NPI

Nakasone Peace Institute

Research Report

FY2023 Maritime Security Study Group Report

Building Response Procedures and a Multilateral Joint Posture to Deter a Taiwan Contingency

Part 1: Analysis of the European Hybrid CoE Conceptual Model, Assumptions for Developing a Research Model, and Hybrid Threat Case Studies

Maritime Security Study Group

March 2024

中曽根平和研究所
Nakasone Peace Institute

Contents

Introduction

1 Research Outline

Over the three-year period from FY2023 to FY2025, the Maritime Security Study Group is working to develop a comprehensive checklist for addressing hybrid threats from People's Republic of China (PRC) that would likely be organized as a complex set of tools aimed at the unification of Taiwan. The Study Group will also propose measures to deter escalation to a full-fledged military invasion and examine a multilateral joint deterrence posture that puts the items on the checklist into practice.

Since the beginning of Russia's invasion of Ukraine, the possibility of an invasion of Taiwan by China has become a focus of attention, and many research institutes have been engaged in research on various scenarios and impacts related to a Taiwan contingency. Although some of these studies have focused on China's unification operations over the Taiwan front, many of them limit their analytic scope to certain areas, such as cyber and intelligence. As a result, studies into new domains, such as space and electromagnetic waves, where the arms race among major powers including Russia and China is significant, or economic and social aspects where so-called hybrid warfare could be widely deployed before the start of military aggression, remain scarce or are totally unreported. These gaps make it challenging to gain a good understanding of the overall picture of hybrid threats. Given the prolonged war in Ukraine and its serious impact on war casualties and the global economy, deterrence of the use of force will be the No. 1 priority for Japan's diplomacy in responding to a Taiwan contingency. At the same time, it is also important to be able to effectively address hybrid threats in gray zone situations. In this context, it is essential to systematically analyze hybrid threats in all domains, military and non-military, and to develop specific countermeasures.

In other words, deterring a Taiwan contingency must include not only directly preventing the use of force against Taiwan itself but also effectively dealing with hybrid threats at an earlier stage. Failure to do so would raise two risks. The first risk is that China would be allowed to achieve its objectives unilaterally while avoiding the use of force, and the second is allowing China to create an environment favorable to the use of force in its various forms. This study attempts to capture a broad view of a Taiwan contingency and will focus in particular on hybrid warfare response within that context, examining and analyzing the corresponding strategies.

Therefore, with the "40 tools of hybrid threat activity" and "13 affected domains" enumerated as a checklist in the Conceptual Model for Hybrid Threat Analysis said to have been used by the European Centre of Excellence for Countering Hybrid Threats (Hybrid

© Nakasone Peace Institute

The views expressed in this work are solely those of the author and do not necessarily reflect the views of Nakasone Peace Institute.

CoE) during Russia’s invasion of Ukraine, the Study Group will conduct a threat analysis pertaining to hybrid warfare against Taiwan. The applicability of the “40 tools of hybrid threat activity” to multiple scenarios and the specific cases that could be targets of activity in the “13 affected domains” will be verified. Through the verification, the Study Group will develop a unique framework specific to Taiwan, bearing in mind the differences in the security environment between Europe and East Asia (Figure 1). In this way, the specific threats that may arise in each domain of the framework are applied, organized, and analyzed to obtain an overall picture of the hybrid threat.

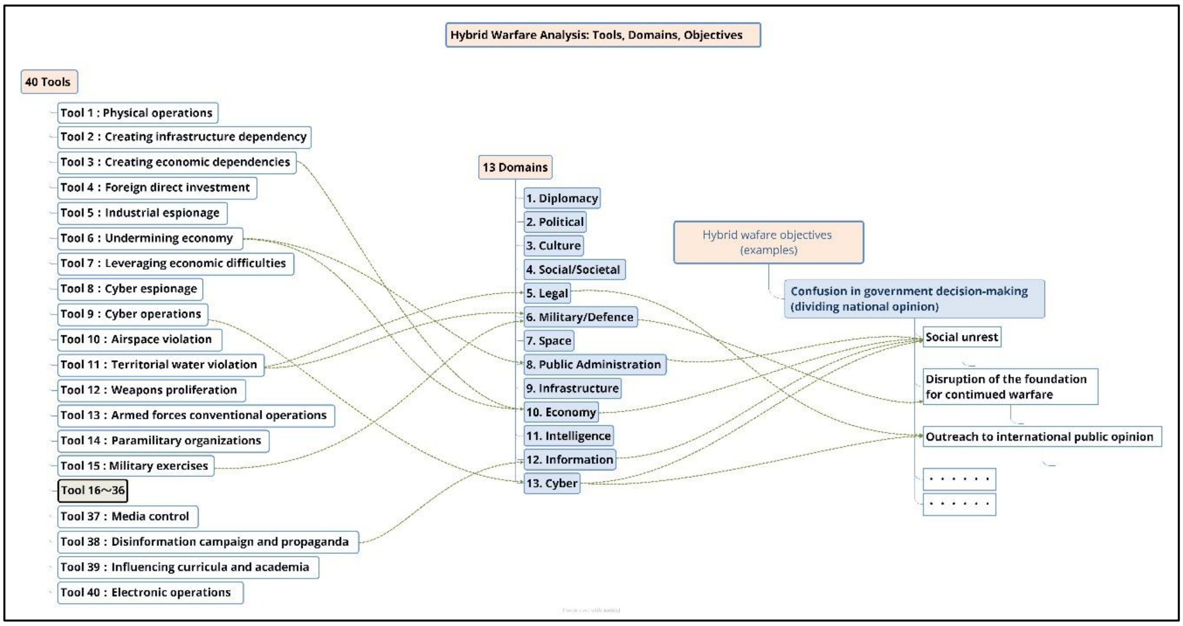
Moreover, the Study Group will submit a comprehensive policy proposal that can be adapted to a variety of situations including a method to utilize the above 40 tools to continuously monitor the situation together with a list of specific diplomatic and security response measures that Japan should undertake in the case that escalation in multiple domains is observed.

