How Does the Tallinn Manual 2.0 Shed Light on the Threat of Cyber Attacks against Taiwan?

Chih-Hsiang Chang
Graduate, Institute of Interdisciplinary Legal Studies, National Taiwan University

r07a41028@ntu.edu.tw

Abstract: This paper will identify possible unsettled issues when applying jus ad bellum and jus in bello to case scenarios based on China's cyber operations against Taiwan, pursuant to the rules of international law governing cyber or military operations attributable to States reflected in Tallinn Manual 2.0. This paper will argue that because of Taiwan's legal international status as a sovereign State, the different responsive actions it may take, should it be faced with any such aggressive cyber or military attack, may be considered controversial. This paper will then identify the possible legal issues that may pertain under current international law, should any such armed conflict occur between China and Taiwan.

Keywords: cyber attack, cyber armed conflict, international humanitarian law, the Tallinn Manual 2.0, Taiwan Strait Crisis, right of self-defence.

1. Introduction

As a regional power in Asia, China does not shy away from its ambition to "reclaim Taiwan" as its territory, and recent military aggression has inevitably pushed Taiwan and China to the edge of another Taiwan Strait Crisis. Apart from the constant threat of kinetic attacks, Taiwan has also become a hotspot for frequent disinformation and cyber operations in both the private and public sectors, which have often been identified as suspicious activities, conducted by hackers from China.

Russia's invasion of Ukraine in 2022 is a typical case of how multiple cyber operations, both prior to and during an assault, can be deployed either to hike up geo-political tensions, or as a precursor to actual armed conflict. Consequently, should China adopt similar tactics towards Taiwan, it may use similar tactics and initiate cyber attacks against Taiwan, whether during peacetime or in an actual war. Thus, it is important to examine what possible legal challenges Taiwan would be faced with, given its current international status, while dealing with the threats from cyberspace, particularly since it is often treated by other sovereign States as merely a de facto self-governing entity and not a fully-recognised State.

This paper will answer the following questions:

1. How will Taiwan be governed by the Tallinn Manual 2.0 Rules regarding armed conflict?
2. What legal issues may arise if Taiwan applied the Tallinn Manual 2.0, should it be targeted by Chinese cyber attacks?
3. Combating the cyber attacks, what are possible lawful responses for Taiwan to choose from under the framework of international law?

This paper's methodology will be as follows: (i) a brief review of the controversy over Taiwan's current international legal status, (ii) a contemporary history and geo-political power struggle assessment will be described, (iii) the controversies in terms of applying IHL to Taiwan in terms of armed conflict will be explained, (iv) publicly-known cyber operations against Taiwan will be examined, (v) case scenarios, based on the rules of the Tallinn Manual 2.0, will be described in order to determine how malicious cyber operations shall be governed with regard to international law, and (vi) critical legal issues regarding Taiwan's exercise of its rights to self-defence in the event of a cyber attack will be discussed.

2. The Legal Status of the Republic of China (Taiwan)

To discuss how the international humanitarian law shall be applied if Taiwan becomes a party of an armed conflict, the first priority would be to determine whether Taiwan may be deemed to be a sovereign State.
Taiwan and the Republic of China (ROC) are practically — and diplomatically — synonymous in the eyes of today's international society; however, there is a divergence between its de jure and de facto legal status which cannot be ignored.

2.1 Historical background

After the implementation of the Treaty of Shimonoseki (1895) between the Empire of Japan and Qing China,

Taiwan (the Formosa Island and the Pescadores) fell under the rule of Japan as an oversea colony until Japan surrendered to the Allied Powers in 1945, when it renounced its rights over Formosa and Pescadores in the San Francisco Peace Treaty of 1951 (Chen, 1998).

Following General Order No.1 by General Douglas MacArthur, Taiwan experienced a post-World War II military occupation by ROC, whose government (the government formed by the Chinese Nationalist Party, which is also known as KMT) was led by Generalissimo Chiang Kai-Shek. However, following its defeat in a civil war (1945-1949) by the Chinese Communists Party, Chiang fled to Taiwan with his army and imposed perpetual martial law on the island for 38 years in the name of the Nationalist Chinese authorities (1949 to 1987), which caused the islanders to suffer what they called "the white terror" employed by an authoritarian regime, notorious for violating human rights (Chen, 1998).

