure of deterrence against a situation short of “nuclear war” as exemplified by the “paradox of stability and instability.” Even in the context of extended deterrence, such measure may possibly cause the problem of “de-coupling” between surrounding countries exposed to the challenge of a challenger and extra-regional countries providing extended deterrence. This is because extra-regional countries become concerned with the possibility of being exposed to a nuclear attack by the challenger by intervening into the conflict between the challenger and surrounding countries and this may consequently make extra-regional countries hesitant to intervene in the conflict with surrounding countries “being abandoned.” In order to avoid such a situation, extra-regional countries need to have the thought of “nuclear escalation dominance” that they do not hesitate over an intervention in the conflict even at the risk of being exposed to a nuclear attack themselves. The resolve not to hesitate over the escalation to the nuclear stage is required.

What is important for deterrence at the stage of “nuclear war” is the understanding that nuclear deterrence does not simply mean deterrence of a nuclear war but it also casts a long “shadow” over a full range of the conflict stages. While nuclear deterrence is indispensable to prevent a nuclear war, the strategic stability at the nuclear stage may cause the failure of deterrence against other situations short of a nuclear war. In order to prevent the failure of deterrence against situations below the nuclear stage, the thought of accepting an escalation of a conflict into the higher stage including the “nuclear war” stage is required. Today, the interest in nuclear deterrence appears to be declining despite its importance. But it remains as the most important area for deterrence.

Next, the stages of conflict by conventional forces is the situation where nuclear deterrence between states is working (or the situation where at least one of the actors does not have nuclear weapons), and can be defined as the situation where limited war by conventional forces may arise. The situation can be broadly categorized into a “regional conflict” and a “localized conflict” depending on its scale and intensity. The “regional conflict” means the situation where a broader region-wide conflict arises due to an act of challenge by a state intending to change the status quo *with the involvement of an extra-regional country (particularly the United States).* The assumptions include the situation where Russia mounts an armed attack on a member state of the North Atlantic Treaty Organization (NATO) in Central and Eastern Europe and NATO invokes the collective defense clause with the U.S. involvement in the conflict or the situation where China launches an armed attack against one of the surrounding countries (or the region) on the Korean Peninsula, in the Taiwan Strait or the South China Sea and the United States gets involved. Such conflict may basically take the form of a conventional war with the high intensity, may be waged on a large scale and may cover a wide area for a long period of time. From the perspective of deterrence, the importance in this kind of conflict is the response to the Anti-Access/Area Denial (A2/AD) capability of a challenger. It is because the challenger tries to keep an extra-regional country from coming to help the surrounding countries or delay such defense assistance and attempts to change the status quo while such country is being held off. For surrounding countries under attack or an extra-regional country coming to help them, how to defeat the A2/AD capability of the attacker would be an important task for deterrence.

A lot of studies have been conducted on responses to the A2/AD capability in the past. The most important of them is the “AirSea Battle Concept

(ASBC)”[43] released by the Center for Strategic and Budgetary Assessment (CSBA) in 2010 as the operational concept. Against the threat of the A2/AD capability, this concept offered the prescription that calls for “Withstanding the initial attack”; “Executing a blinding campaign against (an adversary’s) battle networks”; and “Executing a suppression campaign against (an adversary’s) long-range ISR and strike systems.” As the capabilities required for the above, the study cited “capabilities to withstand sustained attacks”; “capabilities to disrupt, destroy and defeat an adversary’s networks”; “power-projection capabilities to neutralize an adversary’s A2/AD platforms”; and “maritime interdiction capabilities to execute the blockade operations.” This concept initially became subject to some criticisms,[44] but was eventually adopted as an official document by the Department of Defense and the essence of the concept has taken firm root in the understanding that the ASB Concept’s solution to the A2/AD challenge is “to develop networked, integrated forces capable of attack-in-depth to disrupt, destroy and defeat adversary forces (NIA/D3).[45],[46] Later on, ASBC was renamed to the “Joint Concept for Access and Maneuver in the Global Commons (JAM-GC)” as the cross-Armed Forces initiative beyond the Navy and the Air Force,[47] but there has been no change in the essence of seeking to defeat the A2/AD capability of an adversary.