Furthermore, building on these response measures and the shared security interests and role-sharing with the United States and Australia as the primary partners, the Study Group will propose a competitive strategy in which Japan’s diplomacy would play a leading role in maintaining peace and stability in Northeast Asia.

2 FY2023 Research

The Study Group will apply the hybrid threat analysis framework to analyze how the 40 various tools (hereafter referred to as “tools”) of hybrid threat activity presented by Hybrid CoE intertwine and affect the target domains (hereafter referred to as “domains”). The study attempts to analyze the process by which these tools increase social unrest and disrupt or change the decision-making of the target government, which is considered to be one of the ultimate objectives of hybrid warfare. The analysis of the process will be based on specific cases to enhance understanding and visualization of the process to as great an extent as possible.

Figure 1 Hybrid Warfare Analysis: Tools, Domains, Objectives


Hybrid Warfare Analysis: Tools, Domains, Objectives
40 Tools
Tool 1 : Physical operations
Tool 2 : Creating infrastructure dependency
Tool 3 : Creating economic dependencies
Tool 4 : Foreign direct investment
Tool 5 : Industrial espionage
Tool 6 : Undermining economy
Tool 7 : Leveraging economic difficulties
Tool 8 : Cyber espionage
Tool 9 : Cyber operations
Tool 10 : Airspace violation
Tool 11 : Territorial water violation
Tool 12 : Weapons proliferation
Tool 13 : Armed forces conventional operations
Tool 14 : Paramilitary organizations
Tool 15 : Military exercises
Tool 16～36
Tool 37 : Media control
Tool 38 : Disinformation campaign and propaganda
Tool 39 : Influencing curricula and academia
Tool 40 : Electronic operations
13 Domains
1. Diplomacy
2. Political
3. Culture
4. Social/Societal
5. Legal
6. Military/Defence
7. Space
8. Public Administration
9. Infrastructure
10. Economy
11. Intelligence
12. Information
13. Cyber
Hybrid wafare objectives (examples)
Confusion in government decision-making (dividing national opinion)
Social unrest
Disruption of the foundation for contimued warfare
Outreach to international public opinion
・・・・・・
・・・・・・

Source: Prepared by the Maritime Security Study Group.

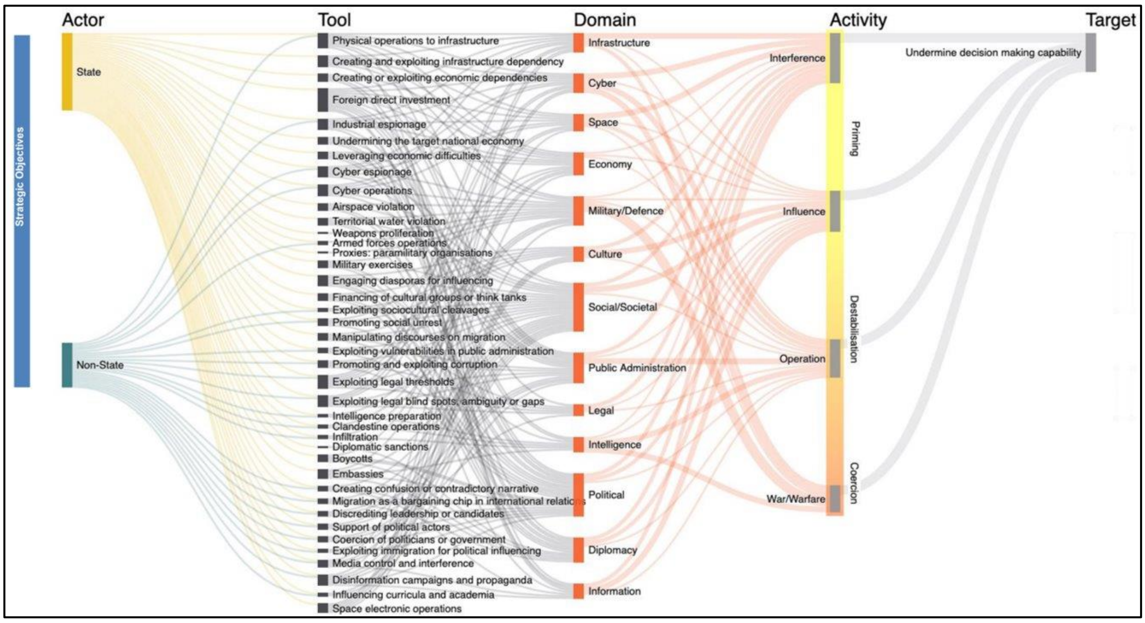
Section 1: Analysis of European Hybrid CoE Conceptual Model

During the 2014 Crimean crisis, Russia occupied and annexed Crimea almost bloodlessly, using irregular methods (blocking communication networks, spreading fake news, and using social networking service (SNS)) to manipulate public opinion prior to the military invasion by regular forces. A similar development was predicted when Russia launched its invasion of Ukraine in February 2022, but the hybrid warfare by Russia was not successful, and, in contrast to the invasion of Crimea, a military invasion of Ukraine was conducted. One possible factor that contributed to the difference in understanding the invasions in 2014 and 2022 is the “Conceptual Model for Hybrid Threat Analysis” (hereafter referred to as the “Conceptual Model”). The Conceptual Model was developed by Hybrid CoE, in cooperation with the Joint Research Centre of the European Commission, over a period of about two years starting in July 2018, and is believed to have been used to systematically understand the various events that occurred during Russia’s invasion in 2022. In this research, using this Conceptual Model as a reference, we first analyze the outline and concept of the Conceptual Model as follows.[1]