However, as a consequence of the United Nations General Assembly (UNGA) Resolution, 2758 of 1971, which not only terminated the membership of the Republic of China (ROC), but also resulted in most members of the international community recognizing the People's Republic of China (PRC) as the only representative of China instead of ROC. Thus, during the 1970s and 1980s, faced with the dual challenge to its Chinese representational legitimacy and relentless local campaigns in Taiwan for civil rights, the KMT leadership eventually conceded to a transformation to democracy through "Taiwanization" (Chen, 1998). During the 1990s, new articles of the Constitution, allowing for general elections of legislators and the president of the central government, were instituted. In 1996, the Taiwanese were able to enjoy full political democratic power. Then in 2000, came the remarkable peaceful transfer from the KMT to the Democratic Progressive Party (DPP) (Chiang & Hwang, 2008).

2.2 Controversies surrounding Taiwan's legal status

Theories regarding Taiwan's legal status fall into three categories.

1. That Taiwan should be part of China through "acquisitive prescription"; this has long been advocated by the PRC through its "one China principle". Hence, PRC treats Taiwan as a "renegade province" through State practice.
2. That ROC (Taiwan) "has emerged as an independent State" (Chiang & Hwang, 2008); hence it should be considered a sovereign State, even though it is officially called the Republic of China. Although it has never officially declared its independence - a requisite under the "Declaratory Theory of Recognition" – its supporters believe that its statehood is self-evident through State practice.
3. That Taiwan is an international condominium of the Allied Powers; therefore, the issue regarding its sovereignty is not an internal affair of China and should be settled through peaceful multilateral actions. They reject the PRC's claim, and deny the legitimacy of the ROC since Generalissimo Chiang was only acting as a delegate on behalf of those States that were parties to the San Francisco Treaty; it is those States that should collectively either decide the future of Taiwan, or transfer it to the United Nations Trusteeship Council.

Apart from theoretical disputes, the official position of the ROC has changed dramatically. Before 1973, it was much closer to that of PRC than to other major powers. The main difference was that ROC claimed to be the only legitimate government of China. However, after PRC obtained the representation of China in the UN in 1973, ROC limited its sovereign claim to those territories that had been under its effective control since 1949 – Taiwan (Formosa), Penghu (the Pescadores), Kinmen (Quemoy) and Matsu (Chiang & Hwang, 2008); this remains its official position to date.

Prior to 1973, the international legal mainstream and major powers favoured the third position; however, substantial changes have reshaped the latter's foreign policies since then; also, following Taiwan's democratization, many scholars agree that Taiwan is "a self-governing entity whose legal status remains indeterminate", thus it is prevented from possessing the usual rights, obligations, and immunities of a recognized independent State, even though it is both "edging towards formal separation" and is "functioning as a de facto State" (Crawford, 2006).

2.3 Tallinn Manual 2.0 and Taiwan: The Application of the Law in Terms of a Cyber Operation in nexus with an Armed Conflict

To identify whether a cyber operation in nexus with an armed conflict could occur between Taiwan and China,

and to examine the legal issues regarding international humanitarian law should it do so, it is crucial to define what an armed conflict is and what its nature might be.

Pursuant to Common Article 2 of the Geneva Conventions of 1949 and the accompanying International Committee of the Red Cross (ICRC) Commentary, an international armed conflict (IAC) exists whenever there is resort to hostile armed force between two States. The threshold of a non-international armed conflict (NIAC) is much higher. Common Article 3 covers a "conflict not of an international character occurring in the territory of one of the High Contracting Parties"; however, it lacks a clear definition. Nevertheless, the International Criminal Tribunal for the Former Yugoslavia (ICTY) provided a standard in the Tadić judgement, which required two conditions: a protracted armed violence (i) between government authorities and organized armed groups, or (ii) between such groups within a State.

Regarding cyber operations, the Tallinn Manual 2.0 states that "cyber operations executed in the context of an armed conflict are subject to the law of armed conflict" (Rule 80); however, two requisites must be satisfied: (i) the existence of cyber operations, and (ii) a nexus between the cyber activity in question and the conflict for the law of armed conflict to apply to that activity. Regarding the classification, the definitions of a cyber IAC and a NIAC are included in Rules 82 and 83, and they must fully reflect the principles of Common Articles to the Geneva Conventions of 1949 and the standard from the Tadić judgement.

