Application of International Law to Cyber Conflicts Outline of Japan's Legal Response Against Low-Intensity Cyber Conflicts Through Countermeasures

Tetsunosuke Jinnai

Application of International Law to Cyber Conflicts
Outline of Japan's Legal Response Against Low-Intensity Cyber Conflicts Through Countermeasures

Tetsunosuke Jinnai[1][0000-0002-8896-7448]

[1] Institute of Information Security, Japan
dgs213101@iisec.ac.jp

Abstract. Cyber conflicts are an important security challenge, but the applicable legal regime remains ambiguous. Especially, low-intensity cyber conflicts, which do not amount to armed conflicts under international law, are difficult to handle legally because the boundary between conflicts and crimes is ambiguous. Domestic debates on the legal response to such cyber conflicts so far have mainly focused on the applicability of self-defense under Japan's extreme pacifist constitution. However, applying self-defense to low-intensity conflicts is quite difficult under the constitution, and further progress in the debate is unlikely. This study proposes specific ways to respond to cyber conflicts by utilizing countermeasures as a new legal framework. In the first part, after touching on an overview of the application of international law in cyberspace, this study will show the advantages of countermeasures under low-intensity cyber conflicts. In the latter part, through some scenario analyses, this study will clarify concrete ways of how to apply countermeasures, foreseeable problems, and how to respond to them as conclusions. The rationale for this study was mainly based on a literature review, including previous studies, and the scenario study method was also used to draft the conclusions.

Keywords: Cyber Conflicts, Law of International Responsibility, Countermeasures.

1 Current Status and Perception of the Problems in Cyber Conflicts

The intensification of cyber conflicts in recent years has become a serious security concern for Japan. Japan's new cyber security strategy [1] released in 2021, expresses the sense of crisis in its situational awareness; “As such, the situation in cyberspace, while not amounting to national emergency per se, can no longer be deemed purely in peacetime.” From the perspective of international law, cyber conflicts have various characteristics that differ from conventional international conflicts, such as diversity of legal entities, anonymity, and dilution of the concept of national borders. The most important

characteristic is that most cyber conflicts are conducted below the threshold of armed conflicts, and the boundary between conflicts and crimes is obscure, which makes it difficult to determine the applicable legal framework. Figure 1 explains an example of the legal classification of cyber conflicts. To effectively deal with cyber conflicts, Japan is required to make its legal position clear against cyber incidents and respond to the situation immediately.

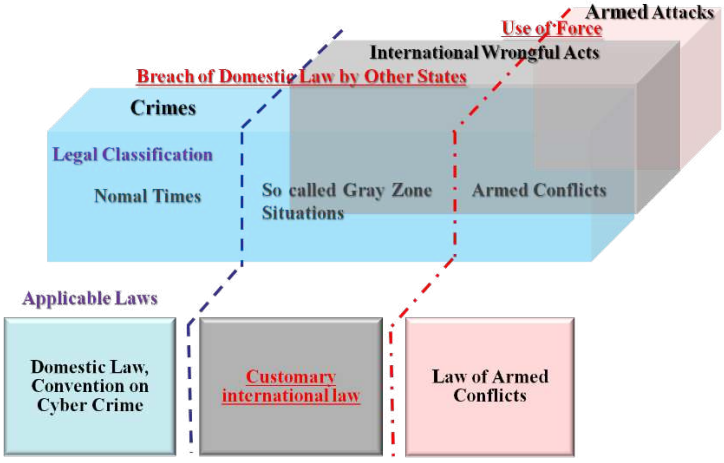

Fig. 1. Schematic of the Legal Classification of Cyber Conflicts.[1]

Conversely, Japan's current situation shows that the development of cyber protection capability lags that of neighboring countries. Legislations to deal with cyber conflicts have not been sufficiently studied [2].[2] In particular, the severe restrictions on administrative agencies originated from the "renunciation of war" and "secrecy of communications" stipulated in Japan's constitution,[3] as well as the unclear role of each ministry and agency in the security in the cyber domain as seen in the Basic Act on Cybersecurity,[4] are hindering effective responses.

Still, seeing the situation of academic studies in this field, the mainstream of discussions domestically on cyber conflicts seemed to be on the application of self-defense

---

1 This figure shows an example of the legal classification of cyber conflicts. Use of force and breach of domestic law straddle over the boundary of each category.

