NPI Research Note

September 1, 2024

Evaluating the Applicability and Challenges of the Conceptual Model for Hybrid Threat Analysis for Deterrence of a Taiwan Contingency

Kawashima Takashi
Senior Research Fellow, NPI

Introduction

The purpose of this article is to examine and assess the significance and challenges associated with applying the Conceptual Model for Hybrid Threat Analysis to China's hybrid warfare against Taiwan and of utilizing it as a model to deter a Taiwan contingency. The model was developed and reportedly used by the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) in analyzing Russia's invasion of Ukraine.

Russia's invasion of Ukraine has elucidated three key lessons for deterring a full-scale military invasion: (1) the importance of preventing invasion by strengthening deterrence (defense buildup), (2) the need to prepare for irrational decision-making, and (3) the importance of addressing combined activities by military and non-military means, what is referred to as hybrid warfare.

Since the beginning of Russia's invasion of Ukraine, there has been increasing attention on the possibility of an invasion of Taiwan by China with many research institutes and researchers analyzing various scenarios and impacts related to a Taiwan contingency. When applying these studies to the lessons learned from Russia's invasion of Ukraine, the following observations are revealed.

Regarding item (1), the importance of preventing invasion by strengthening deterrence (defense buildup), an analysis based on a comparison of military power of the U.S., China, and Taiwan shows that China's military power has an overwhelming advantage over that of Taiwan in terms of the performance and quantity of troops and equipment.[1] In terms of the U.S. and China's military power, China surpasses the U.S. in ground forces,[2] and, in terms of naval power, the People's Liberation Army (PLA) Navy possesses more warships than the United States Navy and is even considered to be the largest naval force in the world.[3] However, in terms of air power, the U.S. holds a superior

[1] Japan Ministry of Defense, *Reiwa 6-nen-ban Boei Hakusho* [Defense of Japan (Annual White Paper) 2024] (Japanese), Nikkei Printing Inc., 2023, pp. 102-104.
https://www.mod.go.jp/en/publ/w_paper/wp2024/DOJ2024_EN_Full.pdf (English)
[2] Ibid. p. 42.
[3] Ibid. p. 72.

position.[4] Reports by research institutes in the U.S., Center for Strategic and International Studies (CSIS),[5] and Japan, the Sasakawa Peace Foundation[6] and the Japan Forum for Strategic Studies (JFSS)[7] highlight the challenges that Japan and the U.S. would face in the event of a Taiwan contingency. They also point out the enormous damage that such a contingency would have on Japan, the United States, and China, resulting in long-term negative economic impact.[8]

Therefore, taking into account the status of U.S., China, and Taiwan military power, together with the reports from the research institutes, it is difficult to expect that there is an overwhelming military deterrent effect by Taiwan and the U.S. that would prevent an invasion aimed at Taiwan unification by China. On the other hand, from the perspective that such an invasion would cause enormous damage to both China and Taiwan/U.S., there is a potential deterrent effect in the sense of dissuading both sides from resorting to the use of force.

Regarding item (2), the need to prepare for China's irrational decision-making, in March 2021, then Commander Philip Davidson of the U.S. Indo-Pacific Command referred to the "possibility of China's military invasion of Taiwan within six years."[9] In addition, in October 2022, at the National Congress of the Chinese Communist Party (CCP), the Xi Jinping regime reiterated its positioning of Taiwan as a core interest and declared its commitment to achieving Taiwan's unification.[10] While expressing its intention to pursue peaceful unification, China has clearly pledged it would never renounce the use of force. In response to these facts, many experts considering various domestic factors in China are of the opinion that there are no immediate signs of a Taiwan contingency.[11] However, China's decision-making, especially in the case of a declaration of independence by Taiwan (i.e., the dissolution of the Republic of China, which governs Taiwan, and the establishment of the

---

4 Ibid. p. 42.

5 Mark F. Cancian, Matthew Cancian, and Eric Heginbotham, *The First Battle of the Next War: Wargaming a Chinese Invasion of Taiwan*, Center for Strategic and International Studies (CSIS), 2023. https://www.csis.org/analysis/first-battle-next-war-wargaming-chinese-invasion-taiwan (accessed August 8, 2024).

6 The Sasakawa Peace Foundation and The Heritage Foundation, "Report on FY2022 TTX (Table Top Exercise) Taiwan Contingency Scenario: Escalation from Low-Intensity Hybrid Warfare," 2023. https://www.spf.org/japan-us-alliance-study/en/global-data/user17/20240328112121392.pdf (last accessed August 8, 2024).

7 Japan Forum for Strategic Studies (JFSS), "*Dai-3-kai Seisaku Simyureshon no Seika Gaiyo 'Tettei Kensho: Shin-senryaku 3-bunsho to Taiwan Kiki' — 2027-nen ni Muketa Kadai* — [In-depth Review: Three New Strategic Documents and the Taiwan Crisis," a summary of the results of the third policy simulation — Challenges for 2027 —]" (Japanese), 2023. https://www.jfss.gr.jp/taiwan_study_group/ (last accessed August 8, 2024).

8 Mark F. Cancian, Matthew Cancian, and Eric Heginbotham, op. cit., pp. 142-145.

9 "'*Chugoku, 6-nen inai ni Taiwan Shinko no Osore' Bei Indo-Taiheiyo Gunji Shireikan* ['China could invade Taiwan within the next six years,' U.S. Indo-Pacific Commander]" (Japanese), AFP, March 10, 2021.

10 "Full text of the report to the 20th National Congress of the Communist Party of China," Xinhua, 2022, pp. 44-45.

11 "NPI Webinar: Birth of Taiwan's New Lai Ching-te Administration and Future U.S.-China-Japan-Taiwan Relations," May 31, 2024.
Moderator: Shin Kawashima, Executive Director of Research, Nakasone Peace Institute.
Panelists: Yasuhiro Matsuda, Professor, University of Tokyo; Madoka Fukuda, Professor, Hosei University / Visiting Fellow, Nakasone Peace Institute.
https://npi.or.jp/event/2024/06/05101818.html (Japanese) (last accessed August 8, 2024).

Republic of Taiwan or the State of Taiwan[12]), is unknown. For this reason, it is necessary to prepare for the possibility that, given the active operations of the People's Liberation Army (PLA), an unintended accidental clash could develop into a serious armed conflict.

Regarding item (3), the importance of addressing combined activities by military and non-military means (hybrid warfare), the author notes the following. In 1999, two colonels in China's People's Liberation Army Air Force, Qiao Liang and Wang Xiangsui, published a co-authored book, entitled *Chogensen: 21-seiki no 'Atarashii Senso'* [Unrestricted Warfare: The 'New Warfare' of the 21st Century]. The book presented the concepts of trade warfare, financial warfare, terror warfare, ecological warfare, smuggling warfare, media warfare, drug warfare, cyber warfare, technical warfare, resource warfare, and economic assistance warfare.[13] In 2003, the CCP revised the "People's Liberation Army Political Work Regulations" and stated that China would "develop public opinion, psychological, and legal warfare and disintegrate the enemy forces."[14] Furthermore, in 2019, for the first time, the PLA's perception of war as "Intelligentized Warfare" was presented.[15]

Due to the variables including China's strategic vision combining military and non-military means, the strengthening of deterrence by Japan and the U.S., as well as the possibility of China's irrational decision-making mentioned discussed above, China may not proceed with the decision to launch a full-scale military invasion against Taiwan. However, it can be said that hybrid warfare aimed at achieving China's objectives while avoiding the costs and damage of a military invasion has already begun.

Furthermore, while many experts indicate a high probability of the use of hybrid warfare, such as information warfare, psychological warfare, and cyber warfare in the event of a Taiwan invasion by China,[16] there is also a possibility that other new tools beyond these may be used.

---

[12] Yoshiyuki Ogasawara, "*Shitteiruyode Shiranai 'Taiwan Dokuritsu' no Shin no Imi* [The True Meaning of 'Taiwan Independence' as You May Know but Don't Know]," Toyo Keizai Online, https://toyokeizai.net/articles/-/681217 (Japanese) (last accessed August 8, 2024).
The article lays out the following issues regarding "Taiwan independence."
- Taiwan has a well-established rule of law, and even if the current president and government of Taiwan were to declare independence, there would be no grounds for it and nothing would change.
- In order for Taiwan to achieve independence, a new constitution must be enacted, which requires an amendment process to the current Constitution of the Republic of China. The conditions for constitutional amendment are that three-fourths of the members of the Legislative Yuan must be present, and the proposed amendment must be approved by three-fourths of those present. Thereafter, a majority of voters must approve the amendment in a public referendum (national referendum).

[13] Qiao Liang (author), Wang Xiangsui (author), Shinnosuke Sakai (editorial supervisor), *Chogensen: 21-seiki no 'Atarashii Senso'* [Unrestricted Warfare: 'New Wars' in the 21st Century] (Japanese), KADOKAWA, 2020, p. 205.