2.4 If Taiwan becomes involved in an armed conflict with China, would it be considered to be international or non-international?

The debate about whether Taiwan's statehood plays a significant role in terms of International Humanitarian Law (IHL). If a position (regardless of reasons) is adopted by arguing that Taiwan is not an independent State, then the requirement of "a protracted armed violence", implying greater extent, duration, or intensity of hostilities, must be satisfied. This approach would not favour Taiwan if it were to face imminent hostilities that endanger the safety of its people, especially when one of China's strategies is to initiate a surprise attack to consolidate its military advantage and create a fait accompli, which may leave other stakeholders, or the UN, to find it too hard, or too late, to intervene.

In the cyber context, a similar problem regarding the threshold of NIAC also exists. In the Tallinn Manual 2.0, the Experts noted that "the precise parameters of the phrase 'in the context of' are less clear in a non-International armed conflict," because "a State retains certain law enforcement obligations and rights with respect to its territory, notwithstanding the armed conflict" (Commentary to Rule 80). Considering there are more uncertainties about whether certain cyber operations qualify as cyber attacks, thereby meeting the standard of armed attack under Article 51 of the UN Charter (see Sections 3.2 & 3.3), treating Taiwan as a non-sovereign State increases the difficulties of applying IHL on cyber attacks. Therefore, if applying the Declaratory Theory stricto sensu, IHL may not favour Taiwan should it face imminent hostilities that endanger the security and welfare of its people.

2.5 Cyber attacks Governed by International Humanitarian Law

i. The definition of the term "cyber attack"

Rule 92 of the Tallinn Manual 2.0 defines a cyber attack as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects", which follows Article 49(1) to Additional Protocol I of the 1949 Geneva Conventions (AP I), stating "acts of violence against the adversary, whether in offense or defence."

The Tallinn Manual 2.0 also states that "any cyber operation rising to the level of an armed attack in terms of scale and effects pursuant to Rule 71 qualifies as a 'use of force' if it is conducted by or otherwise attributable to a State (Commentary to Rule 69). In addition, the Experts "unanimously concluded that some cyber operations may be sufficiently grave to warrant classifying them as an 'armed attack' within the meaning of the Charter." (Commentary to Rule 71). However, they agreed that de minimis damage or destruction does not meet the threshold of harm required by Rule 92 (Commentary to Rule 92). In summary, the Tallinn Manual 2.0 does not deny that certain cyber operations alone can be armed attacks and therefore constitute armed conflict. In compliance with IHL, the Tallinn Manual 2.0 proposes numerous Rules to limit the scope of lawful military objectives that cyber attacks may target.

Two of its important principles are discussed through a case study, (i) civilian infrastructure is protected by existing IHL rules, particularly the principles of distinction, proportionality and precautions in attack, and (ii)

civilian data shall be protected from significant disruption. Intentional violations of these, directed against civilian objects may be war crimes (Article 8(2)(b)(ii) of the Rome Statute (1998).

ii. The unsettled issues in the Tallinn Manual 2.0 relevant to targets attacked by cyber means

Before applying the Tallinn Manual 2.0 on scenarios in Taiwan, note that several issues remain unsettled due to divisions among State's positions and practices concerning the definition of "damage or destruction to objects" in Rule 92, based on Article 52(2) of AP I.

The first concerns whether "interference by cyber means with the functionality of an object" constitutes "damage or destruction to objects" (Rule 92). The Experts were broadly split on this issue. The majority insisted that only when restoration of functionality requires replacement of physical components, does interference qualify as damage. The second position, held by some members of the majority, was that such interference "extends to situations in which reinstallation of the operating system or of particular data is required in order for the targeted cyber infrastructure to perform the function for which it was designed". The third position, adopted by a few Experts, held that how an object is disabled is irrelevant; instead, the loss of usability of cyber infrastructure constitutes damage that qualifies as a cyber attack if cyber infrastructure in question is targeted (Commentary to Rule 92 of Tallinn Manual 2.0).