2 The International Institute for Strategic Studies (U.K.) produced a report that assessed 15 countries' cyber power. It ranks a country's cyber capacity and effectiveness and ranks Japan in the lowest layer, tier.3, due to the delay in developing effective domestic legislation for cyber operations.

3 The Constitution of Japan, articles 9 and 22.

4 The Basic Act on Cybersecurity, article 18, provides that "The national government is to provide necessary measures with the intention to.... clarify the division of roles among relevant bodies as actions to address threats which may critically affect the country's safety concerning Cybersecurity-related incidents," which means that those have not been clarified yet.

so far. However, the debate on the application of self-defense to low-intensity cyber conflicts[5] easily leads to the one lowering the threshold of the use of force, which is quite challenging under Japan's pacifist constitution. These discussions do not seem to be progressing realistically. Therefore, the focus of this paper is to recommend responses to low-intensity cyber conflicts by creating a new framework using countermeasures under international law.

2 Previous Research

In the field of international law, discussions on the application of international law to cyberspace have been held at the Government Experts' Group at the United Nations and the United Nations Open-ended Working Group on Cybersecurity. Both submitted their final report documents in 2021 [3,4]. In addition, there are many previous studies on the application of international law to cyber conflicts. In particular, the Tallinn Manual [5], which is a compilation of expert opinions on international law, seems to have a strong influence even though it is not legally binding. Especially speaking of countermeasures, Michael N. Schmitt [6], the proponent of the Tallinn Manual, and the leader of its compilation has argued for the use of countermeasures, and Jeff Kosseff [7] of the U.S. Naval War College has published a paper strongly arguing for the necessity of collective countermeasures.

However, looking back to the studies in Japan, the number is not large, furthermore, most of them focus on self-defense such as [8]. Little has been done to the application of countermeasures to cyber conflicts with considering unique Japanese legal policy situations.[6] Given this situation, it can be considered that this paper has novelty in this field.

3 Internationally Wrongful Cyber Acts

3.1 Overview of International Wrongful Cyber Acts

First, it is necessary to clarify what are lawful and unlawful acts in cyberspace under international law. The Article of State Responsibility [9] provides the elements of an act of violation of international law by a State, which consist of acts or omissions that are attributable to States under international law and constitute a breach of the state's international obligations.[7] The requirements are clearly stated in the Tallinn Manual 2.0 [5] to be applicable in cyberspace as well. The following is a discussion of the specific application of each requirement, considering the characteristics of cyberspace.

---

[5] Here, “low-intensity cyber conflicts” means the cyber conflicts which don't achieve the threshold of armed conflicts.

[6] For example, there are several studies about self-defense in cyberspace that are done by Japanese researchers, but it is difficult to find the works related to the application of countermeasures to cyber conflicts considering specific Japanese situations.

[7] Draft Articles on Responsibility of States for Internationally Wrongful Acts, article 2.

3.2 Attribution to the State

In principle, only sovereign States can be legal entities in international law, and the status of legal entities of individuals and international organizations is mainly created by treaties between States. [8] In other words, to hold someone responsible for an illegal act, it is necessary to attribute it to States. The cases in which a State can be held responsible generally fall into two categories: (1) acts of State organs and (2) acts of private individuals [10]. The second case is further divided into the following categories: acts of private individuals under the directions of States, State endorsement of the acts of private individuals, and violation of the principle of due diligence. In cyber conflicts, many indirect cyber operations are using non-State actors as proxies, so the attribution of private acts to States becomes a major issue.

3.3 Breach of the State's International Obligations

Regarding the second requirement, breach of international obligations, the Articles of State Responsibility [9] provide that "a breach of an international obligation by a State exists if the conduct of the State is not consistent with that required of the State by the international obligation, regardless of the origin or nature of the obligation."[9] In general, obligations regarding the context of cyber conflicts include (1) the principle of State sovereignty, (2) the prohibition of intervention, (3) the prohibition of the use of force, and (4) due diligence.

The principle of State Sovereignty. It can be said that States have generally established a consensus that the principle of State sovereignty applies to cyberspace. Malicious cyber activities by a State against another State's cyberinfrastructure without the latter's consent may be a violation of sovereignty. However, there is no consensus on the lawfulness of cyber espionage or unauthorized remote access from outside the State's territory [5].

