NPI

Nakasone Peace Institute

Final Report

Establishing Response Guidelines and Building a Multilateral Deterrence Posture for Deterring a Taiwan Contingency — Essential Measures for Countering Hybrid Warfare

Maritime Security Study Group

March 2026

中曽根平和研究所
Nakasone Peace Institute

Contents

Introduction

1. Overview of Research Project

The Maritime Security Study Group at Nakasone Peace Institute (NPI) conducted a three- year research project on "Establishing Response Guidelines and Building a Multilateral Deterrence Posture" from fiscal year 2023 through fiscal year 2025.

In conducting this research, it was essential to establish a clear interpretation of the term "Taiwan contingency." Rather than interpreting it in a narrow sense as a full-scale military invasion of Taiwan by China, the Maritime Study Group adopted a broader interpretation. Specifically, as used in this report, the term covers not only a full-scale invasion but also includes scenarios in which China combines various means, both military and non-military, and, without resorting to a full-scale military invasion, advances toward forced unification through what are known as hybrid warfare methods.

Based on this understanding, while numerous studies and simulations have been conducted regarding a full-scale military invasion of Taiwan by China—including analyses incorporating non-military elements—there has not been sufficient examination of scenarios in which China seeks the forced unification of Taiwan through hybrid warfare without escalating to a full-scale military invasion. In recognition of this gap, this study places particular emphasis on the analysis of hybrid warfare.

In the event that China seeks to achieve the forced unification of Taiwan through the use of diverse hybrid warfare methods, it is anticipated that the target of such measures would extend beyond Taiwan to include Japan, the United States, and other relevant countries. With the recognition that effective countermeasures would therefore require robust multilateral coordination, this study examines the specific directions such cooperation should take.

If these specific measures can be employed to effectively respond to China's use of various hybrid warfare methods, it will be possible to both prevent forced unification that falls short of a full-scale military invasion as well as to deny China the opportunity to shape conditions to its advantage in advance in the case that it abandons such efforts and attempts to proceed to a full-scale invasion. Taken together, these efforts are expected to contribute significantly to the overall deterrence of a Taiwan contingency.

2. Research in FY2023

The conceptual model developed by the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) was analyzed to provide guidelines for this study. Based on these guidelines, and as a premise for constructing an original conceptual model applicable to a Taiwan crisis, this study defines hybrid warfare as follows:

> Hybrid warfare is defined as the pursuit of objectives that have traditionally been accomplished through full-scale military warfare by employing a combination of means, both military and non-military, without escalating to full-scale military war.

On this basis, the research proceeded assuming scenarios in which China would attempt to unify Taiwan by combining various means in a gray-zone environment, while avoiding the outbreak of full-scale military war.

As fieldwork for this research project, visits were conducted to the European Centre of Excellence for Countering Hybrid Threats, NATO Strategic Communication Centre of Excellence, and research institutions in Finland and Latvia, where the exchange of views was held with scholars specializing in hybrid warfare.

In addition, based on the 40 tools identified in the conceptual model by the European Centre of Excellence for Countering Hybrid Threats, the Study Group began work to compile a casebook extracting anticipated concrete activities as well as relevant past examples employing these tools.

3. Research in FY2024

On the premise that China would conduct hybrid warfare aimed at the forced unification of Taiwan by skillfully alternating between a "coaxing approach" and a "hardline approach," a hypothetical model was developed based on the "means and activities" identified in the process of compiling the casebook.

In constructing this hypothetical model, priority was given to identifying Japan's vulnerabilities. Therefore, rather than focusing on assessing the probability of the use of individual hybrid methods, the model was designed to incorporate as comprehensively as possible those means that could possibly arise within a series of scenarios.

With this hypothetical model in hand, field research visits were made to multiple research institutions in Taiwan to solicit their views on the validity of the model. At the same time, exchanges were conducted regarding the challenges Taiwan currently faces, which provided the Study Group with valuable insights for examining the vulnerabilities confronting Taiwan.

Building on this, and based on the hypothetical model, the study then used Taiwan as a base to conduct a revised analysis of hybrid methods directed against Japan, the United States, and other relevant countries. After identifying Japan's vulnerabilities in this context, policy recommendations were formulated to strengthen resilience in response to each of these methods.

4. Research in FY2025

Amid expectations of major changes in the global framework, this study was conducted based on a projected model of China's hybrid warfare aimed at the forced unification of Taiwan. The relationship between such hybrid operations and attempts at unification through full-scale military invasion was reorganized and reanalyzed. The study also identified the significance of countering hybrid warfare in deterring a Taiwan contingency.

Drawing on the outcomes of the FY2024 visit to Taiwan, the analysis reexamined the vulnerabilities Taiwan faces in the field of hybrid warfare. In light of Japan's efforts to strengthen its own resilience, the study further considered effective forms of multilateral cooperation to neutralize

the various hybrid methods that China is likely to employ against Taiwan.

Further exchanges of views were conducted with researchers from Taiwan, the United States, Australia, and the Philippines with regard to the appropriate form of multilateral cooperation. Taking account of the outcomes of these discussions, a webinar that included researchers from other countries was convened to further broaden debate, after which formulation of the final recommendations was completed.

The collection of case studies on hybrid methods discussed in the research will be further expanded. In addition, the cases examined in the study—including projected scenarios identified through the research—will be compiled into a database, including both English-language and Japanese language versions, and made publicly available online for use in future research conducted internationally.

Chapter 1: Deterrence of a Taiwan Contingency and Countering Hybrid Warfare

1. Definition of Hybrid Warfare

In recent years, the term "hybrid warfare" has come into frequent use in security-related discourse. However, the meaning attributed to this term is not necessarily the same among different authors, and the security implications they seek to describe using it also vary. Accordingly, this study begins by clarifying the definition of hybrid warfare adopted herein.

The etymology of "hybrid" derives from plant breeding in which two different strains are crossed. The term "hybrid warfare" is generally understood to denote warfare that combines traditional military means with various non-military means to be used together as a combined whole. On this point, there is broad agreement among scholars.

However, significant differences arise among analysts regarding how hybrid warfare is positioned in relation to full-scale military war. Here, "full-scale military war" refers to high-intensity conflict fought between the regular armed forces of two or more states, employing their respective firepower capabilities. As shown in Figure 1, the definition of hybrid warfare can be divided into three categories based on how they relate to full-scale military war.

Three Definitions of Hybrid Warfare

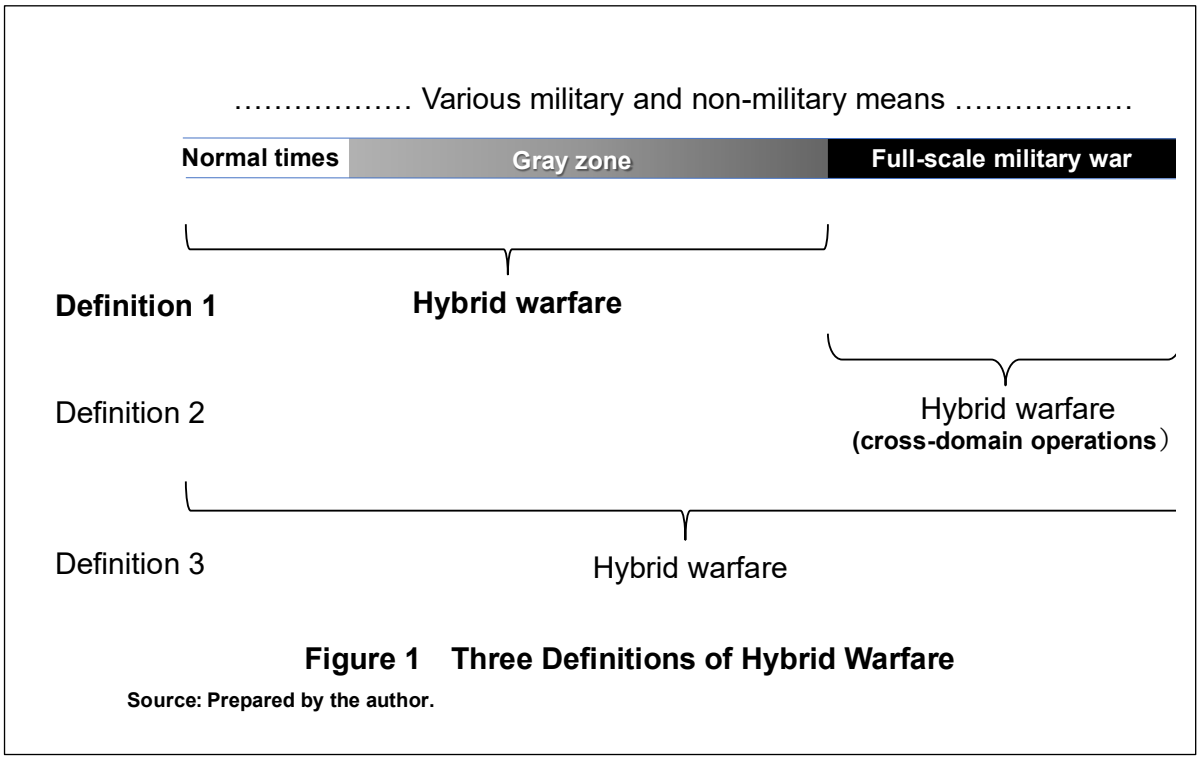

Figure 1　Three Definitions of Hybrid Warfare

Source: Prepared by the author.

Figure 1 Three Definitions of Hybrid Warfare

Source: The Essential Mechanism of Hybrid Warfare—"Fight in the cognitive space" integrating military and non-military means to achieve the ultimate objectives— by Matsumura Goro; February 2, 2024, Nakasone Peace Institute; https://www.npi.or.jp/en/research/data/npi_research_note_matsumura_20240202.pdf

The broadest of them is Definition 3, which includes everything from peacetime and "gray-zone" battles short of full-scale military conflict to the use of various hybrid methods within full-scale military war itself. For example, Hirose Yoko employs the term in this broad sense in her book *Hybrid Warfare: Russia's New National Strategy* (in Japanese).[1]

In contrast, the premise of Definition 2 is the view that the term "war" itself properly refers to high-intensity armed conflict; therefore, the use of hybrid methods in situations falling short of such conflict are not included within the category of hybrid warfare. From a similar perspective, some argue that analyzing these activities under the framework of "hybrid warfare" is itself misleading. Instead, they contend that the focus should be placed on the employment of various new methods within the context of full-scale military war, and that such developments should be examined through the framework of cross-domain operations (also referred to as all-domain operations or multi-domain operations).[2] If one adopts the position that the essence of war will continue to be use of force centered on firepower, and that new and diverse methods are employed to most effectively exert armed force, then this interpretation can be considered valid.

By contrast, Definition 1 conceptualizes hybrid warfare as the employment of various military and non-military means in situations that do not escalate to full-scale military war or in which escalation to such war is intentionally avoided in order to achieve strategic objectives. This definition has been adopted by many scholars.[3] Even if full-scale military war is unlikely to disappear in the future, when assuming that new forms of conflict short of full-scale war will become increasingly significant, adopting the concept of hybrid warfare as articulated in Definition 1—clearly distinguished from full-scale military war—allows for greater analytical clarity.

The focus of this study is placed on China's efforts to achieve the forced unification of Taiwan without resorting to a full-scale military invasion. Therefore, in this report, the term "hybrid warfare" is used in the sense of Definition 1 and is defined as "the pursuit of objectives traditionally achieved through full-scale military war by combining a range of military and non-military means in order to attain those objectives without escalating to full-scale military war."

---

[1] Hirose Yoko, Haiburiddo Senso: [*Roshia no Atarashii Kokka Senryaku* "Hybrid Warfare: Russia's New National Strategy"] (Japanese), Kodansha Gendai Shinsho, Kodansha Ltd., 2021.

[2] Yoshikazu Watanabe, Takeshi Inoue, and Takahiro Sasaki, *Puchin no "Chogensen": Sono Zenbo to Shippai no Honshitsu* "Putin's 'Unrestricted Warfare': Its Whole Picture and the Essence of Failure"] (Japanese), Wani Books Plus, Wani Books Co., Ltd., 2022, pp. 7-11.

[3] In Shida Junjiro, [*Haiburiddo Senso no Jidai: Nerawareru Minshushugi* "Hybrid War Era: Enduring Threats to Democracy"] (Japanese), Namiki Shobo publisher, 2021, the adoption of Definition 1 is appropriate after referring to many previous studies, pp. 11-62. The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), jointly established in Helsinki, Finland, in 2017 by NATO, the EU, and their member states, works to address hybrid threats in situations that do not lead to full-scale military war under a similar recognition. "Hybrid threats as a concept," Hybrid CoE, https://www. hybridcoe.fi/hybrid-threats-as-a-phenomenon/ (last accessed September 13, 2023).

2. Four Patterns of Forced Unification of Taiwan by China

Methods China might attempt in the forced unification of Taiwan include not only a full-scale military invasion in which the People's Liberation Army physically occupies Taiwan but also an approach relying on hybrid warfare methods to compel unification without resorting to a large-scale invasion.

In this case, hybrid warfare would likely precede any full-scale military invasion and in some cases could escalate into such an invasion. However, there could be several variations in the relationship between these two approaches. Figure 2 organizes these possibilities into four distinct patterns. Patterns 1 to 4 and the characteristics of the relevant deterrence efforts are organized as shown in Figure 2.

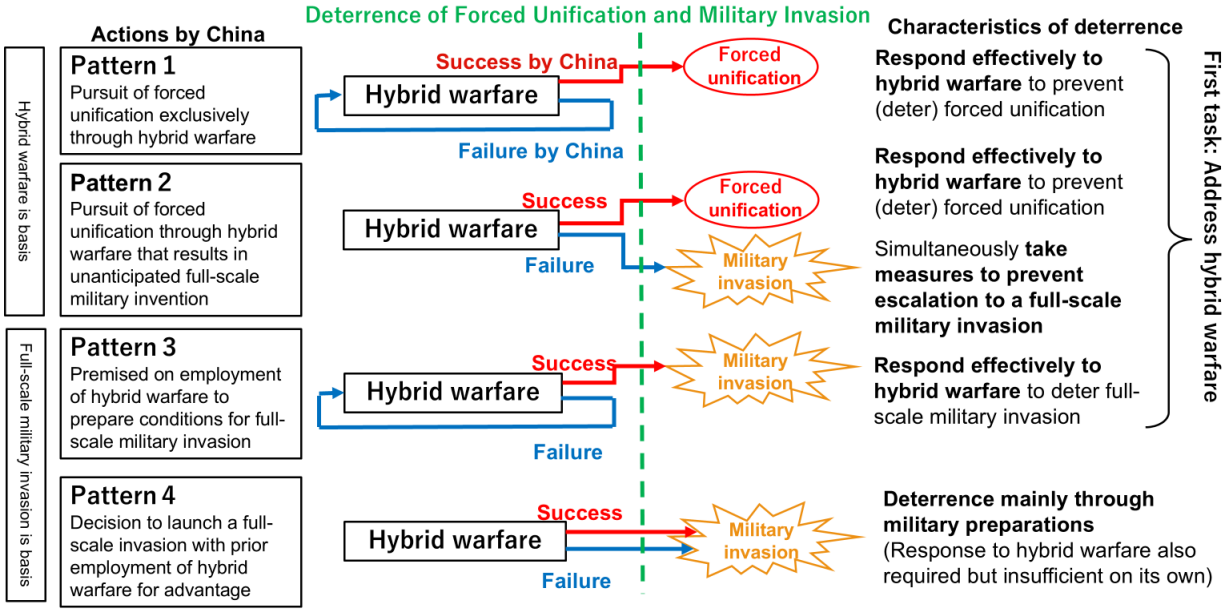

Figure 2. Four Patterns of Forced Unification of Taiwan by China

(Prepared by the author based on Figure 2 (page 4; footnote 6) in the Maritime Security Study Group Report of Nakasone Peace Institute. https://www.npi.or.jp/en/research/data/npi_policy_maritime_security_en_20250331.pdf)

Figure 2 Four Patterns of Forced Unification of Taiwan by China

Source: "Countering Hybrid Warfare to Prevent the Forced Unification of Taiwan —Addressing China's Dual Threats of Hybrid Warfare and Full-scale Military Invasion—" Matsumura Goro, November 19, 2025; Nakasone Peace Institute; https://www.npi.or.jp/en/research/data/npi_research_note_matsumura_20251119_en.pdf

China's strategic approach can be broadly divided into two categories: one that places primary emphasis on forcibly unifying Taiwan through hybrid warfare methods, and another that centers on occupying Taiwan through a full-scale military invasion.

In the former case in which primary emphasis is placed on hybrid warfare, Pattern 1 refers to a scenario in which hybrid methods are pursued consistently and escalation to full-scale military invasion is avoided. In contrast, Pattern 2 describes a scenario in which hybrid warfare is pursued, but failure in that effort compels a reluctant transition to full-scale military invasion. The danger inherent in this pattern lies in the outbreak of full-scale war at a time unforeseen by either party.

Initially, it may seem paradoxical that a strategy centered on hybrid warfare would, upon failure, be forced to shift to full-scale military invasion. However, multiple factors could combine to produce such an outcome: the necessity to avert a domestic political crisis caused by failure; the desire to avoid putting the country into a disadvantageous position in international politics; or to avoid a decline in the credibility of future threats after large-scale military force has failed to achieve its intended effect. Under such circumstances, leadership might feel compelled to escalate to a full-scale invasion that it had not originally intended to undertake. Russia's invasion of Ukraine can be regarded as an example of this pattern.

In contrast, Patterns 3 and 4 assume from the outset that preparations are made with a full-scale military invasion in mind. As part of these preparations, certain conditions are first established through the use of hybrid warfare. In Pattern 3, a full-scale military invasion is launched only if those efforts succeed. In Pattern 4, hybrid warfare is conducted as well, but regardless of whether it succeeds or fails, it is predetermined from the outset that the process will proceed to a full-scale military invasion.

In either case, it is expected that diverse hybrid methods will be employed against Taiwan across political, diplomatic, economic, socio-cultural, informational, and military domains. At the same time, various hybrid methods would likely be directed at Japan, the United States, and others to create conditions favorable to the forced unification of Taiwan. Therefore, if Japan and the United States cooperate with Taiwan to take sufficient countermeasures against China's hybrid warfare and thereby cause it to fail, it would be possible to prevent forced unification under Pattern 1. However, in the case of Pattern 2 and beyond, the analysis becomes more complex due to the additional factor of a potential transition to full-scale military invasion.

In responding to Pattern 2, it is necessary not only to counter hybrid warfare but also to prevent a situation in which the success of those countermeasures compel China to shift to a full-scale military invasion. In other words, it is necessary to strengthen the military capabilities of Taiwan and those supporting it as a deterrent against invasion. Furthermore, since large-scale military intimidation carried out as part of hybrid warfare carries the potential of escalating into full-scale invasion if it fails to achieve its objectives, it is important to strengthen international norms that discourage resorting to large-scale intimidation.

Patterns 3 and 4 represent model cases at opposite extremes for analytical clarity. However, if China were to actually undertake a military invasion, the course of events would likely fall somewhere between these two patterns. That is, the situation is more complex than a simple binary choice between refraining from invasion if hybrid warfare fails and proceeding with invasion regardless of success or failure. Rather, it is more likely that the more successfully China is able to shape favorable conditions through hybrid warfare, the lower the threshold for deciding on military invasion becomes. Conversely, the more such efforts are thwarted, the higher that threshold rises. In this sense, the more effectively hybrid warfare is countered, the greater the likelihood of deterring a military invasion.

3. Significance of Responding to Hybrid Warfare

As mentioned in the preceding section, effectively countering China's hybrid warfare and thwarting its attempts does not necessarily guarantee deterrence against a full-scale military invasion. However, effective countermeasures against hybrid warfare are important for both preventing forced unification below the threshold of military invasion, as well as for deterring or responding to an actual military invasion.

Based on this assumption, it is necessary to consider whether it is possible to pre-emptively deter hybrid warfare itself, which employs a combination of various methods. Generally speaking, it is extremely difficult to deter each individual method used in hybrid warfare before it is actually employed.

There are two main reasons for this challenge. First, the individual methods used in hybrid warfare vary widely, ranging from very minor actions carried out during peacetime to highly aggressive and intense measures, making it extremely difficult to determine the exact point at which their use was initiated.

Next, while it is common for methods from various fields to be used in combination to achieve a specific objective, it is initially difficult for the defending side to discern the unified purpose or the interconnections among them. By the time these details become clear, hybrid warfare is already underway.

For this reason, when considering the deterrence of hybrid warfare, it is unrealistic to prevent the use of every possible method in advance. Instead, various countermeasures should be implemented in each field to prevent further escalation, with the aim to make the attacker abandon the objective at an early stage, before it is ultimately achieved, thereby stabilizing the situation.

From this perspective, if Japan, the United States, Taiwan, and other countries each adopt measures to reduce vulnerabilities and enhance resilience in their respective fields, this will diminish the effectiveness of China's hybrid methods. While it is impossible to fully prevent the onset of hybrid warfare, it is important to reduce the impact of each individual hybrid method by strengthening one's own resilience. At the same time, it is imperative to impose costs on the adversary to create hesitation in continuing operations, thereby compelling abandonment of hybrid warfare attempts midway.