1 Overall Conceptual Model

The overall Conceptual Model for Hybrid Threat Analysis (Figure 2) is as follows:

Figure 2 Overall Conceptual Model for Hybrid Threat Analysis


Strategic Objectives
Actor
State
Non-State
Tool
Physical operations to infrastructure
Creating and exploiting infrastructure dependency
Creating or exploiting economic dependencies
Foreign direct investment
Industrial espionage
Undermining the target national economy
Leveraging economic difficulties
Cyber espionage
Cyber operations
Airspace violation
Territorial water violation
Weapons proliferation
Armed forces operations
Proxies: paramilitary organisations
Military exercises
Engaging diasporas for influencing
Financing of cultural groups or think tanks
Exploiting sociocultural cleavages
Promoting social unrest
Manipulating discourses on migration
Exploiting vulnerabilities in public administration
Promoting and exploiting corruption
Exploiting legal thresholds
Exploiting legal blind spots, ambiguity or gaps
Intelligence preparation
Clandestine operations
Infiltration
Diplomatic sanctions
Boycotts
Embassies
Creating confusion or contradictory narrative
Migration as a bargaining chip in international relations
Discrediting leadership or candidates
Support of political actors
Coercion of politicians or government
Exploiting immigration for political influencing
Media control and interference
Disinformation campaigns and propaganda
Influencing curricula and academia
Space electronic operations
Domain
Infrastructure
Cyber
Space
Economy
Military/Defence
Culture
Social/Societal
Public Administration
Legal
Intelligence
Political
Diplomacy
Information
Activity
Interference
Priming
Influence
Destabilisation
Operation
Coercion
War/Warfare
Target
Undermine decision making capability

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

[1] Takashi Kawashima, “*Haibriddo Kyoi Bunseki no Furemuwaku: Oshu Haiburiddo Kyoi Taisaku Senta no Konseputo Moderu o Tsujite* [A Framework for Hybrid Threat Analysis: Through the Conceptual Model of the European Centre of Excellence for Countering Hybrid Threats]” (Japanese), NPI Commentary, 2022.

The analytical framework for this Conceptual Model has four pillars: (1) actors, (2) tools, (3) domains, and (4) activities. The framework is outlined below.

2 Conceptual Model Framework

(1) **Actors**

Actors are divided into two categories: state actors and non-state actors. The term “state actors” here refers mainly to authoritarian states that are hostile to the democratic countries that make up the EU, NATO, etc. Maintaining the regime’s power and harboring a fear of democratic states tend to be the main characteristics of these states.[2] Russia, China, Iran, and North Korea are cited as specific examples, with Russia and China, in particular, identified as key actors in hybrid threat activity.[3]

A non-state actor is an entity that plays a part in international relations and that exercises sufficient power to interfere, influence, and cause change without any affiliation to the established institutions of a state. A characteristic feature is that states, through non-state actors, often conduct activities for hostile purposes against other states.[4] Representative examples include Hezbollah, Islamic State (IS), and Private Military Companies (PMCs).[5]

In addressing hybrid threat, besides identification of state and non-state actors, as mentioned above, it is important to **analyze the strategic objectives of the actors**.[6]

2) **Tools**

Tools are the methods used by state and non-state actors to exert hybrid threats on a target.[7] In the Conceptual Model, 40 tools are presented based on past cases. Actors combine these tools to generate hybrid threats.

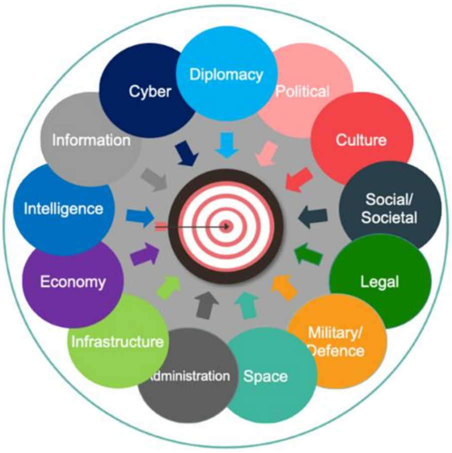
3) Domains

In the Japanese security context, the term “domains” is translated to “*ryoiki*” in Japanese, generally meaning “territory/sphere,” but here it means groupings of instruments of national power; in other words, a “domain” is any of a number of diplomatic, intelligence, military, economic or other national instrument of power that may be targeted by an actor conducting

[2] European Commission and 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 (last accessed May 1, 2022).
[3] Ibid. p. 16.
[4] Ibid. p. 22.
[5] Ibid. p. 16.
[6] Ibid. p. 15.
[7] Ibid. p. 33.

hybrid threat.[8] Actors target a domain with hybrid threats to ultimately achieve their goals. As shown in Figure 3, there are 13 domains listed that form politics, economics, and society, such as infrastructure and cyber, in addition to military/defense. Actors combine multiple tools belonging to each domain in the attempt to achieve their goals (center of figure).

Figure 3 Domains and Actors' Goals



Source: European Commission and Hybrid CoE, *The Landscape of Hybrid Threats: A Conceptual Model Public Version*, 2021, p. 27.

In this Conceptual Model, it is explicitly stated that currently there is no theoretical basis for grouping the domains: "there is no prevailing or universal approach to structuring instruments of national power" and that as an "open list," **review and revisions are required depending on each case**.[9]

- **Tools and affected domains of hybrid threat activity**

Table 1 below shows an indicative list of tools that can be used by a hostile actor to achieve its objective, together with the potentially affected domains.

[8] Ibid. p. 26.

[9] Ibid. pp. 26-27.