The Prohibition of Intervention. The prohibition of intervention is a principle that States refrain from intervening in the domestic jurisdiction of other States, and there is no discussion on the application of this principle in cyberspace [5]. However, there is no established agreement on what the specific components of domestic jurisdiction are [10]. In general, whether an act violates the prohibition of intervention is determined by whether it relates to the above-mentioned domestic jurisdiction and whether it is inherently coercive. Intervention without a coercive element does not constitute unlawful intervention [11]. For example, a large-scale DDoS attack on a government agency to force the country to withdraw from a military alliance, or an attempt to hack into another country's election system to falsify the results of a particular election would be a violation of this rule.

---

[8] Therefore, in principle, non-State actors cannot owe the responsibility of international wrongful cyber acts.

[9] Draft Articles on Responsibility of States for Internationally Wrongful Acts, article 12.

The Prohibition of the Use of Force. Regarding the obligation to refrain from the use of force, while article 2 of the UN Charter[10] prohibits it, article 51 permits the exercise of individual or collective self-defense only in the event of an armed attack. Although there are various arguments about the difference between the use of force and armed attacks, in the Nicaragua case judgment [11], the court described armed attacks as the "most grave forms of the use of force" and expressed the idea of distinguishing between the two. Additionally in the judgment, the court adopted the scale and effects test as criteria to determine whether a specific act constitutes an armed attack.[11] Given the fact, Tallinn Manual 2.0 [5] applies the test as criteria to judge whether a cyber act meets the threshold of use of force. Although the difference between the use of force and armed attacks in cyberspace and the detail of the test are still unclear, it has been established from the past discussions that a cyber act that causes physical damage such as death or injury to a person or destruction of property would at least meet the criteria of the use of force. On the other hand, there is no consensus on whether non-physical damage such as data destruction can be satisfied with the threshold of the use of force or not [5].

Due Diligence. "Due diligence" is an obligation that States must exercise due diligence in ensuring territory and objects over which they enjoy sovereignty are not used to harm other States [12]. This obligation seems to be widely recognized as a general law principle, however, the scope of actions required is quite ambiguous [5]. In the context of cyber conflicts, a territorial state is obliged to crack down on illegal cyber activities conducted from within its territory against other countries. If the territorial State is aware of the fact but does not take any action, the injured State can pursue the violation of due diligence of the territorial State. It is noticeable that Japan's Ministry of Foreign Affairs has expressed the same idea [13].

4 Response to Internationally Wrongful Cyber Acts

Next, this paper will describe the legal frameworks for dealing with international wrongful cyber acts. To solve international disputes, UN Charter provides peaceful resolutions such as negotiation, enquiry, mediation, etc.[12] In addition, retaliatory measures such as economic sanctions, freezing assets, and blocking communications also can be taken. However, both are often ineffective in real cyber conflicts and more effective means are required. The Articles of State Responsibility [9] provide various circumstances precluding wrongfulness and those can be strong tools for responding to

[10] Charter of the United Nations, article 2 paragraph 4 and Article 51.

[11] *Ibid,* paras. 194-195. The court said, "the prohibition of armed attacks may apply to the sending by a State of armed bands to the territory of another State, if such an operation, because of its scale and effects, would have been classified as an armed attack rather than as a mere frontier incident had it been carried out by regular armed forces."

[12] Charter of the United Nations, article 33.

internationally wrongful acts.[13] Among those, there seem to be three considerable approaches for low-intensity cyber conflicts: "self-defense", "necessity", and "countermeasures."

4.1 Self-Defense

Self-defense allows for powerful counterattacks and collective responses including the use of force which might end conflicts soon and minimize damage. In addition, it can be exercised against non-State actors without worrying about attribution. However, to exert self-defense against cyber acts below the threshold of armed conflicts will be against the mainstream interpretation of international law, which claims that self-defense can be applied only against armed attacks [11].[14] Also, it seems difficult to apply self-defense to the situation considering the extreme pacifist constitution and foreseeable intense backlash from domestic and international public opinion. Furthermore, there is a high possibility of escalation into a full-scale armed conflict, because taking self-defense meagers means giving the other party justification for the use of force automatically. Although there are arguments [14] in Japan that self-defense should be recognized in low-intensity cyber conflicts, [15] it seems unrealistic under the situation above noted.