For deterrence against a “regional conflict,” it is vitally important for both surrounding countries subject to a challenge by an adversary seeking to change the status quo and an extra-regional country coming to help during the time of conflict to share the operational concepts and capabilities to defeat the A2/AD capability of an adversary as presented by ASBC/JAM-GC. For surrounding countries in particular, it is important to mitigate the damage from an attack by an adversary by “withstanding the initial attack” and “executing a blinding campaign against battle networks” of an adversary and buy time until an extra-regional country arrives to provide assistance. An extra-regional country, for its part, should seek to neutralize an adversary’s A2/AD capability by "executing a suppression campaign against [an adversary's] long-range ISR and strike systems," have an adversary realize the difficulty in changing the status quo, conduct the distant blockade operations by leveraging its maritime interdiction capability, and impose massive costs on an adversary to seek an end of hostilities under favorable terms. Thus, for deterrence of a "regional conflict," it is required to seek the realization of deterrence by denial and punishment (or imposition of costs).

A "localized conflict," which is distinguished from a "regional conflict," can be defined as a situation where a localized conflict arises *without the involvement of extra-regional countries (particularly the United States)* as the scale and intensity of the act of challenge by an adversary seeking to change the status quo are limited. This represents a challenge greater than an "armed attack" under international law, and it may be easier to comprehend it as a localized conflict that does not involve a direct militarized intervention by an extra-regional country and does not (yet) expand into a region-wide conflict. For example, the assumptions include a situation where Russia conducts a limited-scale armed attack on the Caucasus, not a NATO member, or on Middle East countries or a situation where China conducts a limited armed attack on surrounding counties in the East China Sea or in the South China Sea, and there the surrounding countries can deal with such situations on their own. The conflict situation at this stage can be varied, and there may be cases where the conflict can be contained as a short-term, small-scale and limited one without inviting an intervention by an extra-regional country while there may also be cases where the conflict takes the form of a "localized conflict" on its way to escalate into a "regional conflict." At any rate, a "localized conflict" is relatively limited in its scale and intensity, and as long as there is no direct militarized intervention by an extra-regional country, it is in the stage of conflict that requires independent responses by affected surrounding countries.

From the perspective of deterrence, what is important in a "localized conflict" is to enhance the deterrence by denial of surrounding countries that become subject to a challenge by an adversary seeking to change the status quo. Generally speaking, there exists a considerable gap in national power (or capability) between the challenger and surrounding countries. In this sense, surrounding countries may find it difficult to deal with the situation on their own without an intervention by an extra-regional country. On the other hand, however, a challenger for its part, in light of the risk of inviting an intervention by an extra-regional country with the excessive use of force, has an incentive to limit its challenge to the extent of not inducing that risk. More specifically, the assumptions include, for example, an attack on a state that does not have an explicit alliance with an extra-regional country, an attack on a remote island or on surrounding areas for which defense commitments by an extra-regional country are ambiguous, and attacks in outer space and/or cyberspace where the identification, or attribution, of an attacker is difficult. Thus, depending on the limitations on the scale and intensity of the challenge, it is considered possible for surrounding countries to execute a certain measure of deterrence by denial on their own.

The capability required of surrounding countries in the “localized conflict” of such nature is assumed to be the capability to maintain the superiority based on the denial (or at least not to give the superiority to an adversary) in land, sea, airspace and other conflict domains. Since the challenger has an incentive to fear the cost and risk of an expansion of the conflict as a result of a possible intervention by an extra-regional country, the main purpose of surrounding countries would be to hit the challenger’s weak points, demonstrate their capability to block the attainment of the challenger’s aims and demoralize it. Specific efforts to worth mentioning include “withstanding the initial attack” and “executing a blinding campaign against battle networks” of an adversary, not much different from the responses to a “regional conflict” discussed above. If possible, other desirable efforts may include “neutralizing an adversary’s ISR and strike systems" and "recapturing the seized territories." However, since the essential objective of surrounding countries is to increase the cost of conflict for a challenger by avoiding an early defeat and "buying time" to make the challenger worn out and wait for the arrival of an extra-regional country to provide defense assistance, their attempt at deterrence is deemed to center on equivalent defensive (denial) efforts.

Finally, the "gray zone" stage of conflict means acts of challenge seeking to change the status quo in general that fall short of an "armed attack" under international law. As there are various modes for challenges on this stage it is difficult to discuss them categorially. Representative examples include harassment and infringement activities (including those on the sea and in air) by paramilitary and/or law-enforcement organizations. Also assumed are acts of violating resolutions of the Security Council of the United Nations, such as repeated test-firing of missiles and nuclear testing as well as actions to circumvent U.N. sanctions. They also include export and import sanctions in contravention of international rules and economic enforcement measures such as regulations on investment and economic activities. Also conceivable is the theft of information, unlawful access and attacks in cyberspace, or interference in domestic politics of other countries as part of information or psychological operations. As the modes of conflicts on the "gray zone" stage are so varied, there exists no unified prescription against them. But we still can cite the following two essential commonalities.

