NPI

Maritime Security Study Group Research Progress Report

Increasingly Complex and Sophisticated "Hybrid Warfare" during Peacetime:

Japan's Comprehensive Response and the Japan-US Response

Saito Takashi (former Chief of Staff, Joint Staff), Chairman
Research Committee on Maritime Security

Overview of current research

This study group is focused on research delving into law enforcement in a "gray zone," situation. Besides returning to the basics, we have expanded our scope of inquiry to include not only law enforcement but also the domain of "space" to be considered along with land, sea, and air domains; and the "cyber domain" and the "electromagnetic domain" as conceptual spaces. In addition, the scope has been expanded to the "cognitive domain" in which—rather than relying on information warfare and public opinion warfare—advanced information processing technologies are used for the ultimate goal of influencing the decision-making of national leaders. Thus, this research deepens investigation into the nature of so-called "hybrid warfare." Even in the conventional area of the sea, there are subjects related to the seabed—such as underseas resources and underseas cables—that should be considered from a new perspective as well. With this view, it is essential to be aware that competition between countries has already begun in peacetime.

Battles in the cyber, electromagnetic, and space domains can occur independently but in "hybrid warfare" in which these battles are intricately intertwined, our research addresses Japan's role in the Japan-US alliance and what the rules-based international order should be.

Our ongoing research proceeds with recognition of the following issues:

- Besides the three conventional domains of land, sea, and air, the additional space, cyber, electromagnetic, and cognitive domains are becoming increasingly complex and elaborate as a result of rapid technological innovations. While these domains are being controlled by various means, the use of "hybrid warfare," which involves both conventional and new domains of warfare, by both state and non-state actors, is likely to become the norm in the future.

- China is skillfully avoiding the military intervention of other countries while harnessing and utilizing all available national means to pursue its own superiority during peacetime. It is actively engaged in behaviors designed to achieve its determined national goals. The means China is adopting to achieve these ends can, depending on the circumstances, include military force. Russia has already carried out this type of military action in Ukraine and elsewhere. Thus, it is highly likely that state actors and others will imitate and utilize these means.

- In particular, the trends in China toward reforming the People's Liberation Army Strategic Support Force; trends in the China Coast Guard, whose liaisons with the People's Liberation Army are being strengthened under the direction of the Central Military Commission; the Chinese goal of achieving hegemony in the space domain; and its insistence on claiming territorial rights indicate that, rather than showing any willingness to adopt a more yielding position, China is instead increasing its activities in these areas.

- At the same time, the conflict between the US and China is becoming increasingly serious. The post-corona world is highly unpredictable; thus, the escalation of an unexpected event or a miscalculation into a major military conflict cannot be ruled out. However, despite the fact that globalization has suddenly lost a great deal of momentum as a result of the COVID-19 pandemic, if we base our strategy on a cool-headed and dispassionate calculation, we will see that a state of emergency in which large-scale military conflict rapidly develops in a peaceful world such as ours with widespread economic ties is highly unlikely.

- Currently, countries are already engaged in competition or conflict over national interests at a level below that of armed attack and the line between "peacetime" and "contingency" has already become blurred. Therefore, it is necessary to do away with a dualistic view of security that clearly delineates "peacetime" from "contingency," as represented by the Japanese proverb "Soldiers are trained for a hundred years for the purpose of a single morning's battle."

With awareness of the above issues, the research is currently moving in the following direction:

General argument: Concentration of comprehensive national power

Modern warfare does not rely solely on military means but is rather a "total war" that includes the economy, resources, and information. However, in recent years, new means of war have been added, such as electromagnetic and cyber warfare. Because of the unique characteristics of these new means of waging war, even if there is an attack, it is difficult to judge whether a military objective was intended when these means are utilized. Thus, it is necessary to recognize that these means represent a new category that goes beyond the dualism of "war" and "peace." Specifically, this requires that the response to "hybrid warfare," which develops during peacetime, not only rely on diplomatic and defense

authorities but also include government-affiliated organizations and private industry in order to concentrate the comprehensive power of the country.

Particularly in the domains of space, cyber, electromagnetism, and deep-sea resources, which previously were not considered military domains, comprehensive initiatives in the form of "industry-government-academia collaboration," in which government-affiliated organizations, university research facilities, and private industry work together, are required.