4.2 Necessity

An advantage of applying necessity to low-intensity cyber conflicts is that it does not require attribution, and there is a possibility that it can resort to the use of force as a response measure even in low-intensity cyber conflicts.[16] However, the applicable conditions for applying it in cyber conflicts are unclear, especially it is difficult to imagine the situation in low-intensity cyber conflicts meeting the condition of "it is the only way for the State to safeguard an essential interest against a grave and imminent peril" which is provided in the Articles of State Responsibility [9]. Therefore, necessity seems not to be a promising measure in the circumstance, and it should be applied as supplemental means in case both self-defense and countermeasures are not applicable.

4.3 Countermeasures

Compared to the former two means, countermeasures may be able to deter the escalation of conflicts well by negotiating with the other party while appropriately counterattacking through the minimum and adequate forces. The U.S. strategy of persistent

---

[13] Draft Articles on Responsibility of States for Internationally Wrongful Acts, article 20-25.

[14] There are a few opinions that self-defense can be applied to the use of force that does not meet the threshold of an armed attack, such as the USA, but they are in the minority.

[15] For example, the Liberal Democratic Party's "First Proposal of the Liberal Democratic Party Cyber Security Task Force" (April 24, 2018) advocates "cyber self-defense."

[16] According to Tallinn Manual2.0, there still has been discussion as to whether to include the use of force as a means of necessity.

engagement policy seems to adopt a similar approach [15]. In addition, the range of situations that countermeasures can deal with is wider, from "use of force" to "violation of sovereignty", making them easy to apply. In Japan, another positive reason is that it is easier to harmonize with domestic laws. However, unlike self-defense, responses that include the use of force cannot be taken and strict proportionality is required, which may result in insufficient coercive effects to bring the responsible State back to its duty. Especially, if collective countermeasures cannot be used, although some studies strongly insist on the necessity of them [6,7,16,17,18],[17] Japan will have to respond alone, which means a lack of implementation power. Furthermore, the biggest issue is attribution, and it is necessary not only to identify the perpetrator of the act but also to attribute the act to some State.

As described above, although countermeasures still have various challenges, overall, they seem to be suitable to prevent escalation of conflict and are easier to apply to Japan due to few restrictions under domestic laws. Regarding the lack of coercive power, there are some possible ways to supplement the drawbacks. First, from the short-term perspective, setting a relatively high threshold for the interpretation of the use of force leads to the consequence that there is wider room by the threshold of use of force, which means Japan can implement stronger means as countermeasures. Besides that, avoiding attribution problems by actively utilizing due diligence is promising. Second, From the long-term perspective, it is preferable to actively advocate the legalization of collective countermeasures. Also, it would be effective to consider enhancing collective attribution schemes through international cooperation. Table 1 summarizes the advantages and disadvantages of each legal response measure.

Table 1. Comparison of legal response measures

	Self-defense	Countermesures	Necessity
Requirement	➢ The existence of an armed attack. (in the general interpretation) ➢ Necessity(imminence) ➢ Proportionality	➢ The existence of preceding internationally wrongful acts. ➢ Attribution to a State ➢ Proportionality	➢ State's essential interest faces grave and imminent peril. ➢ The sole means of averting that peril.
Advantage	➢ The use of force is available. ➢ Collective responses are available.	➢ Can respond to a wide variety of malicious acts from abroad. ➢ Easy to fit Japan's domestic laws.	➢ There is no need to prove the preceding internationally wrongful acts and attribution to a State.
Disadvantage	➢ Against the mainstream of interpretations of international law. ➢ High possibility of the escalation of disputes. ➢ Antipathies of public opinion at home and abroad. ➢ Difficult to fit Japan's domestic laws.	➢ The use of force is not available. ➢ Attribution to a State is required. ➢ Proof of continuity of wrongful activities is required. ➢ Collective responses are not allowed.	➢ The threshold of invocation is extremely high in low-intensity cyber conflicts. ➢ Requirements are highly ambiguous.

[17] A number of international legal scholars, including Michael N. Schmitt, Jeff Kosseff, Gary Corn, and Sean Watts, have expressed their views on the need for collective countermeasures, and the perceptions of countries appear to be changing. For example, Estonian President Kersti Kaljulaid made a positive affirmation of collective countermeasures in her keynote speech at the 2019 CyCon.