First, the most important feature is that the basic means of response has to be non-military. Military means do have a certain role in responses to situations short of an "armed attack." However, since acts of challenge are basically conducted in non-military forms, military responses tend to be avoided with the aim of averting any escalation. Because of this, non-military responses become necessary in accordance with the mode of challenges. But what sorts of responses are required depend on the situation. For example, in the case of challenges made by paramilitary and/or law-enforcement organizations, responding law-enforcement organizations are required to improve and expand their capabilities. In the case of economic enforcement measures, countermeasures should be taken to mitigate their economic losses. The cyber and information/psychological challenges require the enhancement of corresponding capabilities. At any rate, deterrence against conflicts on the “gray zone” stage is highly likely to call for the adoption of a “whole-of-government approach” that leverages the comprehensive strength of a state, including military as well as non-military means.

Another important feature is that it is deemed impossible to achieve the complete removal of acts of challenge by deterrence at this stage. While there is the clear definition of threshold of an “armed attack” under international law, there is no common understanding of the clear threshold (red line) of conflicts on the “gray zone” stage that shows the one “has crossed the line.” Consequently, “failure of deterrence” often tends to be subjective, and the prediction of countermeasures also becomes ambiguous. For this reason, deterrence at this stage essentially becomes uncertain. In reality, deterrence on the “gray zone” stage takes on the aspect of escalation control where deterrence and defense are executed simultaneously. It has to be the posture under which “defense” measures are constantly taken by regarding challenges under certain levels as impossible to deter while “deterrence” is sought against an escalation of situations beyond those levels.

As discussed above, there are multiple stages of escalation for deterrence and they, by nature, call for respective unique responses. For this reason, the concept of “full-spectrum” deterrence requires the posture to be able to take appropriate responses for deterrence at all levels (depending on the situation, requiring simultaneous responses to multiple situations). What is important in doing so is to understand the nature that multiple escalation stages are mutually related. Deterrence at the higher stage cannot necessarily prevent a challenge at the lower stage, and more than that, it could induce a failure of deterrence at the lower stage. However, it would still be wrong to make light of deterrence at the higher stage by becoming obsessed with deterrence at the lower stage. A challenger keeps its challenge at the lower stage because deterrence at the higher stage is working. It is of vital importance to satisfactorily improve deterrence simultaneously at the all stages of conflict.

(3) "Cross-Domain" Deterrence

As a result of contemporary wars being waged beyond the traditional domains, the two important aspects have come to be pointed out. One is the importance of gaining the superiority in new domains such as outer space and cyberspace. Military operations today depend on the non-traditional new domains in all aspects. For this reason, the achievement of the superiority in the new domains is also gaining in importance in terms of deterrence. Another is the importance of "cross-domain" synergy that links the superiority in a particular domain to the superiority in other domains. As the transition and diffusion of power continue today, it is no longer possible to demonstrate the superiority over others in every domain. As a result, an emphasis came to be placed on asymmetric countermeasures that make up for the inferiority in one domain by the superiority in other domains. Below, the author first mentions efforts to seek to gain the superiority in new domains. After that, the author examines the task of realizing "cross-domain" synergy.

The retention of access to outer space is crucially important in military operations today. Regardless of whether it is command and control (C2), intelligence, surveillance and reconnaissance (ISR), or positioning, navigation and timing (PNT), the loss of access to outer space could give rise to the dysfunction of the entire military activities. For this reason, having the capability to maintain the superiority in outer space (at least keep an adversary from gaining the superiority) now takes on the essential importance for deterrence. The problem is that deterrence in outer space is likely to be completely different from deterrence in the traditional domains.[48] For example, the situational awareness tends to be inadequate for activities in outer space. In addition to the difficulty in detecting an attack and specifying the attribution, the "damage assessment" to determine the extent of damage is also difficult. Besides, there are no natural objects in outer space to intercept an attack, making the "defense" of satellites difficult. These problems become even more serious when it comes to non-kinetic attacks, such as laser, electronic and cyber-attacks. In addition, as attacks in orbit are unlikely to directly threat human lives, this brings on the problem of lowering the threshold for executing an attack. The immature code of conduct for outer space is also likely to lead to the failure of deterrence. Overall, the failure of deterrence and the escalation of situations can occur more easily in outer space.