Taken together, strengthening hybrid warfare countermeasures by Japan, the United States, and Taiwan can play an effective role in four stages:

1. Neutralizing China's hybrid warfare methods as they occur and stabilizing the situation.
2. Preventing China from continuing hybrid warfare to forcibly unify Taiwan.
3. Deterring China from launching a full-scale military invasion of Taiwan.
4. Contributing to effective responses in the event that China does carry out a full-scale military invasion.

4. Impact of Global Developments on China's Hybrid Warfare

In the three years since this research project was begun, shifts in the global landscape, the rapid advancement of technologies such as AI, and events like the global pandemic are factors that have complicated the ability to predict the effects of China's hybrid warfare. Nevertheless, this study attempts to provide a broad overview.

(1) Impact of Destabilization of U.S.-European Relations

Exploiting situations advantageous to China

China is likely to take advantage of international instability caused by Russia's invasion of Ukraine and the reactions of the United States, Europe, and others by conducting hybrid warfare aimed at weakening the relationship between Taiwan and the United States. Going forward, China is expected to maximize such situations to increase Taiwan's distrust of the United States and to create conditions favorable to itself. In particular, with the January 2025 inauguration of a second Trump administration, which advocates an "America First" policy, China may see an opportunity to drive a wedge between the United States and its allies and partners. This could increase the likelihood of hybrid warfare aimed at weakening relations, generating mutual distrust, and undermining ties between the United States, Taiwan, Japan, and other allied or partner nations.

・Rebuilding economic and military relations

In the midst of ongoing economic tensions between the United States and China, China is likely to strengthen its economic and military ties with other countries in order to undermine U.S. influence. For example, China may seek to enhance cooperation with countries in Central Asia, Southeast Asia, and Africa, as well as rebuild relations with Europe, with the aim of isolating the United States internationally. As a result, China's "wolf warrior diplomacy" and other aggressive foreign policy attitudes may temporarily recede from the spotlight.

・Restructuring supply chains

As economic tensions between the United States and China are ongoing, China is likely to promote diversification of supply chains and build international economic relationships that serve its own interests, separate from the U.S.-dominated dollar settlement system.

・Technological self-reliance and strengthening asymmetric capabilities

U.S. tariffs and export controls imposed on China affect the country's economic growth and technological development. In response, China is expected to accelerate domestic technological self-reliance while further fortifying asymmetric methods such as cyberattacks and information manipulation.

・Propaganda criticizing U.S. policies

China is likely to expand and intensify propaganda criticizing U.S. policies both domestically and

internationally, aiming to boost national patriotism while garnering support from Global South countries.

・Propagating the message that "the U.S. may abandon Taiwan"

China may circulate information to European countries that casts doubt on U.S. reliability, encouraging them to reconsider their relationship with the United States. Within Taiwan, China could also disseminate information designed to generate distrust by suggesting that "the U.S. may abandon Taiwan," and conduct hybrid warfare intended to make these messages appear credible.

・Generating a decline in U.S. military support for Taiwan

China may conduct repeated military exercises around Taiwan to test the level of U.S. involvement in Taiwan's security. In the long term, as the United States shifts more of its defense burden onto allies and focuses on maintaining the balance of power among major powers, China may seek to create a situation in which U.S. military support for Taiwan declines.

(2) How North Korea and Russia Could Influence Unification of Taiwan

China, Russia, and North Korea have been portraying a rapidly growing closeness, but it is unclear whether this is genuine. For example, if China were to move to employ military force to unify Taiwan, it is uncertain how Russia and North Korea would become involved militarily. Given their limited capabilities, both countries may prefer to avoid direct military support. Based on this premise, Russia and North Korea may instead indirectly support China's hybrid warfare to maintain their relationship with China. Going forward, it is necessary to consider the possibility that China, Russia, and North Korea could cooperate in hybrid warfare activities, particularly in critical areas such as cyberattacks and attacks on infrastructure.

(3) Impact of Russia's Invasion of Ukraine

・Possibility of applying pressure through missile and nuclear threats

China may draw lessons from the nuclear blackmail employed by Russia during its invasion of Ukraine.

・Adoption of Russian hybrid warfare know-how

China's hybrid warfare capabilities are reported to be approximately five years behind those of Russia, but they appear to be rapidly catching up.[4]

(4) Rapid Advancement in Generative AI Technology

China's generative AI technology is advancing rapidly, and, in particular, there has been improvement in the accuracy of deepfakes created using generative AI. China is leveraging these technologies to disseminate strategic narratives whose authenticity is difficult to verify across social media and video

[4] National Institute for Defense Studies, https://www.nids.mod.go.jp/

platforms. In addition, the poisoning of training data for large language models (LLMs) by malicious actors requires attention as a new means of hybrid warfare capable of significantly impacting public opinion in target countries.

(5) Impact of the COVID-19 Pandemic

The pandemic appears to have provided an opportunity for China to diversify its hybrid warfare methods.

- In order to counter international criticism regarding the origin of the virus and the country's own response to the outbreak, China appears to have gained experience in propaganda and public opinion manipulation.
- With the increase in remote work and online activities, China further recognized the strategic value of cyberattacks and information theft in cyberspace.
- China also appears to have learned that it can exercise diplomatic influence through the provision of medical supplies.

Chapter 2: An Analysis of the Conceptual Model of the European Centre of Excellence for Countering Hybrid Threats

During the Crimea crisis in 2014, prior to launching a conventional military invasion, Russia skillfully employed unconventional means such as disrupting communication networks, spreading fake news, and manipulating public opinion through social media, and occupied and "annexed" Crimea with almost no bloodshed. A similar course of events had been predicted when Russia launched its invasion of Ukraine in February 2022. However, Russia's hybrid warfare was not successful at that time, ultimately leading to a full-scale military invasion. One factor that has attracted attention as a cause of the difference between 2014 and 2022 is the set of countermeasures based on the "Conceptual Model of Hybrid Threats" (hereafter referred to as the "Conceptual Model").

The Conceptual Model was developed over a period of approximately two years from July 2018 by the European Centre of Excellence for Countering Hybrid Threats, with the cooperation of the Joint Research Centre of the European Commission and is thought to have been used to systematically understand the various events that occurred during Russia's invasion. The present study referenced the Conceptual Model in its research, so the following presents an analysis of the outline and fundamental principles.[5]

Structure of the Conceptual Model

The overall structure of the Conceptual Model of Hybrid Threats is as follows.

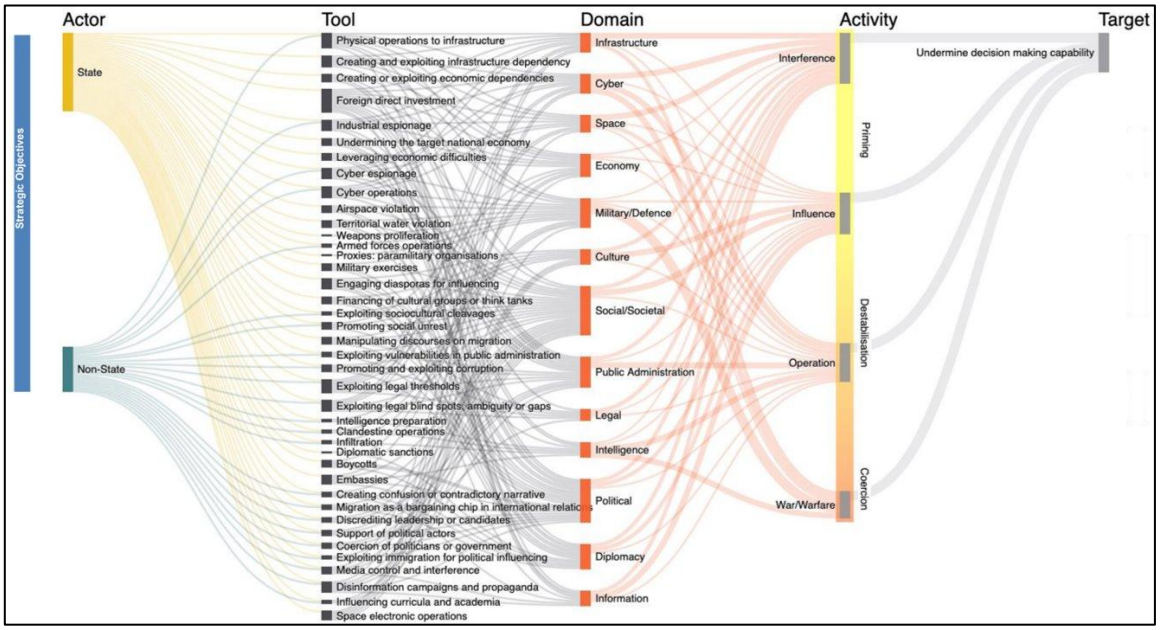

Figure 3: Structure of the Conceptual Model of Hybrid Threats

Source: European Commission, & Hybrid CoE, *The Landscape of Hybrid Threats: A Conceptual Model Public Version*, 2021, p. 13.

[5] Kawashima Takashi, "A Framework for Hybrid Threat Analysis: Through the Concept and Model of the European Centre for Hybrid Threat Countermeasures," NPI Commentary, 2022.

1. Overview of the Conceptual Model

The analytical framework of this Conceptual Model consists of the following four pillars:

(1)Actors

(2) Tools

(3) Domains

(4) Activities

Each of these elements will be outlined below.

2. Framework of the Conceptual Model

(1) Actors

Actors are classified into two categories: state actor and non-state actor. The term "state actor" primarily refers to authoritarian states that oppose the institutions and alliances representing democratic countries, such as the EU and NATO. A characteristic that these states have in common is that the objective of their regimes is to maintain domestic power, and they tend to exhibit mistrust toward democratic nations.[6] Specific examples include Russia, China, Iran, and North Korea, with Russia and China in particular regarded as principal actors in hybrid threats.[7]

The term "non-state actor," on the other hand, refer to entities that, while not belonging to the formal institutions of a state, have sufficient capacity to be involved in international relations and have the power to interfere, influence, and effect change. There are many cases in which states conduct harmful activities against other countries through non-state actors.[8] Representative examples include Hezbollah, ISIL, and private military companies (PMCs).[9] In responding to hybrid threats, it is important to both identify these state and non-state actors as well as to analyze the strategic objectives of the actors involved.[10]

(2) Tools

Tools refer to the means employed by state and non-state actors to exert hybrid threats against a target.[11] The Conceptual Model identifies 40 types of tools based on past cases which actors combine to construct hybrid threats.

---

[6] European Commission, & Hybrid CoE, The Landscape of Hybrid Threats: A Conceptual Model Public Version, 2021, pp. 16-18, https://www.hybridcoe.fi/wp content/uploads/2021/02/conceptual_framework reference-version-shortened good_cover_-_publication_office.pdf (Accessed May 1, 2022.)

[7] Ibid., p. 16.

[8] Ibid., p. 22.

[9] Ibid., p. 16.

[10] Ibid., p. 15.

[11] Ibid., p. 33.

(3) Domains

In Japan, the term *domain* is sometimes referred to as "*ryōiki*" (area) in the context of security; however, in this study, domain denotes a grouping of elements of national power that are treated as targets against which actors employ tools to launch hybrid threats.[12] Actors target domains to achieve their ultimate strategic objectives. As shown in Figure 4, in addition to the military/defense domain, thirteen groupings that constitute the political, economic, and social spheres—such as infrastructure and cyber—are listed as domains. Actors combine multiple tools, categorized under each domain in an attempt to achieve the objectives indicated at the center of the figure.

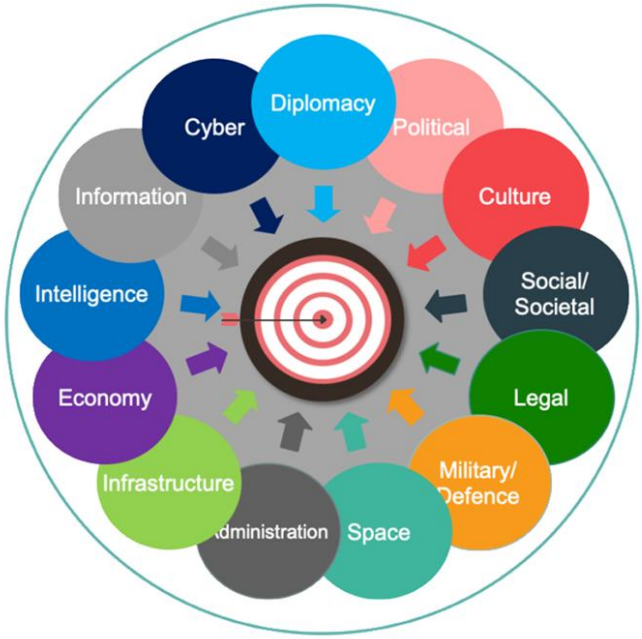

Figure 4: Conceptual Diagram of Domains and the Objectives of Actors
Source: European Commission, & Hybrid CoE, *The Landscape of Hybrid Threats: A Conceptual Model Public Version*, 2021, p. 27

In this Conceptual Model, the classification of domains does not follow a strictly theory-driven grouping; rather, it is acknowledged that the categories may require revision or adaptation depending on the specific case.[13]

Tools employed in hybrid threat activities and the domains affected

The tools that hostile actors can employ for achieving their objectives, as well as the domains potentially affected, are organized in Annex 1.

---

[12] Ibid., p. 26.
[13] Ibid., pp. 26-27.

Actors may use tools to influence one or more domains and may also target vulnerabilities within those domains. In addition to direct effects, their actions may produce "cascade effects" that spread to other domains.[14]

One point to note in Annex 1 is that the mere indication of the use of a particular tool does not necessarily mean that it constitutes a hybrid threat. For example, cyber operations may be conducted as part of a hybrid threat in coordination with other tools, or they may be carried out independently.[15] When a cyberattack by a hacker occurs, it is necessary to analyze its connection to an actor with strategic objectives and its linkage with other tools, and to anticipate at an early stage the overall impact arising from their combination.

(4) Relationship Between Phases and Activities

Activities conducted through the use of hybrid warfare tools vary in intensity according to the three phases: Priming Phase, Destabilization Phase, and Coercion Phase.[16] In this report, the relationship between each phase and the corresponding activities is organized in Annex 2.

The relationship between phases and activities in Annex 2 is not definitively fixed. In the Priming Phase, activities primarily take the form of disruption, with some elements of influence. In the Destabilization Phase, activities mainly involve influence, with some operational implementation. In the Coercion Phase, activities primarily consist of operational implementation. It is assumed that hybrid warfare is constructed in accordance with each phase by combining activities conducted through the use of various hybrid warfare tools. The details of each phase are explained below.

● Priming phase[17]

In this phase, the actor conducts "interference" against the target country through various activities using different hybrid warfare tools. The actor's ultimate goal is to cause the target country to lose situational awareness and to cause its top government leadership to make decisions voluntarily that are favorable to the actor.[18] The activity that follows "interference" is "exertion of influence."[19] Activities in this phase are ambiguous and inconspicuous, making it difficult to immediately recognize them as a hybrid threat.

● Destabilization phase[20]

In this phase, the actor intensifies activities using various hybrid warfare tools across all domains. These activities become overt, more aggressive, and often involve physical strikes or violence,

[14] Ibid., pp. 11-12.
[15] Ibid., pp. 32-33.
[16] Ibid., p. 10.
[17] Ibid., pp. 37-40.
[18] Ibid., p. 37.
[19] Ibid., p. 38.
[20] Ibid., pp. 40-41.

although the actor's own involvement tends to remain concealed.

For example, an armed conflict may occur, and reports of casualties, along with comments from bereaved families or injured soldiers, are disseminated (disruption). Subsequently, as reports of an increase in casualties and additional comments from families continue to spread, anxiety among soldiers' families rises (influence exertion). This anxiety then spreads throughout society, increasing distrust toward the government and leading to the incitement of demonstrations and similar actions. In the destabilization phase, the actor's goal is to disrupt the target country and destabilize it to a level where it can be easily coerced. If the desired effects are not achieved, the actor may return to the Priming Phase and adjust to a more effective combination of tools.

● **Coercion phase**[21]

In this phase, employment of multiple hybrid threats that include political and economic methods, destruction, information and disinformation dissemination, propaganda activities, covert operations by special forces, and military support to hostile forces in the target country are carried out in an effort to forcibly achieve strategic objectives against the target country.

All domains become potential targets of hybrid threats, and limited military means such as terrorism, sabotage, subversion, and guerrilla warfare may also be employed. Furthermore, if full-scale military war begins, each of these tools may be utilized to advance the military campaign advantageously.

While warfare during the Coercion Phase is listed here as part of the activities, the use of these tools in full-scale war is regarded as cross-domain operations within the context of military war and is therefore outside the scope of this study.

[21] Ibid., pp. 41-42.

Chapter 3: Analysis of Hybrid Warfare Methods and Case Studies

In this chapter, cases that include the potential use of operational methods are collected from publicly available information and classified and analyzed, based on the 40 tools identified in Chapter 2 (including Figure 3) as available to hostile actors to achieve their objectives.

1. Overview and Specific Examples of Operational Methods

The 13 tools are listed according to methods: infrastructure, economy, cyber, military, culture, society, administration, law, intelligence, diplomacy, politics, information, and technology. An overview of these 13 operational methods is provided in Annex 3, and specific examples are presented below.

(1) Infrastructure-related Operational Methods

Infrastructure forms the foundation of the daily lives and economic activities of the citizens. Therefore, when subjected to influence operations, the functioning of infrastructure may be halted or degraded, causing significant disruption to society.

In hybrid warfare, in particular, "operational methods related to infrastructure," when combined with other methods—such as the dissemination of disinformation through social media and mass media—can amplify public anxiety. As a result, the effects are not limited to the targeted infrastructure itself but can also spread across multiple domains, including the economy and society.

● Example of infrastructure attack-related operational method

When the submarine cable serving Taiwan's Matsu Islands was cut in February 2023, it disrupted not only telephone service but also internet banking and airline reservations. In Taiwan, more than 20 incidents of submarine cable cuts have been reported over the past five years.[22]

Submarine cables play a wide-ranging role not only in communications but also in the economy, finance, and national security. Around the world, roughly 500 major cables are laid, with a total length of about 1.5 million kilometers (equivalent to circling the Earth about 37 times).[23]

Cuts to submarine cables often occur in open waters where there are no witnesses, making it difficult to identify the vessel responsible. Even if a vessel can be identified, proving intent is difficult if the act was disguised as an accident, and, if the cutting occurs on the high seas, enforcement under

---

[22] Yomiuri Shimbun Online, 「*Kaitei keburu setsudan de denwaya netto shadan,Chugoku-sen kanyo ka…Taiwan honto de doyo no jitai kenen* "Undersea Cable Cut, Telephone and Internet Outages, Chinese Ships Possibly Involved... Concerns about Similar Incidents on Taiwan Island,"」 (Japanese) March 2, 2023, https://www.yomiuri.co.jp/world/20230302-OYT1T50368/ (Accessed September 19, 2025).

[23] METI Journal online「*Dēta no daidōmyaku" kaitei kēburu Nihon e no `shinrai' teko ni sekai shea kakudai mezasu* "Submarine Cables: The "Longest Artery of Data" - Aiming to Expand Global Market Share by Leveraging Trust in Japan"」 (Japanese) December 25, 2023 https://journal.meti.go.jp/p/40663/（Accessed on September 19, 2025）.

international law is also challenging.

Japan is connected by approximately 30 submarine cables, and it is said that the cutting of one or two would not have a major impact.[24] However, because the landing points for these cables are concentrated in specific areas, this concentration has become a vulnerability.

● **Example of creating and exploiting infrastructure dependency**

After Russia's annexation of Crimea in 2014, Ukrainian telecommunications companies withdrew from the Crimean Peninsula, and in 2017 the Ukrainian government halted the provision of internet connectivity services to the region.

Meanwhile, the Russian state-owned telecommunications company Rostelecom laid a communications cable connecting mainland Russia and the Crimean Peninsula, switching Crimea's internet connectivity to routes via Russia. As a result, residents of Crimea began accessing the internet through Rostelecom and became subject to censorship and surveillance by the Russian authorities.[25]

(2) Economy-related Operational Methods

Economy-related operational methods are methods that exert influence on an opponent's economy in order to significantly affect national decision-making and social functions. Particularly in hybrid warfare, when combined with information manipulation through fake news and social media, these tools of manipulation can incite public dissatisfaction and distrust toward the government, making them one of the extremely critical tools of hybrid warfare.

● **Example of economy-related operational method**

During Russia's invasion of Ukraine in 2022, about one-third of Europe's natural gas consumption relied on imports from Russia, most of which were supplied through pipelines connecting Russia and Europe.[26] This situation became a major issue in relation to sanctions imposed on Russia.[27]

In September 2022, Russia completely halted gas supplies to Europe via Nord Stream 1, citing pipeline repairs. Russia significantly reduced the volume of gas exported to Europe, and Western countries criticized Russia for using energy supplies as a weapon of war, although Russia has denied

---

[24] NHK「*Shirarezaru kaitei keburu no sekai* "The Untold World of Submarine Cables"」 (Japanese) June 20, 2023, https://www3.nhk.or.jp/news/html/20230620/k10014104331000.html (Accessed September 19, 2025).