[14] *Zhongguo renmin jiefangjun wuqi zhuangbei guanli tiaoli* [Regulations on the Administration of Weaponry of the People's Liberation Army of China] (January 2003) https://www.gov.cn/test/2005-06/28/content_10543.htm (Chinese) (last accessed August 8, 2024).

[15] Li Minghai, "*Shi shenme zai tuidong zhanzheng xiang zhineng hua yanbian* [What is driving the war to become intelligent?]" (Chinese), *Jiefangjun Bao* [PLA Daily] (November 6, 2018).

[16] Jun Osawa, "*Taiwan Yuji to Haiburiddo Senso* [Hybrid warfare in a Taiwan contingency]," International Information Network Analysis IINA Sasakawa Peace Foundation, https://www.spf.org/iina/en/articles/osawa_01.html (last accessed August 8, 2024); Kazuhisa Ogawa, *Nihonjin ga shiranai taiwan yuji* [A Taiwan Contingency that Japanese Do Not Know] (Japanese),

In order to grasp and address the overall picture of these threats, it is necessary to have a perspective and framework for comprehensive and combined analysis of the various tools of hybrid threat activity by military and non-military means that China could use to unify Taiwan. The "Conceptual Model for Hybrid Threat Analysis" of the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) categorizes and visualizes past cases of hybrid threats involving authoritarian states, including Russia, China, and Iran, and organizes hybrid threat activity into 40 tools, making it possible to comprehensively and thoroughly analyze hybrid warfare. Additionally, the model can simulate the possible impacts of these various tools of hybrid threat activity on multiple domains and estimate their combined effects.

The significance of utilizing this model is that it provides a basis for anticipating the overall picture of hybrid threats posed by China aimed at the unification of Taiwan and for developing countermeasures to prevent, as early as possible, the situation from escalating. For this reason, this research is positioned as a foundational study for deterring a Taiwan contingency. However, since the model was created based on the assumption that past or ongoing hybrid threats will be analyzed, it is necessary to identify and resolve challenges related to analyzing future hybrid threats.

Therefore, to evaluate the applicability and challenges of utilizing the Conceptual Model for Hybrid Threat Analysis for the deterrence of a Taiwan contingency, this article first defines "hybrid warfare," "hybrid threats," and "deterrence of a Taiwan contingency" as the scope of the study in Section 1. Section 2 outlines the Conceptual Model for Hybrid Threat Analysis and describes its characteristics. Section 3 organizes the challenges of applying the model to a Taiwan contingency. Section 4 organizes the relationship between the Conceptual Model and China's strategies using military and non-military means, etc., and verifies the usefulness of the Conceptual Model.

Bungeishunju Ltd., 2024, pp. 210-211; Kenji Minemura, *Taiwan Yuji to Nihon no Kiki* [Taiwan Contingency and Japan's Crisis] (Japanese), PHP Institute, Inc., 2024, pp. 230-238, etc.

1. Scope of this study

(1) Demarcation by the definition of hybrid warfare and hybrid threat

(a) Hybrid warfare

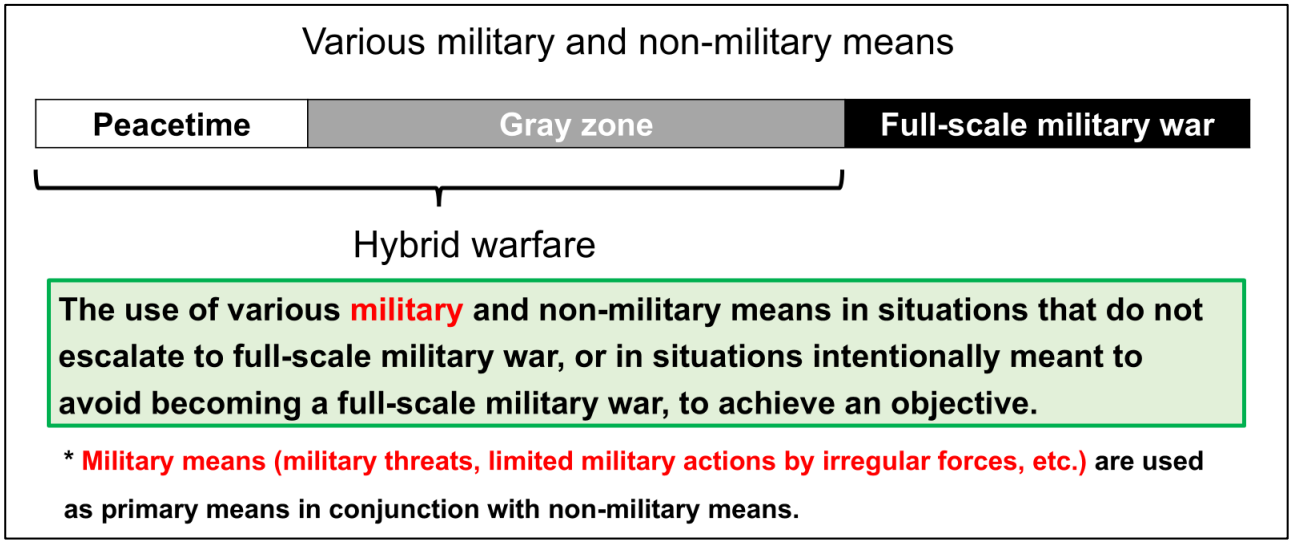

Figure 1 Definition of Hybrid Warfare in this Study
Source: Prepared by the author based on Matsumura Goro, "The Essential Mechanism of Hybrid Warfare: 'Fight in the cognitive space' integrating military and non-military means to achieve the ultimate objectives," Nakasone Peace Institute, 2023, p. 2.

Since the theme of this study is the deterrence of a Taiwan contingency, as shown in Figure 1, the author uses the definition of hybrid warfare as "the use of various military and non-military means in situations that do not escalate to full-scale military war, or in situations intentionally meant to avoid becoming a full-scale military war, to achieve an objective."

In this definition, emphasis is placed on the assumption that the subject of analysis has the intention of avoiding a full-scale military invasion. The reason for this assumption is that even in cases where a full-scale military invasion is planned from the outset and military and non-military means (cyberattacks, etc.) are used to facilitate the invasion, in practice, similar actions are taken. However, in a case in which a military invasion is planned, the situation would be positioned as a "cross-domain operation" and the response focuses on deterrence through the buildup of military power. For this reason, it falls outside the scope of this study.

(b) Hybrid threat

While hybrid threats involve both military and non-military means, conventional operations conducted by regular forces are excluded from the definition of hybrid threats.

(2) Demarcation by perspective of invasion and deterrence by military and non-military means

In the security field, "deterrence" generally refers to the prevention of military invasion before it occurs. Types of deterrence corresponding to different tools employed for invasion can be outlined as follows.

First, since military invasions have a clear starting point, it is possible to deter them (or not allow them to start) through the buildup of military power. On the other hand, hybrid warfare, which involves a complex combination of diverse military and non-military tools, has an unclear starting point, generally making deterrence difficult to achieve. For this reason, detecting signs of hybrid warfare and taking response measures to prevent the achievement of the actor's objectives are key measures for deterrence.

Based on the above nature of the relationship between the tools of invasion and deterrence, the deterrence of a Taiwan contingency in this study refers to "various measures taken at as early a stage as possible to stop situations from escalating in order to prevent (deter) China from annexing Taiwan through hybrid warfare, in a situation short of a full-scale military war," while also considering deterrence against a transition to a full-scale military invasion.

In the next section, from the viewpoint that early detection of signs of hybrid threats and rapid and appropriate responses together with strengthening of resilience are key to preventing actors from achieving their objectives in hybrid warfare as defined in item (1) above, the author will examine analytical procedures for hybrid threats using the Conceptual Model.

2. Overview of the Conceptual Model for Hybrid Threat Analysis

The overall picture of the Conceptual Model for Hybrid Threat Analysis is shown in Figure 2.