In order to enhance deterrence in outer space with such features, initiatives corresponding to the new domain of outer space should be taken. The first important step is the initiative to enhance the space situational awareness (SSA) to better understand orbital phenomena. Such initiatives can be undertaken with the posture to strengthen surveillance by making use of satellites and ground radars, and it is vitally important to link this initiative to prompt and appropriate responses, including the detection of an attack, identification of an attacker and the assessment of damages. What is required next is an initiative to strengthen resilience designed to maintain the function of attacked space assets. Damage to individual satellites from attacks cannot be avoided entirely, but they can still retain the function as space assets if the function of lost portions can be supplemented and replaced by other means. What are need for this include the capability to promptly launch replacement satellites, the capability to build up space assets by deploying a large number of small and expendable satellites, and the capability to partially replace the function of space assets in places other than outer space (for example, in the form of high-altitude unmanned aerial vehicles (UAVs)). Finally, the possession of the offensive capabilities in outer space is another matter for consideration. Defense in outer space is far from easy, but if the possession of the offensive capabilities can weaken space assets of an adversary, the likelihood increase of deterring an attack by an adversary afraid of a counterattack. In the new domain of outer space, the strengthening of deterrence is possible through the above-mentioned initiatives.

Deterrence in cyberspace has commonalities with deterrence in outer space. Most of threats in cyberspace are routine challenges on the very low threat level and have the features that should be dealt with according to defense and hygiene rather than deterrence. However, some threats, particularly strategic intrusions and attacks on the higher threat level by state actors, should be dealt with deterrence.[49] This is because the inhibition of access to the military networks could mean a military defeat and an attack on socially critical infrastructure is the problem directly linked to the survival of a state. However, there exist a variety of problems in terms of deterrence in cyberspace as well.[50] For example, there are no limitations on the speed or distance in cyberspace. Attackers face no geographical constraints, while defenders are required to deal with dispersed attacks within a fraction of a second. There also exists a major disadvantage that a minor action could produce a significant impact. A simple manipulation could cause a massive impact. The low barrier to entry also poses a problem. The threshold of executing an attack is low as it is possible to launch an attack at a relatively low cost. In addition, there is the lack of transparency. Problems in the detection, attribution and damage assessment in relation to attacks are all difficult to overcome, allowing an attacker to make an assault under the veil of anonymity. The code of conduct is also premature. There is no common understanding concerning legitimate actions. All of these aspects create an unfavorable situation that gives an advantage to attackers over defenders. As there are strong motivations for preventive or preemptive actions in cyberspace, failures of deterrence and an expansion of escalation can occur very easily.

Deterrence initiatives in cyberspace can be considered in the same way as those in outer space. The first important initiative is the strengthening of cyber situational awareness (CSA) to capture an attack situation in cyberspace in a timely manner. It is important for deterrence to put the system in place to constantly monitor the network, instantly detect an attack, identify an attacker and assess the damage incurred. What is required next is the strengthening of resilience to prevent the system from losing its function even under an attack. The primary purpose would be to analyze an attack detected, mitigate its impact and minimize the damage to the system by recovering the damage incurred as soon as possible. The demonstration of the resilience capability represents deterrence by denial in cyberspace. In cyberspace where an attacker has an upper hand, the thought of “active defense” with focus on the cyber offense is emphasized.[51] Also indispensable is the initiative of cyber exploitation for an intrusion into the network of an adversary prior to the occurrence of a conflict to find its vulnerability. Deterrence in cyberspace is pursued with the above methods.

The ideas of deterrence and superiority are also important in the information and psychological domains, though these domains do not attract as much attention as the domains of outer space and cyberspace. To begin with, the establishment of “information dominance” in every domain by having the situational awareness capability superior to an adversary, looking through the disguise and deceit by an adversary and deceiving an adversary by concealing one’s intentions and abilities have been the basics of military operations since ancient times.[52] It is also important to pursue psychological superiority. The objective of war is to deprive an adversary of the willingness to continue the fighting and the objective of deterrence is to deprive an adversary of its intent for challenge. Responses that lack the consideration of the psychological impact do not lead to the achievement of the objective. Establishing the information dominance and gaining a psychological advantage over an adversary are the key to a victory and deterrence. Initiatives in the information and psychological domains become all the more important for threats on the "gray zone" stage short of an "armed attack." An adversary tries to manipulate domestic politics of other countries and/or international opinion by making use of information and psychological maneuvering that is less costly and unlikely to invite a counterattack. A democracy based on the openness of society is vulnerable to these types of challenge. For this reason, countermeasures are required to find out information manipulation by an adversary and defeat that psychological maneuvering. The importance of the information and psychological domains is not particularly peculiar to the modern age, but they are increasingly growing in importance in the wake of globalization and technological advancement.