[25] Asahi Shimbun GLOBE+, 「*Ukuraina kara Roshia ni kirikaerareta netto setsuzoku Kurimiahanto no ihen; Nihon kara kansoku* "Internet connection switched from Ukraine to Russia: Anomalies in the Crimean Peninsula observed from Japan"」 (Japanese) July 17, 2022, https://globe.asahi.com/article/14669860 (Accessed September 19, 2025).

[26] Nikkei Shimbun: 「*Nihonkeizaishinbun 'Roshia—Oshu-kan paipurain to wa Doku shohi-ryo no taihan izon* "What is the Russia-Europe pipeline? Germany relies heavily on it for most of its consumption"」 (Japanese) February 8, 2022, https://www.nikkei.com/article/DGXZQOUB0860Q0Y2A200C2000000/ (Accessed September 19, 2025.)

[27] Harada Daisuke, 「*Tairo sensai no genjo to mitoshi* "Current Status and Outlook of Sanctions Against Russia"」 Japan Institute of International Affairs, (Japanese) October 14, 2022, pp. 8-15, https://www.jiia.or.jp/topic-cdast/event/20221014-01.pdf (Accessed September 9, 2025).

this claim.[28]

As of 2025, the European Union (EU) regards excessive dependence on Russian energy as a security threat and is advancing efforts aimed at completely phasing out Russian energy.[29]

(3) Cyber-related Operational Methods

Cyber-related instruments of manipulation are characterized by the difficulty of determining whether the actors involved are states or non-state entities. State involvement is easy to deny, and the highly covert nature of the activities makes it difficult to determine when these influence operations actually began.

Particularly in hybrid warfare, cyberattacks are often used as part of complex operations coordinated with other instruments of manipulation, including economic, informational, and military methods, by disrupting communications through cyberattacks and exploiting the resultant confusion to conduct military operations among other means.

● **Example of cyber-related operational method**

During the 2022 Russian invasion of Ukraine, Russia carried out cyberattacks against Ukrainian government institutions, the military, media, and critical infrastructure even before the invasion began. These cyberattacks are believed to have been aimed at disrupting infrastructure facilities and secretly obtaining diplomatic and military information. However, it has been reported that they did not lead to large-scale damage because the Ukrainian government and companies such as Microsoft had taken countermeasures in advance.[30]

(4) Military-related Operational Methods

Military exercises and violations of airspace or territorial waters are used as means of applying psychological pressure on a target country's population and government by demonstrating one's own military power. In particular, exercises or military deployments near borders or in disputed areas may be conducted with the aim of generating anxiety in the opposing country and securing an advantage in diplomatic negotiations.

---

[28] BBC News Japan「*Roshia no gasu ote, Oshu e no kyokyu o 3-kakan teishi shuri no tame to* "Russian gas giant suspends supply to Europe for 3 days for repairs."」 (Japanese) https://www.bbc.com/japanese/62747358 (Accessed September 19, 2025).

[29] JETRO: 「*Oshu-I , Rosia-san enerugi kara no kanzen dakkyaku keikauo happyo, 2027 nenmatsu madeni gasu yunyu kinshi e*, "European Commission announces plan to completely phase out Russian energy, ban gas imports by end of 2027,"」 (Japanese) May 9, 2025. https://www.jetro.go.jp/biznews/2025/05/1e677dd0cec3e0c2.html （Accessed September 19, 2025）.

[30] Uchida Yasushi, 「*Ukuraina Shinko ni Manabu saiba kogeki, butsuri kogeki no mae ni juyo shisutemu funo-ka* "Cyberattacks: Lessons from the Invasion of Ukraine - Disabling Critical Systems Before Physical Attacks,"」 *Nikkei CrossTech,* (Japanese) September 15, 2022, https://xtech.nikkei.com/atcl/nxt/column/18/02438/091500018/ (Accessed September 19, 2025)

Especially in hybrid warfare, it is possible to amplify the effectiveness of such operations by combining multiple elements such as cyber, information, and legal methods. For example, cyberattacks may first paralyze information systems and disrupt military command structures and communications before military forces are deployed; propaganda and disinformation may be used alongside military exercises to manipulate public opinion in the target country and generate distrust toward its government; or ambiguities in international law may be exploited to justify military actions.

● **Example of military-related operational method**

On May 23–24, 2024, China conducted military exercises in the waters surrounding Taiwan. During these exercises, realistic computer graphics were used to simulate live-fire attacks that did not actually take place,[31] and Chinese-affiliated media reported that "young pilots in Taiwan's air force are seeking to resign due to fatigue," thereby manipulating information with the intent to generate anxiety among Taiwan's residents.[32] These methods are aimed at applying psychological pressure on Taiwanese society, spreading concerns about war among Taiwan's voters, and thereby weakening support for the Democratic Progressive Party (DPP) administration, with the objective of undermining the stability of Taiwan's governance and its will to defend itself.[33]

(5) Culture-related Operational Methods

Culture-related operational methods act directly on people's identities and values, and therefore can have long-term influence, such as generating support domestically and internationally, causing social division and confusion, shaping public opinion, and undermining identity. These methods are also characterized by being difficult to perceive and less likely to encounter resistance.

Particularly in hybrid warfare, cultural content such as films, music, and literature can be disseminated through media and social media to spread specific values or historical perspectives, thereby influencing the perceptions and identities of people in the target country.

● **Example of culture-related operational method**

Russia has claimed that the human rights of large numbers of ethnic Russians living in the Donbas region of eastern Ukraine are being violated and has carried out military intervention and political support activities while appealing to the international community that such actions are justified as humanitarian intervention.[34]

---

[31] Baidu Hundred Masters: "Taiwanese Grand Masters" Multi-Army Combination; Combination 3D Fictional Animation Painting Cloth" https://baijiahao.baidu.com/s?id=1799902122318826057 (Accessed September 9, 2019).

[32] Global Times, PLA drills shock 'Taiwan independence' secessionist forces, May 26, 2024, https://www.globaltimes.cn/page/202405/1313033.shtml (Accessed September 19, 2025).

[33] Iida Masashi, 「*Taiwan o kakomu Chugoku ni your gunji enshu—sono tokucho, nerai to kongo no tenbo,* "China's Military Exercises Surrounding Taiwan: Their Characteristics, Objectives, and Future Prospects"」 NIDS Commentary, No. 325, (Japanese) National Institute for Defense Studies, May 28, 2024, p. 4.

[34] President of Russia, "Address by the President of the Russian Federation," February 24, 2022,

In the "annexation" of the four eastern regions after 2022, referendums were held based on the purported "will" of Russian-speaking residents.[35] In territories occupied by Russia, Ukrainian-language education has been restricted while Russian-language education has been strengthened,[36] the content of textbooks has also been revised in line with Russia's historical narrative, and cultural assimilation among younger generations has been promoted.

(6) Society-related Operational Methods

Society-related operational methods weaken a state's governing capacity by inflaming existing social fissures such as ethnic conflict, economic inequality, and political dissatisfaction. In particular, in hybrid warfare, when combined with the manipulation of public opinion through fake news and social media, such methods can intensify social divisions and discontent, encouraging internal destabilization.

In democratic states, it is difficult to impose controls on speech due to the principle of freedom of expression, and public opinion and mass media have significant influence. As a result, such societies may be particularly vulnerable to information manipulation and psychological warfare.

● **Example of society-related operational method**

ISIL expanded its influence by exploiting sectarian conflicts following the Iraq War and the security vacuum created by the Syrian Civil War, and in 2014 it declared the establishment of a caliphate. It employed tactics combining terrorism, guerrilla warfare, and conventional military operations, while also recruiting young people through social media and spreading extremist ideology. Furthermore, it exploited sectarian and tribal rivalries to inflame social divisions and weaken the governing capacity of the state. By incorporating socially marginalized groups and those with grievances into its ranks and converting them into fighting forces, it created a structure that promoted not only military pressure from outside but also internal collapse from within.[37]

(7) Administration-related Operational Methods

Operational methods related to administration aim to reduce trust in government by inciting residents' anxiety and dissatisfaction toward administrative institutions. Activities are carried out that amplify

---

http://en.kremlin.ru/events/president/news/67843 (Accessed September 21, 2025.

[35] "Address by the President of the Russian Federation" President of Russia, September 21, 2022 (Russian) http://kremlin ru/events/president/news/69390 (Accessed September 21, 2025).

[36] Amnesty International Japan「*Ukuraina: Kodomo no shorai e no kogeki Roshia no shinko de seigen sareru gakko kyoiku*, "Ukraine: Attack on children's future - School education restricted by Russian invasion"」(Japanese) December 14, 2023, https://www.amnesty.or.jp/news/2023/1214_10208.html (Accessed September 21, 2025).

[37] Public Security Intelligence Agency「*Iraku /Revanto Isuramu kokuno taicho to kongo no tenbo* "Islamic State of Iraq and the Levant (ISIL) decline and future outlook"」(Japanese) https://www.moj.go.jp/psia/ITH/topic/topic_01.html (Accessed September 19, 2025)

concerns about the systems, personnel, and response capabilities of administrative bodies.

Corruption is considered a highly covert operation because it works to the advantage of the actor until it is exposed. Hybrid warfare in particular often involves cyberattacks on the systems of administrative institutions, disrupting them and disrupting the lives of residents and fueling public dissatisfaction.

Furthermore, because administrative responses to disasters and accidents directly affect the lives and property of residents, social media and other platforms are used to stimulate anxiety and dissatisfaction, thereby causing confusion within administrative institutions.

●Example of administration-related operational method

In April 2018, Jyan Hong-wei, Director General of the Department of Cyber Security at Taiwan's Executive Yuan, announced that Taiwanese government departments receive between 20 million and 40 million cyberattacks every month. In 2017, there were about 360 minor incidents, such as the defacement of government-affiliated websites, as well as 12 serious incidents, including the shutdown of critical systems and the leaking of documents. Approximately 80% of these attacks were attributed to China's "cyber units,"[38] and they are believed to be operations aimed at undermining Taiwanese residents' trust in government authorities.

(8) Law/legal-related Operational Methods

Operational methods related to law exercise influence in ways that appear legitimate by exploiting international law or the domestic laws of the opposing country, without the use of armed force. In democratic states, legal legitimacy forms the foundation of policy; therefore, attacks conducted through legal means are extremely effective in restricting actions, drawing criticism, and weakening the target.

In hybrid warfare in particular, legal claims may be disseminated through the media or social media to manipulate international public opinion, or economic sanctions and tariff measures may be implemented based on legal justifications. In this way, legal measures are often employed in combination with information and economic tools.

● Example of law/legal-related operational method

China claims almost the entire South China Sea as waters under its jurisdiction, describing them as "historic waters," a claim that lacks a basis in international law. This claim was rejected by a ruling issued in July 2016 by the Permanent Court of Arbitration (PCA) under the United Nations Convention on the Law of the Sea (UNCLOS). However, China has not complied with the ruling and has not withdrawn its claim.

---

[38] "Taiwanese government department encounters over 20 million cyberattacks every month, comprehensive attack, 80% believed to originate from mainland" Radio Free Asia, (Chinese) April 5, 2018, https://www.rfa.org/cantonese/news/htm/tw-web-04052018074556.html (Accessed September 19, 2025).

Another example is the *China Coast Guard Law* of the People's Republic of China, which came into effect in February 2021. This law contains provisions whose consistency with international law has been questioned, including ambiguous areas of application and authority regarding the use of weapons. Specifically, Article 22 states, "in cases of illegal infringement on sovereignty is committed by foreign organizations or individuals in the seas, all necessary measures, including the use of weapons, may be taken.[39] While this statement itself cannot necessarily be said to violate international law, even before the enforcement of the Coast Guard Law China had repeatedly taken hardline actions against vessels from neighboring countries in the South China Sea. Therefore, the enactment of the law can be seen not so much as the creation of new authority, but rather as a form of psychological warfare publicizing its hardline stance.

In this way, China attempts to make unilateral changes to the status quo by arbitrarily altering interpretations of international law and enacting domestic laws to achieve political objectives.

(9) Intelligence-related[40] Operational Methods

Operational methods related to intelligence are covert activities conducted to achieve a state's objectives. They are generally carried out in such a way that, even if discovered, the state can claim no involvement. This makes them extremely difficult to detect.

Compared with other activities, there are extremely few confirmed cases of this method, and it is believed that only a small number become publicly known. In hybrid warfare in particular, agents may be used to spread disinformation through local media and social media, thereby inciting dissatisfaction among local residents and reducing trust in the government or by supporting riots in cooperation with local groups. In addition, there are cases in which operatives gain access to critical facilities and plant malware on servers, in coordination with cyberattacks.

● Example of intelligence-related operational method

In Taiwan, in 2024, 64 people were indicted in espionage cases in which China's involvement was suspected. Of these, 43—about 70%—were active-duty or retired members of the Taiwan military.[41] It has been reported that departments such as the Chinese Communist Party's United Front organizations recruited or coerced Taiwan military personnel, in some cases attempting to obtain military secrets or acquire U.S.-made transport helicopters.[42]

---

[39] Article 22 of the Coast Guard Law of the People's Republic of China.

[40] In this report, the term "intelligence" is used not in the narrow sense of information analysis for decision-making, but in a broader sense that includes espionage activities and covert operations primarily conducted by intelligence agencies.

[41] National Security Bureau, R.O.C. "Analysis of the infiltration methods in the espionage case," pages 1-2. https://www.nsb.gov.tw/zh/assets/documents/%E6%96%B0%E8%81%9E%E7%A8%BF/ed8fddb8-3d99-4d3f-9414-c9b360f2df5a.pdf (Accessed September 9, 2025).

[42] Yomiuri Shimbun: 「*Taiwan ga Chūgoku kan'yo no supai saita no 64-ri kiso,-gun kankei-sha 7-wari… Nakadai tōitsu mezashi sesshoku kyōka* "Taiwan indicts 64 people, the highest number ever, for spies linked to China, 70% of whom are military personnel... Strengthening contacts with China in pursuit of unification"」

(10) Diplomacy-related Operational Methods

Operational methods related to diplomacy are a key means of exercising influence in the international community without using military force. Diplomacy, military power, and economic power function in coordination as the "three pillars" that support a state's international influence, making economic and military activities particularly compatible with in hybrid warfare.

For example, hybrid warfare operations may be combined with economic aid or military cooperation to influence the policies of another country. In addition, diplomats and government officials can also influence the formation of international public opinion by disseminating propaganda through the media in conjunction with information warfare.

●Example of diplomacy-related operational method

In recent years, the number of countries that have severed diplomatic relations with Taiwan and established diplomatic ties with China has increased, often with the aim of obtaining economic benefits or strengthening relations with China. China repeatedly asserts that "Taiwan is an inalienable part of China's territory," while requiring friendly countries to reaffirm the "One China" principle. In recent years, China has also begun to seek explicit support from friendly countries for the unification of Taiwan with China.[43]

In January 2017, Nauru recognized China as a state and consequently severed diplomatic relations with Taiwan, reducing the number of countries and entities maintaining diplomatic relations with Taiwan to 12.[44]

(11) Politics-related Operational Methods

Operational methods related to politics target politically-involved individuals and therefore have the potential to significantly influence a state's direction. At the same time, signs of such activities are difficult to detect, and there are very few cases in publicly available information that have been identified as political operations conducted by foreign actors. This is likely due not only to the high level of secrecy surrounding these activities, but also to the possibility that even when government agencies are aware of them to some extent, there are circumstances that prevent them from making such information public.

In hybrid warfare in particular, activities are conducted in combination with information

---

(Japanese) January 15, 2025 https://www.yomiuri.co.jp/world/20250115-OYT1T50020/ (Accessed September 19, 2025).

[43] Fukuda Madoka,「*Hitotsuno Chugoku gensoku no yukue* "The Future of the 'One China' Principle"」 Sakura Japan Foundation, (Japanese) May 31, 2025. http://www.sief.jp/21/2025/0531bundai.pdf (Accessed September 9, 20215).

[44] Ministry of Foreign Affairs of Japan「*Taiwan kiso deta* "Basic data on Taiwan"」(Japanese) https://www.mofa.go.jp/mofaj/area/taiwan/data.html Accessed September 19, 2025).

manipulation, including disseminating information favorable to supported politicians and spreading fake news about opposing candidates.

● **Example of politics-related operational method**

In December 2024, it was revealed that Chinese authorities had supported travel to China for several hundred Taiwan politicians ahead of Taiwan's presidential and legislative elections held in January 2024.

Under Taiwan law, receiving funding from "external hostile forces," including China, during election campaigns is prohibited. According to information provided by Taiwan officials to Reuters, security agencies investigated more than 400 cases of visits to China over the previous month, many of which involved local opinion leaders such as village chiefs. It is reported that subsidies for accommodation, transportation, and meal expenses for these visits were paid by organizations under the Taiwan Affairs Office of the PRC State Council.[45]

(12) Information-related Operational Methods

Operational methods related to information influence people's thinking, judgment, and values themselves, and therefore constitute one of the key means of undermining decision-making and social stability in a target country. Through social media and video-sharing platforms, it is possible to disseminate disinformation and biased narratives and manipulate public opinion through emotionally appealing content.

In recent years, fake videos and audio generated by generative AI have advanced to a level that makes them difficult to distinguish from authentic content, increasing their effectiveness as tools for influence perceptions. In democratic states, where there is a broad space for free expression, such disinformation can spread easily, and verifying its authenticity often requires a considerable amount of time.

In hybrid warfare in particular, the following types of combined methods are employed:

- Simultaneously conducting DDoS attacks on or defacing the websites of government institutions and media organizations while spreading disinformation on social media to amplify confusion.
- Disseminating propaganda portraying military exercises or troop deployments as "defensive measures."
- Implementing economic sanctions or export restrictions while internationally portraying the narrative that the opposing country's policies are the cause.

---

[45] Yimou Lee「*Chugoku tokyoku, Taiwan seijika suhyaku-ri no ryoko shien soto-sen nado hikae* "Chinese authorities provide travel support for hundreds of Taiwanese politicians ahead of presidential election, etc."」(Japanese) Newsweek Japan, Reuters, December 1, 2023 https://www.newsweekjapan.jp/headlines/world/2023/12/475397.php (Accessed September 19, 2025).

In this way, operational methods related to information have a high degree of compatibility with other methods and serve to amplify their influence.

● **Example of information-related operational method**

In March 2022, the European Union enacted legislation to completely ban the provision within the EU of five Europe-focused channels of the Russian state television network RT as well as the state-run radio and news website Sputnik in order to prevent propaganda spreading disinformation related to Russia's aggression against Ukraine. This measure was taken after RT and Sputnik were judged to have been disseminating disinformation and being used by President Vladimir Putin to destabilize Western countries.[46]

(13) Technology-related Operational Methods

Among operational methods related to technology, interference with Global Navigation Satellite Systems (GNSS) can have particularly serious effects. GNSS jamming renders receivers unable to determine their position by overpowering legitimate signals with strong radio transmissions. In contrast, GNSS spoofing transmits false signals that are stronger than the authentic ones, thereby misleading receivers into calculating incorrect positions or times.

Such attacks may have the following impacts on social infrastructure:

- Deviation of maritime vessels from their intended routes
- Misguidance of aircraft
- Time-synchronization errors in financial systems

In hybrid warfare in particular, combining GNSS spoofing with cyberattacks can disrupt the guidance of drones and missiles, cause disorder in logistics, and damage financial systems. In addition, by combining traffic disruptions caused by GNSS interference with the spread of disinformation, it is possible to generate social unrest and reduce public trust in the government.

● **Example of GNSS interference-related operational method**

In June 2017, in the vicinity of the Black Sea, an incident occurred in which more than 20 vessels displayed incorrect position information due to "spoofed" GPS signals.[47]

It has also been reported that Russia has repeatedly deployed the R-330Zh Zhitel electronic warfare system, a cellular jamming and direction finding system that possesses GPS spoofing capabilities, in the Donbas region where fighting continues, to interfere with drones operated by the

---

[46] Council of the European Union, "EU imposes sanctions on state-owned outlets RT/Russia Today and Sputnik's broadcasting in the EU," Council of the European Union, March 2, 2022, https://www.consilium.europa.eu/en/press/press-releases/2022/03/02/eu-imposes-sanctions-on-state-owned-outlets-rtrussia-today-and-sputnik-s-broadcasting-in-the-eu/ Accessed September 21, 2025.

[47] Dana Goward, "Mass GPS Spoofing Attack in Black Sea?" The Maritime Executive, July 11, 2017, https://maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea (Accessed September 21, 2025).

Ukrainian military and the Organization for Security and Co-operation in Europe (OSCE). Since 2019, such interference activities have reportedly increased.[48]

These cases suggest that interference activities targeting GNSS are becoming increasingly sophisticated and large-scale. Furthermore, with future advances in science and technology, it will be necessary to remain vigilant about the possibility that various advanced technologies—such as quantum engineering and biotechnology—may also be used as operational tools.