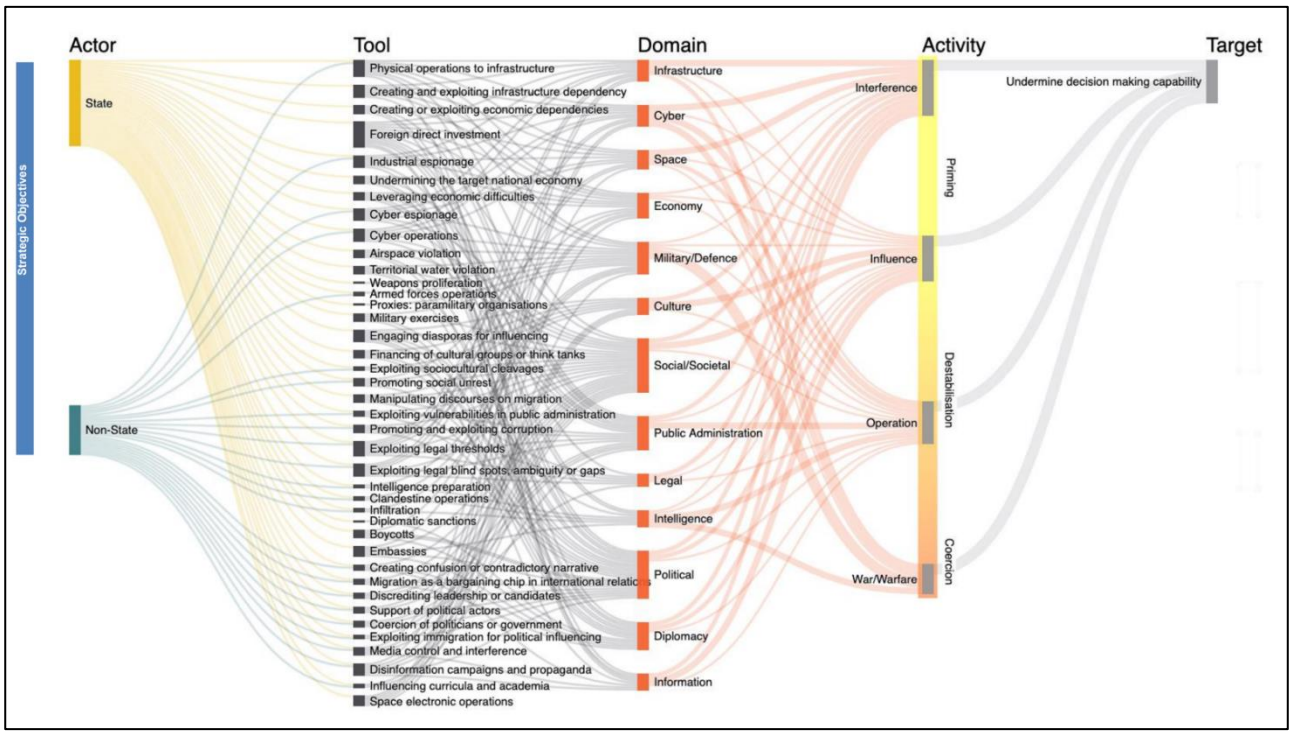

Figure 2 Overall Picture of the Conceptual Model for Hybrid Threat Analysis
Source: European Commission and Hybrid CoE, *The Landscape of Hybrid Threats: A Conceptual Model Public Version*, Publications Office of the European Union, 2021, p. 13.

(1) Hybrid threat actor (Actor)

Hybrid threat actors are divided into state and non-state actors.

State actors in the Conceptual Model refer to authoritarian states that are hostile to the democratic countries that make up the EU, NATO, etc. The model cites Russia, China, Iran, and North Korea as examples.[17]

A non-state actor is an entity that plays a part in international relations and that exercises sufficient power to interfere, influence, and effect change without any affiliation to the established institutions of a state.[18] Hezbollah, Islamic State (IS), and Private Military Companies (PMCs) are representative examples.[19]

---

[17] European Commission and Hybrid CoE, *The Landscape of Hybrid Threats: A Conceptual Model Public Version*, Publications Office of the European Union, 2021, p. 16, https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf (last accessed August 8, 2024).
[18] Ibid. p. 22.
[19] Ibid. p. 16.

(2) 40 operational tools of hybrid threat activity (Tools)

The 40 tools refer to tools of hybrid threat activity used in past cases as observed by Hybrid CoE. Actors have used these tools to affect one or more domains or to target vulnerabilities in a domain.[20]

(3) 13 affected domains (Domains) and targets to be achieved by hybrid threat activity (Targets)

Affected domains (Domains) are groupings of instruments of national power that are targets against which an actor uses tools of hybrid threat activity to exert hybrid threats. The targets of hybrid threat activity (Targets) are the ultimate goals that actors aim to achieve by conducting hybrid threat activity.[21]

Figure 3 visualizes these 13 affected domains and the target of hybrid threat activity.

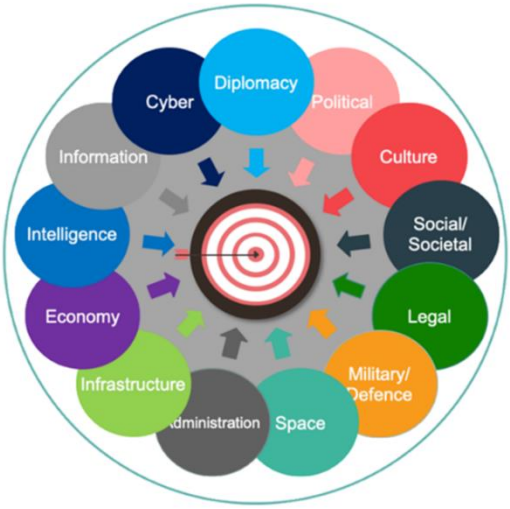

Figure 3 13 Affected Domains and Targets of Hybrid Threat Activity
Source: European Commission and Hybrid CoE, op. cit., 2021, p. 27.

[20] Ibid. p. 26.
[21] Ibid. p. 26.

(4) Hybrid threat phases (Phases) and activities (Activities)

Hybrid threats are exerted through different specific activities (Activities) according to different chronological phases (Phases) of escalation (degree of coercion to achieve an objective). The three phases are divided with degrees of escalation increasing from the priming phase to the coercion phase. Activities escalate to interference, influence, and operation, ultimately leading to war.[22]

Table 1 summarizes the relationship between the chronological phases of escalation and hybrid threat activity.

Table 1 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. ・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.
Destabilization	
Coercion	・War/warfare = Use hybrid threat tools in military warfare to gain an advantage in military warfare.

Source: Prepared by Maritime Security Study Group of the Nakasone Peace Institute based on European Commission and Hybrid CoE, op. cit., 2021, p. 13.

[22] Ibid. pp. 36-42.

Figure 4 illustrates hybrid threat activities in the Conceptual Model from the perspective of an actor.

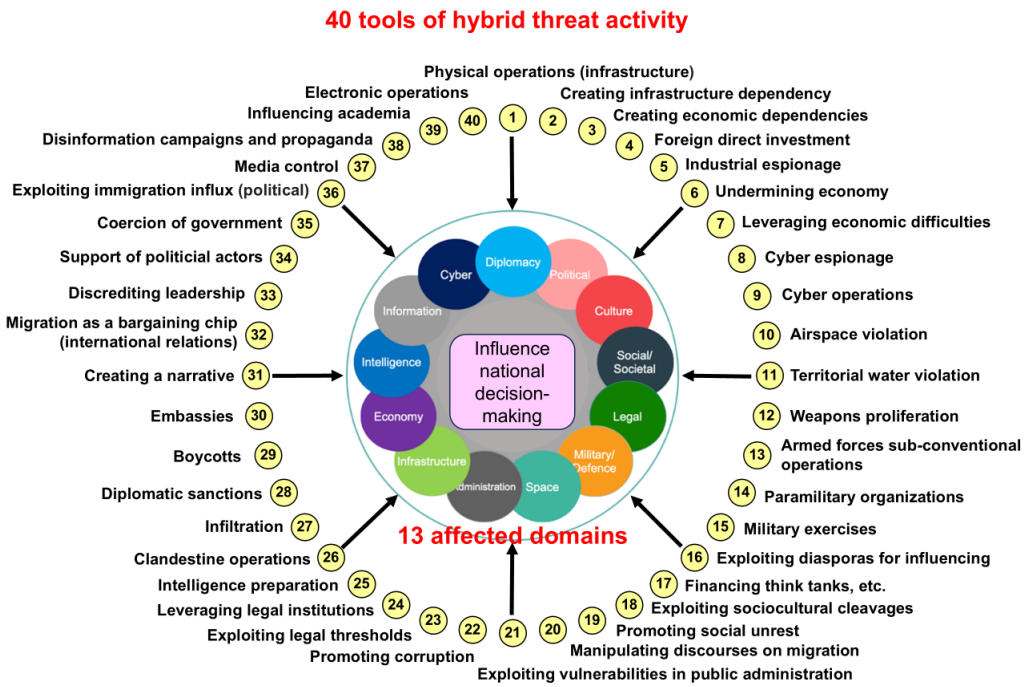

Figure 4 Hybrid Threat Activity

Source: Prepared by the author based on European Commission and Hybrid CoE, op. cit., 2021, p. 27.

(5) Characteristics of the Conceptual Model

The Conceptual Model assumes a "responsive" or "pull-type" analysis process, in which detected signs of hybrid threats are matched to the operational tools of hybrid threat activity after which the actors and their goals are brought into focus. The thinking process for using this Conceptual Model as a pull-type analysis model is shown in Figure 5.