The challenges in the information and psychological domains take many forms, straddle all the other domains and initiatives to deter them are also wide-ranging. However, the basic approach after all is the strengthening of the situational awareness capability in each domain. Nobody can conduct deterrence or defense unless one is incapable of realizing the existence of challenges or maneuvering. It is necessary to counter the military challenges that go beyond an "armed attack" and also counter the maneuvering at the lower stage short of an "armed attack." The importance of the elements of attack detection, attacker identification and damage assessment is common with the other domains. There is no difference in the significance of strengthening resilience against an adversary's challenges. It is necessary to strengthen countermeasures against the inhibition, modification and deceit of information. It is also necessary to protect the military and social networks, prevent the psychological upset on our side, and the counter manipulation of public opinion with fake news. The proper distribution of information and psychological defense contribute to the strengthening of resilience. Finally, we need to have the capability to launch the information and psychological offense against an adversary. Every possible effort is required to be undertaken to shatter an adversary's confidence and deprive it of the intent for challenge through information manipulation and psychological offense. While some aspects of the deterrence responses in the information and psychological domains do not received adequate consideration, it is vitally important to make redoubled efforts going forward.

The author referred to the initiatives to gain superiority in the new domains above. In the end, the author considers the task of realizing “cross-domain” synergy that straddles multiple domains. In a future war, it is far from certain whether one can achieve the superiority in every domain. Thus, it is required to exert “cross-domain” efforts to make up for the inferiority in a certain domain with the superiority in other domains. For example, an emphasis may be placed on the efforts to make up for inferiority in the traditional domains with superiority in the new domains. Instead of symmetric deterrence to fight on an equal footing (in the same domain) with an adversary, what is important is asymmetric deterrence to aim an adversary’s weak points by leveraging one’s own advantages in different domains. Actually, “cross-domain” synergy has been sought among traditional military services in the form of “integration” among them. This has produced some effects in achieving the superiority through the synergy among domains. However, the promotion of integration involves considerable problems. Cooperation among organizations having different cultures and backgrounds is fundamentally difficult. The sharing of operational concepts is not so easy and cooperation in terms of capabilities tend to be insufficient, and friction among the organizations could prevent an ideal synergy. While even cooperation among the traditional military services is difficult, further cooperation with the new domains is required in the future. In addition, cooperation with non-military organizations is also required under a “whole-of-government approach” to deterrence. The promotion of integration or cooperation on the government-wide scale invites many problems. However, solving these problems will become important for deterrence in the future.

How can we overcome the problems associated with the promotion of “cross-domain” synergy or integration? By simplifying the problems as much as possible, the author would like to address the three aspects of the concept, capability and organization. The task is to seek to share the deterrence strategy or the operational concept in order to paint the “common operational picture” corresponding to the deterrence situation that straddles multiple domains. ASBC/JAM-GC addressed earlier forms of this initiative. As a first step, it is necessary to promote the sharing among the military services corresponding to the three traditional domains, and then include the new domains in the future. On the basis of this, it would be ideal to be able to share the concept, including non-military organizations other than the regular armed forces. Next, in terms of the capability, the task to be taken up is to undertake the initiative to build the capability to promote cooperation among the different military services and organizations. The examples include the promotion of information sharing among the military services and organizations, building of the mutually connected networks that makes it possible, and the repetition of practical training and exercises based on a common operational concept. Finally, in terms of organization, the redesigning of organizations is necessary for strengthening cooperation. This includes the establishment of a unified combatant command organization and the command center of a unified combatant command (including the commander), an expansion of the liaison personnel among the military services and organizations, promotion of interagency cooperation and enhanced cooperation with organizations outside the government, such as local governments and private-sector organizations. Regarding the new domains of outer space and cyberspace, the task will start with the launching of an organization responsible for these domains in the first place. Though there are a lot of problems toward realizing the “cross-domain” synergy, it is necessary to exercise steady and patient efforts to strengthen deterrence.