5 Scenario Analysis: Application and Challenges of Countermeasures to the Low-Intensity Cyber Conflicts

As mentioned earlier, countermeasures seem to be the most effective legal mechanism in the response to low-intensity cyber conflicts, but it is foreseeable that several issues will occur in actual situations. This paper clarifies the details and how to handle them through specific scenario analysis. The following three scenarios shown in Table 2 are typical cases of low-intensity cyber conflicts that Japan might encounter in near future.

Table 2. Hypothetical Cases of Low-Intensity Cyber Conflicts.

Case	Situation
Case1	Functional damage to military assets and facilities
Case2	Functional damage to critical infrastructures
Case3	Political turmoil and social unrest by Information Operation

5.1 Assumed Situation

This section explains the premise in common with each scenario. The location of each State is shown in Figure 2[18]. Japan and State C have had a territorial dispute regarding a small Island in the East China Sea for many years. One day, an accidental public vessels collision happened in the disputed area, which resulted in several casualties on the State C side. State C demanded an apology and compensation from Japan, but Japan refused. Both States dispatched more public vessels and aircraft including military assets to the area, and tensions have been rising.

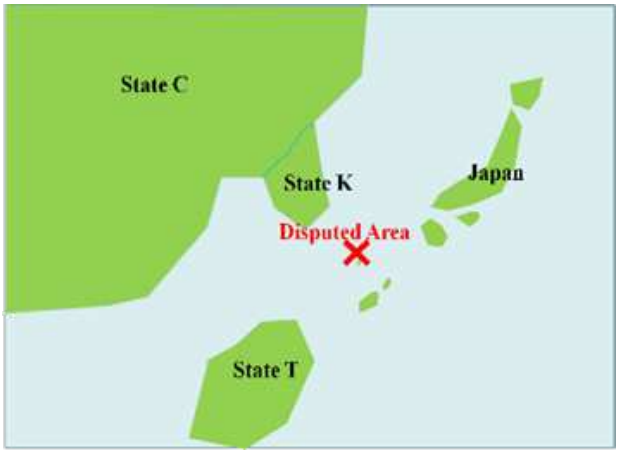

Fig. 2. The locations of each State

[18] Please note that the scenarios and premises are fictional.

5.2 Case 1: Functional damage to military assets and facilities

Assumption. State C invaded Japan Self-Defense Force's (JSDF) C4ISR (Command, Control, Communication, Computer, Intelligence, Surveillance, and Reconnaissance) system by installing malware. The exploitation caused serious data loss and temporal suspension of the system. The incident was caused by the installation of malware in JSDF's internal system via USB through an internal informant, and the malware spread immediately via internal email communication. Eventually, the data in the contaminated terminals was lost, and communications were temporarily cut off. Additionally, during the incident, numerous other unauthorized remote accesses to JSDF's external systems, mainly came from State C, had been confirmed.

Regarding specific damage, JSDF's activities were inactive for several days and many assets had to withdraw from the area. Additionally, the fact of enemy penetration of C4ISR system protection degraded the credibility of the security of the system, and existing of betrayers gave serious damage to the soldier's morale. However, there was no physical damage.

Response. This part discusses how to apply countermeasures to the situation specifically. First, let's see the requirements. Regarding the existence of prior international wrongful cyber acts, the damage that Japan received should be assessed. In this assumption, armed attacks cannot be recognized because physical damage has not occurred. However, since the target is JSDF facilities, there is a military context, and the use of force might be recognized even without any physical damage. In addition, hindering JSDF's effective response would fall under the category of a violation of sovereignty. Furthermore, if State C's involvement and intention to advantageously solve the territorial dispute are clear, it may deserve unlawful intervention.

In this case, Japan might be able to attribute the incident to State C by obtaining evidence of its involvement through investigation of the insider, analyzing the malware code, detecting unique signatures, and identifying IP addresses regarding the unauthorized accesses. The tension between State C and Japan just before the incident should be taken into consideration.