(14) Other Operational Methods

In the Maritime Security Study Group "election interference" is understood as a phenomenon in which the operational methods analyzed in items 1–13 act in combination. However, in this report, election interference has been intentionally presented as an independent category as a method that should receive focused attention in the future. In addition, the "impact of generative AI" has also been organized as an additional item, as it is judged to have the potential to exert cross-cutting and serious effects on existing operational methods.

Election Interference

Election interference refers to influencing voting behavior by guiding public opinion through employing dissemination of disinformation and propaganda with the intention to generate anxiety and anger among voters. Specifically, the following methods are employed:

- Circulation of scandals or fake news intended to damage the credibility of candidates
- Providing financial support to particular candidates or political parties (support for political actors)
- Manipulation of vote tabulation through cyberattacks

Because it is carried out through the combination of multiple methods, election interference can be considered a typical form of hybrid warfare.

● Example of election interference

According to the investigative report by U.S. Department of Justice Special Counsel Robert S. Mueller III, large-scale and systematic interference by the Russian government in the 2016 U.S. presidential election was identified.

Russia's Main Intelligence Directorate of the General Staff (GRU) hacked emails belonging to the Democratic National Committee (DNC) and Hillary Clinton's campaign, and the stolen information was released through outlets such as "DCLeaks," "Guccifer 2.0," and "WikiLeaks." In addition, Russia's Internet Research Agency (IRA) disseminated large amounts of disinformation and divisive content on social media. Using Facebook advertisements, it targeted audiences according to specific racial, regional, and political characteristics. Furthermore, it is reported that the IRA was

[48] "Russian GPS-Jamming Systems Return to Ukraine" *Medium*, May 5, 2019, https://dfrlab.org/2019/05/23/russian-gps-jamming-systems-return-to-ukraine/ (Accessed September 21, 2025).

involved in both promoting support for Trump as well as activities related to anti-Trump movements (e.g., Black Lives Matter (BLM)), thereby inflaming divisions within the United States.[49]

Impact of generative AI

Compared with conventional information-processing technologies, generative AI has achieved significant advances in terms of speed, scale, accuracy, and personalization; therefore, it has the potential to greatly influence the increasing sophistication of hybrid warfare. The following outlines its specific impacts:

- Through the use of generative AI, malware and similar tools can be created more easily, leading to increasingly sophisticated and large-scale cyberattacks.
- Because text, images, audio, and video can be generated instantly, the spread of disinformation and propaganda is accelerating, causing an information flood on social media and other platforms. As a result, determining the authenticity of information becomes even more difficult.
- Messages optimized for individual users based on their attributes and interests can be generated and distributed, allowing operators to penetrate deeply into their targets' psychology and therefore encourage behavioral change.
- With LLMs, it has become possible to engage in dialogue using natural language similar to that of humans, making them more likely to be mistaken for reliable sources of information and enabling intentional persuasion through convincing narratives and logical arguments.
- Efforts are increasing to publish large volumes of information and commentary online that favor a particular country, with the aim of introducing bias during the training process of LLMs.
- Content generated by generative AI is difficult to distinguish from that produced by humans, and the disappearance of language barriers is making it increasingly difficult to identify the origin of such communications.
- By imitating human cognitive frameworks, generative AI can influence the formation of values and beliefs.

2. Results of the Case Analysis

The cases collected in this study were compiled into a database, and an analysis was conducted to identify trends for each type of hybrid warfare operational method. Although the number of cases remains limited and does not provide comprehensive coverage, the analysis offers useful insights into initial trends.

The results of the analysis of the cases, organized by characteristics, frequency, and scope of impact for each operational method, are presented in Annex 4. As additional cases are accumulated

---

[49] Kawaguchi Takahisa, 「*Roshia ni your seiji kainyu-gata no saiba katsudo – 2016-nen amerikadaitoryo senkyo kainyu no shudo to ito* "Russia's Political Interference-Type Cyber Activities: Methods and Intentions of Interference in the 2016 US Presidential Election」 (Japanese) Sasakawa Peace Foundation, International Information Network Analysis IINA. https://www.spf.org/iina/articles/kawaguchi_01.html (Accessed September 19, 2025).

and the analysis is further developed, more refined trend analysis is expected to become possible.

Chapter 4: China's Hybrid Warfare for the Forced Unification of Taiwan

1. The Coaxing Approach and the Hardline Approach

The hybrid warfare that forms the core of Patterns 1 to 3 presented in Chapter 1, Section 2 appears to occupy a similar position in each case. Therefore, it can be broadly divided into two categories: a "Coaxing Approach" and a "Hardline Approach." These two categories are adopted as the basic premise of this study based on their inferred objectives and characteristics.

Coaxing Approach

The approach that aims to promote pro-China sentiment in Taiwan, suppress anti-China forces, and establish a government that moves toward unification with the mainland is the definition of the "Coaxing Approach" in this report.

To achieve the above objectives, China would strengthen the functions that sustain Taiwan, especially in the economic sphere, by increasing Taiwan's dependence on China, in order to create a situation in which Taiwan cannot function without China. At the same time, China would work to secure international acceptance of Taiwan as part of China, thereby guiding Taiwan as a whole in a pro-China direction.

For this approach to succeed, it would likely require that China's economy remain strong, even as economic relations between China and Japan, the United States, and their partner countries continue to trend toward separation. On that basis, China would also conduct hybrid warfare against those countries in order to cause deterioration in their relations with Taiwan.

Hardline Approach

The approach that seeks to provoke internal conflict within Taiwan, creating a state of civil unrest, and then, amid that confusion, establish a government that moves toward unification with the mainland is the definition of the "Hardline Approach" in this report. To achieve the above objectives, China would work to isolate Taiwan within the international community while using various means to create political, economic, and social disruption in Taiwan. This kind of activity would intentionally produce an extremely unstable political situation. If necessary, at Taiwan's request, China would not hesitate to send security forces or the military, thereby achieving de facto unification.

At the same time, China would conduct hybrid warfare against Japan and the United States in parallel in order to drive a wedge between them, making it difficult for the United States to intervene even if Taiwan were to fall into civil unrest. In order to create division between Japan and the United States, China may adopt a Hardline Approach against the United States while pursuing a Coaxing Approach toward Japan, given the current state of U.S.–China relations.

In practice, China is unlikely to rely solely on either the Coaxing Approach or the Hardline Approach; rather, it is likely to shift between the two depending on circumstances.

For example, if public opinion in Taiwan becomes strongly negative against China and the Coaxing Approach does not function effectively, China may shift to the Hardline Approach. However, if the situation later becomes favorable for China, it may return to the Coaxing Approach.

Below, the Coaxing Approach (left blue box) and the Hardline Approach (right red box) are compared and examined for each phase of hybrid warfare (Table 1).

After that, the details of each approach are described in greater detail using specific examples (Tools).

Table 1: Hybrid Warfare Directed at Taiwan in Each Phase of the Coaxing and Hardline Approaches

Coaxing Approach	Hardline Approach
【Priming Phase】	**【Priming Phase】**
Taiwan / Coaxing / Priming	Taiwan / Hardline / Priming
TCP1: Intelligence activities (operations)	THP1: Intelligence activities (operations)
TCP2: Inviting pro-China politicians	THP2: Intimidation of politicians and erosion of trust
TCP3: Pro-China initiatives	THP3: Political and social division
TCP4: Disruption of Taiwan's diplomatic activities	・Division between pro-unification and pro-independence factions, etc.
TCP5：Strengthening economic interdependence with Taiwan	THP4: Prevention from joining international organizations
・Economic carrot and stick	THP5: Disruption of Taiwan's economic activities
・Dependence on infrastructure	THP6: Military intimidation (high intensity)
TCP6: Military intimidation (low intensity)	Military exercises, airspace violations
TCP7: Undermining trust between Japan and the United States	**【Destabilization Phase】**
【Destabilization Phase】	Taiwan / Hardline / Destabilization
Taiwan / Coaxing / Destabilization	THD1: Generating distrust in Taiwan's administrative capabilities
TCD1: Anti-China forces lose credibility	・Disruption of civilian ship navigation.
TCD2: Promoting importance of cooperation with China	THD2: Instigating social unrest and anxiety about war
・Promoting a "peace framework"	・Disruption of banking and medical services, stirring up a crisis
・Cooperating to strengthen economic ties	THD3: Disruption of Taiwan-U.S.-Japan cooperation
TCD3: Generating distrust of the United States	・Severing of submarine cables, etc.
【Coercion Phase】	**【Coercion Phase】**
Taiwan / Coaxing / Coercion	
TCC1：Strengthening ties with China	
TCC2: China's control of Taiwan's information space	

TCC3: Open and covert interference in elections

TCC4: Establishment of an authority that advocates unification

Taiwan / Hardline / Coercion

THC1: Disruption of social and economic activities

- Interference with critical infrastructure
- Disruption of economic activities due to military exercises
- Disruption of economic activities

THC2：Isolation of Taiwan's information dissemination

- Disruption of communication networks

THC3：Instigating civil war

THC4：Limited military intervention

- Military intervention in civil wars
- Missile launch on islands

Source: Maritime Security Study Group, Nakasone Peace Institute

2. Coaxing Approach Toward Taiwan

The outline of the hybrid warfare that China would carry out against Taiwan in each phase of the Coaxing Approach is as follows (details are shown in Annex 5).

(1) Priming Phase

In the Priming Phase, China would conduct intelligence activities, cultivate pro-China politicians in Taiwan, co-opt figures from Taiwan's pro-China camp, obstruct Taiwan's diplomatic activities, strengthen economic interdependence with Taiwan, carry out low-intensity military intimidation, and generate distrust toward Japan and the United States.

To promote pro-China sentiment in Taiwan, China would undertake political operations aimed at cultivating Taiwan's leadership and citizens, exercise media control, and provide financial support to cultural organizations and think tanks in order to generate pro-China public opinion within Taiwan.

In addition, depending on the degree of pro-China orientation of Taiwan's government, China would carry out relatively low-intensity military intimidation. At the same time, it would disseminate China-favorable narratives and disinformation intended to weaken Taiwan's trust in Japan and the United States by making such claims as "Japan is hesitant to support Taiwan" and "the United States will not help Taiwan."

(2) Destabilization Phase

In the Destabilization Phase, China would carry out activities such as discrediting anti-China forces, promoting the importance of cooperation with China, and generating distrust toward the United States.

Through the spread of disinformation, narratives, and propaganda, including activities in cyberspace using bots, as well as the occurrence of riots or assassinations staged to appear as actions

by anti-China groups, China would attempt to politically isolate anti-China forces from the general public in Taiwan.

At the diplomatic level, China would also seek to draw Taiwan closer by promoting a "peace framework" that emphasizes greater autonomy than the "one country, two systems" model. At the same time, by spreading disinformation and propaganda, China would generate distrust toward the United States in Taiwan, encouraging Taiwan to distance itself from the United States and therefore to become diplomatically isolated.

(3) Coercion Phase

In the Coercion Phase, China would carry out various influence and operational activities across the political, economic, and social domains, including actions in the information space.

By establishing economic frameworks between China and a pro-China government in Taiwan, China would increase Taiwan's economic dependence on China. At the same time, it would seek to dominate the information space—through control of Taiwan's internet environment and influence over Taiwan's media through acquisitions and other means—in order to support the establishment of a pro-China government and suppress anti-China discourse.

Further, China would interfere in Taiwan's elections by using bots on social media and spreading disinformation, including such claims as that Taiwan would immediately enter a state of war if anti-China forces came to power.

Furthermore, through financial support to pro-China groups in Taiwan, assistance to strengthen police capabilities to suppress anti-China forces, and support for legislation by a pro-China government aimed at cracking down on anti-China elements, China would work to establish and maintain a pro-China government. Through cooperation in the suppression of anti-China forces and violently suppressing opposition, China would ultimately secure a decision in favor of unification.

3. Hardline Approach Against Taiwan

The following outlines the hybrid warfare that China would employ against Taiwan in each phase of the Hardline Approach (details are shown in Annex 6).

(1) Priming Phase

In the Priming Phase, China would conduct intelligence activities, intimidate politicians and undermine their credibility, deepen political and social divisions, organize boycotts from international organizations, obstruct Taiwan's economic activities, and carry out high-intensity military intimidation.

To provoke conflict within Taiwan, China would attempt to divide the government and the public by discrediting politicians and interfering illegally in elections. It would also use media to exploit existing social and cultural fissures within Taiwan such as religious ties with the mainland and tensions between mainlanders and native Taiwanese in order to deepen political and social divisions.

In addition, China would obstruct Taiwan's diplomacy with countries friendly to Taiwan and

hinder Taiwan's diplomatic and economic activities in the international community by organizing boycotts intended to exclude Taiwan from international organizations and international events.

Furthermore, China would generate fears of war through military exercises around Taiwan, long-range missile test launches, and activities crossing the median line by assets belonging to the Chinese military and other official sectors, as well as by China's maritime militia.

(2) Destabilization Phase

In the Destabilization Phase, China would carry out activities such as generating distrust in the administrative capacity of the Taiwanese government, heightening social unrest and fears of war, and obstructing cooperation among Taiwan, the United States, and Japan.

By interfering with the navigation of Taiwanese vessels around the islands of Kinmen and Matsu, and conducting drone flights overhead, China would force the Taiwanese government to respond under heightened tension. This would place additional strain on its administrative capacity and increase public distrust toward the government within Taiwan.

China would also conduct cyberattacks against critical infrastructure—including banks, medical institutions, and transportation, energy, and water systems—as well as attacks involving physical destruction, such as the cutting of submarine cables. These actions would aim to stir social unrest and disrupt coordination with the United States, Japan, and other partners.

Furthermore, China would intensify fears of war by spreading disinformation designed to create a sense of crisis, such as claims that Taiwanese officials are preparing personal escape plans, and by carrying out higher-intensity military activities, including missile launch exercises in waters around Taiwan.

(3) Coercion Phase

In the Coercion Phase, China would carry out actions aimed at disrupting social and economic activities, isolating Taiwan's information output, engineering civil unrest, and conducting limited military intervention. China would continue attacks on Taiwan's economic, social, and communications infrastructure, including physical destruction. At the same time, it would more forcefully obstruct Taiwan's economic activities by using military assets, such as conducting joint China–Russia exercises in waters connected to Taiwan and implementing a close blockade around Taiping Island. China would also isolate Taiwan's information output by cutting submarine cables, destroying cable landing stations, launching cyberattacks on data centers and communication networks, and conducting electronic interference against satellite communications. On that basis, China would create a state of civil unrest within Taiwan, including an armed uprising by pro-China proxy forces. Using requests from pro-China groups as a pretext, China would then carry out military intervention, including the deployment of forces to Taiwan.

Chapter 5: Hybrid Warfare Against Japan in the Event of the Forced Unification of Taiwan

1. Overview

Based primarily on the premise of hybrid warfare directed at Taiwan, hybrid warfare against Japan is broadly divided into two categories: "Attempt to Decouple Japan and Taiwan" (Coaxing Approach; left blue box) and "Attempt to Decouple Japan and the U.S." (Hardline Approach; right red box), and their overall characteristics are compared (Table 2).

Table 2: Hybrid Warfare Directed at Japan in Each Phase of the Coaxing and Hardline Approaches

Coaxing Approach	Hardline Approach
【Priming Phase】 Japan / Coaxing / Priming JCP1: Intelligence activities JCP2: Taiwan issue is touted as an internal matter JCP3: Hardline operations against Japan, including the economy ・Strengthening China's dominance in the Asian economy JCP4: Intimidation through military exercises near the Nansei Islands JCP5: Communicating the narrative of unity between China, Taiwan, and Okinawa	**【Priming Phase】** Japan / Hardline / Priming JHP1: Intelligence activities JHP2: Interference in Japan's security policy JHP3: Hardline operations against the U.S. and coaxing operations toward Japan JHP4: Military exercises in the waters around Japan JHP5: Division of public opinion over Okinawa ・ Generating distrust and anxiety toward the U.S. military
【Destabilization Phase】 Japan / Coaxing / Destabilization JCD2: Operations to hinder strengthened Japan-Taiwan cooperation ・Excluding Japan and the U.S. from Taiwan's economy ・Appealing for stronger economic cooperation with China JCD3: Obstruction of communication between Japan and Taiwan	**【Destabilization Phase】** Japan / Hardline / Destabilization JHD1: Generating distrust in the government's administrative capabilities ・ Social anxiety due to limited social functioning, leading to distrust of the government ・ Generating distrust of the government regarding protection of civilian vessels JHD2: Risk to the Japan-U.S. Alliance ・ Strengthening Japan-China economic relations ・ Risk of Japan getting involved in a war ・ Risk of U.S.-China conflict JHD3: Obstruction of communication between Japan and the U.S.
【Coercion Phase】 Japan / Coaxing / Coercion JCC1: Divisive operations against Japan and Taiwan's democratization forces ・Disinformation that "Taiwan is democratically moving toward unification" ・Scandal disinformation about anti-China forces ・Economic benefits on the condition of recognition of unification as a fact.	**【Coercion Phase】** Japan / Hardline / Coercion JHC1: Divisive operations against Japan and the U.S. ・Interference with sensitive information exchange between Japan and the U.S. ・Interference with the operational capabilities of the Japan Self-Defense Forces and U.S. military bases in Japan

JCC2：Forming public opinion in favor of unification ・Disinformation that international opinion largely supports unification	・Generating anxiety among residents living near bases JHC2：Building public opinion for non-intervention in Taiwan ・Disinformation that “the unification faction has an overwhelming advantage in Taiwan” JHC3: Delaying the recognition of an “Important Influence Situation,” etc.

Source: Maritime Security Study Group, Nakasone Peace Institute

2. Directed at Japan: Decouple Japan–Taiwan Relations through Employment of the Coaxing Approach Toward Taiwan

In employment of the Coaxing Approach toward Taiwan, the primary objective of China’s hybrid warfare against Japan is to drive a wedge between Japan and Taiwan. The outline of the hybrid warfare that China would conduct against Japan in each phase is as follows (details are provided in Annex 7).

(1) Priming Phase

In the Priming Phase, China would conduct intelligence activities, weaken anti-China forces while cultivating pro-China elements, implement hardline measures against Japan including economic pressure, carry out military exercises near the Nansei Islands to intimidate, and disseminate narratives emphasizing the historical unity of China, Taiwan, and Okinawa. To drive a wedge between Japan and Taiwan, China would conduct various intelligence activities—including cyber operations and espionage—to divide Japan and Taiwan and gather information on vulnerabilities in Japan’s critical infrastructure. In addition, China would infiltrate government and public institutions, economic organizations, and other bodies to recruit collaborators.

In the diplomatic and economic spheres, China would adopt hardline actions against Japan, disrupt Japan’s economic relations with other Asian countries, take a strong stance on the release of treated water from the Fukushima Daiichi nuclear plant, and escalate tensions in the Senkaku Islands, including involving Taiwan. Furthermore, China would carry out military intimidation through exercises near the Nansei Islands and disseminate narratives emphasizing the historical unity of China, Taiwan, and Okinawa.

(2) Destabilization Phase

In the Destabilization Phase, China would carry out operations to obstruct closer Japan–Taiwan cooperation and disrupt communication between Japan and Taiwan. It would exert increased pressure on Taiwan and Japan/U.S. businesses and impose broad restrictions on Taiwan’s multinational companies, effectively excluding Japan and the United States from Taiwan’s economic sphere. In addition, China would disrupt Japan–Taiwan communication through actions such as cutting submarine cables through the use of fishing boats, escalating tensions in the Senkaku Islands,

particularly in response to Japan's maritime security actions, provoking anti-Japanese sentiment within Taiwan, and spreading disinformation suggesting that Taiwan has no expectations of Japan.

(3) Coercion Phase

In the Coercion Phase, China would work to divide Japan from pro-democracy forces in Taiwan and influence public opinion within Japan to favor unification. Through a variety of methods—including cyber operations using bots on social media—it would spread disinformation such as "Taiwan is moving toward unification democratically" and "the international community largely accepts unification." China would also adopt economic coercion against Japan, such as threatening or implementing economic sanctions if Japan refuses to recognize the *fait accompli* of unification.

3. Directed at Japan: Decouple Japan-Taiwan Relations through Employment of the Hardline Approach Against Taiwan

Based primarily on the hardline approach against Taiwan, the primary objective of China's hybrid warfare against Japan is to drive a wedge between Japan and the United States. The outline of the hybrid warfare that China would conduct against Japan in each phase is as follows (details are provided in Annex 8).

(1) Priming Phase

In the Priming Phase, China would conduct intelligence activities, interfere in Japan's security policy, pursue appeasement tactics toward Japan while maintaining a hardline stance against the United States, carry out military exercises in waters around Japan, and deepen divisions in public opinion regarding Okinawa.