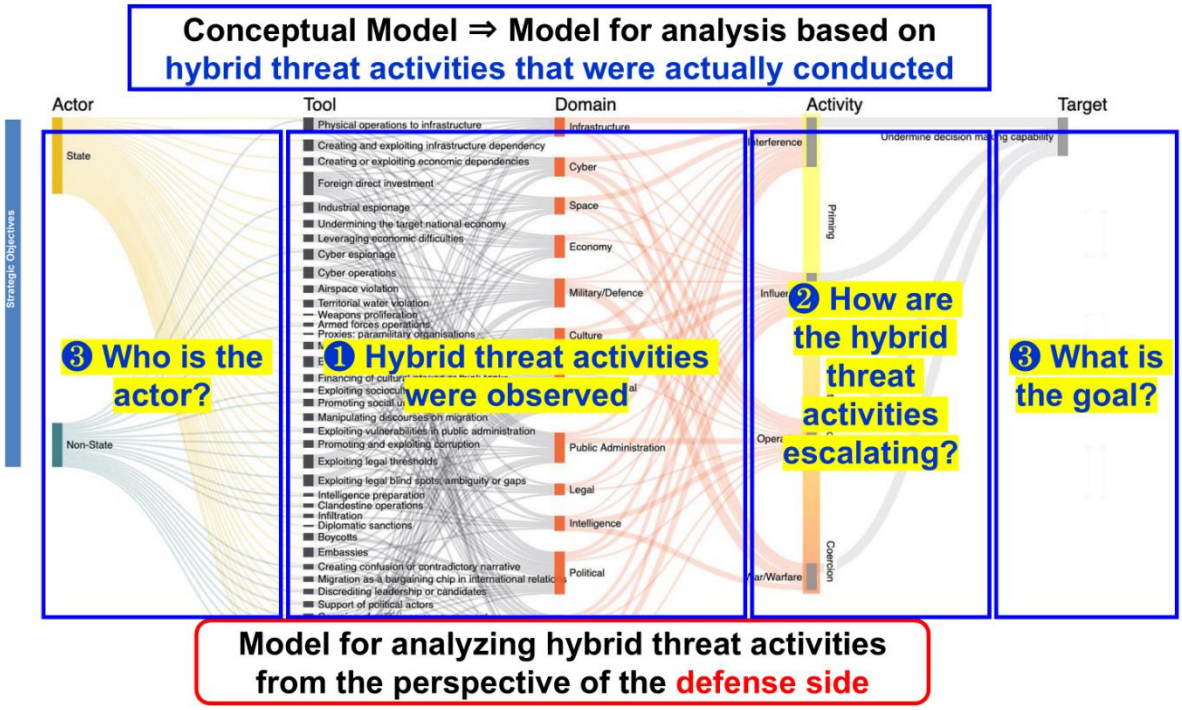

Figure 5 Thinking Process for Using the Conceptual Model as a Pull-type Analysis Model
Source: Prepared by the author based on the Conceptual Model
* Pull-type analysis: Analyze activities that have already been conducted and draw out evaluations.

In applying the Conceptual Model used to examine the deterrence of a Taiwan contingency, it is possible to clearly set the actor as China and the ultimate goal as unification of Taiwan. At the same time, it is necessary to reconfigure the pull-type analysis process into a "push-type" of thinking analysis. This involves calculating backward from the ultimate goal to the individual goals in the escalation process and potential operational tools of hybrid threat activity that could be selected to achieve those goals to analyze a predictive scenario. Figure 6 shows the thinking process for using this Conceptual Model as a push-type analysis model.

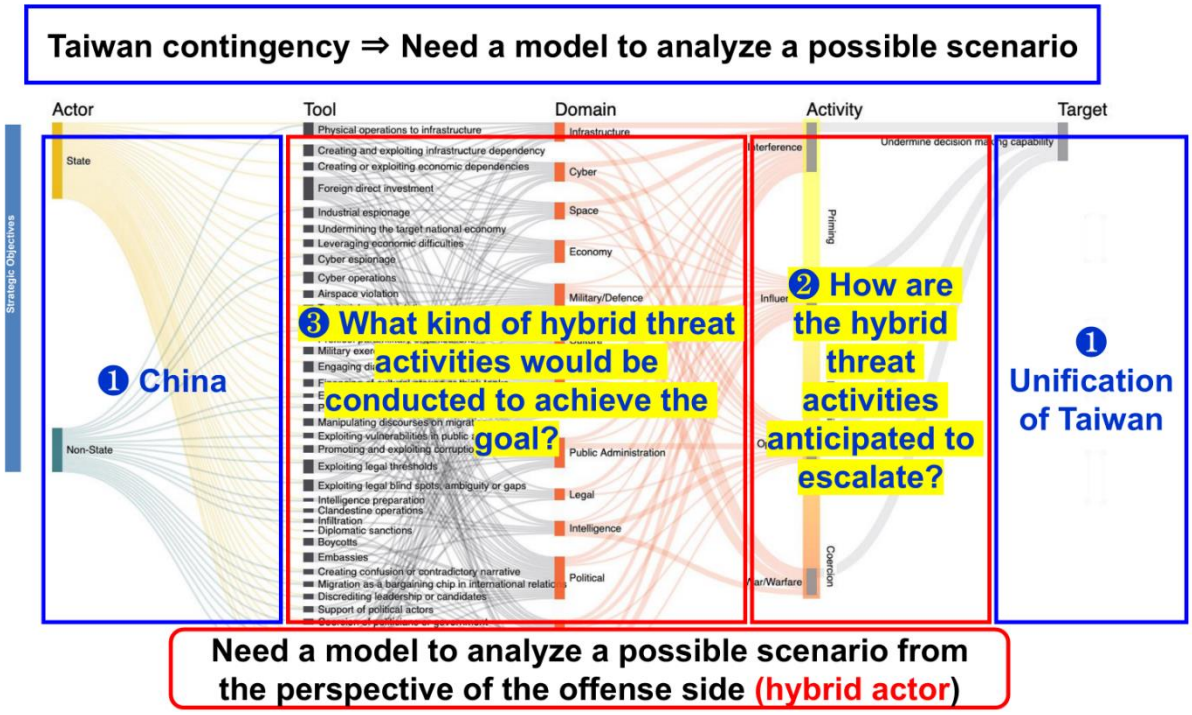

Figure 6 Thinking Process for Using the Conceptual Model as a Push-type Analysis Model
Source: Prepared by the author based on the Conceptual Model
* Push-type analysis: Envisioning events that have not yet occurred and predicting and enumerating possibilities.

In the next section, the author will discuss the challenges of applying the Conceptual Model to a Taiwan contingency.

3. Challenges in applying the Conceptual Model to the deterrence of a Taiwan contingency

In the context of a specific scenario in which the ultimate goal is the unification of Taiwan, the author will discuss the challenges of reconfiguring the thinking process into a push-type analysis. This reconfiguration starts with the ultimate goal and works backward to predict individual goals in the escalation process and the hybrid threat tools selected to achieve that goal. The analysis will focus on addressing hybrid warfare through the representative military operations process known as the "OODA loop" (Observe, Orient, Decide, Act).[23] Of the four stages of hybrid threat response operation, the first three (observe, orient, decide) respectively require different analytic outputs that each involve: (1) methods for detecting signs of hybrid threats (observation), (2) methods for predicting escalation (orientation), (3) methods for predicting results of combined hybrid threats (assessment necessary for decision making), and (4) visualization of analysis results (presentation of the assessment to support decision maker). The "action" stage is for the operation side (e.g., law enforcement authority responsible for addressing territorial water intrusion).

[23] A strategic thinking process for decision-making and execution that involves winning and losing, consisting of Observe, Orient, Decide, and Act.

(1) Methods for detecting signs of hybrid threats

In applying the Conceptual Model, the first challenge is that it organizes the tools of hybrid threat activity into 40 categories based on past cases of hybrid threats. However, in order to detect the signs, specific events observed in the real world must be enumerated in advance.

Table 2 40 tools of hybrid threat activity

① Physical operations against infrastructure	⑪ Territorial water violation	㉑ Exploiting vulnerabilities in public administration	㉛ Creating confusion or a contradictory narrative
② Creating and exploiting infrastructure dependency	⑫ Weapons proliferation	㉒ Promoting and exploiting corruption	㉜ Migration as a bargaining chip in international relations
③ Creating or exploiting economic dependencies	⑬ Armed forces conventional/sub-conventional operations	㉓ Exploiting legal thresholds	㉝ Discrediting leadership and/or candidates
④ Foreign direct investment	⑭ Paramilitary organizations (proxies)	㉔ Leveraging legal institutions	㉞ Support of political actors
⑤ Industrial espionage	⑮ Military exercises	㉕ Intelligence preparation	㉟ Coercion of politicians and/or government
⑥ Undermining the target national economy	⑯ Exploiting diasporas for influencing	㉖ Clandestine operations	㊱ Exploiting immigration influx for political Influencing
⑦ Leveraging economic difficulties	⑰ Financing cultural groups and think tanks	㉗ Infiltration	㊲ Media control and interference
⑧ Cyber espionage	⑱ Exploitation of sociocultural cleavages	㉘ Diplomatic sanctions	㊳ Disinformation campaigns and propaganda
⑨ Cyber operations	⑲ Promoting social unrest	㉙ Boycotts	㊴ Influencing curricula and academia
⑩ Airspace violation	⑳ Manipulating discourse on migration	㉚ Embassies	㊵ Electronic operations

Source: Prepared by the author based on European Commission and Hybrid CoE, op. cit., 2021, pp. 33-35.