Conclusion

In this article, the author attempted to put the theoretical basis of the concept of deterrence in order, and pointed out that the interest in the concept of deterrence that declined for a period of time after the Cold War is rising again today against the backdrop of the three changes. These changes are the renewed interest in the strategic competition between great powers, rising concerns over actions seeking to change the status quo that are short of an “armed attack,” and the growing interest in the new domains of warfare. Then, the author mentioned that the building of the posture of “complex,” “full-spectrum” and “cross-domain” deterrence is required in today’s world.

What the author would like to add in the closing is that for deterrence today, there is an increasing need to understand the individual “complex,” “full-spectrum” and “cross-domain” components in an integrated manner. Deterrence is complex enough with the individual components alone, but the actual situation of deterrence further combines these three components. The mode of deterrence can change significantly depending on who is an actor making a challenge, whether it is an expansionist great power, or a rogue state or a non-state actor. At the same time, however, we also have to make a judgment on the stage of challenge, whether it is short of or beyond an “armed attack,” and if it is beyond, how high on that stage it is. Furthermore, it is also necessary to pay attention to a domain where a challenge is being undertaken, whether it is in the traditional domain or in the new domain. How should we respond to a challenge in which domain by what sort of “cross-domain” synergy? The mode of deterrence through the combination of the three components becomes extremely complicated. On top of that, there is even the possibility of the multiple complicated situations of deterrence arising simultaneously. Today’s deterrence structure needs to be able to respond to such complicated deterrence situations.

The author would like to further point out the implications of the discussions in this article for the building of Japan’s deterrence structure in the future. The discussions in this article are the discussions of deterrence in general and do not specifically bear Japan in mind. But some of the discussions may serve as a useful reference for Japan's initiatives going forward. For example, there is the impression that nuclear deterrence, responses to the A2/AD capability, limited defense of islands, and responses to the "gray zone" situations have been discussed independently of each other. But based on the idea of "full-spectrum" deterrence, they should be discussed essentially in an integrated manner. Furthermore, regarding the new domains of deterrence, in Japan, the importance of the domains of outer space and cyberspace has drawn keen interest, but not much attention has been paid the importance of the information and psychological domains. However, there is the possibility of psychologically influencing an adversary through "information dominance" becoming increasingly important in the future. The author would be more than happy if the discussions in this article should serve to provide meaningful insights for the building of Japan's deterrence structure in the future.

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

[2] Bernard Brodie, *The Absolute Weapon*, Harcourt, Brace, 1946.

[3] The Whitehouse, "The National Security Strategy of the United States of America," March 2006, p. 43.

[4] Ministry of Defense, "National Defense Program Guidelines for FY2011 and beyond," December 17, 2010.

[5] Ministry of Defense, "National Defense Program Guidelines for FY2014 and beyond," December 17, 2013.

[6] Mr. Kazuhiro Hashida, director of the Department of Strategic Studies, School of Defense Sciences, National Defense Academy (former chief of the Strategic Research Office, Center for Air Power Strategic Studies, Air Staff College) contributed valuable comments to the preparation of this article. The author would like to take this opportunity to express the gratitude to him.

[7] Furthermore, there exists the risk of failure of deterrence with the threat of excessive retaliation depriving the opponent of moderate options and leaving only extreme options. Thomas C. Schelling, *The Strategy of Conflict,* Harvard University Press, 1999, p. 6.

[8] Richard Ned Lebow, *Between Peace and War,* Johns Hopkins University Press, 1981.

[9] Robert Jervis, Richard Ned Lebow, and Janice Gross Stein, *Psychology and Deterrence,* Johns Hopkins University Press, 1985, Chap.1–2.

[10] Alastair Iain Johnston, *Cultural Realism: Strategic Culture and Grand Strategy in Chinese History,* Princeton University Press, 1995.

[11] Graham Allison and Philip Zelikow, *Essence of Decision: Explaining the Cuban Missile Crisis,* 2nd ed., Addison Wesley Longman, 1999, Chap. 3.

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

[13] Glenn Snyder, *Deterrence and Defense: Toward a Theory of National Security,* Princeton University Press, 1961, pp. 14–16.

[14] Robert Jervis, *Perception and Misperception in International Politics,* Princeton University Press, 1976, Chap. 3.

[15] Robert Jervis, "Cooperation under the Security Dilemma," *World Politics*, vol. 30, no. 2, Jan., 1978, pp. 167–214.