Through various intelligence activities—including cyber espionage—China would collect information on vulnerabilities related to the Japan Self-Defense Forces (JSDF), U.S. forces stationed in Japan, and critical infrastructure within Japan. It would also infiltrate personnel into government and other public institutions, economic organizations, and similar bodies, while seeking to recruit collaborators.

In the diplomatic and economic spheres, China would attempt to court Japan by offering economic incentives and softening its stance on issues such as the Senkaku Islands. At the same time, China would reduce the frequency of exercises around Japan that pose a direct threat to Japan while conducting provocative exercises targeting U.S. forces, thereby fostering a sense of unease among the Japanese public.

Furthermore, China would disseminate narratives and disinformation related to U.S. actions—such as claims that the Japan–U.S. alliance does not contribute to Japan's security but instead increases the risk of being drawn into war, and that the United States would not intervene in a China–Taiwan conflict. It would also encourage distrust and anxiety against U.S. forces by spreading biased or false information about crimes committed by U.S. military personnel in Okinawa. In addition,

China would attempt to undermine trust in both the Japanese and U.S. governments by promoting narratives about historical connections between China and Okinawa and by spreading narratives related to the Battle of Okinawa.

(2) Destabilization Phase

In the Destabilization Phase, China would carry out activities aimed at generating distrust in the Japanese government's administrative capacity, highlighting the risks of the Japan–U.S. alliance, and disrupting communication between Japan and the United States.

Using tactics such as cyber operations that cause system failures in banks and hospitals, the intrusion of large numbers of Chinese fishing boats into Japan's EEZ, and the exploitation of ambiguity between law enforcement and military activities, China would seek to undermine confidence in the Japanese government's administrative capabilities.

At the same time, while offering economic advantages to Japan, China would emphasize the risks of a U.S.–China conflict and the possibility of Japan being drawn into war. This would be done through military activities such as exercises simulating missile and air attacks on U.S. bases and missile launch exercises that extend beyond the Second Island Chain, thereby shaping public opinion in Japan to view the Japan–U.S. alliance as a risk.

In addition, China would disrupt information sharing between Japan and the United States by cutting submarine cables using fishing boats and similar methods.

(3) Coercion Phase

In the Coercion Phase, China would conduct operations to divide Japan and the United States, shape public opinion in Japan in favor of non-intervention in a Taiwan contingency, and obstruct the recognition of situations such as an "Important Influence Situation."

Through methods such as electronic warfare and cyberattacks, China would disrupt communications through submarine cables and satellite networks, thereby hindering information sharing between Japan and the United States. It would also attack critical infrastructure within Japan—such as electricity, gas, and water systems—thereby reducing the operational capabilities of the JSDF and U.S. forces stationed in Japan, which depend on these systems.

Furthermore, China would spread disinformation—such as claims that "pro-unification forces overwhelmingly dominate in Taiwan"—to shape public opinion in Japan in favor of non-intervention in a Taiwan contingency. It would also attempt to obstruct the Japanese government's recognition of situations such as an "Important Influence Situation" by promoting propaganda claiming that such a recognition would constitute an act of war against China.

4. Hybrid Methods China could Employ Against Japan

The results of the analysis of the various hybrid methods that China could employ against Japan, and the Japanese domains that they would target, are presented in Annex 9.

Chapter 6: Hybrid Warfare Against the United States and Other Countries

1. Hybrid Warfare Against the United States

The Case of a Coaxing Approach Toward Taiwan

If China adopts a Coaxing Approach toward Taiwan, the primary aim of its hybrid warfare against the United States would likely be to portray Taiwan as increasingly pro-China, thereby developing distrust toward Taiwan and diminishing U.S. willingness to support it.

To achieve this aim, China would likely employ various hybrid methods with the following objectives.

- Generate distrust within the United States of Taiwan authorities' suppression of anti-China forces and residents who are becoming increasingly pro-China.
- Incite debate within the United States over whether U.S. involvement is necessary in a unification process that does not involve the use of force.
- Compel responses based on the assumption of China–Taiwan economic integration, using both economic incentives and coercion.
- Disrupt communication between the United States and Taiwan (through physical disruption of communications, information manipulation, etc.).

The Case of a Hardline Approach Against Taiwan

If China adopts a strategy based on the Hardline Approach against Taiwan, the primary objective of its hybrid warfare against the United States is likely to be to prevent the United States from intervening in a situation of civil unrest in Taiwan. To achieve this, China would likely employ various hybrid means with the following objectives:

- Increase distrust against Taiwan and reduce support for it within the United States.
- Heighten anxiety within the United States regarding the risks of war, including not only military risks but also economic risks.
- Encourage international and domestic U.S. public opinion that the principle of non-interference in internal affairs should apply to the Taiwan issue.
- Increase distrust and dissatisfaction against Japan, particularly by amplifying uncertainty regarding the use of U.S. military bases in Japan.
- Disrupt communication between Japan and the United States (through physical disruption of communications, information manipulation, etc.).
- Undermine U.S.–Philippines cooperation, particularly by increasing uncertainty regarding the use of bases in the Philippines.

2. Hybrid Warfare Against Other Relevant Countries

If China adopts a strategy based on the Coaxing Approach toward Taiwan, it would likely conduct efforts to internationally legitimize China–Taiwan unification and to build a majority of countries that support it.

Therefore, under either approach, China would likely employ various hybrid methods, such as information manipulation, the dissemination of narratives, economic inducements (using both incentives and coercion), and the use of international organizations (such as joint membership arrangements involving China and Taiwan).

In addition, if China adopts a strategy based on the Hardline Approach, it would likely seek to shape international opinion that even if civil unrest occurs in Taiwan, it is an internal matter of China and that other countries—including the United States—should not intervene.

Specifically, by employing the various hybrid warfare methods described above against target countries, China would seek to undermine multilateral cooperation to achieve the following objectives:

- Undermine multilateral cooperation such as ASEAN+3 and the ASEAN Regional Forum (ARF), as well as minilateral frameworks such as the Quad, AUKUS, Japan–U.S.–Australia, and Japan–U.S.–ROK cooperation.
- Weaken the alignment of ASEAN countries, particularly those surrounding the South China Sea.
- Undermine the region by expanding engagement with Pacific Island Countries.

Chapter 7: Taiwan's Vulnerabilities to Hybrid Warfare in Key Domains

Diplomacy

・ Due to China's "One China Principle," Taiwan's participation in international organizations is restricted, and with only a small number of countries maintaining formal diplomatic relations with it, Taiwan's diplomatic activities are limited.

・ As a result, Taiwan also faces constraints in conducting international activities and receiving support in cooperation with other countries.

Political

・ There is a persistent confrontation between pro-China and anti-China forces, creating a constant risk of intensified political polarization.

・ Elections may be subject to interference through Chinese inducements of incentives and the spread of disinformation.

Culture

・ Due to historical and linguistic proximity to Chinese culture, Taiwan has conditions that make it susceptible to China's cultural influence operations (such as through films, music, and publishing).

・ Taiwan is also vulnerable to influence operations conducted through shared folk beliefs with the mainland, such as the Mazu faith.

Social/Societal

・ When the Republic of China government relocated to Taiwan in 1949, mainlanders who arrived with it suppressed the native Taiwanese who had already been living in Taiwan. The resulting tensions still persist within society.

・ Because Taiwan frequently experiences disasters such as earthquakes and typhoons, there is a risk that society could be destabilized by disinformation exploiting such events.

Legal

・ Due to China's "One China Principle," Taiwan's status under international law has been rendered ambiguous.

・ China continues attempts to nullify arrangements such as the median line and the Air Defense Identification Zone (ADIZ) through the creation of multiple *faits accompli.*

Military/Defense

・ Given the large military gap with China, deterrence remains uncertain due to the United States' strategy of ambiguity.

・ Regarding the basic concept of military defense, there are differing views within the government

and the military—such as whether to prioritize rapid defeat of an adversary or a protracted defense—creating potential divisions over defense planning and force development.

・ Development of cross-domain capabilities—including space, unmanned systems, cyber, and electromagnetic domains—has been slow.

・ The Taiwanese military faces internal challenges such as institutional reform and maintaining political neutrality, making it vulnerable to influence operations from China.

Space

・Due to limited budgets and technological capacity for space development, the establishment of an independent satellite network has been slow, resulting in a high level of dependence on other countries.

Administration

・ Strong rivalry between the ruling and opposition parties exists at both the central and local levels, creating vulnerabilities such as difficulty in implementing consistent administrative policies.

・ Although digital administration has advanced, the security framework has not kept pace.

Infrastructure

・ Electricity, logistics, and medical services are highly dependent on digital systems, making them vulnerable to cyberattacks.

・ Taiwan relies heavily on submarine cables for international internet communications, creating a significant vulnerability.

・ More than 90% of energy is dependent on imports, creating a high risk of supply disruptions.

Economy

・ Taiwan’s economy is highly dependent on the semiconductor industry, and disruptions to raw material imports or product exports would create significant economic risks.

・ Economic ties with China are close, making Taiwan vulnerable to both economic sanctions and economic incentives.

Intelligence

・Historically, divisions such as mainlanders vs. native Taiwanese and Kuomintang (KMT) vs. the Democratic Progressive Party (DPP) have created conditions that heighten vulnerability to Chinese espionage activities.

・Compared with China’s intelligence and counterintelligence system, Taiwan has vulnerabilities stemming from the nature of being a democratic society.

Information

・ Because social media plays a major role in political debate, Taiwan is susceptible to information manipulation in the online space, including the spread of disinformation.

- Pro-China media outlets—including those acquired by China—exert a certain level of influence.

Cyber

- Cyber defense tends to lag behind China's overwhelming cyberattack capabilities.
- Because administrative functions are highly digitized, cyberattacks could have significant impacts if they succeed.
- Institutionalized frameworks for international cooperation in cyber defense have not yet been established.

Chapter 8: Japan's Vulnerabilities to Hybrid Warfare in Key Domains

Assuming that China seeks the forced unification of Taiwan and simultaneously conducts hybrid warfare not only against both Taiwan and Japan, the vulnerabilities in Japan's various domains are analyzed as follows.

Diplomacy

・While Japan's foreign policy is based on the Japan–U.S. alliance, there remains a strong sense of public distrust toward the United States. Due to economic or diplomatic pressure, or social anxiety during crises, public opinion could shift significantly toward greater distrust of the U.S.

・The situation surrounding the Senkaku Islands could become more complicated because both the Chinese government and the Taiwan authorities make their own claims regarding the Islands.

Politics

・Japan may be caught in a political dilemma between accommodating China due to economic interests with China and responding to the United States' strict economic policies toward China.

・Some political forces in Japan have strong anti-U.S. sentiments. These could be exploited through scandals, economic assistance, or similar means to draw them toward a pro-China position.

Culture

・The gap in perception between residents of Okinawa and residents of mainland Japan could be exploited.

・If the narrative claiming that China, Taiwan, and Okinawa originally belonged to the same cultural sphere is reinforced, it could create the impression that Taiwan is also trying to divide Okinawa from Japan and therefore increase distrust toward Taiwan.

Society

・ Military intimidation—such as missile launches into surrounding waters—along with disinformation campaigns and cyberattacks could heighten anxiety, especially among residents living near military bases, potentially leading into anti-base protests.

・ If the Taiwan situation becomes unstable, there is a possibility that large numbers of refugees could flee to Japan, and the spread of disinformation could further generate social unrest.

・There is also a risk that the Nansei Islands could be drawn into armed conflict, and the spread of false information could again cause social instability.

Law

・ If Japan officially recognizes a "Survival-Threatening Situation" (存立危機事態) and takes

various response measures (ultimately including a defense operation), there could be political conflict in the Diet over approval.

・If the United States begins preparations for military intervention, Japan may recognize the situation as an "Important Influence Situation" (重要影響事態) and conduct various activities by the Self-Defense Forces. This could also lead to political disputes in the Diet over approval.

・With regard to the situation surrounding the Senkaku Islands, there is a possibility that actions by Japan Coast Guard could be used in Chinese propaganda portraying them as unilateral military operations by Japan, potentially creating international misunderstandings. Further, this could also intensify criticism of Japan in Taiwan and be used as propaganda to influence public opinion in Taiwan to reinforce China–Taiwan coordination.

Military

・There may be a situation in which support by Japan of U.S. strategy against China (an "Important Influence Situation") and the defense of Japan itself (a situation affecting national defense) occur simultaneously.

・In the event of a Taiwan crisis, there could be confusion over evacuating residents of the Nansei Islands and protecting refugees.

・Intrusions into Japan's territorial waters and airspace, along with increased military exercises around Japan, could cause public anxiety as well as inflame hardline views and divide society. At the same time, they could increase the burden on monitoring and surveillance by relevant agencies, potentially draining defense resources.

・GPS signal spoofing and disinformation could directly affect surveillance and monitoring, potentially leading to misjudgments and incorrect responses.

・Nuclear blackmail could undermine confidence in the credibility of the United States' nuclear deterrence.

Space

・Disruptions to Japan–U.S. command, control and communications that rely on space systems could lead to communication breakdowns between Japan and the United States.

・Many aspects of daily life—such as communications, geodesy (including GPS), and information services—rely on space infrastructure. Interference with satellites could therefore cause social anxiety and distrust of the government.

Administration

・Actions such as interference with Japanese civilian vessels by China Coast Guard ships could increase public distrust in the government, particularly regarding its ability to protect maritime rights and interests as a maritime nation.

・Concerns about the safety of residents, including civil protection measures for people in the Nansei Islands, could also increase distrust toward the government.

Infrastructure

・The functions of U.S. military bases in Japan and Japan Self-Defense Force bases depend on civilian infrastructure (electricity, water, gas, logistics). Disruptions—particularly from cyberattacks by unknown perpetrators—could cause concern about the reliability of Japan–U.S. coordination.

・Both Japan and Taiwan are highly dependent on submarine cables. Damage or disruption to these cables could obstruct policy coordination between Japan and the U.S., and between Japan and Taiwan.

Economy

・Given the high reliance of the Japanese economy on China, economic pressure, both hard and soft, could translate to political pressure.

・Cooperation with Taiwan in semiconductor technology could also become a target of external pressure.

Intelligence

・Limited sources of intelligence on Taiwan, combined with disruptions in communications with Taiwan (isolation), may lead to discrepancies in the perceptions among Japan, the United States, and Taiwan.

Information

・The mass spread of disinformation through fake accounts regarding domestic infrastructure failures, combined with simultaneous cyberattacks, could increase social anxiety. Likewise, the large-scale spread of disinformation, especially AI-generated fake images about Taiwan, the United States, and the international community, could increase social unrest and divide public opinion in Japan.

・Covert activities conducted through cyber methods or by operatives may remain unnoticed until it is too late to respond effectively.

Cyber

・In the invasion of Ukraine, public and private sector support from the United States and others was crucial in responding to serious cyber incidents and crises. In Japan's case, if legal frameworks, institutions, and division of roles for accepting such support are not discussed in advance, confusion could arise during a crisis.

・There is a risk that responses to critical national cyber security matters potentially involving state actors may be delayed. In particular, China has several possible state-sponsored cyber actors, and responses may be slow against cyberattacks where state involvement is deliberately kept ambiguous.

・Although cyber warfare and electromagnetic warfare are closely interconnected, there is a possibility that the insufficient consideration of security in Japan's electromagnetic wave management system may be exploited.

Chapter 9: Basic Approach to Countering Hybrid Warfare and the Importance of Multilateral Cooperation

As indicated in Chapter 1, within the context of hybrid warfare, it is not realistic to expect that all possible methods can be fully prevented prior to their use. Instead, it is important to take various measures in each field to ensure that the situation does not escalate further. The goal is to make the attacking party give up—preferably at an early stage, before it can ultimately achieve its objectives—and thereby stabilize the situation.

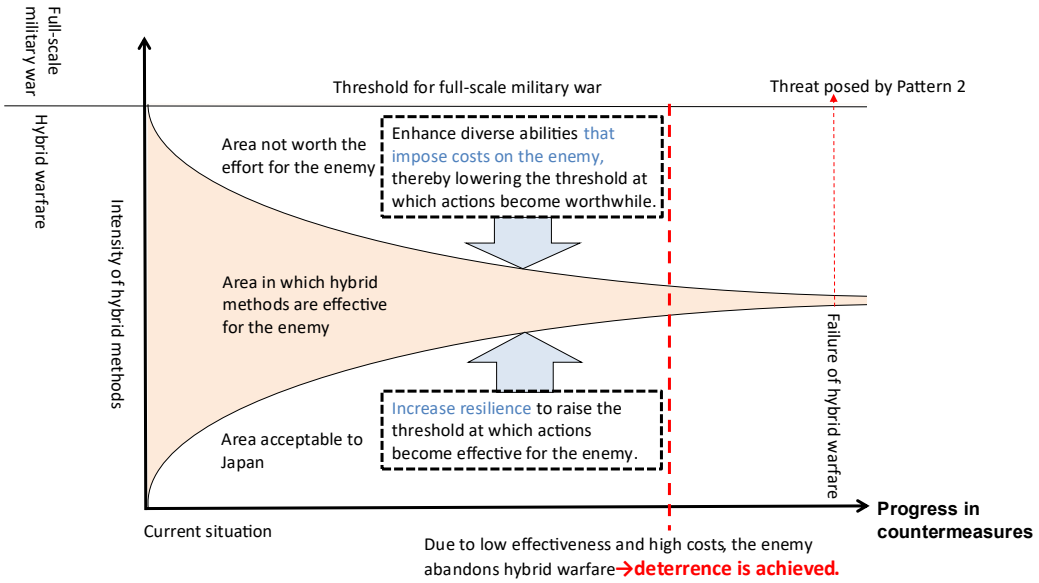

Figure 5. Conceptual Diagram of Hybrid Warfare Deterrence

Prepared by the author based on "DETERRENCE: Proposing a more strategic approach to countering hybrid threats" Figure 1, page 12; footnote 8)

Figure 5: **Conceptual Diagram of Hybrid Warfare Deterrence**

Source: Prepared by the author based on "DETERRENCE: Proposing a more strategic approach in countering hybrid threats," by Vytautas Kersanskas. Figure 1 (page 12; footnote 8). "op cit", p.12, Also in: "Countering Hybrid Warfare to Prevent the Forced Unification of Taiwan —Addressing China's Dual Threats of Hybrid Warfare and Full-scale Military Invasion—" November 19, 2025; Matsumura Goro.
https://www.npi.or.jp/en/research/data/npi_research_note_matsumura_20251119_en.pdf

Lithuanian researcher Vytautas Keršanskas, who studies hybrid warfare, presents a very meaningful idea from this perspective.[50] According to his research, for various hybrid warfare methods to be effective, the intensity of the threat must be high enough to actually cause negative effects on the

[50] Vytautas Kersanskas, "DETERRENCE: Proposing a more strategic approach to countering hybrid threats," Hybrid CoE Paper 2, March 2020. https://www.hybridcoe.fi/wp-content/uploads/2020/07/Deterrence_public.pdf

target society, but at the same time, it must be low enough to avoid provoking a decisive counterattack, including the use of military force, from the defending side. In other words, the attacker's chance of success lies in using hybrid methods within the range between the minimum intensity required for the attack to have an effect and the maximum intensity that would trigger retaliation. Viewed from the defending side's perspective, the strategy is the opposite. By strengthening society's resilience against various hybrid tactics in order to nullify them, while at the same time lowering the red line for triggering countermeasures, the space within which hybrid tactics can effectively operate becomes increasingly narrow, like the area shown in Figure 5.

In theory, it is possible to argue that the defending side's counterattack should be considered to be an attack using large-scale military force, and that deterrence should therefore be maintained by clearly establishing a strong red line indicating the use of force. However, this approach would not deter a full-scale military war as described as Pattern 2 in Chapter 1; however, rather than deterring the full-scale military war described as Pattern 2 in Chapter 1, this approach effectively presupposes that the defending side would trigger an undesirable military conflict.

Therefore, lowering this red line should not mean lowering the threshold for retaliation with large-scale military force. Instead, while responses may include limited military actions, it is more realistic for the threshold to focus mainly on non-military measures, such as diplomatic and economic sanctions that impose unbearable costs on China. This corresponds to the statement in Figure 5: "Strengthening diverse capabilities to impose costs on the adversary and lowering the threshold at which aggression becomes worthwhile."

Various methods used in hybrid warfare target vulnerabilities that exist across different domains of the target country, such as politics, diplomacy, the economy, society, culture, information, and the military.

For example, these methods may include: encouraging political divisions within the target country; damaging relations with countries that the target country relies on diplomatically; disrupting overseas supply chains that are economically vulnerable; exacerbating historical conflicts between regions; manipulating the fluid information environment that depends on social media and similar platforms; and exposing military weaknesses to the public. By combining such methods, the attacker seeks to expand cracks starting from the weakest points in the target society.

Therefore, if Japan, the United States, Taiwan, and other countries each take measures to reduce vulnerabilities and strengthen resilience in their respective fields, the effectiveness of various hybrid tactics can be reduced. As a result, the attacker would have to use methods of higher intensity in order to achieve any meaningful effect. In response, if China were to employ means of greater intensity, it would become more difficult to conceal state involvement. In that case, Japan, the United States, and Taiwan should impose sanctions and other countermeasures that force China to pay a high cost for each individual tactic. Doing so would help deter further escalation of hybrid warfare. In particular, deterrence would be more effective if costs can be imposed immediately each time hybrid tactics are detected, and if the accumulated effect of these various costs creates a situation that China cannot sustain.