The Conceptual Model, as shown in Table 2, organizes the tools of hybrid threat activity into 40 categories, but, because the categories are generalized, in its current form, the Model is insufficient as an indicator for detecting signs of hybrid threats.

Therefore, in order to establish methods for surveillance and for detecting signs, it is necessary to investigate examples of operational tools of hybrid threat activity used in the past and anticipate in advance what specific tools may be used and what activities may be carried out. Figure 7 shows an example of this method for researching past cases.

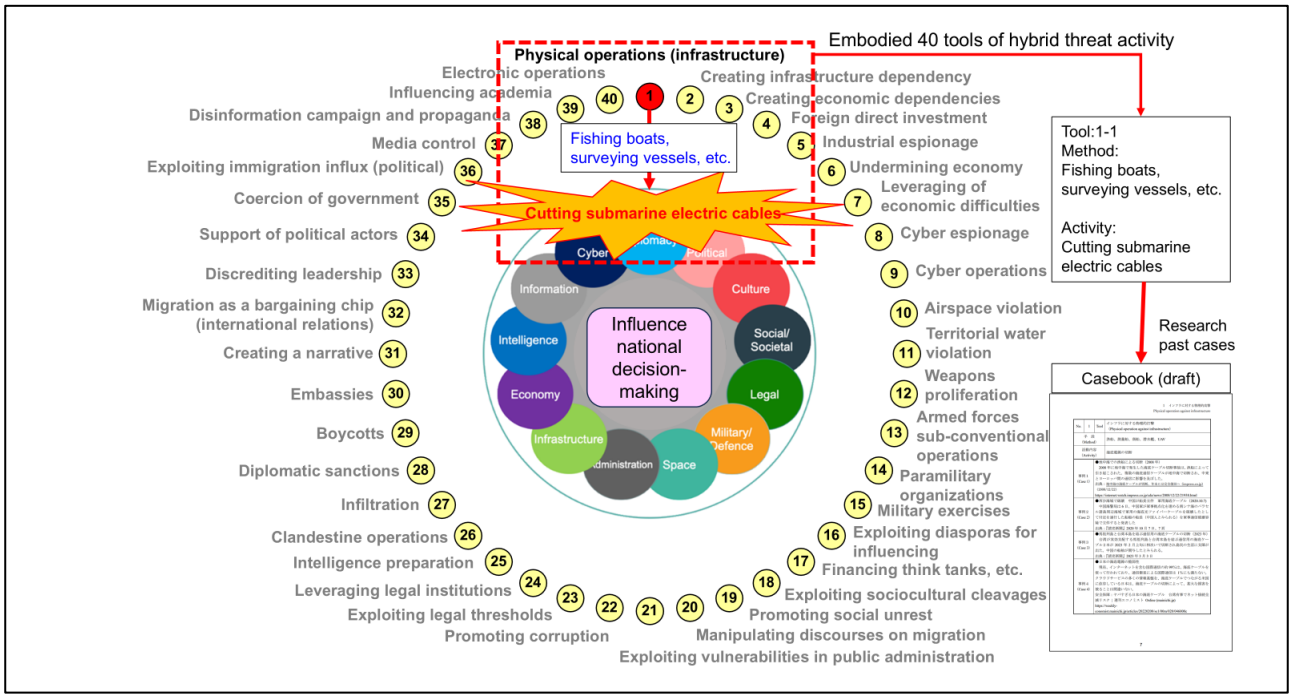

Figure 7 Methods for Researching Tool of Hybrid Threat Activity

1. "Physical Operations against Infrastructure"

Source: Prepared by the author based on European Commission and Hybrid CoE, op. cit., 2021, p. 27.

For example, as shown in Figure 7, in the category of hybrid threat activity tool number 1, "physical operations against infrastructure," cases of cutting submarine electric cables by fishing boats and surveying vessels, etc. were observed. These incidents were organized by method (fishing boats, surveying vessels, etc.) and activity (cutting submarine electric cables), and past cases corresponding to this method and activity were grouped together for analysis. An example of collected past cases is shown in Table 3.

Table 3 Examples of Past Cases Compiled in the Casebook

No.	1-1	Tool	Physical operations against infrastructure
Method			Fishing boats, surveying vessels, merchant vessels, submarines, unmanned air vehicles (UAVs)
Activity			Cutting submarine electric cables
Case 1			● **Cutting of submarine cables in the Mediterranean Sea by a ship (2008)** A submarine cable severing incident in the Mediterranean Sea in 2008 was suspected to have been caused by a ship's anchor. Several submarine communication cables (SEA-ME-WE3, SEA-ME-WE4, and FLAG cables) were cut in the Mediterranean Sea, affecting communications from Zambia to India and Taiwan. Source: "Repairs start on Mediterranean telecoms cables," *Reuters*, December 22, 2008, https://jp.reuters.com/article/repairs-start-on-mediterranean-telecoms-cables-idUSTRE4BJ0G4/.
Case 2			● **Destruction in waters near the Paracel Islands: China files case against captain for destroying military submarine cables (October 7, 2020)** On October 6, 2020, the China Coast Guard Bureau announced that it would file a case against the captain (believed to be Chinese) of a vessel that was passing in the vicinity of the Paracel Islands in the South China Sea, where China's military is building a military base, for destroying submarine fiber-optic cables used for military communication. Source: *Yomiuri Shimbun* newspaper (October 7, 2020), p. 7.
Case 3			● **Cutting of submarine cables connecting the Matsu Islands and the main island of Taiwan (2023)** In early February 2023, two submarine communication cables connecting the Matsu Islands, effectively controlled by Taiwan, to the main island of Taiwan were cut in quick succession, disrupting the lives of Matsu Island's residents. Chinese vessels are believed to have been involved. Source: *Yomiuri Shimbun* newspaper (March 3, 2023).

Source: Prepared by the Maritime Security Study Group, Nakasone Peace Institute.

This case, when compiled with past cases, is useful not only for detecting signs of hybrid threats but also has the potential to lead to analysis of the actor's characteristics as well as trends in the tools used for hybrid threat activity, depending on how data is accumulated.

(2) Methods for predicting escalation

The second challenge is how to analyze the potential escalation of hybrid warfare by China against

Taiwan in the future.

The Conceptual Model was created as a gauge to understand the current escalation of hybrid threats and not for predicting future escalation. For that reason, this study divides China's hybrid warfare against Taiwan into a "hardline approach" and a "conciliatory approach" with the assumption that China's strategy would shift according to current circumstances between the two approaches. China's specific objectives behind these strategies can be inferred (Table 4).

Table 4 Prediction of Hybrid Warfare against Taiwan

Phase	Hardline approach	Conciliatory approach
Priming phase	• Intelligence activities • Intimidation and compromising credibility of politicians • Political and social division • Boycott from international organizations • Interference with Taiwan's economic activities • Military threat (strong)	• Intelligence activities • Involving pro-China politicians • Involving pro-China factions • Interference with Taiwan's diplomatic activities • Strengthening economic interdependence with Taiwan • Military threat (weak) • Fostering distrust of Japan and the U.S.
Destabilization phase	• Fostering distrust of the government's administrative capacity • Promotion of social unrest and anxiety about war • Obstacles to coordination between Taiwan, the U.S., and Japan	• Discrediting anti-China forces • Promoting the importance of Taiwan-China coordination • Fostering distrust of the U.S.
Coercion phase	• Disruption of social and economic activities • Isolation of information dissemination in Taiwan • Creation of a state of civil war • Limited military intervention	• Strengthening ties with China • China's control of Taiwan's information space • Open and overt intervention in elections • Establishment of a government advocating unification

1 The two approaches are not a choice between the two but rather can be shifted as needed based on the status of China's achievement of its hybrid warfare objectives, the judgment of the leadership, and other factors.
2 Each phase does not necessarily escalate in a linear direction but could also de-escalate at times.

Source: Prepared by the author.

The hardline approach seeks to incite internal conflict within Taiwan in order to create a state of widespread turmoil and, in the midst of this turmoil, to establish a government that will work toward unification. To this end, China aims to isolate Taiwan from the international community and destabilize Taiwan's politics, economy, and society through various tools. If the situation becomes sufficiently unstable, upon Taiwan's request, China may send in security forces or troops to achieve de facto unification.