Table 1 List of Tools and Potentially Affected Domains

	Tool	Affected domains (underlines added by author for emphasis)
1	Physical operations against infrastructure	**Infrastructure**, Economy, Cyber, Space, Military/Defence, Information, Social/Societal, Public Administration
2	Creating and exploiting infrastructure dependency (including civil-military dependency)	**Infrastructure**, Economy, Cyber, Space, Military/Defence, Public Administration
3	Creating or exploiting economic dependencies	**Economy**, Diplomacy, Political, Public Administration
4	Foreign direct investment	**Economy**, Infrastructure, Cyber, Space, Military/Defence, 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/Defence, Public Administration
9	Cyber operations	**Infrastructure**, Space, Cyber, Social/Societal, Public Administration, Military/Defence
10	Airspace violation	**Military**/Defence, Social/Societal, Political, Diplomacy
11	Territorial water violation	**Military**/Defence, Social/Societal, Political, Diplomacy
12	Weapons proliferation	**Military**/Defence
13	Armed forces conventional/sub-conventional operations	**Military**/Defence
14	Paramilitary organizations (proxies)	**Military**/Defence
15	Military exercises	**Military**/Defence, 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/Defence, Culture, Social/Societal, Public Administration, **Legal**, Intelligence, Diplomacy, Political, Information
24	Leveraging legal rules, processes, institutions and arguments	Infrastructure, Cyber, Space, Economy, Military/Defence, Culture, Social/Societal, Public Administration, **Legal**, Intelligence, Diplomacy, Political, Information
25	Intelligence preparation	**Intelligence**, Military/Defence
26	Clandestine operations	**Intelligence**, Military/Defence
27	Infiltration	**Intelligence**, Military/Defence
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**, Information, 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**, Social/Societal

	political influencing	
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/Defence

Source: Prepared by the authors based on European Commission and Hybrid CoE, *The Landscape of Hybrid Threats: A Conceptual Model Public Version,* 2021, pp. 33-35.

The above Table 1 lists the tools used in past cases that Hybrid CoE has observed. Actors have used these tools to affect one or more domains or to target vulnerabilities in a domain. In addition to the effect on the domain directly targeted, there may be a "cascade effect" that impacts other related domains.[10] It is important to note that **just because there are indications of use of a tool listed in this table it does not necessarily mean that it is a hybrid threat.** For example, cyber operations may be conducted in conjunction with other methods as part of a hybrid threat activity or on their own.[11] When a hacker launches a cyberattack, it is essential to analyze whether it is related to actors with strategic objectives and whether the cyberattack works in conjunction with other tools used by that actor. Early prediction on the overall impact that could result from the combination of these tools is necessary.

4) Activities

The intensity of hybrid threat activity in which the various tools are used is **divided into the following three phases**.[12] The activities performed in each phase are organized by the Study Group as shown in Table 2 below.

The relationship between phases and activities in Table 2 is not completely fixed. It is thought that each hybrid threat activity using each tool will be combined to construct hybrid warfare suited to each phase. The "priming" phase consists mainly of interference and some influence, the "destabilization" phase is mainly influence and partly operation, and the "coercion" phase consists mainly of operation. The details of each phase are described below.

[10] Ibid. pp. 11-12.
[11] Ibid. pp. 32-33.
[12] Ibid. p. 10.

- **Priming phase**[13]

During the priming phase, the actor "interferes" with the target country with activities employing various tools. The actor's ultimate goal in this phase is to lead the target country to a situation in which it loses situational awareness and its leaders "voluntarily make harmful choices and decisions" in the actor's favor.[14] The next activity after "interference" is "influence."[15] Activities in this priming phase are difficult to immediately assess as hybrid threats and are ambiguous and unobtrusive. Therefore, in addressing hybrid threats it is critical to detect early signs by using the Conceptual Model and to predict the development of the situation, including cascading effects to other domains, by analyzing the actors' objectives.[16]

- **Destabilization phase**[17]

The destabilization phase is the stage in which the actor intensifies activities using various tools in each domain. Activities become overt and more aggressive and may involve multiple physical operations and violence, but the actors themselves are expected to conceal their involvement. The following scenarios are possible examples of the transition from the priming phase to the destabilization phase. When an armed conflict or skirmish occurs, reports of casualties and comments from bereaved families and injured soldiers, etc. are made public (interference). Then, as reports of rising casualties and comments from bereaved families increase, the anxiety of the families sending off soldiers increases (influence). Furthermore, as this unrest spreads throughout society, distrust of the government's response increases, and activities fueling demonstrations become more widespread. The goal of the actors in the destabilization phase is to destabilize the target country to a level at which it can be shaken and easily subdued. However, if the desired effect is not achieved, "the activity either reverts to priming to wait another and better opportunity, to tailor a better combination [of tools] or create new vulnerabilities…."

- **Coercion phase**[18]

This phase involves a "combination of covert and open military operations, combined with political and economic measures, subversion, information/disinformation operations and propaganda/fake news, the covert or open deployment of special forces," and military

[13] Ibid. pp. 37-40.
[14] Ibid. p. 37.
[15] Ibid. p. 38.
[16] Ibid. p. 5.
[17] Ibid. pp. 40-41.
[18] Ibid. pp. 41-42.

assistance to hostile forces within the target country. The ultimate objective is to compel or coerce strategic objectives on the target country. Operations using hybrid threat tools potentially targeting all domains are conducted. Limited military means such as terror, sabotage, subversion, guerrilla warfare, etc. are also utilized.

Furthermore, it is envisioned that a full-scale military war may be initiated with hybrid threat tools employed to take further advantage. In this sense, although war may also be described as an activity in the coercion phase, the use of hybrid threat tools in such a full-scale war should be discussed as part of a cross-domain operation within the military sphere. This research categorizes it as such and excludes it from the scope of this study.