Viewed as a whole, it may be impossible to prevent hybrid warfare from starting. However, it is possible to reduce the effectiveness of each individual hybrid tactic by strengthening our own resilience, and at the same time impose costs on the attacker whenever such tactics are used, making them hesitate to continue. Through this process, the opponent may be forced to abandon its hybrid warfare attempts midway.

To reject China's attempt to forcibly unify Taiwan at the hybrid warfare phase and ultimately force it to give up and stabilize the situation, Japan, the United States, and Taiwan must urgently reduce vulnerabilities and strengthen resilience across all domains—including politics, diplomacy, the economy, society, culture, information, and the military. At the same time, it is necessary to establish systems capable of detecting China's hybrid tactics at an early stage and comprehensively assessing their intentions, and based on that assessment, to create an international framework that can steadily impose costs on each use of such tactics.

To achieve this, it is not enough for Japan, the United States, and Taiwan to act alone. It is necessary to work in cooperation with partners such as Australia, the Philippines, Republic of Korea, and like-minded countries in ASEAN, Europe, and Oceania.

Chapter 10: Recommendations for Multilateral Cooperation to Prevent China's Unification of Taiwan[51]

1. Multilateral Cooperation to Reduce the Vulnerabilities of Japan, Taiwan, and Others

(1) Security and Military Framework

a. Strengthening cooperation among allies and like-minded countries

- Strengthen mutual trust and response capabilities among participating countries through military intelligence sharing and bilateral/multilateral exercises, with a focus on responding to hybrid warfare. In this regard, make use of various frameworks such as coordinating Japan-Australia-India-U.S. (Quad) with countries such as the Philippines and Viet Nam.

b. "Strategic communication" coordinated with allies and like-minded countries

- Build a cooperative framework to achieve high-quality strategic communication that contributes to stability. This framework would combine deterrence and response measures demonstrated through actions, such as practical scenario exercises by allies and partners, with the timely release of steady and accurate information to avoid misunderstandings.
- Continue efforts to protect freedom of navigation in the waters surrounding Taiwan.

c. Making deterrence visible

- Actively promote the transfer of defense equipment from Japan to further strengthen the law-enforcement and maritime surveillance capabilities of the Philippines. At the same time, work to build a shared understanding that such capability building does not increase tensions but rather it contributes to regional stability.
- Increase both official and unofficial exchanges between the military of Taiwan and the armed forces of other countries, and share knowledge on advanced technologies, new operational domains, and civil–military relations.
- Conduct multilateral joint exercises based on disaster scenarios in Taiwan.

(2) Strengthening Economic and Infrastructure Resilience

a. Preparing for an economic blockade

- Even if China were to claim that a de facto maritime blockade of Taiwan is merely law enforcement as a state asserting sovereignty over the Taiwan region, share the understanding

[51] For details on measures that Japan should take independently to reduce its vulnerability, please refer to Chapter 6, "Policy Recommendations Based on Japan's Vulnerability in Hybrid Warfare," of the Maritime Security Study Group's 2024 Research Report. https://www.npi.or.jp/research/data/npi_policy_maritime_security_20250331.pdf (English)

that such actions are contrary to the international political and economic order, and promote international cooperation to ensure the safety of maritime transport in the Western Pacific.

- Build an international backup system for Taiwan's semiconductor and satellite technologies.
- Strengthen cooperation with various countries to diversify energy supply sources.

b. Reorganization of supply chains

・Aim to move away from supply chains that depend heavily on China, and promote diversification of international markets through initiatives such as building cooperative frameworks like "Pax Silica."[52]

c. Economic support and cooperation

- Strengthen support and joint economic activities so that Taiwan can actively participate in economic cooperation with countries of the Global South.
- In light of the strategic importance of the Pacific Island Countries, actively expand economic assistance led by Japan, as well as assistance coordinated with like-minded countries.

d. Strengthening infrastructure resilience

- Build an international collaborative framework to ensure the security of submarine cables in the Pacific region.
- Strengthen international collaboration for the stable use of space-related assets, both those deployed in orbit and those installed on the ground.
- Begin discussions on measures such as creating cross-border backup systems to improve the resilience of data centers in each country.

(3) Diplomatic and Institutional Frameworks

a. Utilizing existing international frameworks

- Utilize existing global cooperation and training frameworks such as the Global Cooperation and Training Framework (GCTF)[53] to help stabilize Taiwan's international standing and create a basis for Japan to expand quasi-official relations.

・Express support and conduct lobbying efforts for Taiwan's participation in international organizations such as the World Health Organization (WHO) and the International Civil

[52] Pax Silica is a multilateral cooperation framework established in December 2025 by the United States, Japan, South Korea, Australia, and other countries, with the aim of stabilizing and strengthening the supply chain for semiconductors and critical minerals essential for AI.

[53] The Global Cooperation and Training Framework (GCTF) is a capacity-building initiative launched in 2015 between the United States and Taiwan, and is now joined by Japan, Australia, and Canada. Through this framework, activities are carried out to deepen exchanges on shared regional challenges—such as public health and environmental issues—by organizing workshops and inviting officials and experts from various countries, particularly those in Southeast Asia and Oceania.

Aviation Organization (ICAO).

- Cooperate in providing support for Taiwan's participation in international organizations and in assisting countries that maintain diplomatic relations with Taiwan.

b. Strengthening international law and norms

- Promote international discussions to establish rules of conduct for military and law-enforcement agencies to prevent clashes in maritime and air areas of the East China Sea and the South China Sea where boundaries based on sovereignty or jurisdiction have not been clearly determined.
- Strengthen compliance with the United Nations Convention on the Law of the Sea regarding safe navigation in the Taiwan Strait.

(4) Cooperation in the Space, Cyber, and Electromagnetic Domains

a. Promotion of technological cooperation

- Promote technological cooperation with allies and like-minded countries to address emerging threats in new domains such as space, Unmanned Aerial Vehicle (UAV), and the electromagnetic spectrum.
- Establish a framework for providing satellite technology to Taiwan, with Japan taking a leading role in supporting this effort.

b. Response to cyber threats and related issues

- Promote technological cooperation with allies and like-minded countries to address emerging threats in new domains such as space, unmanned systems, and the electromagnetic spectrum.
- Establish a framework for providing satellite technology to Taiwan, with Japan taking the lead in supporting this effort.

(5) Cooperation in the Information Space

a. Allies and like-minded countries sharing common values coordinate to communicate a shared narrative

- In light of the fact that China is disseminating worldwide various narratives regarding its unilateral claims, like-minded countries that share values such as freedom and democracy should work together to communicate a common narrative globally.

b. Strengthen cooperation to counter the spread of disinformation and manipulative information by China

- In response to efforts by China to spread disinformation or information that, although based

on facts, is biased or one-sided (malinformation), like-minded countries should cooperate to counter this through the rapid dissemination of accurate information and fact-checking.

(6) Comprehensive Response to Hybrid Threats

a. Promotion of multilateral hybrid scenario exercises

- It is necessary to share an understanding of what hybrid warfare is through seminars and similar activities with various countries. Multilateral exercises of scenarios assuming hybrid warfare will be conducted to deepen this shared understanding.

b. Multilateral information-sharing network

・Establish a multilateral information-sharing network to comprehensively respond to disinformation, cyberattacks, and other actions by China.

c. Establishment of a hybrid threat response center

・In the future, establish a "Hybrid Threat Response Center" in the East Asia region, and create a permanent framework for information sharing and consultations on countermeasures related to hybrid threats.

2. Multilateral Cooperation to Impose Costs on China's Hybrid Attacks

・ Intensify international criticism of China's use of force, aggressive military actions, and provocative acts against ships and aircraft engaged in surveillance, even if the acts are small scale, and increase pressure by further promoting international frameworks that call for restraint, such as the Code for Unplanned Encounters at Sea.[54]

・ In response to economic pressure from China, countries should cooperate to implement countermeasures in areas such as trade and investment.

・ If China's involvement in the destruction of submarine cables, aerospace infrastructure, or similar assets is confirmed, consider imposing penalties through relevant international organizations.

・ Form international pressure by bringing cases against actions by China that violate international law to bodies such as the International Court of Justice.

・ If involvement by the Chinese government in cyberattacks is confirmed, coordinate actions such as active cyber defense or similar measures to neutralize the source of the attacks.

・ If comprehensive analysis based on information sharing among countries suggests that China is conducting hybrid attacks using multiple methods, present this evidence to advance China's international isolation and consider coordinated countermeasures.

---

[54] The Code for Unplanned Encounters at Sea (CUES) is a set of guidelines agreed upon by 21 countries, including China, at the 2014 Western Pacific Naval Symposium (WPNS), aimed at avoiding accidental military clashes at sea; however, its scope is limited to naval vessels and aircraft, and it does not have legally binding force.

Conclusion: Policies to Pursue Going Forward

Over the past three years, the NPI Maritime Security Study Group has examined the possibility of hybrid warfare that China could carry out against Taiwan. Although the research is still ongoing and many issues remain, we outline here the subjects our study group has tackled together with those that should be pursued in the future.

1. Japan's Initiatives to Address the Situation

Public Awareness: Video distribution

Research on this project began with discussions on the question of what hybrid warfare actually is. There was also deliberation as to whether the public release of such research would serve Japan's national interest. However, exchanges with researchers internationally reinforced the view that an informed public understanding of emerging threats is essential. With this recognition, we decided to develop and distribute a video titled "What Is Hybrid Warfare?" as an effort to promote public awareness.

Public Awareness: Creation and maintenance of a case database website

An online case database (in Japanese and English) was developed and published. However, the database remains a work in progress, and a key challenge going forward will be establishing sustainable mechanisms for its maintenance and continued expansion.

Further Analysis of Cases: Use of AI

This research was conducted based on 40 tools, but it remains unclear whether this is sufficient, and further in-depth study is necessary. At the same time, there is a need to explore additional methods for analyzing cases using generative AI and related technologies. This remains a task for future research.

Addressing Vulnerabilities Through Cross-Ministerial Coordination

An analysis of Japan's vulnerabilities to hybrid threat revealed that vulnerabilities are widespread across many government ministries and agencies, making it necessary to establish a system that enables coordinated responses across ministries and agencies.

2. Efforts Toward a Multilateral Response

Building a Common Understanding with Allies and Like-Minded Countries (Seminars and Scenarios)

Seminars and similar forms of collaboration with partner countries should facilitate the sharing of specific national cases (issues), including those related to the 40 tools, in order to develop a shared

understanding of hybrid warfare.

Further, allies and like-minded countries should conduct simple scenario-based exercises assuming cases of hybrid warfare in order to further deepen this shared understanding.

Strengthening Strategic Communication with Allies and Like-Minded Countries

Through practical scenario-based exercises conducted with allies and like-minded countries, it is necessary to build cooperative frameworks for strategic communication, including the dissemination of reliable information as a countermeasure to disinformation and propaganda.

Strengthening Technical Cooperation with Allies and Like-Minded Countries

It is also necessary to develop multilateral cooperation frameworks for areas such as infrastructure protection and coordination on malware countermeasures, particularly through the joint development of cyber defense technologies.

Establishing a Hybrid Threat Response Center in East Asia

In the future, a Hybrid Threat Response Center should be established in the East Asian region to create a permanent framework for information sharing and consultation on countermeasures related to hybrid threats.

Hybrid threats transcend national boundaries and affect every corner of society. Therefore, responses must also involve cooperation that goes beyond those borders. This research represents an initial step toward establishing a foundation for future efforts in policy development, technological advancement, and international cooperation.

We would like to express our sincere appreciation to the Ministry of Foreign Affairs of Japan for the opportunity to conduct this research.

Annex 1 Tools of Hybrid Threat Activity and Affected Domains

	Tool	Affected domains
1	Physical operations against infrastructure	Infrastructure, Economy, Cyber, Space, Military/Defense, Information, Social/Societal, Public Administration
2	Creating and exploiting infrastructure dependency (including civil-military dependency)	Infrastructure, Economy, Cyber, Space, Military/Defense, Public Administration
3	Creating or exploiting economic dependencies	Economy, Diplomacy, Political, Public Administration
4	Foreign direct investment	Economy, Infrastructure, Cyber, Space, Military/Defense, Public Administration Intelligence, Information, Political, Legal
5	Industrial espionage	Economy, Infrastructure, Cyber, Space, Intelligence, Information
6	Undermining the opponent's national economy	Economy, Public Administration, Political, Diplomacy
7	Leveraging economic difficulties	Economy, Public Administration, Political, Diplomacy
8	Cyber espionage	Infrastructure, Space, Cyber, Military/Defense, Public Administration
9	Cyber operations	Infrastructure, Space, Cyber, Social/Societal, Public Administration, Military/Defense
10	Airspace violation	Military/Defense, Social/Societal, Political, Diplomacy
11	Territorial water violation	Military/Defense, Social/Societal, Political, Diplomacy
12	Weapons proliferation	Military/Defense
13	Armed forces conventional/sub-conventional operations	Military/Defense
14	Paramilitary organizations (proxies)	Military/Defense
15	Military exercises	Military/Defense, Diplomacy, Political, Societal
16	Engaging diasporas for influencing	Political, Diplomacy, Social/Societal, Culture, Intelligence, Information
17	Financing cultural groups and think tanks	Societal, Culture, Political, Diplomacy

18	Exploitation of sociocultural cleavages (ethnic, religion and culture)	Social/Societal, Culture
19	Promoting social unrest	Infrastructure, Social/Societal, Economy, Political
20	Manipulating discourses on migration to polarize societies and undermine liberal democracies	Social/Societal, Culture, Political, Legal
21	Exploiting vulnerabilities in public administration (including emergency management)	Public Administration, Political, Social/Societal
22	Promoting and exploiting corruption	Public Administration, Economy, Legal, Social/Societal
23	Exploiting thresholds, non-attribution, gaps and uncertainty in the law	Infrastructure, Cyber, Space, Economy, Military/Defense, Culture, Social/Societal, Public Administration, Legal, Intelligence, Diplomacy, Political, Information
24	Leveraging legal rules, processes, institutions and arguments	Infrastructure, Cyber, Space, Economy, Military/Defense, Culture, Social/Societal, Public Administration, Legal, Intelligence, Diplomacy, Political, Information
25	Intelligence preparation	Intelligence, Military/Defense
26	Clandestine operations	Intelligence, Military/Defense
27	Infiltration	Intelligence, Military/Defense
28	Diplomatic sanctions	Diplomacy, Political, Economy
29	Boycotts	Diplomacy, Political, Economy
30	Embassies	Diplomacy, Political, Intelligence, Social/Societal
31	Creating confusion or a contradictory narrative	Social/Societal, Information, Diplomacy
32	Migration as a bargaining chip in international relations	Social/Societal, Diplomacy, Political
33	Discrediting leadership and/or candidates	Political, Public Administration, Social/Societal
34	Support of political actors	Political, Public Administration, Social/Societal
35	Coercion of politicians and/or government	Political, Public Administration, Legal
36	Exploiting immigration for political influencing	Political, Social/Societal

37	Media control and interference	Information (Media), Infrastructure, Social/Societal, Culture
38	Disinformation campaigns and propaganda	Social/Societal, Information, Political, Cyber, Culture, Public Administration
39	Influencing curricula and academia	Social/Societal, Culture
40	Electronic operations (GNSS jamming and spoofing)	Space, Cyber, Infrastructure, Economy, Military/Defense

Source: Based on European Commission, & Hybrid CoE, The Landscape of Hybrid Threats: A Conceptual Model Public Version, 2021 , pp. 33-35

Annex 2　Relationship between Phase and Activity

<table>
<tr><th>Operational Phase</th><th>Hybrid Threat Activity</th></tr>
<tr><td>Priming Phase</td><td rowspan="3">・Interference
By using hybrid threat tools, create confusion in the opponent’s activities in the target domain and lay groundwork for movement toward destabilization.

・Influence
By using hybrid threat tools, exert some form of influence on the opponent’s activities in the target domain, aim to create destabilization, and facilitate conduct of operations.
・Operation
By combining and exercising hybrid threat tools, compel the opponent to take the desired actions in order to achieve the objective.

・War/warfare
Within military war, use hybrid threat tools in order to gain advantage in the military war.</td></tr>
<tr><td>Destabilization Phase</td></tr>
<tr><td>Coercion Phase</td></tr>
</table>

Source: Based on the European Commission, & Hybrid CoE, The Landscape of Hybrid Threats: A Conceptual Model Public Version, 2021, p. 13

Annex 3　Overview of 13 Tools and Activities (grouped by affected domain)

(1) Infrastructure-related tools

Physical operations against infrastructure	Physical sabotage against infrastructure such as communications, data, transportation, energy production, and water resources
	Example: severing submarine cables
Creating and exploiting infrastructure dependency (including civil-military dependency)	An actor creates dependence on infrastructure—such as energy, communications, and water—and uses it to exert influence
	Example: Controlling pipelines, dams, submarine cables, or satellites to restrict supply and destabilize the target country

(2) Economy-related tools

Creating or exploiting economic dependencies	Build a dependency relationship between the target country and own country through trade and other means, and exercise influence
	Example: importing key products from target country and exporting rare resources or critical goods in supply chains
Foreign direct investment	Exercise influence by directly investing in private companies in target country
	Example: Make investments to control resources and infrastructure; investments to increase overall economic control
Industrial espionage	Obtain industrial information from companies, research institutes, etc. in the target country and exercise industrial influence
	Example: Gain collaborators, poaching engineers, acquiring technology through capital relationships
Undermining the opponent’s national economy	Exert influence by controlling essential goods and services for target country's major industries
	Example: Impose export restrictions on important resources and components, and control of international markets
Leveraging economic difficulties	Exercise influence by supporting economically disadvantaged residents in target country
	Example: Industrial expansion in areas with poor employment conditions, purchase agricultural products, encourage overseas work in one’s own country

(3) Cyber-related tools

Cyber espionage	Conduct preparation for cyberattacks in cyberspace and obtain military, industrial, and social intelligence
	Example: Infiltrate government or corporate servers to obtain information
Cyber operations	Restrict target country's actions in cyberspace and conduct cyberattacks in ways that serve one's own interests
	Example: spread disinformation using bots; disrupt or destroy critical infrastructure systems; and cause physical damage through such systems

(4) Military-related tools

Airspace violation	Use manned or unmanned military aircraft to violate airspace and carry out intimidation or intelligence-gathering activities
	Example: continued, routine occurrence of such incursions and incursions by large numbers of aircraft during major exercises
Territorial water violation	Apply pressure by repeatedly intruding into territorial waters, contiguous zones, or Exclusive Economic Zones (EEZs), whether by military or civilian entities, and creating *faits accompli*s
	Examples: Mass large numbers of fishing boats, exercise of jurisdiction by law enforcement vessels, activities of research ships, activities by naval warships
Weapons proliferation	Exercise influence through arms exports to target country or its neighboring countries
	Example: Build a dependency relationship through arms exports to target country; gain a military advantage through exports to neighboring countries
Armed forces conventional/sub-conventional operations	Conduct limited attacks such as border incursions by conventional forces, and use quasi-conventional forces to intimidate and exert influence through covert operations
	Example: Conduct intimidation through border incursions, artillery fire, and attacks on warships; infiltration by special forces to create unrest in the target country through destruction, etc.
Paramilitary organizations (proxies)	Use paramilitary organizations in the target country as a proxy force to destabilize the country by instigating civil unrest, etc.
	Example: Use armed groups, secretly supply weapons to arm proxy forces

Military exercises	Conduct military exercises of various scales to check and intimidate the target country and its allies
	Example: Conduct various exercises, large-scale exercises, exercises near the target country that disrupt economic activities; missile launches, testing of new weapons

(5) Culture-related tools

Engaging diasporas for influencing	Leverage ethnic groups from own or other countries residing in the target country to carry out operations aimed at social destabilization
	Example: Lead anti-government movements, conduct separatist movements, spread disinformation, incite cultural conflict
Financing cultural groups and think tanks	Provide funding, officially or unofficially, to cultural organizations, think tanks, etc., in target country and exert influence over them
	Example: Provide funding to organizations that directly promote own country's views, or indirectly expand influence through funding
Exploitation of sociocultural cleavages (ethnic, religion and culture)	Exploit cultural conflicts in a target country's society, stemming from ethnic, religious, or cultural factors, to instigate social division
	Example: Promote or incite ethnic or religious conflicts; revive and exacerbate historically rooted conflicts
Influencing curricula and academia	Infiltrate university faculty and alter curricula to promote own country's narrative or language
	Example: Co-opt academics through funding or promotion of positions, and subtly alter the curriculum