However, to demonstrate that the internationally wrongful acts are continuing, it is necessary to show that the incident in the system is not a single, isolated act, but a series of complex actions together with the remote accesses, and that recurrence is highly likely. Without proving State C's involvement in it, only the remote access from its territory would be pursued as a violation of due diligence, which means that countermeasures can only be implemented to the extent that its negligence to control its territory effectively. Therefore, it is difficult to implement enough effective countermeasures to force State C to stop its internationally wrongful acts.

Next, the question is how degrees Japan can conduct harmful countermeasures against State C. In this assumption, a wide range of options seems to be possible from deleting or exposing confidential data by infiltrating into State C's governmental system as an equivalent mean to directly take down the C&C servers in State C related to the incident. However, it is necessary to avoid being regarded as the use of force.

What are the Challenges? There seem to be three challenges in this scenario. The biggest one is how to prove the continuity of international wrongful cyber acts and their attribution. To do that, consideration should be given to enhancing attribution capabilities including cooperation with allies such as the USA [19][19] and revising domestic laws to enable more effective intelligence activities. Another one is which organization takes responsibility to conduct the countermeasure operations and what kind of specific procedures in the government is required to integrate the efforts of many organizations, as well as the laws that provide the basis of taking such actions. The last one is the foreseeable lack of coerciveness to stop State C's wrongful acts, especially in the case of due diligence. From the legal perspective, it is necessary to consider what effective measures can be taken below the threshold of use of force to conduct effective cyber operations giving reasonable damage against State C. To do so, enhancing cyber intelligence capability and identifying State C's COG[20] is necessary. Besides that, considering the Japanese current technological level, collective countermeasures seem to be indispensable to conducting effective cyber countermeasure operations, even though the legality of it is uncertain for now [18,20]. [21]

5.3 Case 2: Functional Damage to Critical Infrastructures

Assumption. Aiming for political turmoil and social unrest in Japan, State C hacked into the industrial control system of power generation and transmission facilities owned by a private company that supplies electricity to the metropolitan area in Japan, and remotely shut down the power supply, causing a large-scale blackout. The incident was triggered by the exploitation of an employee's computer with a spear-phishing mail attack in a power company that mainly provides electricity to the area. After the exploitation, malware spread rapidly and finally reached the power control system. Immediately after then, the power supply to the center area of Tokyo was cut off by remote access. About 6 million households in the 23 wards of Tokyo, including government offices and various companies, were affected by the blackout, and it took about three days for the power to be restored. Despite no major disruption to government agencies and medical facilities due to the backup power systems and priority restoration, the economic damage was awful. Part of the source code of the malware was written in State C language, and the IP address of the attacker's C&C servers was identified to the area in State C, K, and T territories. However, no new damage has been confirmed since the recovery.

---

[19] The Guidelines for Japan-U.S. Defense Cooperation (April 27, 2015) says “To help ensure the safe and stable use of cyberspace, the two governments will share information on threats and vulnerabilities in cyberspace in a timely and routine manner, as appropriate.”

[20] COG: Center of Gravity. Identifying the enemy's COG and attacking it enable countermeasures to be more effective with causing less damage.

[21] Concerning self-defense, the U.S.–Japan Security Consultative Committee affirmed that collective self-defense will be applied to a cyber-attack in certain circumstances, based on the U.S.-Japan Security Treaty. However, there is no such agreement regarding international wrongful cyber acts below the threshold of armed attack.

Response. Although the incident does not clear the threshold of armed attacks because of the lack of physical damage, there is a possibility that the use of force can be recognized depending on the scale and effect of the economic damage. In addition, an attack on critical infrastructure, including governmental institutions, may constitute a violation of sovereignty as in Case I.

However, the fact that the power outage was promptly restored, and no new damage was caused might be regarded as the end of the internationally wrongful act. To take countermeasures, the possibility of continued violation of international law by the same entity must be explained. As for the attribution, it might be possible to prove State C's violation of the due diligence principle by the fact it was remotely operated from C&C servers in State C's territory, even though there was no concrete evidence to demonstrate State C's involvement in the incident. As in Case I, proportionality and being under the threshold of the use of force are necessary for the implementation of countermeasures.

What Are the Challenges? In this scenario, the biggest challenge would be attribution, because of the suspension of State C's international wrongful cyber acts. How can Japan explain the remaining threats of furthermore attacks? What kind of evidence is required to demonstrate it? Additionally, when Japan takes countermeasures against State C's violation of the due diligence principle, is it possible to aim at State C's critical infrastructure? Can the proportionality rule be cleared considering the damage Japan received? Furthermore, if State C has declared that it regards malicious cyber acts against its critical infrastructure as the use of force, do Japanese countermeasures breach the prohibition of “use of force?” Those are still open questions.