© Nakasone Peace Institute

The views expressed in this work are solely those of the author and do not necessarily reflect the views of Nakasone Peace Institute.

Table 2 Relationship between Phases and Activities

Chronological phase	Hybrid threat activity
Priming	Interference = Use hybrid threat tools to disrupt the activities of the adversary in the target domain and lay the groundwork for destabilization.
Destabilization	Influence = Use hybrid threat tools to create destabilization and facilitate operations by influencing the activities of the adversary in the target domain. Operation = Exercise a combination of hybrid threat tools to coerce the adversary into taking a desired action and achieve an objective.
Coercion	War/warfare = Use hybrid threat tools in military warfare to gain an advantage in military warfare.

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

Section 2: Assumptions for Analysis Using the Conceptual Model

This section will first define hybrid warfare and then conduct an analysis using the Conceptual Model to discuss possible scenarios about the hybrid warfare that China could engage in its efforts to unify Taiwan.

1 Definitions of Hybrid Warfare

In recent years, the term "hybrid warfare" has become increasingly prevalent in security-related discussions. However, the meaning of this term varies according to the analyst, and therefore, the implications for security also differ according to the intended definition. To this end, this section will first clarify the definition of hybrid warfare in this report.

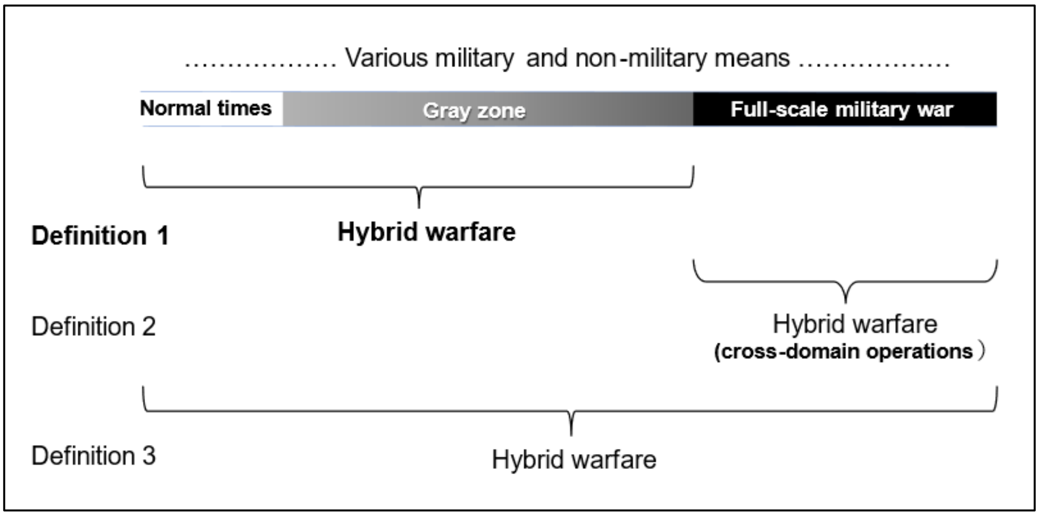
The term "hybrid" was originally used in thremmatology, or the science of breeding domesticated animals and plants, to refer to the crossing of two different lineages,[19] but the term has since evolved to describe the use of multiple means in combination, such as hybrid vehicles powered by both gasoline and electricity. Faithful to this etymology, the term "hybrid warfare" is thought to refer to a type of warfare that combines traditional military means of warfare with various non-military means of warfare. The views of many analysts are in general agreement on this point.

However, what varies greatly among analysts is how to position hybrid warfare in relation to full-scale military war. Full-scale military war here refers to high-intensity conflict between the regular forces of two or more states, each using their own firepower capabilities. As shown in Figure 4, the definition of hybrid warfare in relation to full-scale military war can be divided into three categories.

[19] A.S. Hornby, *Oxford Advanced Learner's Dictionary of Current English*, Oxford University Press, 1974, p. 425.

The views expressed in this work are solely those of the author and do not necessarily reflect the views of Nakasone Peace Institute.

Figure 4 Three Definitions of Hybrid Warfare



Source: Matsumura Goro, "The Essential Mechanism of Hybrid Warfare: 'Fight in the cognitive space' integrating military and non-military means to achieve the ultimate objectives," 2023, p. 2. *In this discussion, "hybrid warfare" is used as a synonymous term with "hybrid war."

The broadest definition shown here is Definition 3, which includes everything from fighting in normal times and gray zone situations that do not escalate to full-scale military war, as well as the use of various hybrid methods in full-scale military war. For example, Hirose Yoko, in her book *Haiburiddo Senso: Roshia no Atarashii Kokka Senryaku* [Hybrid Warfare: Russia's New National Strategy] (in Japanese) uses the term in this broad sense of hybrid warfare.[20] Definition 2, on the other hand, is based on the premise that the term "war" itself is used for high intensity armed conflicts. Therefore, the use of hybrid methods in situations that have not risen in intensity is not included within this category of hybrid warfare. From the same perspective, there are also those who argue that analyzing a category that consists of the framework of hybrid warfare is itself misleading. Instead, the perspective should be the use of cross-domain operations (sometimes referred to as all-domain operations or multi domain operations), within the framework of full-scale military war.[21] Advocates of this approach take the position that the essence of warfare will continue to be the use of force, primarily firepower, and that new and diverse methods will be employed most effectively within the realm of military war. Definition 1, in contrast, defines hybrid warfare as the use of various military and non-military means in situations that do not escalate to full-scale

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

[21] 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.

The views expressed in this work are solely those of the author and do not necessarily reflect the views of Nakasone Peace Institute.

military war, or in situations intentionally meant to avoid becoming a full-scale military war, to achieve an objective. This is a term used by many analysts.[22] Even if full-scale military wars do not completely disappear in the future, new methods of warfare that do not lead to full-scale military war will become important. In this context, clearly distinguishing between the concept of hybrid warfare as introduced in Definition 1 and full-scale military war would contribute to a more clear and precise discussion.