Discussion I: Issues with domestic systems

When discussing "hybrid warfare," one of the problems that arises is how to respond, particularly when the situation has not developed to the level of armed conflict. At present, the law that can be applied during situations that are below the level of an armed conflict is "Act on the Peace and Independence of Japan and Maintenance of the Nation and the People's Security in Armed Attack Situations etc." Chapter III Article 21 of this Act indicates that the "measures and other required policies" that are to be applied to "a contingency situation" are as follows:

1) Enhancement of the system for gathering and compiling information about the circumstances and analyzing and evaluating the situation

2) Preparation for formulating a response policy for use in various situations

3) Strengthening cooperation between the police, the Japan Coast Guard and other related organizations, and the Self-Defense Forces.

The above three measures apply to "hybrid warfare," which was assumed by the committee that drew up the Act to not have reached the level of armed conflict. Further effort is necessary to carry out this policy.

① Enhancement of a system for surveillance and intelligence gathering

Key to a response to hybrid warfare is the early detection of the signs and prevention of their becoming established facts. For that purpose, it is necessary to enhance the information collection and monitoring system for the entire country regarding the space, cyber, electromagnetic, and cognitive domains, as well as the conventional surveillance and information gathering of sea and airspace.

② Creating a lateral command structure for the cognitive domain

"Cognitive warfare," which in recent years has consisted of spreading "fake news" via social networking sites (SNS) and identifying public trends using artificial intelligence (AI) and big data processing technology, is conducted with the ultimate aim of influencing the decisions made by national leaders. It is thus far more complex, diverse, and sophisticated than conventional public opinion, legal, and psychological warfare, out of which it grew. Response to cognitive warfare cannot rely solely on military intelligence; rather, the ability to gather wide-ranging information via the Internet and technological trends, the ability to evaluate and disseminate information to the international community and a command structure that is able to harness the full power of the country are now required.

③ Constructing a lateral organization in the cyber domain

The term "cyber" refers to a complex system that includes the exploitation of private data and sensitive information held by private corporations and government organizations for the purpose of causing social confusion by interfering with financial institutions, engineering the breakdown of essential infrastructural elements, and coordinating cyber and electromagnetic attacks in order to disrupt and paralyze governmental or working unit command structures. These events cannot be dealt with individually, but rather require an organizational structure that provides a general overview of the entire situation and can respond laterally.

④ Centralized management of satellite orbit data

In the space domain, to ensure the secure utilization of satellites, the ability to avoid debris and intentional interference is of utmost importance. It is therefore important for countries that share problem awareness to share information. This in turn requires that data regarding the orbits of satellites be monitored in a centralized manner. At that time, coordinating with Japan Aerospace Defense Ground Environment (JADGE) should be considered.[1]

⑤ Reinforcing collaboration among the police, the Japan Coast Guard, and the Self-Defense Forces

Rather than only reinforcing collaboration during actual and map-based training exercises, there must be a shared awareness of the facts that, while collaborative efforts place greater demand on our own human resources, the command and control relationships between the military and law enforcement agencies will be clarified, and there is a need to respond appropriately to hybrid warfare, which lacks a clear distinction between peacetime and contingencies. For this reason, it is necessary to organize the command and control relationship between the Self-Defense Forces and law enforcement agencies that will respond during peacetime through activity such as coast guard operations, security operations, and defense operations. It is also important to increase the interoperability of equipment utilized by the Maritime Self-Defense Force and the Japan Coast Guard. In such cases, the restrictions imposed by Article 25 of the Japan Coast Guard Law that prevent involvement in military actions must not be interpreted as impeding military and non-military cooperation.

⑥ Need for the early involvement of other ministries and agencies in the Alliance Coordination Group (ACG)

Other ministries and agencies now participate as needed in the Alliance Coordination Group (ACG),[2] which is part of the current alliance coordination mechanism. An important part of an effective response to the increasingly prevalent hybrid warfare is the ability to detect as soon as possible the signs of its operation. The early detection of such indications over a wide area requires not only collaboration between the defense and diplomatic ministries but also for the relevant ministries and agencies to take the initiative from the beginning and lead cooperation between Japan and the US. In that

sense, continuous involvement by other ministries and agencies in the ACG even prior to the appearance of any indication of cyber warfare is required.