5.4 Case 3: Creating Political Turmoil and Social Unrest by Information Operation

Assumption. State C launched a negative campaign against Japan's government on the Internet by falsifying the websites of the Japanese government and private companies, spreading fake news, exposing secrets, etc., intending to lower support for the current government in Japan. Since the collision in the disputed area, there have been several cases of tampering with the websites of celebrities. On those websites, many opinions supporting State C have been posted, and a lot of information related to the regime scandal has been posted on the Internet. Some of them turned out to be fake news. As a result, the current approval rate for the government dropped significantly. Most of the IP addresses were routed through public proxy servers located in State K and T. However, a part of them was found to be routed through State C's territory, but the State C government denied any involvement. As for the fake news, there were some errors in characters which are common in the sentences of translation from State C's language to Japanese.

Response. Infiltrating and falsifying government websites will deserve to violation of sovereignty, but the legal perspective of doing the same things against private ones is

ambiguous. In short, countermeasures can't be applied to the latter acts because countermeasures require internationally wrongful acts. Although such acts can be against the domestic laws of each State, international law mentions nothing about a State's violation of another State's domestic laws. So, in this scenario, Japan can apply the countermeasures only within the limits that State C did against the government websites in terms of the proportionality rule.

What are the Challenges? The challenge in this scenario is the legal character of the infringement against private systems. Nowadays Information Operations have a strong influence on governments' policies and societies around the world. However international law doesn't say anything about the wrongfulness of those as far as the operations are aimed at only private systems and do not cause any physical damage. More discussions seem to be required about this matter. Besides that, the Attribution of wrongful cyber acts through third States will be also a big issue.

6 Proposals

Finally, this paper suggests some proposals that Japan should consider conducting effective countermeasure operations in low-intensity cyber conflicts. So far, this paper has explained an overview of the international law applicable to low-intensity cyber conflicts and demonstrates that countermeasures can be a powerful tool in the situation, of Japan. And then, this paper clarifies how to apply countermeasures to concrete cases through the scenario analysis, and several challenges are also identified during the analysis. To conquer them, this paper proposes the following realistic policies which Japan should take; (1) clarifying the responsible organization and establishing domestic legislation about cyber countermeasures (2) taking initiative in the campaign for the legalization of collective countermeasures, (3) improving attribution capability including collective ways with allies, and (4) developing ethical and legal norm to prohibit the malicious cyber acts against private enterprises.

6.1 Clarifying the Responsible Organization and Establishing Domestic Legislations about Cyber Countermeasures

To conduct cyber countermeasure operations, it is imperative to clarify a responsible organization and establish proper domestic legislation to provide legitimacy to the operation. For now, Japan does not have clear domestic laws to provide such operations with a concrete legal basis. It means that Japan cannot react to the immediate cyber threats with countermeasures, so this matter should have the biggest priority.

6.2 Taking Initiative for Legalization of Collective Countermeasures

A drawback of countermeasures is the possible lack of enough power to persuade a responsible State to stop conducting its malicious cyber acts. In that case, collective

countermeasures are highly lucrative. Indeed, there are still many negative opinions about its legality of it, however, many international law experts have recognized and insisted on the necessity of establishing a new legal framework that enables States can take collective countermeasures. Japan should express clear support for the idea and lead the argument.

6.3 Improving Attribution Capability Including Collective One with Allies

Regarding the improvement of the attribution capability, it will be important for Japan not only to enhance its capacity but also to cooperate with other countries, including mutual exchanging technical support and intelligence. To do so, the criteria and legal requirements enough to attribute malicious cyber activity to a responsible State should be clarified. Especially it is necessary to consider what kind of evidence is required and how deep accountability an injured State owes to attribute.

6.4 Developing Ethical and Legal Norm to Prohibit the Malicious Cyber Acts Against Private Entities

The biggest defect of countermeasures is that the malicious cyber acts against private entities will be out of their scope, whereas the most common cyber incidents fall in this category. Particularly disinformation activities are becoming formidable threats due to the development of technology and change in social structures. To deal with this issue, the new ethical and legal norm seems to have to be considered. Japan should try to construct those norms by cooperating with other States. It can also be considered an effective way that Japan insists on the continuation of a framework such as the UN Groupe of Government Experts and taking leadership.