In this research, the focus will be on the emergence of states and non-state actors that aim to achieve objectives previously achieved through full-scale military war by various methods, including military and non-military means, without resorting to full-scale military war. Therefore, this report will use the term "hybrid warfare" in the sense of Definition 1 in order to examine hybrid methods as the main focus.

2 Possible Scenarios China could take for Hybrid Warfare Aimed at Unifying Taiwan

In the Taiwan presidential and legislative elections in January 2024, the Democratic Progressive Party's (DPP) Lai Chung-te was elected president, while in the Legislative Yuan, the DPP was relegated to the position of the second-largest party behind the Kuomintang (KMT). As a result, for the next four years, Taiwan will continue to experience a government divided between the Executive Yuan and Legislative Yuan.

From China's perspective, continuation of the DPP government signifies Taiwan's ongoing wariness toward China, a situation that presents challenges for China's efforts to promote pro-China sentiment and proceed with its unification agenda. On the other hand, the emergence of a government divided between the Executive Yuan and Legislative Yuan could lead to an intensification of political conflict in Taiwan in the future. This situation could create opportunities for China to exploit.

Taking into account this political situation in Taiwan, the following two scenarios could possibly be used by China to launch hybrid warfare aimed toward Taiwan unification in the future without reaching the threshold of a full-scale military invasion.

(1) Hardline approach

The hardline approach scenario would involve China's use of various methods to intensify political conflict within Taiwan and create extreme political instability. In such a scenario,

[22] In Junjiro Shida, *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. 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).

pro-China factions could resort to civil war to seize power and then request that China send in security forces or military troops to thereby achieve de facto unification.

If this approach is taken, various tools of hybrid threat activity would be used against Taiwan to achieve the following objectives in each phase.

- **Priming phase**

-Inducement of escalation of pro-China and anti-China confrontation
-Undermining of economic activities, etc., and creating social dissatisfaction and unrest
-Decline in government credibility
-Cultivation of pro-China puppet forces (covert infiltration operations until needed without revealing them publicly)

- **Destabilization phase**

-Promotion of social unrest originating from disruption of social and economic activities
-Weakening of the government's administrative and security capacity
-Manufacture of domestic dissent, inciting violence, etc.
-Preparation of puppet force (including within the Taiwan military)
-Promotion of distrust of the U.S.

- **Coercion phase**

-Paralysis of various functions, etc., and loss of government authority
-Establishment of pro-China illegitimate government by puppet forces
-Creation of a state of civil war, shaping of public opinion calling for assistance from China
-Military intervention in stages (escalating from covert to open)
-Manipulation of the international situation that does not allow U.S. intervention

(2) Conciliatory approach

The conciliatory approach scenario involves increasing Taiwan's dependency on China, mainly in economic terms, and creating a situation in which Taiwan's economy could not exist without China. If China succeeds in raising the momentum toward economic benefits to overcome resistance in Taiwan to the one country, two systems idea, it is possible that, rather than utilizing a confrontational carrots and sticks tactic to escalate internal division within Taiwan, China could take a conciliatory approach in an attempt to guide Taiwan as a whole in a pro-China direction. This approach would involve showcasing benefits, including false promises, while simultaneously making known the risks of not complying.

The goals for the use of hybrid methods against Taiwan at each phase of the process could be as follows.

- **Priming phase**

-Cultivation of pro-China sentiment at the grassroots (including information manipulation)
-Strengthening interdependence through trade, investment, etc. between China and Taiwan

The views expressed in this work are solely those of the author and do not necessarily reflect the views of Nakasone Peace Institute.

-Trade and investment support for developing countries, etc.
-Cultivation of pro-China political forces (including covert infiltration operations, funding, etc.)
-Promoting skepticism and distrust towards democracy

- **<u>Destabilization phase</u>**

-Open and covert interference in elections
-Discrediting anti-China political forces
-Open support for pro-China political forces (economic and diplomatic support as “carrots”)
-Fostering distrust of the U.S., Japan, etc., and creating diplomatic friction and confrontation
-Interference in trade, investment, etc. with countries in conflict with China

- **<u>Coercion phase</u>**

-Crafting the establishment of a government that advocates unification with China
-Support for the suppression of anti-China forces in Taiwan
-Formation of international public opinion in favor of absorption and unification

The difference between the two approaches is that the hardline approach employs a hybrid strategy of both carrots and sticks simultaneously to exert pressure on the Taiwan government to create intense confrontation, including not ruling out armed conflict in Taiwan. On the other hand, the conciliatory approach aims to present exaggerated benefits and to mislead the Taiwanese people into believing that not aligning with China involves risks, thereby steering Taiwan as a whole toward a pro-China direction.

Regardless of the approach China takes, it is expected that Taiwan’s political system will always be affected by China’s use of hybrid methods. In the priming phase, depending on the success or failure of the approach and the global political and economic situation at the time, there may be a shift back and forth between the two approaches. If Taiwan sways in favor of China, China might take a more conciliatory approach and, conversely, China might take a more hardline approach if the situation were to swing in the opposite direction. If China foresees success in either direction, it is believed that hybrid warfare would escalate from the destabilization phase to the coercion phase, becoming more intense.

Furthermore, if despite China’s taking a hardline approach and proceeding to the coercion phase, even leading to the deployment of the People’s Liberation Army, establishing a pro-China regime takes too long, the possibility of a shift from hybrid warfare to a full-scale military invasion cannot be ruled out.

As this possibility suggests, whether China adopts a hardline approach or a conciliatory approach in the future is likely to change as the situation evolves. It is important to recognize here that the objectives of China’s hybrid warfare against Japan may vary between a hardline approach and a conciliatory approach.