The conciliatory approach focuses on promoting a pro-China orientation in Taiwan in order to establish a government that will weaken the anti-China faction and work toward unification. To achieve this, China would encourage an increase in Taiwan's dependency on China particularly in

terms of the economy and create a situation in which Taiwan cannot function independently. Simultaneously, China would work to integrate Taiwan as part of China to be accepted as part of China in the international community, thereby leading Taiwan as a whole in a pro-China direction.

With regard to hybrid warfare by China against Taiwan through hardline and conciliatory approaches, the author outlines possible patterns of escalation prediction, assuming specific scenarios in the priming phase, destabilization phase, and coercion phase.

The two approaches, hardline and conciliatory, are not a choice between the two but rather can be shifted as needed based on the status of China's achievement of its hybrid warfare objectives, the judgment of the leadership, and other factors. In addition, each phase does not necessarily escalate in a linear direction but could also de-escalate at times.

Therefore, anticipating the objective and intent of China's future activities within each phase provides a framework for ensuring smooth and rapid situational awareness. It is also essential in planning appropriate responses for escalation management.

(3) Methods for predicting results of a combined analysis of hybrid threats

The third challenge is that while the Conceptual Model is ideal for analyzing past cases and ongoing events, when attempting to cover all combined threats the number of analyses may be excessive.

This study considers a simplified prediction model to resolve this problem. The specifics are as follows.

Hybrid threats have the characteristic of being able to efficiently attack target countries or societies through the simultaneous use of multiple interrelated tools of hybrid threat activity rather than the independent use of a single tool. To analyze this characteristic, in April 2023, the Hybrid CoE developed a comprehensive resilience ecosystem (CORE) model (Figure 8), an advanced version of the Conceptual Model.

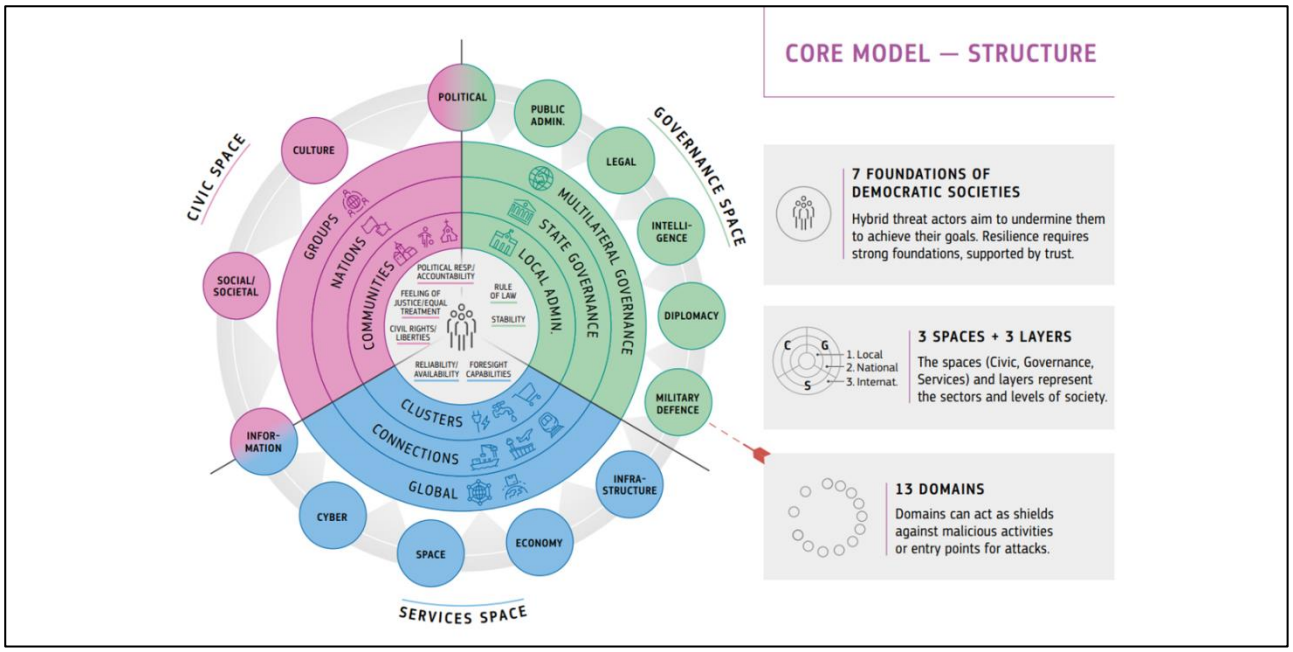

Figure 8 Overview of the CORE Model
Source: Prepared by the author based on European Commission and Hybrid CoE, *Hybrid Threats: A Comprehensive Resilience Ecosystem*, Publications Office of the European Union, 2023, p. 10.

An overview of the CORE model is as follows.

First, the seven foundations of democratic societies (rule of law, stability, political responsibility and accountability, feeling of justice and equal treatment, civil rights and liberties, reliability and availability, and foresight capabilities) are set in the center of the circle of the CORE model as the goals of the hybrid threat activities. The three layers outside the center of the circle are divided from the inside into three levels: local, national, and international. The CORE model is divided into three spaces: civic space (pink area), governance space (green area), and services space (blue area). The 13 affected domains are located in the outer circle and are divided into one of the three: governance space, civic space, or services space.[24]

The relationship between the CORE model and the Conceptual Model is shown in Figure 9.

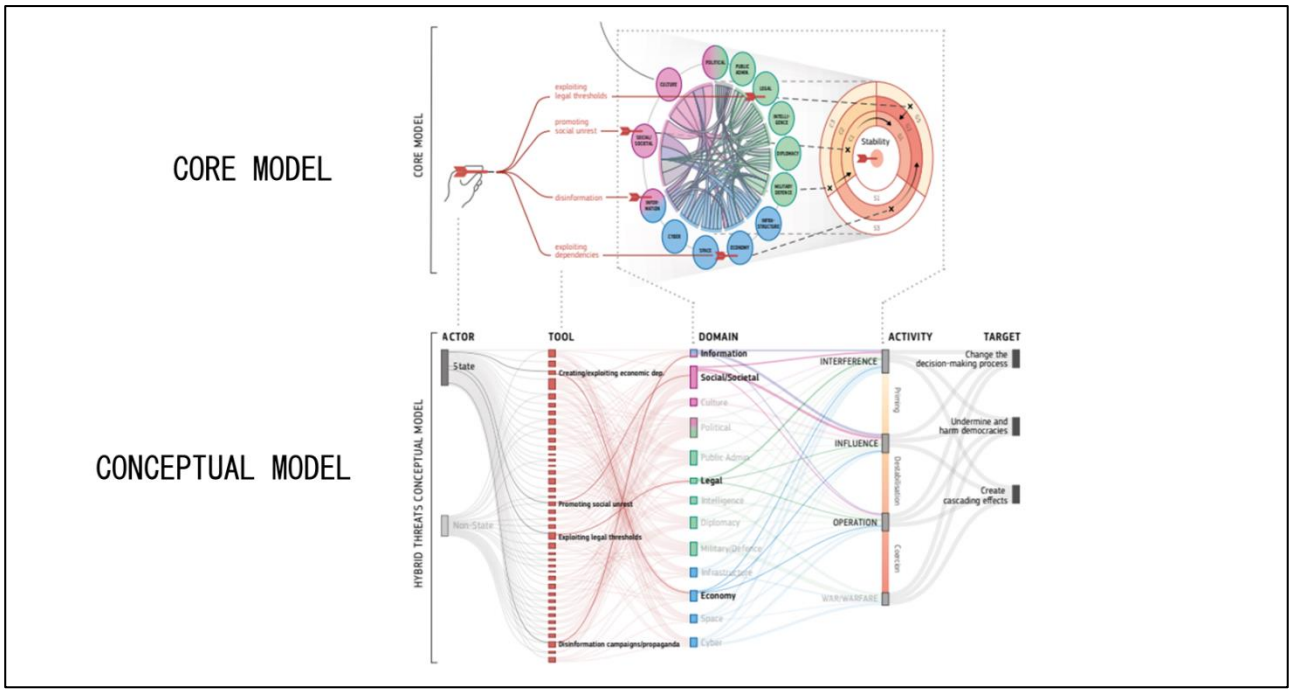

Figure 9 Relationship between the CORE Model and the Conceptual Model
Source: Prepared by the author based on European Commission and Hybrid CoE, op. cit., 2023, p. 11.