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

[17] James D. Fearon, "Signaling Foreign Policy Interests: Tying Hands versus Sinking Costs," *Journal of Conflict Resolution,* Vol. 41, No. 1, February 1997, pp. 68–90.

[18] James D. Fearon, "Domestic Political Audiences and the Escalation of International Disputes," *The American Political Science Review,* Vol. 88, No. 3, September 1994, pp. 577–592.

[19] Andrew H. Kydd, *Trust and Mistrust in International Relations,* Princeton University Press, 2006, Chap. 7.

[20] Amending the policy of "tao guang yang hui (韜光養晦)" adopted under the leadership of Deng Xiaoping, meaning "to conceal one's strengths and bide one's time," China made a shift to the policy of proactively seeking overseas expansion, declaring that while the previous policy is kept firmly, but the diplomacy will be taken in a more assertive form "堅持韜光養晦、積極有所作為".

[21] The Permanent Court of Arbitration's ruling found that China's claims of "historic rights" within the nine-dash line, which Beijing uses to demarcate its claims in the South China Sea, are without legal foundation, that the features in the South China Sea claimed by China cannot be recognized as "islands" and the exclusive economic zone (EEZ) does not exist around them, and that China is infringing on the Philippine sovereign rights within its EEZ by construction of artificial islands there. The Permanent Court of Arbitration, "In the Matter of the South China Sea Arbitration before An Arbitral Tribunal Constituted Under Annex VII to the 1982 United Nations Convention on the Law of the Sea between The Republic of the Philippines and The People's Republic of China," PCA Case No 2013–19, July 12, 2016.

[22] The White house, "National Security Strategy of the United States of America," December 2017; U.S. Department of Defense, "Summary of the 2018 National Defense Strategy of the United States of America," January 2018.

[23] "Little green men" or "Russian invaders"? *BBC News,* March 11, 2014.

[24] Russian President Vladimir Putin publicly denied the alleged interference in the U.S. presidential election at a press conference after the U.S.-Russia summit meeting in Moscow in July 2017. The Whitehouse, "Remarks by President Trump and President Putin of the Russian Federation in Joint Press Conference," July 16, 2017.

[25] Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars,* The Potomac Institute for Policy Studies, 2007. The method of executing war by combining military means and non-military means is articulated in the "Gerasimov Doctrine," announced in February 2013 by Chief of the General Staff of the Armed Forces of Russia, Gen. Valery Gerasimov. Valery Gerasimov, "The Value of Science is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," *Military Review,* January-February 2016, pp. 23–29.

[26] Linda Robinson, et al, "Modern Political Warfare: Current Practices and Possible Responses," RAND Corporation, (2018); Thomas G. Mahnken, Ross Babbage, and Toshi Yoshihara, "Countering Comprehensive Coercion: Competitive Strategies against Authoritarian Political Warfare," Center for

Strategic Budgetary Assessment, 2018; National Endowment for Democracy, "Sharp Power: Rising Authoritarian Influence," December 2017.

[27] Frank G. Hoffman and Michael C. Davies, "Joint Force 2020 and the Human Domain: Time for a new conceptual framework?" *Small War Journal,* June 10, 2013.

[28] Thomas Cremins, "How to maximise the benefits of a new space age," World Economic Forum, January 18, 2015.

[29] Todd Harrison et al, "Escalation & Deterrence in the Second Space Age," Center for Strategic and International Studies, December 2017.

[30] VADM Arthur K. Cebrowski and John J. Garstka, "Newtork-Centric Warfare: Its Origin and Future," *Proceedings*, Vol. 124, No.1, January 1998, pp. 28–35.

[31] Martin C. Libicki, "Cyberdeterrence and Cyberwar," RAND Corporation, 2009; R. Goychayev, et al., "Cyber Deterrence and Stability," Pacific Northwest National Laboratory, September 2017; Defense Science Board, "Task Force on Cyber Deterrence," February 2017.

[32] Qiao Liang and Wang Xiangsui, "Chogensen: 21 Seiki no 'Atarashii Senso' (Unrestricted Warfare: China's Master Plan to Destroy America)," Kyodo News, 2001.

[33] As a typical example of that, for instance, Michael Green, et al., "Countering Coercion in Maritime Asia: The Theory and Practice of Gray Zone Deterrence," Center for Strategic and International Studies, May 2017.