The views expressed in this work are solely those of the author and do not necessarily reflect the views of Nakasone Peace Institute.

In the case of a hardline approach, with the eventual possibility of a full-sale military invasion in mind, the primary objective would be to thwart U.S. military intervention, and, when necessary, drive a wedge between Japan and the United Stares to prevent cooperation between Japan and U.S. military action. This could involve using various hybrid methods, possibly involving Japan directly, to achieve these objectives.

In contrast, in the case of the conciliatory approach, hybrid methods may be used to create distrust in Taiwan toward both Japan and the U.S. Rather than causing division between Japan and the U.S., the aim may be to create a sense of skepticism towards supporting Taiwan in Japan and in the United States so that Taiwan would be isolated.

As mentioned above, China's options for Taiwan are thought to actually fluctuate between a hardline approach and a conciliatory approach. In this research, however, in order to clarify the characteristics of the case in which a hardline approach is adopted and the case in which a conciliatory approach is adopted, the Study Group will make a distinction between the two approaches for future discussion.

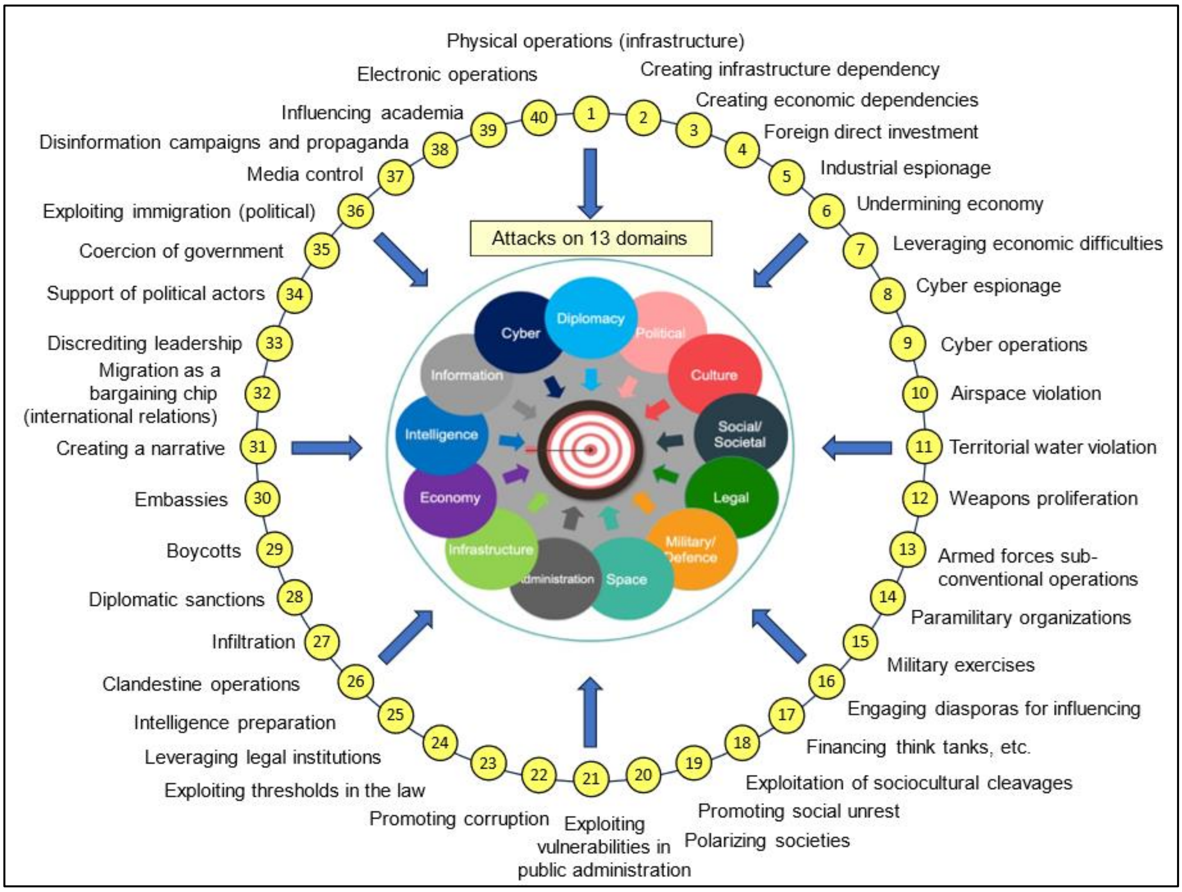
Section 3: Methods and Activities and Case Studies

Based on the 40 tools presented in the Conceptual Model, the methods and activities that could be implemented in response to a Taiwan crisis were examined with reference to past cases. These data are compiled in a separate casebook.

Since the "methods" and "activities" identified are expected to become important elements in the process of deepening hybrid warfare study in the future, the Study Group has selected examples from the casebook and included them in this report to enhance the visualization of hybrid warfare.

In the process of creating the casebook, in our overview of Japan's strategic environment, the Study Group questioned whether these 40 tools were sufficient and whether there are any mismatches. Although the methods and activities derived from the tools are still incomplete, we believe that the methods and activities will be helpful in grasping the overall picture of hybrid warfare.

Figure 5 Example of Methods and Activities (excerpted from the casebook)



Source: Prepared by the Maritime Security Study Group.