The CORE model visualizes the tools of hybrid threat activity as darts, assuming a dart is thrown at a domain to be targeted for hybrid threat activity. The dart that hits the domain will affect other

[24] European Commission and Hybrid CoE, *Hybrid Threats: A Comprehensive Resilience Ecosystem*, Publications Office of the European Union, 2023, p. 10, https://www.hybridcoe.fi/wp-content/uploads/2023/04/CORE_comprehensive_resilience_ecosystem.pdf (last accessed August 8, 2024).

domains in addition to the targeted domain (top center). For example, if a cyberattack is launched against a bank and the financial system comes to a halt, the affected domain is the cyber domain, but the economy and social/societal domains are also affected in such forms as economic loss and social unrest. (*The interconnections between these domains are shown by the lines connecting the domains in the center of the CORE model.)

Thus, the CORE model is a simplified version of the Conceptual Model's interconnections between affected domains.

The actual analysis using the CORE model is shown in Figure 10.

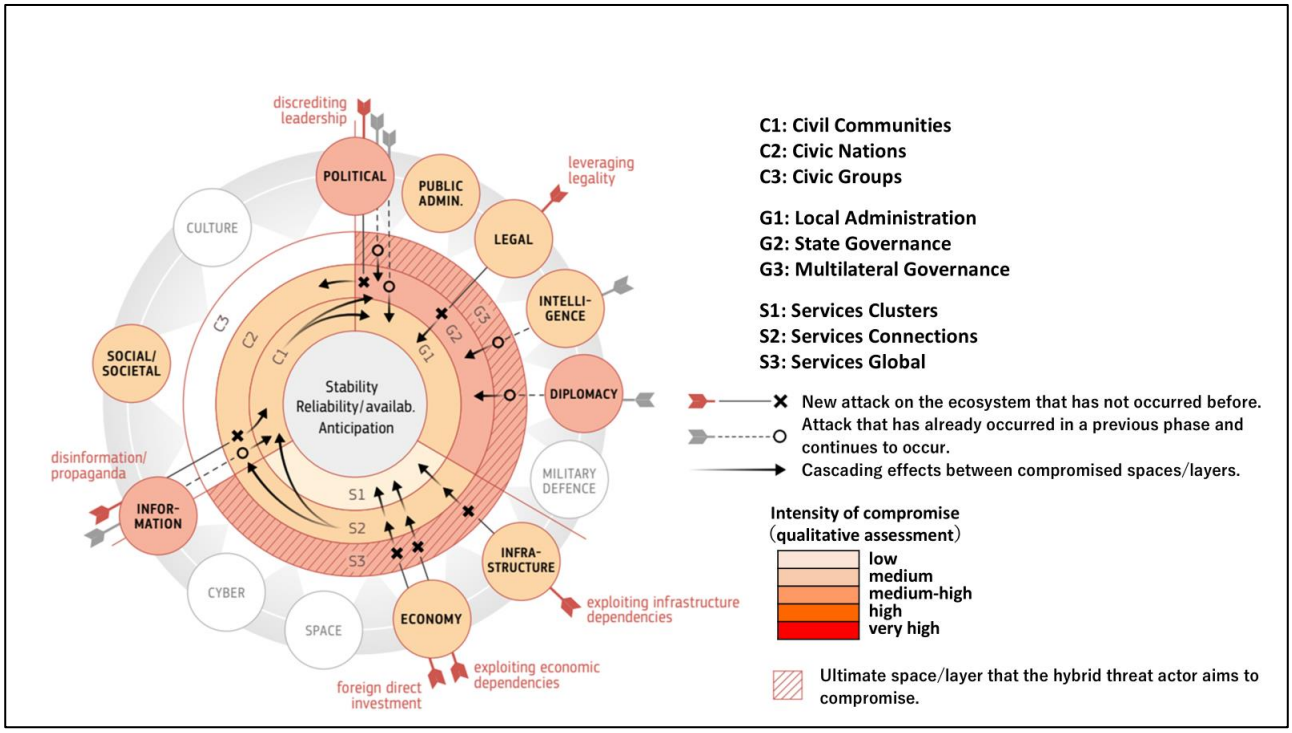

Figure 10 Basic Structure of the CORE Model

Source: Prepared by the author based on European Commission and Hybrid CoE, op. cit., 2023, p. 55.

Red arrows indicate the type of tools of hybrid threat activity and the domain to which the tools of hybrid threat activity are applied, while the black "X" marks indicate the area the tools impact within the three layers. Gray arrows and "O" marks indicate past and ongoing tools of hybrid threat activity. Black arrows indicate the cascading effects of the hybrid threat activity.[25]

As shown in this figure, the CORE model is the best model for analyzing past cases and ongoing events. An example of this model applied to the hybrid warfare against Taiwan is shown below.

[25] Ibid. p. 11.

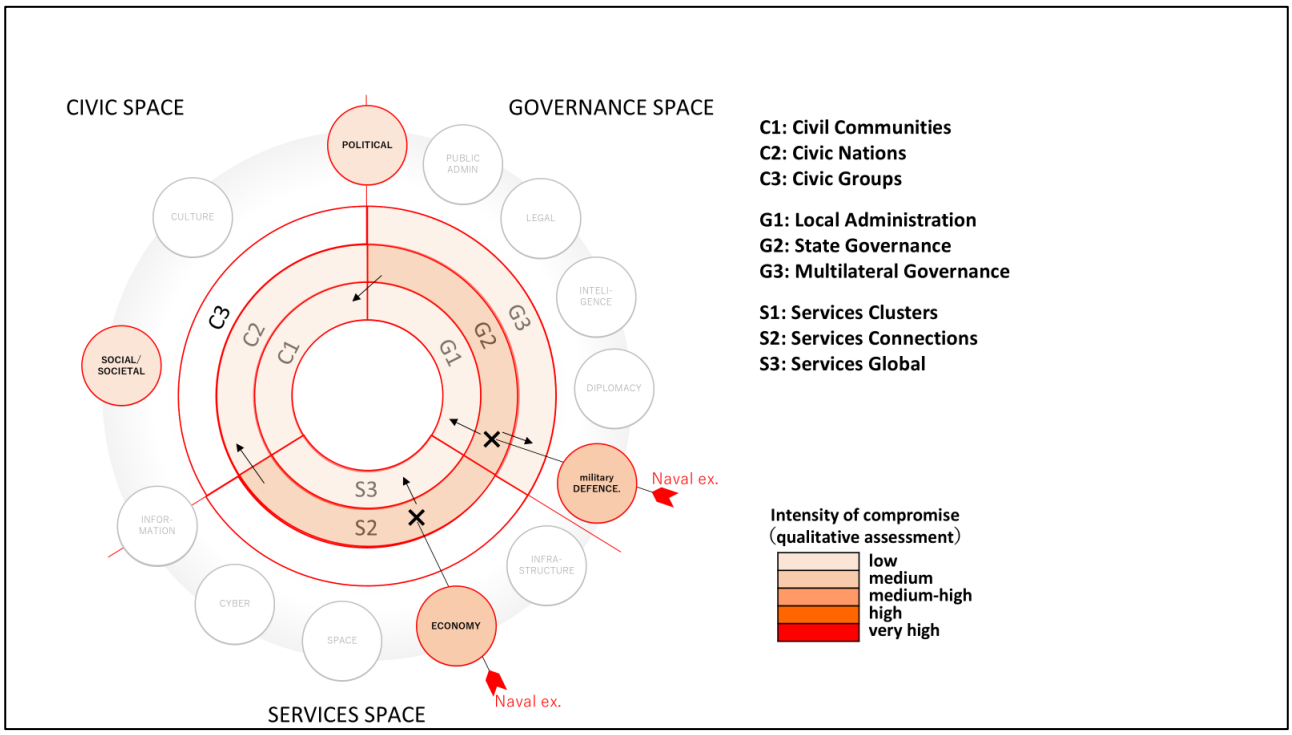

Figure 11 Prediction of a Situation in a Case of Large-scale Exercises by China's Navy in the Waters Surrounding Taiwan
Source: Prepared by the author based on the CORE model.

Figure 11 shows an example of a CORE model analysis that assumes a large-scale naval exercise conducted in the waters surrounding Taiwan, resulting in impediment of Taiwan's maritime traffic.

Red arrows indicate that the military/defense and economy domains have been affected by hybrid threat activity that was conducted through naval exercises as a tool. As a result, low-intensity impacts directly affect the local administration and multilateral governance (G1 and G3) and services global (S3) domains adjacent to the targeted state governance (G2) and services connections (S2), as well as the civic space. This shows that it is possible to use the CORE model to predict a possible scenario. However, even when naval exercises are used as a tool of hybrid threat activity, various predictive scenarios are possible, depending on location, scale, and composition of the military, etc. Predictive scenarios could include cases in which naval exercises have no impact on maritime traffic or civic space. Therefore, it is necessary to consider how to handle a large number of possible predictive scenarios.