7 Conclusion

Responding to low-intensity cyber disputes is a major challenge for the international community as a whole, and various studies and discussions have been conducted on the use of countermeasures. In Japan, however, discussions have been weak and no concrete progress has been seen. Given Japan's unique circumstances, countermeasures have the potential to be an effective means of response, and further research is expected. The proposals made in this paper are realistic and do not require a constitutional amendment, and they can be the first step for Japan to take a leadership role in establishing norms in cyberspace.

References

1. The Government of Japan.: Cyber Security Strategy, https://www.nisc.go.jp/materials/index.html, last accessed 2022/5/12.

2. International Institute for Strategic Studies (IISS).: Cyber Capabilities and National Power: A Net Assessment (2021), https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power, last accessed 2022/5/12.
3. Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, U.N. Doc. A/76/135 (2021).
4. Open-ended working group on developments in the field of information and telecommunications in the context of international security.: Final Substantive Report, U.N. Doc. A/AC.290/2021/CRP.2 (2021).
5. Schmitt, M., (ed.): Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, Cambridge (2017).
6. Schmitt, M.: "Below the threshold" cyber operations: the countermeasures response option and international law. Virginia Journal of International Law 54, 697–732 (2014).
7. Kosseff, J.: Collective countermeasures in cyberspace. The Notre Dame Journal of International & Comparative Law 10, 18–34 (2020).
8. Keiko, K.: Invoking the right of self-defense against cyber-attacks. Junichi Eto (ed.) Aspects of International Law Studies Reaching: The Point and Looking Ahead: Mr. Murase Shinya's Rare Memories, pp. 847–862. Shinzan-sha, Tokyo (2015).
9. Draft Articles on Responsibility of States for Internationally Wrongful Acts, in Report of the International Law Commission on the Work of its Fifty-third Session, UN GAOR 56th Sess., Supp. No. 10, at 43, U.N. Doc. A/56/10 (2001).
10. Sugihara, T.: Lectures on International Law. 2nd edn. Yuhikaku, Tokyo (2013).
11. Case Concerning Military and Paramilitary Activities in and against Nicaragua, 1986 I.C.J.14,181, Merits, Judgement (27 June).
12. Case The Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania), 1949 I.C.J. 105, Merits, Judgement (9 April).
13. Ministry of Foreign Affairs of Japan.: Basic Position of the Government of Japan on International Law Applicable to Cyber Operations, https://www.mofa.go.jp/policy/page3e_001114.html, last accessed 2022/5/12.
14. The Liberal Democratic Party.: First Proposal of the Liberal Democratic Party Cyber Security Task Force (April 24, 2018), https://www.jimin.jp/news/policy/137263.html, last accessed 2022/5/12.
15. Fischerkeller, M., Harknett, R.: Persistent engagement, agreed competition, and cyberspace interaction dynamics and escalation. In: The Cyber Defense Review, Special Edition, International Conference on Cyber Conflict (CYCON U.S.), November 14–15, 2018, Cyber Conflict During Competition, pp. 267–287. Army Cyber Institute, New York (2019).
16. Corn, G., Jensen, E.: The use of force and cyber countermeasures. Temple International & Comparative Law Journal 32 (2), 127–133 (2018).
17. Schmitt, M., Watts, S.: Collective cyber countermeasures?. Harvard National Security Journal 12(2), 373–411 (2021).
18. Roguski, P.: Collective countermeasures in cyberspace: Lex lata, progressive development or a bad idea? In: The 12th Annual International Conference on Cyber Conflict (Cycon 2020), pp. 25–42. NATO CCDCOE Publications, Tallinn (2020).
19. The Government of Japan.: The Guidelines for Japan-U.S. Defense Cooperation April 27, 2015, https://www.mofa.go.jp/region/n-america/us/security/scc/index.html, last accessed 2022/5/12.
20. Ministry of Foreign Affairs of Japan.: Joint Statement of the Security Consultative Committee (2019), https://www.mofa.go.jp/mofaj/files/000470738.pdf, last accessed 2021/12/21.