[34] The notion that the stability of deterrence at a higher stage (typically nuclear deterrence) tends to paradoxically invite the instability of deterrence at a lower stage (typically deterrence by conventional forces). Glenn Snyder, "The Balance of Power and the Balance of Terror," in Paul Seabury, ed., *Balance of Power,* Chandler, 1965, pp. 184–201.

[35] Joint Chiefs of Staff, "Joint Operational Access Concept (JOAC)," January 17, 2012; "Capstone Concept for Joint Operations: Joint Force 2020," September 10, 2012.

[36] T.V. Paul. "Complex Deterrence: An Introduction," in T.V. Paul, Patrick M. Morgan, and James J. Wirtz, eds., *Complex Deterrence: Strategy in the Global Age,* University of Chicago Press, 2009, Chap. 1.

[37] A report of the Congressional Research Service classifies threat actors in cyberspace into the following five types: (1) Cyberterrorists; (2) Cyberspies; (3) Cyberthieves; (4) Cyberwarriors; and (5) Cyberactivists (hacktivists). Catherine T. Theohary and John W. Rollins, "Cyberwarfare and Cyberterrorism: In Brief," Congressional Research Service, March 27, 2015, pp. 2–3.

[38] Herman Kahn, *On Escalation: Metaphors and Scenarios,* Frederick A. Praeger, 1965.

[39] Forrest E. Morgan, et al., "Dangerous Thresholds: Managing Escalation in the 21st Century," RAND project Air Force, 2008.

[40] Needless to say, these stages can be further classified into smaller ladders. And a conflict does not necessarily escalate from a lower stage gradually into a higher stage. It is conceivable that a challenge begins abruptly at a higher stage. Furthermore, it is also conceivable that in a single conflict, there simultaneously exist an area in a less intense situation and an area in a more intensive situation.

[41] U.S. Department of Defense, "Nuclear Posture Review," February 2018, pp. 20–22.

[42] There is no unified definition of the concept of "strategic stability." In this article, the author regards it in the same light as the concept of "first-strike stability" that prevents the first strike. Elbridge Colby, "Defining Strategic Stability: Reconciling Stability and Deterrence," in Elbridge A. Colby and Michael S. Gerson, eds., *Strategic Stability: Contending Interpretations,* US Army War College Press, 2013, p. 48.

[43] Jan Van Tol, "AirSea Battle: A Point-of-Departure Operational Concept," Center for Strategic and Budgetary Assessment, May 2010.

[44] Thomas C. Hammes, "Offshore Control: A Proposed Strategy for an Unlikely Conflict," *INSS Strategic Forum*, No.278, June 2012, pp. 1–14; Jeffrey E. Kline and Wayne P. Hughes, Jr., "Between Peace and the Air-Sea Battle: A War at Sea Strategy," *Naval War College Review,* Vol. 65, No. 4, Autumn 2012, pp. 35–41.

[45] U.S. Department of Defense, "Air-Sea Battle: Service Collaboration to Address Anti-Access & Area Denial Challenges," May 2013, pp. 4–7.

[46] For the difference between the CSBA version of ASBC and the Department of Defense version of ASBC,

see: Kanako AOYANAGI, “US Forces Operational Concept for A2/AD - Air-Sea Battle, Offshore Control, and Deterrence by Denial,” *Air Power Studies*, No. 3, December 2016, pp. 101–111.

[47] The Joint Staff, “Joint Concept for Access and Maneuver in the Global Commons,” January 8, 2015.

[48] Todd Harrison et al, *op cit*., “Escalation & Deterrence in the Second Space age.”

[49] For example, the Defense Science Board of the U.S. Department of Defense regards “attack” and “costly intrusions” as subject to deterrence in cyberspace and excludes other acts of intrusion from the coverage of deterrence. Defense Science Board, *op cit*, pp. 2–4.

[50] Kristin M. Lord and Travis Sharp, ed., “America’s Cyber Future: Security and Prosperity in the Information Age, Volume I,” Center for a New American Security, June 2011, pp. 24–30.

[51] Fred Kaplan, *Dark Territory: the Secret History of Cyber War*, Simon & Schuster, 2016, Chap. 10.

[52] For example, the People’s Liberation Army (PLA) of China is particularly enthusiastic about an “information warfare” to seek “information dominance,” which is said to include all the elements of an electronic warfare, network warfare, psychological warfare, command and control warfare and information warfare. Dean Cheng, *Cyber Dragon: Inside China’s Information Warfare and Cyber Operations,* Praeger, 2017, Chap. 4.