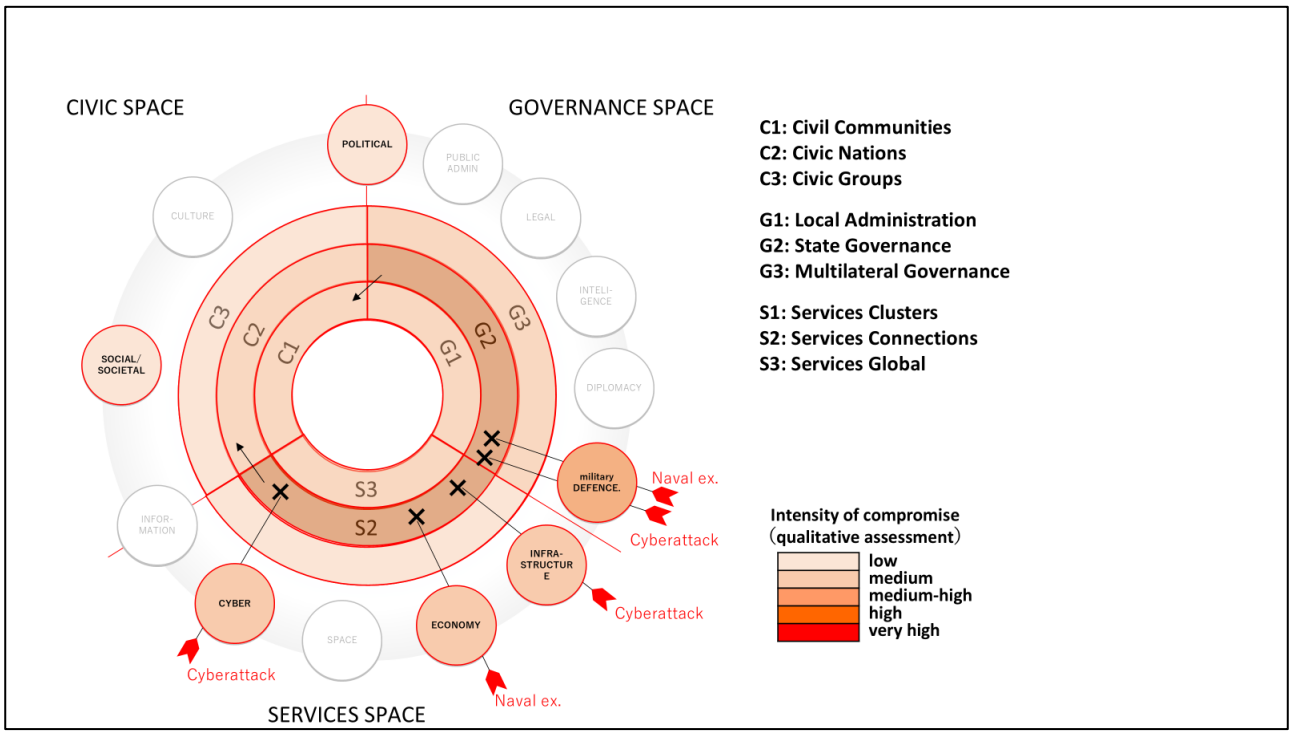

Figure 12 Case of Cyberattacks Launched in Addition to Naval Exercises (Figure 11)
Source: Prepared by the author based on the CORE model.

Figure 12 shows an example of a CORE model analysis of a case in which a cyberattack occurs in addition to a naval exercise and critical infrastructure is affected (Figure 11).

The most important aspect of hybrid threat analysis is to analyze the impact of the use of multiple tools of hybrid threat activity; the CORE model is unique in its ability to analyze the results of the combined hybrid threats.

When the CORE model is used as a predictive model, the number of combinations of tools of hybrid threat activity is likely to be high, and comprehensively covering all combinations of threats could result in a very large number of analyses.

From these combinations, by accumulating and applying case studies, it may be possible to show to a certain extent the patterns of the impact made by tools of hybrid threat activity. It is necessary to examine a simplified version of the model for prediction that takes advantage of these patterns.

(4) Visualization of analysis results

The fourth challenge is that while the analysis results of the Conceptual Model and the CORE model are clear to the experts who perform the analysis, they are difficult to understand for the operators (i.e. decision makers regarding specific measures and tools) who are not familiar with the use of these models. In addition, to make the information visually comprehensible, it is necessary to narrow down and focus on the core elements that must be visualized, which vary according to the Concept of Operation for addressing hybrid threats.

With regard to this challenge, it is necessary to assume in advance the hybrid threats that have the highest probability and largest impact on Japan, and to comprehensively consider specific response measures, the operators and assets involved, and the information and data necessary to support these activities. It is then desirable to formulate a comprehensive hybrid threat response concept that incorporates policy, operation, and intelligence perspectives, and then pursue the necessary specifications for AI and software development.

4. Relationship between the Conceptual Model and China's strategy of using military and non-military means

While the term "hybrid warfare" has been used thus far, this concept is used by NATO and the West, and China does not use the concept of hybrid warfare with respect to actions it undertakes. This disparity raises the question of whether a Conceptual Model for Hybrid Threat Analysis based on the concept used by NATO and the West can analyze activities based on China's realistic strategic framework.

China's latest representative strategic framework includes the Three Warfares, Unrestricted Warfare, and Intelligentized Warfare.

The Three Warfares refer to the activities of public opinion warfare, psychological warfare, and legal warfare. In 2003, the CCP revised the "People's Liberation Army Political Work Regulations" to specify that "(China would) develop public opinion warfare, psychological warfare, and legal warfare and disintegrate the enemy forces."[26] In formulating the Conceptual Model, the Three Warfares were the subject of study, and the Hybrid CoE reflected the basic ideas of the Three Warfares in the Conceptual Model.[27]

Unrestricted Warfare is a concept raised in a co-authored book on military strategy by Qiao Liang and Wang Xiangsui, two colonels in the PLA, published in 1999. The authors of this publication proposed as many as 24 types of combat methods, including conventional warfare, diplomatic warfare, terror warfare, information warfare, financial warfare, cyber warfare, legal warfare, psychological warfare, and media warfare.[28] Most of the 24 types of combat methods in Unrestricted Warfare are covered by the Conceptual Model. However, for some of the methods, such as ecological warfare, it is necessary to determine into which tool or domain within the Conceptual Model they fit, whether new tools or domains should be added, or to take other measures. Examination by applying relevant past cases is required for these methods.

Intelligentized Warfare is defined by People's Liberation Army National Defense University associate professor Li Minghai as "integrated warfare that is waged in the land, sea, air, space, electromagnetic, cyber, and cognitive domains using intelligentized weaponry and related operation

---

[26] See above, "*Zhongguo renmin jiefangjun wuqi zhuangbei guanli tiaoli* [Regulations on the Administration of Weaponry of the People's Liberation Army of China]" (January 2003).
[27] European Commission and Hybrid CoE, op. cit., 2021, pp. 20-22.
[28] Qiao Liang (author), Wang Xiangsui (author), Shinnosuke Sakai (editorial supervisor), op. cit., p. 205.

methods based on Internet of Things (IoT) information systems."[29] The Conceptual Model is considered to cover non-military means such as the cognitive domain of Intelligentized Warfare. However, other domains included in Intelligentized Warfare are outside the scope of this study because they are related to the use of full-scale military power, and the concept may change with future developments in AI, so the subject requires continued attention.

In this way, the Conceptual Model generally covers activities based on China's strategic thinking, and it should be possible to analyze activities based on China's realistic strategic thinking by adding or modifying some of the tools and domains for areas not currently covered by the Conceptual Model.

Conclusion

In analyzing and evaluating the situation of hybrid warfare for deterring a Taiwan contingency, the Conceptual Model is considered highly useful in that it provides a comprehensive understanding of the combined activities by military and non-military means that China could use to unify Taiwan. However, in order to actually use the model to analyze future events such as a Taiwan contingency, it is necessary to address four challenges related to the use of the Conceptual Model. Of these four challenges, item (1) methods for detecting signs of hybrid threats can be addressed by researching past cases in which tools of hybrid threat activity were actually used, anticipating what specific tools might be used and what kind of activities might be conducted, and establishing surveillance targets and corresponding methods for detecting signs of hybrid threats. In addition, to resolve item (2) methods for predicting future escalation, it is useful to divide China's hybrid warfare against Taiwan into a hardline approach and a conciliatory approach, assuming that China's strategy will shift situationally between the two approaches. The remaining two challenges (i.e., items (3) methods for predicting results of combined hybrid threats and (4) visualization of analysis results during the response phase) require examination, including AI and software development. Resolution of these challenges will require collaboration across government, private sector, academia, nations, and regions. Challenge items (3) and (4) should be resolved by establishing a comprehensive hybrid threat response concept that incorporates policy, operation, and intelligence perspectives. Further, by clearly communicating the concept to the technology and industry sectors, development for effective prediction and practical visualization for operations will be promoted.

[29] Li Minghai, above, "*Shi shenme zai tuidong zhanzheng xiang zhineng hua yanbian* [What is driving the war to become intelligent?]" (Chinese), *Jiefangjun Bao* [PLA Daily] (November 6, 2018).