The second unsettled issue is whether data is an "object" under Rule 92, on which the Experts widely diverged. In the view of the majority of the Experts, data is intangible and therefore "neither falls within the ordinary meaning of the term object, nor comports with the explanation of it offered in the ICRC Additional Protocols 1987 Commentary". On the contrary, a minority of the Experts was of the opinion that, for the purposes of targeting, certain data should be regarded as an object. Also, for the minority, it is based on the underlying object and purpose of Article 52 of Additional Protocol I, instead of the nature of harm, the key factor should be "the severity of the operation's consequences". (Commentary to Rule 92)

2.6 Case study: a basic legal analysis of a possible cyber attack against Taiwan

In Section 3.3, principles and rules from the Tallinn Manual 2.0 will be applied to different scenarios, if cyber operations are launched against Taiwan. This case study will proceed based on the assumption that Taiwan is an independent sovereign State. Two questions are posed, (i) if there is a nexus between the cyber operation and the existing armed conflict, can the cyber operation constitute a cyber attack as defined by Rule 92, depending on its scale and effect (Rule 69)? And (ii) is the purported cyber attack against an unlawful target under IHL, according to Tallinn Manual 2.0?

iii. Submarine cables near Taiwan: a possible trigger to armed conflict

In February 2023, submarine cables providing the Internet service in Matsu were damaged, causing a temporary shut-down of the Internet connection. This was not the only incident in recent years, and most have occurred due to civilian fishing vessels, which, according to media reports, have been Chinese dredgers.

It is generally agreed that, should China launch military operations to change the status quo by damaging submarine cables, Internet connectivity on and to Taiwan will be severely restricted, or cut entirely. This could encourage China to create a 'war-mist' during a beginning phase of an invasion. One vulnerable site is in the Luzon Strait near the Philippines, where all cables connecting Hong Kong, Taiwan, South Korea and Japan, are situated, which could disrupt service in the whole of northeast Asia, thus potentially constituting a cyber-attack under Rule 92, violating Article 113 of the United Nations Convention on the Law of the Sea (UNCLOS). Therefore, if China disrupts submarine cables providing most of the Internet service for Taiwan by cyber means, assuming it is technically feasible, do the operations constitute a cyber attack under Rule 92?

Clearly, such operations are violation of States' responsibilities for cable protection if the targeted submarine cables located on the high seas (Article 113 of UNCLOS). The Tallinn Manual 2.0 Experts agreed, in that "the infliction of damage to cables by a State is prohibited as a matter of customary international law since doing so would run contrary to the object and purpose of the law governing submarine cables". Furthermore, they agreed, "there is no legal basis to cut another State's submarine fibre optic cable in order to reduce trans-continental Internet traffic in times of tension" (Commentary to Rule 54).

However, a crucial point is whether the cyber operation caused "damage or destruction to objects" pursuant to Rule 92. If the positions supported by the majority of the Experts were adopted, unless the operations required the replacement of physical components of optical fibres, such as materials for the core, the cladding or the coating, the interference itself would not qualify as damage. However, if the minority's position were followed,

the consequence of successfully blocking the Internet service of Taiwan and other neighbouring countries, resulting in significant economic loss, could be considered a hostile cyber attack.

Even if such a cyber operation did constitute a cyber attack, because communications for military use often share the same cables with commercial communications, it is hard to distinguish the one from the other. Thus the principle of "dual-use objects" renders submarine cables as lawful targets (Rule 95, Tallinn Manual 2.0) while a traditional interpretation of IHL sets a lower bar regarding the principles of distinction (Rule 93, the Tallinn Manual 2.0) and the proportionality (Rule 113) in the case of targeting submarine cables. This aligns with historical precedents and States' practices regarding the application of law of armed conflict on kinetic attacks against submarine cables (Harbin, 2021).

ii. Industrial Control System (ICS) of private companies: the vulnerability of the semiconductor-manufacturing industry

So far, suspicious Chinese cyber operations that have been detected were denial-of-service attacks (DDoS) against government websites, or the dissemination of rumours or disinformation, which mostly "merely cause[d] inconvenience or irritation to the civilian population" and have created minor temporary disruptions, which fall short of armed attacks (Commentary to Rule 92, the Tallinn Manual 2.0) Thus, their scale and effects were largely immaterial (Rule 69, the Tallinn Manual 2.0). However, it has been deemed advisable for private companies to evaluate the potential cybersecurity risks, especially regarding the nexus between the semiconductor industry and national security.