1 Physical operations against infrastructure

Tool: 1-1	
Method	Fishing boats, surveying vessels, merchant vessels, submarines, unmanned air vehicles (UAVs)
Activity	Cutting submarine electric cables

2 Creating and exploiting infrastructure dependency (including civil-military dependency)

Tool: 2-1	
Method	Creating dependency on energy supply (electricity, natural gas, oil)
Activity	Exploiting vulnerability from dependency on energy supply

3 Creating or exploiting economic dependencies

Tool:3-1	
Method	Creating economic dependencies
Activity	Promoting, restricting, or swaying economic activity and expanding one’s influence

4 Industrial espionage

Tool: 5-1	
Method	Cyberattack
Activity	Exploiting sensitive information such as advanced technology through cyberattacks

6 Undermining the opponent’s national economy

Tool: 6-1	
Method	Regulation by government and other public agencies
Activity	Import and export restrictions (strategic mineral resources, agriculture, forestry and fisheries resources)

9 Cyber operations

Tool: 9-1	
Method	Cyberattacks on financial institutions
Activity	Financial transaction failures

11 Territorial water violation (including exclusive economic zone (EEZ))

Tool:11-1	
Method	Government ships (including warships)
Activity	Repeatedly violating territorial waters and attempting to make territorial claims a fait accompli

14 Paramilitary organizations (proxies)

Tool: 14-1	
Method	China Coast Guard (CCG) vessel
Activity	Interference with vessel activities

15 Military exercises

Tool: 15-1	
Method	Preparation and execution of military exercises
Activity	Military threat

18 Exploitation of sociocultural cleavages (ethnic, religion and culture)

Tool: 18-1	
Method	Exploitation of the sociocultural cleavages
Activity	Exploiting contradictions regarding social superiority (discrimination) that come from historical circumstances

20 Manipulating discourses on migration to polarize societies and undermine liberal democracies

Tool: 20-1	
Method	Spreading disinformation and fake news
Activity	Spreading disinformation and exaggerated news reports about immigrants, promoting unrest and hostility. This activity promotes conflict within society and undermines liberal democracies.

22 Promoting and exploiting corruption

Tool: 22-1	
Method	Corruption against military personnel
Activity	Acquisition of military intelligence

23 Exploiting thresholds, non-attribution, gaps and uncertainty in the law

Tool:23-1	
Method	Influence on issues of legal interpretation that divide national opinion (e.g., survival-threating situation)
Activity	Delaying decision-making as a nation

26 Clandestine operations

Tool: 26-1	
Method	Clandestine operations targeting Taiwan's military bases
Activity	Exploring vulnerable points in Taiwan's armed forces

27 Infiltration

Tool: 27-1	
Method	Leveraging a network of operatives
Activity	Promoting social unrest and dividing national opinion

28 Diplomatic sanctions

Tool: 28-1	
Method	Diplomatic pressure on the countries concerned to prevent them from recognizing the target country as a state or building an alliance
Activity	International isolation of the target country

29 Boycotts

Tool: 29-1	
Method	Boycotts from recognition of state or alliance building
Activity	International isolation of the target country

30 Embassies

Tool: 30-1	
Method	Exploiting extraterritoriality of embassies
Activity	Exploiting as a base for various hybrid threat activities

31 Creating confusion or a contradictory narrative

Tool: 31-1	
Method	Transmitting convenient narratives by public organizations
Activity	Mixing lies and unilateral claims with historical facts

32 Migration as a bargaining chip in international relations

Tool: 32-1	
Method	Migration as a bargaining chip in international relations
Activity	Promoting public anxiety and discontent

33 Discrediting leadership and/or candidates

Tool: 33-1	
Method	Revealing scandals
Activity	Revealing scandals and discrediting politicians and others

34 Support of political actors

Tool: 34-1	
Method	Advertising and propaganda
Activity	Using disinformation and propaganda to deliberately manipulate domestic public opinion in favor of a particular political actor

35 Coercion of politicians and/or government

Tool: 35-1	
Method	Bribes (financial assistance)
Activity	Bribing (funding) politicians and government officials to influence policy and decision-making accordingly

37 Media control and interference

Tool: 37-1	
Method	International media acquisitions and influence
Activity	Acquiring overseas media companies and publishers and using their influence through advertising and investment to spread one's own country's message

38 Disinformation campaigns and propaganda

Tool: 38-1	
Method	Creating massive fake accounts and explosively spreading disinformation through SNS social media
Activity	Spreading disinformation through SNS social media

40 Electronic operations (GNSS jamming and spoofing)

Tool: 40-1	
Method	Interception of cell phone location information (GPS) and call content
Activity	Identifying attack targets and gathering information

Conclusion

In FY2023, the Study Group conducted the following research activities:

- Analysis of the Conceptual Model setting the guidance of this research project;
- Organization of the concept of hybrid warfare as a baseline for the Study Group's own conceptual model related to a possible Taiwan crisis; and,

- With reference to the 40 tools introduced in the Conceptual Model, extraction of activities using tools and past cases and their compilation into a casebook.

In FY2024, the Study Group will analyze how the phases (stages of escalation) of methods and activities and “Possible Scenarios China could take for Hybrid Warfare Aimed at Unifying Taiwan” obtained in the process of compiling the casebook intertwine. Based on that analysis, an original conceptual model will be developed. This conceptual model will encompass hybrid threats directed toward Japan and the United States (including other countries in what is referred to as a maritime alliance, as necessary) with Taiwan as the focal point.

In the final fiscal year, the Study Group will conduct research on how to deter and address hybrid threats multilaterally based on the conceptual model.

© Nakasone Peace Institute

The views expressed in this work are solely those of the author and do not necessarily reflect the views of Nakasone Peace Institute.

Maritime Security Study Group

Members (honorifics omitted)

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

Yoshida Yukari, Senior Fellow, National Institute for Defense Studies

Kawashima Takashi, Senior Research Fellow, Nakasone Peace Institute

Yasue Mariko, Senior Research Fellow, Nakasone Peace Institute

© Nakasone Peace Institute

The views expressed in this work are solely those of the author and do not necessarily reflect the views of Nakasone Peace Institute.