(6) Society-related tools

Promoting social unrest	Exacerbate social unrest by inciting various social conflicts and distrust of the government in the target country
	Example: Intentionally provoke conflict by fueling social problems or organizing opposition movements against specific policies
Manipulating discourses on migration to polarize societies and undermine liberal democracies	Manipulate opinions to create prejudice and anxiety about immigrants in the target country and spread extreme political opinions to divide target country's society
	Example: Spread misinformation about immigrant scandals or incite social conflict by posing as an immigrant

(7) Administration-related tools

Exploiting vulnerabilities in public administration (including emergency management)	Exploit deficiencies in the government response to disasters, accidents, etc., to generate distrust and undermine support for the government
	Example: Incite panic or riots during disasters or accidents and spread misinformation to exacerbate anxiety and dissatisfaction
Promoting and exploiting corruption	Undermine public trust in government agencies by encouraging corruption and then use it to own advantage
	Example: Promote corruption in central and local government organizations, the military, and the police; co-opt officials through bribery

(8) Law/legal-related tools

Exploiting thresholds, non-attribution, gaps and uncertainty in the law	Exploit flaws, deficiencies, or ambiguities in target country's laws to undermine social stability
	Example: File lawsuits that incite social division or antisocial behavior that is not clearly defined as illegal, thereby promoting social unrest
Exploiting laws and regulations, drafting processes, legal systems and legal disputes	Exploit legal deficiencies, ambiguities, and complexities of the target government's response to various situations to hinder effective action
	Example: Exploit procedural flaws in fact-finding or ambiguities between law enforcement and the use of force

(9) Intelligence-related tools

Intelligence preparation	Collect information on the vulnerabilities of target country and analyze its weaknesses, using legal or illegal methods
	Example: Collect information on scandals involving politicians, analyzing weaknesses in administrative agencies and the military, etc.
Clandestine operations	Exert social influence through covert operations by agents such as assassination, sabotage, causing accidents, or spreading disinformation
	Example: Create incidents disguised as actual events to exacerbate divisions between countries or within societies.
Infiltration	Exert influence by placing or acquiring collaborators within the government, political parties, administrative agencies, military, major corporations of target country
	Send one’s own agents into target country institutions; recruit collaborators in the target country

(10) Diplomacy-related tools

Diplomatic sanctions	Impose direct diplomatic disadvantages on target country and force other countries to take similar measures
	Examples: Sever diplomatic relations, force a third country to sever diplomatic relations
Boycotts	Organize boycotts to prevent target country from participating in international organizations or events with the aim to diplomatically isolate it
	Example: Exclude target country from international conferences; boycott events such as the Olympics.
Embassies	Use embassies and other overseas diplomatic missions and their staff for leverage, and misuse them for purposes other than their original diplomatic objectives
	Example: Recall ambassadors, close diplomatic missions, expel target country's staff from one's own country
Migration as a bargaining chip in international relations	Use measures such as migration outflow, inflow, transit, reception, and deportation of migrants as bargaining chips in diplomatic negotiations
	Example: send migrants across borders

(11) Politics-related tools

Discrediting leadership and/or candidates	Undermine the credibility of target country's political leaders or candidates through the dissemination of false information, etc.
	Spread scandals, etc., leading to policy failures and undermining authority
Support of political actors	Provide financial and policy support to politicians or political parties that are favorable to one's own country
	Example: Provide political funds through indirect means such as corporations
Coercion of politicians and/or government	Use various means to force politicians or governments to adopt policies favorable to one's own country
	Example: Apply a carrot and sticks approach to coerce the economy of target country or exploit its political weaknesses
Exploiting immigration for political influencing	Exercise influence over the politics of target country by politicizing immigration issues
	Use disinformation or covert schemes to amplify immigration-related issues

(12) Information-related tools

Media control and interference	Bring a foreign country's media directly under control, or use various means to exert influence and intervene in the content of its reporting
	Examples: Acquisition of media outlets, strengthening of capital ties
Disinformation campaigns and propaganda	Spread false or malicious information widely through media, social media, word of mouth, etc.
	Example: Spread information that creates distrust of the government or information that is favorable to one's own country
Creating confusion or a contradictory narrative	Create and spread narratives that cause chaos or conflict in target country, or narratives that support one's own country, through various means
	Example: Create and spread ethnic or religious historical narratives that exacerbate social divisions

(13) Technology-related tools

Electronic operations (GNSS jamming and spoofing)	Disrupt or hijack radio signals, including those transmitted via satellite, using jamming or spoofing signals
	Example: Interference with GPS signals and other radio signals

(14) Other tools

Election interference	Conduct activities to ensure that candidates favorable to one's own country are elected in target country's elections
	Spread misinformation about candidates, provide political funds
Impact of generative AI	Impact of rapidly developing generative AI must be closely monitored
	Example: Because images, audio, and video can be generated automatically and instantaneously, the spread of disinformation and propaganda is accelerating

Annex 4　Results of a Database-driven Analysis of Trends by Operational Method

(1) Infrastructure-related operational methods

Primary Tools	Cases			Actors (case study)						Target country (case study)						
	Total	Cases	Forecast	China	Russia	North Korea	Other	Non-state	Unknown	Japan	Taiwan	USA	Australia	Philippines	Ukraine	Other
Physical operations against infrastructure	17	11	6	5	4	0	0	0	2	0	3	0	0	0	2	6
Creating and exploiting infrastructure dependency	5	2	3	1	1	0	0	0	0	0	0	0	0	0	1	1

・China and Russia are primary actors; some submarine cable cutting remains unattributed

・Submarine cable targets often in adversarial relationship to suspected actors

・Submarine cable sabotage likely to persist due to attribution and enforcement challenges

(2) Economy-related operational methods

Primary Tools	Cases			Actors (case study)						Target country (case study)						
	Total	Cases	Forecast	China	Russia	North	Other	Non-state	Unknown	Japan	Taiwan	USA	Australia	Philippine	Ukraine	Other
Creating or exploiting economic dependencies	8	4	4	3	0	0	1	0	0	0	3	0	0	0	0	1
Foreign direct investment	18	16	2	15	0	0	0	0	0	1	1	0	1	0	0	12
Industrial espionage	1	1	0	1	0	0	0	0	0	1	0	0	0	0	0	0
Undermining the opponent's national economy	24	15	9	10	0	0	5	0	0	2	1	0	2	1	0	9
Leveraging economic difficulties	1	1	0	0	0	0	0	0	1	0	0	0	0	0	0	1

・China is the primary actor; while some operations directly affect Taiwan and others, many target developing countries

・Influence may fluctuate with China's economic conditions, but current trends are likely to persist in the near term

(3) Cyber-related operational methods

Primary Tools	Cases			Actors (case study)						Target country (case study)						
	Total	Cases	Foreca	China	Russia	North	Other	Non-	Unkno	Japan	Taiwan	USA	Australi	Philippi	Ukraine	Other
Cyber espionage	16	16	0	8	3	3	1	0	1	2	0	0	0	0	0	14
Cyber operations	51	44	7	4	11	0	1	0	28	8	2	13	1	0	5	15

・Russia and China are primary actors; many operations remain unattributed

□・Taiwan shows fewer reported cases, but actual cyberattack volume is very high

□・Difficult attribution makes cyber operations likely to remain widely used

□・Gap between reported data and actual cyberattack volume requires caution in future analysis

(4) Military-related operational methods

Primary Tools	Cases			Actors (case study)						Target country (case study)						
	Total	Cases	Forecas	China	Russia	North	Other	Non-	Unknow	Japan	Taiwan	USA	Australi	Philippi	Ukraine	Other
Airspace violation	8	7	1	7	1	0	0	0	0	4	2	1	0	0	0	0
Territorial water violation	13	13	0	12	0	0	1	0	0	9	1	0	0	1	0	2
Weapons proliferation	12	11	1	3	2	2	4	0	0	0	0	0	0	0	0	11
Armed forces conventional/sub-conventional operations	10	4	6	0	0	0	4	0	0	0	0	0	0	0	0	4
Paramilitary organizations (proxies)	9	7	2	7	0	0	0	0	0	1	2	1	1	1	0	1
Military exercises	18	8	10	8	0	0	0	0	0	3	4	0	1	0	0	0

□・China is the primary actor, with Taiwan overwhelmingly the main target

□・Actors are predominantly major arms producers and countries with strong military capabilities

□・Actors are relatively identifiable, but intelligence gathering is key to determining intent

(5) Culture-related operational methods

Primary Tools	Cases			Actors (case study)						Target country (case study)						
	Total	Cases	Forecas	China	Russia	North	Other	Non-	Unknow	Japan	Taiwan	USA	Australi	Philippi	Ukraine	Other
Engaging diasporas for influencing	8	8	0	4	1	0	3	0	0	0	1	2	0	0	0	5
Financing cultural groups and think tanks	8	8	0	3	0	0	2	2	1	0	0	4	0	0	0	4
Exploitation of sociocultural cleavages (ethnic, religion and culture)	4	3	1	3	0	0	0	0	0	2	1	1	0	0	0	0
Influencing curricula and academia	3	3	0	3	0	0	0	0	0	1	0	1	0	0	0	1

□・China is the central actor; targets are often adversarial countries such as Japan and the United States

□・Operations are likely conducted over long periods, with financial flows key to detecting indicators

(6) Society-related operational methods

Primary Tools	Cases			Actors (case study)						Target country (case study)						
	Total	Cases	Forecas	China	Russia	North	Other	Non-	Unknow	Japan	Taiwan	USA	Australi	Philippi	Ukraine	Other
Promoting social unrest	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Manipulating discourses on migration to polarize societies and undermine liberal democracies	6	5	1	0	0	0	0	0	5	0	0	2	0	0	0	3

□・Actors remain unidentified

□・Migration issues readily fuel public discontent, making attribution difficult and complicating distinction from organic activity; intelligence collection methods require review

(7) Administration-related operational methods

Primary Tools	Cases			Actors (case study)						Target country (case study)						
	Total	Cases	Forecas	China	Russia	North	Other	Non-	Unknow	Japan	Taiwan	USA	Australi	Philippi	Ukraine	Other
Exploiting vulnerabilities in public administration	2	1	1	1	0	0	0	0	0	0	0	0	0	0		1
Promoting and exploiting corruption	5	5	0	5	0	0	0	0	0	0	2	1	0	0		2

□・China conducts corruption-related operations across multiple countries

□・This trend is likely to continue

(8) Law/legal-related operational methods

Primary Tools	Cases			Actors (case study)						Target country (case study)						
	Total	Cases	Foreca	China	Russia	North	Other	Non-	Unkno	Japan	Taiwan	USA	Australi	Philippi	Ukrain	Other
Exploiting thresholds, non-attribution, gaps and uncertainty in the law	8	7	1	7	0	0	0	0	0	4	1	0	0	0	0	2
Leveraging legal rules, processes, institutions and arguments	19	16	3	16	0	0	0	0	0	4	1	0	0	0	0	11

□・China primarily targets Japan, advancing claims by combining international law and domestic law

□・Such activities are expected to continue

(9) Intelligence-related operational methods

Primary Tools	Cases			Actors (case study)						Target country (case study)						
	Total	Cases	Forecas	China	Russia	North	Other	Non-	Unknow	Japan	Taiwan	USA	Australi	Philippi	Ukraine	Other
Intelligence preparation	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	1
Clandestine operations	14	13	1	3	3	2	4	0	1	2	1	0	0	0	2	8
Infiltration	31	31	0	15	5	2	8	0	1	2	6	6	0	0	1	16

□・China, Russia, and North Korea are primary actors; main targets include Japan, Taiwan, the United States, and Europe

□・Taiwan shows disproportionately high espionage activity relative to reported cases, requiring careful analysis

(10) Diplomacy-related operational methods

Primary Tools	Cases			Actors (case study)						Target country (case study)						
	Total	Cases	Forecas	China	Russia	North	Other	Non-	Unknow	Japan	Taiwan	USA	Australi	Philippi	Ukraine	Other
Diplomatic sanctions	7	5	2	4	0	0	1	0	0	0	2	1	0	0	0	2
Boycotts	1	1	0	1	0	0	0	0	0	0	1	0	0	0	0	0
Embassies	2	2	0	2	0	0	0	0	0	0	0	2	0	0	0	0
Migration as a bargaining chip in international relations	9	9	0	0	4	0	5	0	0	0	0	0	0	0	0	9

□・China and Russia are primary actors; main targets include Japan, Taiwan, the United States, and Europe

□・Actors are major powers with strong diplomatic capabilities and are highly visible in the news

(11) Politics-related operational methods

Primary Tools	Cases			Actors (case study)						Target country (case study)						
	Total	Cases	Foreca	China	Russia	North	Other	Non-	Unkno	Japan	Taiwan	USA	Australi	Philippi	Ukrain	Other
Discrediting leadership and/or candidates	2	1	1	0	0	0	0	1	0	0	0	0	0	0	0	1
Support of political actors	6	3	3	3	0	0	0	0	0	0	1	0	0	0	0	2
Coercion of politicians and/or government	7	5	2	1	0	0	4	0	0	0	1	1	0	0	0	3
Exploiting immigration for political influencing	9	9	0	0	3	0	2	0	4	0	0	1	0	0	0	8

□・China and Russia are primary actors

□・Low case numbers likely reflect covert activity and possible underreporting by governments

(12) Information-related operational methods

Primary Tools	Cases			Actors (case study)						Target country (case study)						
	Total	Cases	Foreca	China	Russia	North	Other	Non-	Unkno	Japan	Taiwan	USA	Australi	Philippi	Ukraine	Other
Media control and interference	19	19	0	12	3	1	3	0	0	2	1	2	0	0	1	13
Disinformation campaigns and propaganda	32	22	10	16	2	1	2	0	1	4	6	4	0	0	0	8
Creating confusion or a contradictory narrative	8	4	4	3	1	0	0	0	0	1	1	1	0	0	0	1

□・China and Russia are primary actors; main targets include Japan, Taiwan, the United States, and Europe

□・Generative AI is accelerating activity, with cases expected to increase

(13) Technology-related operational methods

Primary Tools	Cases			Actors (case study)						Target country (case study)						
	Total	Case	Forec	China	Russi	North	Other	Non-	Unkn	Japan	Taiwa	USA	Austr	Philip	Ukrai	Other
Electronic operations (GNSS jamming and spoofing)	7	6	1	1	3	0	1	0	1	0	0	0	0	0	0	6

□・Russia is the primary actor, centered on activities in the aggression against Ukraine

□・China alters AIS signals of coast guard vessels

□・GNSS interference is highly effective in disrupting transport and financial systems and is likely to be used more; China is expected to continue altering AIS signals

(14) Other operational methods

Primary Tool	Cases			Actors (case study)						Target country (case study)						
	Total	Cases	Foreca	China	Russia	North	Other	Non-	Unkno	Japan	Taiwan	USA	Austral	Philippi	Ukrain	Other
Election interference	16	14	2	6	5	0	0	1	2	2	4	3	0	0	0	5
Impact of generative AI	9	8	7	3	2	0	1	0	2	1	1	2	0	0	0	3

□・China and Russia are primary actors, with most operations targeting countries of strategic interest

□・Use of generative AI is expected to increase

Annex 5　Coaxing Approach Toward Taiwan (details)

Priming Phase (Coaxing Approach)

*TCP: Taiwan / Coaxing / Priming

TCP1: Intelligence activities

Tool 8 (Cyber espionage)

- Cyber intrusion without leaving traces, preparation to switch to attack when necessary (APT).

Tool 25 (Intelligence preparation)

- Identification of pro-China and anti-China networks.
- Clarification of capital relationships, etc. within the Taiwanese business community.

Tool 27 (Infiltration)

- Infiltration of personnel into political parties, government agencies, private companies, military, etc., and acquisition of collaborators.

TCP2: Incorporate pro-China politicians

Tool 34 (Support of political actors)

- Economic support / policy coordination / manipulation of public opinion.

TCP3: Incorporate pro-China factions

Tool 3 (Creating economic dependencies)

- Strengthen economic ties to win over pro-China factions.

Tool 4 (Foreign direct investment)

- Increase direct investment in Taiwan to strengthen influence within the Taiwanese business community.

Tool 37 (Media control and interference)

- Acquire Taiwanese media to create a pro-China public opinion.

Tool 17 (Financing cultural groups and think tanks)

- Provide financial support to pro-China organizations to expand influence.

TCP4: Obstructing Taiwan's diplomatic activities

Tool 28 (Diplomatic sanctions)

- Interference in Taiwan's diplomatic relations with countries that recognize Taiwan as a state (recognition of strengthening of relations between countries that have diplomatic relations with China and Taiwan, and guidance in the direction of unification of China and Taiwan).

TCP5: Strengthening economic interdependence with Taiwan

● **Economic carrot and stick**

Tool 3 (Creating economic dependencies)

- Strengthening economic dependence of Kinmen and Matsu on China and expanding China's influence over these islands.
- Opening a model district for "Taiwan unification" in Fujian Province.
- Promoting or restricting economic activity to pressure Taiwan residents and expand China's

influence over them.

● **Dependency on infrastructure**

Tool 2 (Creating infrastructure dependency)

・ Strengthening dependency on energy supplies and communications infrastructure and expanding influence.

TCP6: Military intimidation (low intensity)

Tool 15 (Military exercises)

・ Vary the intensity of military exercises in the region in line with the degree of the administration's pro-China sentiment to keep anti-China factions in check.

TCP7: Generating distrust of Japan and the U.S.

Tool 31 (Creating confusion or a contradictory narrative)

・ Dissemination of narratives favorable to China regarding "Japan's past invasion of Taiwan."

・ Dissemination of narratives that the U.S. thinks only about itself in the midst of the global U.S.-China conflict.

Tool 38 (Disinformation campaigns and propaganda)

・ Dissemination of disinformation such as "Japan is skeptical about supporting Taiwan" and "The United States will not help Taiwan."

Destabilization Phase (Coaxing Approach)

*TCD: Taiwan / Coaxing / Destabilization

TCD1: Discrediting anti-China forces

Tool 38 (Disinformation campaigns and propaganda)

・ Spreading disinformation such as anti-China faction scandals.

Tool 26 (Clandestine operations)

・ Inciting riots and assassinations disguised as anti-China faction actions.

TCD2: Promoting the importance of Taiwan-China cooperation

● **Promoting the "peace framework"**

Tool 38 (Disinformation campaigns and propaganda)

・ Promoting the "peace framework," which emphasizes more autonomy than "one country, two systems."

Tool 9 (Cyber operations)

・ Expanding support for Chinese propaganda (false postings by bots, etc.) on social media.

● **Coercion to strengthen economic partnership**

Tool 35 (Coercion of politicians and/or government)

・ Reemphasizing the importance of trade with Taiwan and investment and coercing politicians to take a pro-China policy.

TCD 3: Generating distrust of the United States

Tool 38 (Disinformation campaigns and propaganda)

・ Disinformation (propaganda) that "the United States and China have agreed on a trade deal in

exchange for the United States not supporting Taiwan."

Coercion Phase (Coaxing Approach)

*TCC: Taiwan / Coaxing / Coercion

TCC1: Strengthening ties with China

● **Institutionalization of economic ties**

Tool 3 (Creating or exploiting economic dependencies)

・ The pro-China administration and the government have officially agreed on a framework to integrate the economies of the two regions.

TCC2: Chinese control of Taiwan's information space

● **Strengthening information dissemination in cyberspace**

Tool 9 (Cyber operations)

・ Interference in Taiwan's cyberspace.

Tool 38 (Disinformation campaigns and propaganda)

・ Dissemination of discourse that the Chinese model is superior to the American model for the safe use of cyberspace.

● **Media capture**

Tool 37 (Media control and interference)

・ Controlling Taiwanese media from a capital perspective, eliminating anti-China reporting.

TCC3: Open and covert intervention in elections

Tool 9 (Cyber operations)

・ Intervening in election campaigns by using bots, etc. on social media, etc.

・ Hacking election systems and manipulating the results.

Tool 38 (Disinformation campaigns and propaganda)

・ Disseminating disinformation, such as that a state of war will immediately break out if anti-China forces come to power.

TCC4: Establishment of a government that advocates unification

● **Fully support the newly established pro-China government and cooperate in the suppression of anti-China factions**

Tool 34 (Support of political actors)

・ Financial support for pro-China political parties and politicians.

Tool 21 (Exploiting vulnerabilities in public administration)

・ Support for police capabilities to suppress anti-China factions, including the provision of expertise and equipment.

Tool 24 (Leveraging legal institutions)

・Immediately after the establishment of a pro-China administration, the enactment of laws to crack down on anti-China factions.

Annex 6　Hardline Approach Against Taiwan (details)

Priming Phase (Hardline Approach)

*THP: Taiwan / Hardline / Priming

THP1: Intelligence activities (operations)

Tool 8 (Cyber espionage)

- Cyber intrusion without leaving traces, preparation to switch to attack when necessary (APT).

Tool 25 (Intelligence preparation)

- Explore vulnerable points in the Taiwanese military.
- Explore vulnerable points in critical infrastructure.

Tool 27 (Infiltration)

- Infiltration of personnel into the military, police, Taiwanese authorities, political parties, etc., and acquisition of collaborators.

THP2: Intimidation and undermining of trust in politicians

Tool 33 (Discrediting leadership)

- Exposing scandals. Manipulating information.