The Taiwan Semiconductor Manufacturing Company (TSMC) reportedly controls more than 60% of the world's semiconductors and over 90% of the most advanced ones; it alone contributes 15% of Taiwan's GDP. Therefore, from China's perspective, to sabotage it would not only undermine Taiwan's economic strength, but also cause negative influence on other States, such as the US. Furthermore, Industrial Control System (ICS) is a collective term used to describe control systems and associated instrumentation, including the devices, systems, networks, and controls used to operate and automate industrial processes. This mostly include Supervisory Control and Data Acquisition (SCADA) systems and Distributed Control Systems (DCS), most of which are highly-automated and rely heavily on ICSs, particularly in the semiconductor manufacturing industry. For example, a statistical process control is crucial for semiconductor manufacturers to monitor process variability and detect outliers.

In order to gain leverage, or to coerce Taiwan to submit to its political agenda, if China launched cyber operations against the SCADA systems of TSMC, or the main Taiwanese semiconductor manufacturers, by deleting, or altering technical data, causing significant economic loss and a stock market crash; whether this would satisfy the definition of cyber-attack under Rule 92 is hard to establish due to the lack of consensus about such data falling under that rule; however, it is worth referring to a broader interpretation of Article 52 of AP I, which some scholars agree that "data is an object under IHL, therefore it may be a military objective" (Mačák, 2015).

The Vienna Convention on the Law of Treaties (1969) does not apply to norms of customary law. Therefore, it is possible that a norm exists in parallel in both treaty law and customary law, which is clarified in the Nicaragua judgement of the International Court of Justice (ICJ). Therefore, Article 52(2) can be "described as a 'fundamentally norm-creating' treaty rule of the kind the ICJ considered to be eligible of evolving into custom in the North Sea Continental Shelf cases" (Mačák, 2015). Therefore, by adopting the minority's position, should a destructive cyber attack be initiated against crucial civilian data by cyber means, there is a possibility that, depending on the scale and effects manifested (Rule 69, the Tallinn Manual 2.0), cyber operations against TSMC, or the whole Taiwanese semiconductor industry, may qualify as a cyber attack.

If this conclusion is accepted, the next step would be to examine whether TSMC and other similar companies are lawful military objectives. Although the semiconductor manufacturing industry is a part of the private sector, it is crucial to examine whether this satisfies the "dual-use object" standard in Rule 95. In contemporary warfare, semiconductors are of vital strategic significance, because no military equipment and weaponry, such as satellites, drones, guided missiles and jets, can function without sophisticated electronic chips.

In the Commentary to Rule 100 of the Tallinn Manual 2.0, two scenarios were given. The first one is a factory producing computer hardware or software under contract to the enemy's armed forces; the second is the enemy State's oil export industry, on which its war effort depends heavily. All the Experts agreed on the computer factory case, which by its use is a military objective; however, in the second example, the majority of the Experts rejected the concept that "war-sustaining objects" are lawful military objects, as stated in the US Department of Defence Law of War Manual.

Despite this divergence of opinion, considering the indispensable role electronic chip-producing plays in modern weapon systems, semiconductor companies, such as TSMC, may qualify both as the producer for its armed forces, and as war-sustaining objects, which would render their chip manufacturers both lawful, and vulnerable, military objectives during a war.

3. A dilemma: legality vs legitimacy

Even though the theoretical disagreements surrounding the sovereignty controversies of Taiwan do not substantially affect its active role as an influential political entity in the real-world of international politics, they would make a difference if it chooses to claim the right of self-defence, or to adopt countermeasures to protect its cyber-security as an independent State under international law. Such issues cannot afford to be overlooked, especially in such times of heightened tension.

iv. Self-defence and customary international law

The doctrine of a State's right to self-defence in customary international law was crystalized after the Caroline incident, and the rules in terms of exercising this right were stipulated in Article 51 of the UN Charter. While Article 2(4) strictly prohibits the "threat or use of force in international relations", Article 51 covers one of the rare exceptions for a State to legally employ the use of force, which is explicitly invoked where a UN Member State has suffered an "armed attack" — i.e. a grave form violation of Article 2(4)'s prohibition on the use of force, which was explicitly distinguished from the term 'use of force' in the ICJ Nicaragua judgment.

v. Self-defence in the cyber context: the issue of whether a cyber operation constitutes an armed attack

It was unanimously agreed by the Tallinn Manual 2.0 Experts that some cyber operations "may be sufficiently grave to warrant classifying them as an armed attack" within the meaning of the UN Charter. Consequently, the Experts concurred that the right to employ force in self-defence extends to those armed attacks that are conducted solely through cyber operations, which do not necessarily involve the employment of weapons (Rule 103) (Commentary to Rule 71, the Tallinn Manual 2.0).