Discussion II: Issues of domestic law and international norms in hybrid warfare

① Issues with domestic law

Even if the situation does not rise to the level of an armed attack or clear infringement upon national sovereignty, it has a negative effect on national interests. Such situations have shown signs of occurring not only in the realm of "territorial land and airspace" but also in the cyber domain. In addition, in the space domain, interference with satellites has become a reality. To deal with such a situation, it is necessary to clarify how to respond in accordance with domestic law.

② Issues with international norms

Is there a necessity for regulations that establish traffic rules for satellites and other objects in space similar to the Convention on the International Regulations for Preventing Collisions at Sea (CORLEG)? Although international discussion on regulations concerning space as well as the cyber and electromagnetic domains is currently ongoing, there is need for caution so that the space, cyber, and electromagnetic domains do not become a situation similar to that of the South China Sea.

Discussion III: Japan-US cooperation on hybrid warfare

There is no question that the commitment of the US military is vitally important in deterring and dealing with an armed attack situation. We recognize the increase and deepening of cooperation between Japan and the US for that purpose. However, to respond to hybrid warfare, which is becoming increasingly complex, sophisticated, and therefore difficult to deter, it is important to establish, at the stage below the level of armed conflict, a concrete and explicit cooperative relationship that goes beyond the framework of the current Japan-US defense and diplomatic collaboration. Such a relationship will lead to the deterrence of situations that are below the level of an armed attack.

① Establishment of a new Japan-US framework

For Japan and the US to respond to hybrid warfare, it is necessary to create a new framework for cooperation based on the Japan-US alliance that goes beyond the current "New Guidelines for Japan-U.S. Defense Cooperation." Furthermore, there is a need to create a framework that facilitates a deep level of involvement of all related organizations and agencies and not solely those related to defense and foreign affairs.

② Concrete and explicit Japan-US cooperation in situations below the level of armed attack

After achieving mutual understanding of the legal systems in Japan and the US, the Japanese and US response to situations that are below the level of an armed attack must be concretely and explicitly expressed.

In particular, it is necessary to devise procedures by which cooperation between the Japan Coast Guard, the police, the Japan Self-Defense Forces, the U.S. Armed Forces, and the U.S. Coast Guard can be carried out from the stage of warning and surveillance for the purpose of guarding the coasts and engaging in security operations. This needs to be done in such a way so as to ensure that it is within the policing powers of the Japan Self-Defense Force.

③ Division of roles of and cooperation between the Japan and the United States in the space, cyber, and electromagnetic domains

There is ongoing debate over attacking enemy bases as a form of missile defense, but this debate is taking place on the premise of a Japan-US "shield and spear" policy.

In addition to this debate, the time has come to comprehensively coordinate the roles played by Japan and the US and the procedures for the two countries to collaborate when events in the space, cyber, and electromagnetic domains occur that do not rise to the level of armed conflict. This must include discussion on whether these new procedures should be an extension of the abovementioned premise.

④ Japan-US collaboration for the purpose of forming international norms in the space, cyber, and electromagnetic domains

To prevent hostile actions that would disrupt order in the space, cyber, and electromagnetic domains, there is an urgent need to formulate effective international norms regarding these domains as well as a surveillance system to monitor them. Thus, Japan and the US must cooperate and lead the international community in these efforts.

September 11, 2020

Notes

[1] Japan Aerospace Defense Ground Environment (JADGE): An automatic alert monitoring system that utilizes Japan Air Self-Defense Force radar bases, early warning systems, interceptors, and ground-to-air missiles. It utilizes the four stages of air defense: discovery (flight detection and tracking), identification (belonging to which nation), interception (prevention of the invasion of air space by a craft of unknown origin), and defeat (repelling an enemy craft that has invaded). Ballistic missile defense is operated as part of the common guidance system of the three branches of the Japan Self-Defense Forces.

[2] Alliance Coordination Mechanism, Alliance Coordination Group (ACG): According to the "New Guidelines for Japan-U.S. Defense Cooperation" that was approved in 2015 in a 2 + 2 agreement by Japan and the US, an "Alliance Coordination Mechanism" was established. Its objective is to reinforce the sharing of information between the governments of Japan and the US during times of peace in order to ensure the cooperation of the entire government—including all related agencies—within the alliance in a seamless and effective manner. ACG is an organization that coordinates policies related to the activities of the Japan Self-Defense Forces and the US military through the agreement of the Japan-US Defense Cooperation Sub-Committee. Its members include diplomacy- and defense-related department heads, directors, and supervisors in both governments.