Tool 35 (Coercion of politicians and/or government)

- Blackmail and intimidation, illegal interference in elections.

THP3: Political and social division

● **Division between the unification faction and independence faction**

Tool 37 (Media control and interference)

- Acquiring foreign media companies and publishers, exerting influence through advertising and investment.

Tool 31 (Creating confusion or a contradictory narrative)

- Fortifying the narratives of both the unification and independence factions to create an atmosphere in which compromise is mutually impossible.

Tool 18 (Exploitation of sociocultural cleavages (ethnic, religious, cultural))

- Exploiting religious ties with the mainland (exerting influence through the Mazu belief on both sides of the Taiwan Strait).

● **Division between Taiwanese and Mainlanders**

Tool 18 (exploitation of sociocultural cleavages)

- Exploiting contradictions related to social superiority (discrimination) stemming from historical circumstances to cause domestic chaos.

THP4: Boycott from international organizations

Tool 28 (Diplomatic sanctions)

- Disrupting diplomatic relations with countries that recognize Taiwan as a nation or are pro-Taiwan (isolating Taiwan).

Tool 29 (Boycotts)

- Prevent Taiwan from joining international organizations and events.

THP5: Interference with Taiwan's economic activities

Tool 6 (Undermining economy)

- Import and export regulations by government agencies.
- Temporary suspension of the Economic Cooperation Framework Agreement (ECFA).
- Extensive restrictions on multinational corporations in Taiwan.

THP6: Military intimidation (high intensity)

Tool 15 (Military exercises)

- Military exercises around Taiwan (approaching and passing through the contiguous zone).
- Multiple long-range missile tests in Taiwan's airspace and surrounding areas.

Tool 10 (Airspace violation)

- Crossing the median line and other borders by balloons and unmanned and manned vehicles.

Tool 11 (Territorial water violation (including EEZ))

- Fortifying the activities of fishing boats and the China Coast Guard around Kinmen and Matsu.
- China Coast Guard and naval activities around the Pratas Islands and Taiping Island.

Destabilization Phase (Hardline Approach)

*THD: Taiwan / Hardline / Destabilization

THD1: Generating distrust in the government's administrative capabilities

● Obstruction of civilian vessel navigation

Tool 11 (Territorial water violation)

- Obstruction of vessels navigating near Kinmen and Matsu.

● Violation of territorial airspace

Tool 10 (Airspace violation)

- Flying swarms of drones over Kinmen and Matsu.

THD2: Social unrest, inciting fear of war

● Bank outages

Tool 9 (Cyber operations)

- DDoS attacks making the website of banks inaccessible.

Tool 38 (Disinformation campaigns and propaganda)

- Spreading disinformation such as "XX bank transactions are unavailable."

● Medical disturbances

Tool 9 (Cyber operations)

- Medical anxiety and disorders due to disruptions to a medical institution's electronic medical records.

Tool 38 (Disinformation campaigns)

- Spreading disinformation about disruptions to many medical institutions.

● **Inciting a crisis**

Tool 38 (Disinformation campaigns and propaganda)

・ Spreading rumors that Taiwanese officials are making personal escape plans.

Tool 15 (Military exercises)

・ Missile firing exercises into the waters around Taiwan.

Tool 19 (Promoting social unrest)

・ Generating social unrest by using criminal organizations to increase violent crimes, etc.

THD3: Disruption of cooperation between Taiwan, the U.S., and Japan

● Severing of submarine **cables**

Tool 1 (Physical operations against infrastructure)

・ Severing of submarine cables using fishing boats etc., to disrupt information sharing between Japan, the U.S., and Taiwan.

Coercion Phase (Hardline Approach)

*THC: Taiwan / Hardline / Coercion

THC1: Disruption of social and economic activities

● **Critical infrastructure failures**

Tool 9 (Cyber operations)

・ Failures related to air traffic control, railways, electricity, gas, water, logistics, and oil infrastructure.

● **Disruption of economic activity through military exercises**

Tool 15 (Military exercises)

・ China-Russia joint exercises in the Taiwan contiguous zone.
・ Establishment of legal basis for ship inspections.
・ Blockage of approach to Taiping Island.

● **Interference with economic activity**

Tool 6 (Undermining economy)

・ Severe restrictions on imports and exports, ban on visa issuance.
・ Forced landing of Taiwanese cargo planes in China.

THC2: Isolation of Taiwan's information transmission

● **Communication network disruption**

Tool 1 (Physical operations against infrastructure)

・ Severing of submarine cables and covert destruction of submarine cable landing stations by operatives to disrupt information transmission to the world.

Tool 9 (Cyber operations)

・ Cyberattacks on data centers.
・ Cyberattacks on communication networks.

Tool 40 (Electronic operations)

- Electronic jamming of satellite line.

THC3: Instigating civil war

Tool 14 (Paramilitary organizations (proxies))

- Pro-China proxy forces in Taiwan launch an armed uprising, creating a state of civil war.

THC4: Limited military intervention

● **Military intervention in domestic affairs**

Tool 13 (Armed forces conventional/sub-conventional operations)

- Provide military support upon request from pro-China forces (administration), and dispatch troops depending on the situation.

● **Missile attack on island areas**

Tool 13 (Armed forces conventional/sub-conventional operations**)**

- Launch missiles toward island areas (Pengjia Islet, etc.) to check the U.S. response.

Annex 7　Coaxing Approach Toward Japan (details)

Priming Phase (Decoupling Japan and Taiwan)

*JCP: Japan / Coaxing / Priming

JCP1: Intelligence activities

Tool 8 (Cyber espionage)

- Cyber intrusion without leaving traces, preparation to switch to attack when necessary (APT).

Tool 25 (Intelligence preparation)

- Explore events that could lead to division between Japan and Taiwan.
- Explore vulnerable points in critical infrastructure.

Tool 27 (Infiltration)

- Infiltration of personnel into government agencies, political parties, economic organizations, etc., and acquisition of collaborators.

JCP2: Weakening anti-China faction and cultivating pro-China faction

Tool 38 (Disinformation campaigns and propaganda)

- Spreading disinformation such as claims that anti-China factions in Taiwan are funded by the U.S. and that the majority of Taiwanese people want unification.

Tool 35 (Coercion of politicians and/or government)

- Applying various pressures on pro-Taiwan politicians.

JCP3: Hardline operations against Japan, including the economy

Tool 3 (Creating or exploiting economic dependencies)

- Strengthening China's dominance in the Asian economy and disrupting economic relations between Japan and other Asian countries.

Tool 38 (Disinformation campaigns and propaganda)

- Maintaining a tough stance on the Fukushima treated water issue.

Tool 11 (Territorial water violation)

- Escalating the Senkaku Islands issue by involving Taiwan.

JCP4: Intimidation through military exercises near the Nansei Islands

Tool 15 (Military exercises)

- Intensifying exercises near the Nansei Islands to intimidate.

Tool 38 (Disinformation campaigns and propaganda)

- Condemning Japan's militarization of the Nansei Islands.

JCP5: Communicating the narrative of unity between Mainland China, Taiwan, and Okinawa

Tool 31 (Creating confusion or a contradictory narrative)

- Spreading the narrative that China, Taiwan, and Okinawa have historically been united, and that only through unity can they prosper.

Destabilization phase (Decoupling Japan and Taiwan)

*JCD: Japan / Coaxing / Destabilization

JCD2: Operations to hinder strengthened Japan-Taiwan cooperation

● **Exclusion of Japan and the U.S. from Taiwan's economy**

Tool 6 (Undermining the target national economy)

- Applying pressure on Taiwanese, Japanese, and U.S. companies to regulate imports and exports.
- Imposing extensive restrictions on multinational corporations in Taiwan.

● **Promoting strengthened economic ties between Taiwan and China**

Tool 38 (Disinformation campaigns and propaganda)

- Reemphasizing trade with Taiwan and investment.
- Promoting the "peace framework," which emphasizes more autonomy than the "one country, two systems."

JCD3: Obstruction of communication between Japan and Taiwan

● **Communication disruptions between Japan and Taiwan**

Tool 1 (Physical operations against infrastructure)

- Severing submarine cables using fishing boats, etc. to disrupt information sharing between Japan and Taiwan.

● **Inducing Japan Coast Guard actions over the Senkaku Islands**

Tool 24 (Leveraging legal institutions)

- With the view that sovereignty over the Senkaku Islands belongs to Taiwan, provoking public opinion among Taiwan's anti-Japan factions by triggering Japan Coast Guard actions, thus decoupling Japan and Taiwan.

● **Spreading the rumor that Taiwan has no expectations of Japan**

Tool 38 (Disinformation campaigns and propaganda)

- Spreading the rumor that Taiwan has no expectations of Japan.

Coercion Phase (Decoupling Japan and Taiwan)

*JCC: Japan / Coaxing / Coercion

JCC1: Divisive operations against Japan and Taiwan's democratization forces

Tool 38 (Disinformation campaigns and propaganda)

- Spreading disinformation that "Taiwan is democratically moving toward unification."
- Spreading scandal disinformation about anti-China forces.

Tool 3 (Creating or exploiting economic dependencies)

- Offering economic benefits if Taiwan recognizes unification as a fact, or imposing sanctions if not.

Tool 9 (Cyber operations)

- Using bots and other means on social media to spread a tone that incites anti-Japanese sentiment within Taiwan and anti-Taiwan sentiment within Japan.

JCC2: Forming public opinion in favor of unification

Tool 38 (Disinformation campaigns and propaganda)

- Spreading disinformation that international opinion largely supports “Taiwan unification.”

Annex 8　Hardline Approach Against Japan (details)

Priming Phase (Decoupling Japan and the U.S.)

*JHP: Japan / Hardline / Priming

JHP1: Intelligence activities

Tool 8 (Cyber espionage)

・Cyber intrusion without leaving traces, preparation to switch to attack when necessary (APT).

Tool 25 (Intelligence preparation)

・Explore vulnerable points of the Japan Self-Defense Forces and U.S. military forces stationed in Japan.

・Explore vulnerable points in critical infrastructure.

Tool 27 (Infiltration)

・Infiltration of personnel into government agencies, political parties, economic organizations, etc. and acquisition of collaborators.

JHP2: Interference in Japan's security policy

Tool 31 (Creating confusion or a contradictory narrative)

・ Spreading the narrative that the Japan-U.S. Alliance contributes to war involvement without ensuring security for Japan.

Tool 38 (Disinformation campaigns and propaganda)

・ Spreading disinformation such as that the U.S. has decided not to intervene in a cross-strait conflict and that Taiwan will not resist China.

JHP3: Hardline operations against the U.S. and coaxing operations toward Japan

Tool 3 (Creating or exploiting economic dependencies)

・Offering economic incentives while making diplomatic overtures.

Tool 11 (Territorial water violation)

・Softening stance on the Senkaku Islands issue (e.g., regulating the operations of Chinese fishing boats).

JHP4: Military exercises in the waters around Japan

Tool 15 (Military exercises)

・Reducing exercises that pose a direct threat to Japan while conducting provocative exercises against U.S. Military Forces in the surrounding waters, creating a sense of anxiety among the Japanese public.

JHP5: Division of public opinion over Okinawa

● Generating distrust and anxiety toward U.S. Forces.

Tool 37 (Media control)

・Spreading biased information related to incidents and accidents involving U.S. Forces.

Tool 38 (Disinformation campaigns and propaganda)

・Spreading disinformation about crimes committed by U.S. military personnel, etc.

Tool 9 (Cyber operations)

・Using bots and other means on social media to spread anti-Okinawan sentiment in mainland Japan and anti-mainland Japan sentiment in Okinawa.

● **Emphasis on the historical connection between Okinawa and China**

Tool 31 (Creating confusion or a contradictory narrative)

・Spreading the narrative that China has historically been favorable toward Okinawa, and that Okinawa has instead been oppressed by Japan.

・Dramatically emphasizing the faults of the former Japanese and U.S. governments regarding the Battle of Okinawa.

Destabilization Phase (Decoupling Japan and the U.S.)

*JHD: Japan / Hardline / Destabilization

JHD1: Generating distrust in the government's administrative capabilities

● **Social anxiety due to limited social functioning, leading to distrust of the government**

Bank outages

Tool 9 (Cyber operations)

・ DDoS attacks making the website of banks inaccessible.

Tool 38 (Disinformation campaigns and propaganda)

・ Spreading disinformation such as that transactions with XX Bank are not possible.

Medical disturbances

Tool 9 (Cyber operations)

・ Medical anxiety and disorders due to disruptions to a medical institution's electronic medical records.

Tool 38 (Disinformation campaigns and propaganda)

・ Spreading disinformation about disruptions to medical institutions.

● **Generating distrust of the government regarding the protection of civilian ships**

Tool 11 (Territorial water violation (including EEZ))

・ Generating distrust of the government within Japan due to large numbers of fishing boats intruding into the EEZ, etc.

Tool 38 (Disinformation campaigns and propaganda)

・ Spreading fake images and other disinformation to generate distrust in Japan Coast Guard.

Tool 24 (Leveraging legal institutions)

・ Exploiting ambiguity between law enforcement and military activities.

JHD2: Evoking attention to the risks of the Japan-U.S. Alliance

● **Strengthening economic relations between Japan and China**

Tool 3 (Creating or exploiting economic dependencies)

・ Giving preferential treatment to Japan in terms of imports and investments and strengthening cooperation with Japanese companies.

● **Risk of Japan getting involved in a war**

Tool 15 (Military exercises)

・ Conducting missile launches and airstrike drills simulating attacks on U.S. military bases, publicizing the risks of war.

● **Risk of U.S.-China conflict**

Tool 15 (Military exercises)

・ By launching missiles over the Second Island Chain, China shows that it is willing to go to war with the U.S., and the risks of the U.S.-Japan Alliance are made known to the Japanese people.

JHD3: Obstruction of communication between Japan and the U.S.

● **Communication disruptions between Japan and the U.S.**

Tool 1 (Physical operations against infrastructure)

・ Severing submarine cables using fishing boats, etc. to disrupt information sharing between Japan and the U.S.

Coercion Phase (Decoupling Japan and the U.S.)

*JHC: Japan / Hardline / Coercion

JHC1: Divisive operations against Japan and the U.S.

● **Interference with Japan-U.S. information exchange**

Tool 1 (Physical operations against infrastructure)

・ Interfering with sensitive information exchange between Japan and the U.S. through communication disruptions (submarine cables, satellite communications).

Tool 40 (Electronic operations)

・ Using spoofed communications and other methods to create discrepancies between Japan and the U.S.

● **Interference with the operational capabilities of the Japan Self-Defense Forces and U.S. military bases in Japan**

・ Cyberattacks on Japan's critical infrastructure (electricity, gas, water, etc.) to disrupt the operational capabilities of the Japan Self-Defense Forces and U.S. military bases in Japan, which depend on it.

Tool 38 (Disinformation campaigns and propaganda)

・ Using disinformation to cause anxiety among residents near bases and the families of personnel of U.S. military bases in Japan.

JHC2: Building public opinion for non-intervention in Taiwan

Tool 38 (Disinformation campaigns and propaganda)

・ Spreading disinformation that "the unification faction has an overwhelming advantage in Taiwan."

JHC3: Delaying the recognition of an "Important Influence Situation," etc.

Tool 38 (Disinformation campaigns and propaganda)

・ Propaganda that the recognition of an "Important Influence Situation," etc. is an act of war against China

Annex 9 Relationship between China's Hybrid Warfare Methods Against Japan and Japan's Domains

Target Category	Tool	Japan's Domains Targeted by Cyberattacks												
		Diplomacy	Politics	Culture	Society	Law	Military & Defense	Space	Government	Infrastructure	Economy	Intelligence	Information	Cyber
JHP1 Intelligence activities	Tool 8 (Cyber espionage)	○	○				○			○	○	○		○
	Tool 25 (Intelligence preparation)	○	○				○			○	○	○		
	Tool 27 (Infiltration)	○	○				○				○	○		
JHP2 Interference in Japan's security policy	Tool 31 (Creating a narrative)	○	○	○	○	○	○						○	
	Tool 38 (Disinformation campaigns and propaganda)	○	○		○		○						○	
JHP3 Hardline against US; coaxing toward Japan	Tool 3 (Creating economic dependencies)	○	○								○			
	Tool 11 (Territorial water violation)	○	○				○		○					
JHP4 Military exercises in waters around Japan	Tool 15 (Military exercises)	○	○		○		○						○	
JHP5 Public opinion divided over Okinawa	Tool 37 (Media control)				○								○	
	Tool 38 (Disinformation campaigns and propaganda)			○	○								○	
	Tool 9 (Cyber operations)				○								○	○
	Tool 31 (Creating a narrative)		○	○	○								○	
JHD1 Generating distrust in the government's administrative capabilities	Tool 9 (Cyber operations)			○	○				○	○	○			○
	Tool 38 (Disinformation campaigns and propaganda)			○	○				○	○	○			
	Tool 11 (Territorial water violation (incl. EEZ))		○		○		○		○					
	Tool 24 (Leveraging legal institutions)		○			○			○					
JHD2 Evoking attention of risk of Japan-US Alliance	Tool 3 (Creating economic dependencies)	○	○								○		○	
	Tool 15 (Military exercises)	○	○		○		○						○	
JHD3 Disruption of communications between Japan and the US	Tool 1 (Physical operations (infrastructure))	○						○		○		○		
JHC1 Decoupling Japan and the US	Tool 1 (Physical operations (infrastructure))	○					○	○		○		○		
	Tool 40 (Electronic operations)						○	○				○		
	Tool 38 (Disinformation campaigns and propaganda)		○		○		○						○	
JHC2 Building public opinion in favor of non-intervention in Taiwan	Tool 38 (Disinformation campaigns and propaganda)	○	○		○								○	
JHC3 Delay in designation of Situation that Will Have an Important Influence on Japan's Peace and Security	Tool 38 (Disinformation campaigns and propaganda)		○		○	○	○						○	
JCP1 Intelligence activities	Tool 8 (Cyber espionage)	○	○								○	○		○
	Tool 25 (Intelligence preparation)	○	○								○	○		
	Tool 27 (Infiltration)	○	○								○	○		
JCP2 Weakening anti-China faction and cultivating pro-China faction	Tool 38 (Disinformation campaigns and propaganda)	○	○		○								○	
	Tool 35 (Coercion of government)		○						○					
JCP3 Hardline approach against Japan, including economy	Tool 3 (Creating economic dependencies)	○	○								○			
	Tool 38 (Disinformation campaigns and propaganda)	○			○								○	
	Tool 11 (Territorial water violation)	○	○		○		○						○	
JCP4 Threatening military exercises near the Nansei Islands	Tool 15 (Military exercises)	○	○		○		○						○	
	Tool 38 (Disinformation campaigns and propaganda)	○	○		○								○	
JCP5 Communicating the narrative of Mainland China-Taiwan-Okinawa unity	Tool 31 (Creating a narrative)			○	○								○	
JCD2 Operations to hinder strengthened Japan-Taiwan cooperation	Tool 6 (Undermining economy)	○	○								○			
	Tool 38 (Disinformation campaigns and propaganda)	○	○		○								○	
JCD3 Obstruction of Japan-Taiwan communications	Tool 1 (Physical operations (infrastructure)	○						○		○		○		
	Tool 24 (Leveraging legal institutions)	○	○			○	○		○					
	Tool 38 (Disinformation campaigns and propaganda)	○	○		○								○	
JCC1 Operations to divide Japan and Taiwan's pro-democracy forces	Tool 38 (Disinformation campaigns and propaganda)	○	○		○								○	
	Tool 3 (Creating economic dependencies)	○	○								○			
	Tool 9 (Cyber operations)	○	○	○	○								○	○
JCC2 Formation of public opinion in favor of unification	Tool 38 (Disinformation campaigns and propaganda)	○	○		○								○	

Source: Maritime Security Study Group, Nakasone Peace Institute
Note: Because tools are employed in different ways according to the phase and the objective, the same tool can be used in multiple domains.

Maritime Security Study Group Members

Chairman: Saito Takashi, Former Chief of Staff, Joint Staff, JSDF

Fukumoto Izuru, Former President, Japan Maritime Self-Defense Force Command and Staff College

Tokuchi Hideshi, Research Advisor, Nakasone Peace Institute; President, Research Institute for Peace and Security

Hirata Hidetoshi, Former Commander, Air Training Command, Japan Air Self-Defense Force

Matsumura Goro, Former Commanding General, Northeastern Army, Japan Ground Self-Defense Force

Nakamura Susumu, Senior Research Fellow, SFC Research Institute, Keio University

Sato Koichi, Professor, Oberlin University

Murakami Masatoshi, Associate Professor, Kogakkan University

Yamamoto Katsuya, Senior Research Fellow, Sasakawa Peace Foundation

Aizawa Riho, Research Fellow, National Institute for Defense Studies

Yamamoto MaximillianTakuma

Kawashima Takashi, Research Fellow, National Institute for Defense Studies

Takabatake Futoshi, Senior Research Fellow, Nakasone Peace Institute

Yasue Mariko, Senior Research Fellow, Nakasone Peace Institute

(honorifics omitted)