In the Tallinn Manual 2.0, the threshold required for cyber operations constituting armed attack is high. For instance, the Experts expressed a "general agreement that cyber operations that merely cause inconvenience or irritation to the civilian population do not rise to the level of attack" (Commentary to Rule 92); additionally, the following activities in cyberspace do not qualify as armed attacks: "acts of cyber intelligence, gathering and cyber theft, as well as cyber operations that involve brief or periodic interruption of non-essential cyber services" (Commentary to Rule 71).

3.1 Taiwan to exercise the right of self-defence against cyber attacks by China

vi. Self-defence as a "limited-to-States" right

If Taiwan is not recognised as an independent sovereignty, it complicates the legal relationships between stakeholders, thus rendering the existing sovereignty issues surrounding Taiwan to be more challenging, particularly when pursuing the sensu stricto legality under international law.

Firstly, ROC (Taiwan) cannot claim the right of self-defence because this is limited to sovereign States. Although, in order to protect its people from imminent danger of threat, or use of force, its authorities may argue that the international community should follow the doctrine of "Responsibility to Protect" and take immediate action, military or not, to justify humanitarian intervention from other States by referring to the precedent case of Kosovo; however, this legal doctrine is still highly contested in international law. Additionally, it is generally observed that, unless abhorrent atrocities, such as grave war crimes or genocide are committed repeatedly, most States will tend not to actively support the claims of groups seeking self-determination, and adopt the principle of non-intervention, because they are regarded as the internal affairs of a State.

Secondly, the inconvenient truth of the awkward legal position of the ROC armed forces would be brought to the table. The military forces as a part of the ROC establishment could be regarded as an armed group, which does not act on behalf of a sovereign State, because ROC is no longer regarded as the legitimate regime representing China by the majority of the international community. Although the Taiwanese authorities may claim that as a party of the Treaty of Peace Between the Republic of China and Japan (also known as the Treaty of Taipei, 1952) and a member of the Allied Powers, the ROC and other parties to the San Francisco Peace Treaty, bear an obligation to maintain international peace and security in respect to Article 2 of the UN Charter;

however, this argument does not provide the legal basis to exercise the right of collective self-defence by other States, such as Japan or the US, since Taiwan is a “non-State actor” (Himes & Kim, 2021).

Consequently, in international law, as long as Taiwan is regarded merely as a self-governing entity, a roundabout way to deal with the legalities regarding the countermeasures it may undertake must be proposed. Considering the UN has no systematic integrated policy for engaging, or intervening, with de facto authorities, but only separate guidelines, based on a case-by-case approach, the ambiguity of Taiwan’s status can only bring further legal uncertainty, which could result in the interests of its people being neglected. An alternative solution might be a "quasi-declaration of independence" (Chiang & Hwang, 2008) by which Taiwan implies its intention to be regarded as a sovereign State, which should settle most of the abovementioned legal issues and result in the best outcome.

vii. Taiwan’s strike back: by armed force or by civilians?

Countermeasures may be adopted by a State when two perquisites are satisfied: (i) that the breach of an international obligation owed to the injured State is established, and (ii) that the purported wrongful act is attributable to the responsible State. Launching an armed attack against another State is certainly a violation of the rule prohibiting the use of force under customary international law. However, in the cyber context, if a State decides to "hack back" as a lawful countermeasure against cyber attacks, it is required to identify a violation of international law by the hacker group in order to determine whether, and how, the group's activities were affiliated with the responsible State (Schmitt, 2013).

In Taiwan’s scenario, a cyber countermeasure could be conducted by digital ‘armed forces’. In fact, the Information Communication Electronic Force Command (ICEF), which was inaugurated on July 1, 2017, is crucial to Taiwan’s offensive cyber operations. Its purpose is to consolidate communication, cyber, and electronic warfare units under one authority. Nevertheless, observing the current policy adopted by President Tsai’s administration, it is more likely that the ICEF will develop defensive strategies and tactics, rather than to proactively hack back.

On the other hand, a group of “volunteer hackers” may become involved in the cyber armed conflict, since such participation is not unlawful under IHL. For instance, after the first day of Russia’s invasion, Ukrainian Vice Prime Minister Fedorov publicly called on volunteer hackers and announced a list of thirty-one websites of Russian banks, corporations and government agencies as being valuable targets. Thus, they reportedly amassed an “IT army” of more than 400,000 volunteers. According to some Chinese official reports, China has detected a hacker group called “Green Spot”, which allegedly targets its own State organs, including military institutions, embassies, financial institutions, and its nuclear industry.

However, according to the Tallinn Manual 2.0, the Experts remained divergent regarding the status of patriotic hackers. While the majority agreed that civilians retain civilian status, even if they directly participate in cyber hostilities; however, they themselves may be lawfully targeted. Therefore, unless they qualify as participants en masse in a levée, they will lack combatant immunity for their actions. Furthermore, a minority of the Experts rejected the notion that such individuals would benefit from the protection of Geneva Conventions III or IV, because they qualify neither as combatants or civilians (Commentary to Rule 91).

4. Conclusion

This paper describes the legal risks and uncertainties that are inherent in Taiwan’s uneasy relationship with China, which seems to be perpetually poised to spill over into either cyber, or armed, conflict, thereby threatening its economic stability and the well-being of its people. Because of its peculiar historical circumstances, and given the delicate balance of world politics, Taiwan must take a nuanced approach in order to establish a stable global position. However, the inconsistency between the de jure legal status and de facto international politics, is immense, which means that it would be difficult for the international community to respond should such an unwanted situation arise. At the same time, Taiwan must continue to strive to find a way to protect its people, for the longer it lingers in a state of uncertainty the more risk its people will have to face.

Should such a crisis arise with China, legal barriers could prove to be highly intractable obstacles. They could also present as unstable factors, both for Taiwan itself, and for other States that will have to determine whether, or not, to intervene, since the lawfulness of a State’s actions will play a key role in adopting any response to an armed conflict.

This paper suggests it is likely that Taiwan will continue to be trapped in an obscure zone within the realm of international law. Consequently, it calls for an overall scrutiny and thorough examination of its position in the international community in order to determine how it might develop an integrated legal strategy in response to a possible cyber, or armed, conflict across the Taiwan Strait, irrespective of whether it be kinetic or cyber in nature.

References

Chen, L. C. (1998). "Taiwan's Current International Legal Status", 32 NEW ENG. *L. REV, 675.*

Chiang, H. C., & Hwang, J. Y. (2008). "On the statehood of Taiwan: A legal reappraisal", *The "one China" dilemma*, pp 57-80.

Crawford, J. (2006). *The creation of states in international law*, Oxford University Press.

Harbin, D. (2021). "Targeting submarine cables: new approaches to the law of armed conflict in modern warfare", *Military Law Review, 229(3),* pp 349-380.

Hayward, R. J. (2017). Evaluating the imminence of cyber attack for purposes of anticipatory self-defense. *Columbia Law Review, 117(2)*, pp 399-434.

Himes, A., & Kim, B. J. (2021). "Self-Defense on Behalf of Non-State Actors", *U. Pa. J. Int'l L., 43*, 241.

Jain, J. P. (1963). "The Legal Status of Formosa: A Study of British, Chinese and Indian Views", *American Journal of International Law*, 57(1), pp 25-45.

Mačák, K. (2015). Military objectives 2.0: The case for interpreting computer data as objects under international humanitarian law. *Israel Law Review, 48(1)*, pp 55-80.

Schmitt, M. N. (2013). "Below the threshold cyber operations: The countermeasures response option and international law", *Va. J. Int'l L., 54*, 697.

Schmitt, M. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd ed.), Cambridge: Cambridge University Press.

Note: Unless otherwise indicated, the term "Taiwan", as it is used in this paper, encompasses the island of Taiwan (Formosa), Penghu (The Pescadores), and other islets which fall under the effective control of the Taiwanese authorities. It is important to note that issues regarding the legal status of Kinmen (Quemoy) and Matsu will not be discussed here.