In September last year, Vice President William Lai (□□□) attended the Hacks in Taiwan Conference, a cybersecurity conference held annually in Taiwan. He said: “Taiwan is in a key position on the first island chain and faces a grave threat from China. It suffers 30 million cyberattacks every month.”

Echoing President Tsai Ing-wen’s (□□□) belief that “cybersecurity is national security,” Lai advocates a policy for enhancing the cybersecurity industry on par with the West’s.

In cyberwarfare, defense is costly, and no country, not even those with the best abilities in information and communications technologies, such as the US, can ensure complete cybersecurity.

Cyberattacks are cheap and effective. The essence of cyberwarfare is an extension of electronic warfare, which jams an adversarial country’s radar and interrupts its electronic communications. The US military’s air-land battle doctrine to disrupt an enemy’s electronic capabilities is a case in point.

Bringing the battlefield of cyberwarfare to the enemy’s territory also conforms to the principle of engagement in the military domain. What is more, the stealth architecture deployed in cyberwarfare can minimize the risk of being discovered and can allow plausible deniability, which makes cyberwarfare suitable for use in peacetime. To a certain extent, Taiwan’s capabilities in cyberwarfare could win international respect, and the information gleaned from the adversary could be used as a lever for intelligence exchanges with the US.

Although Taiwan has many advanced hackers (as evidenced by winning many awards in international hacking competitions), their capabilities have not been integrated with the national security apparatus. Some of them might be hired by the government for a short period to perform particular tasks. Due to the lack of persistence in their assignments, their expertise hardly poses a threat to the enemy. Some hackers and their ingenious technologies have been acquired by other countries, such as Israel and the US, causing a “brain drain.”

Here I attempt to explain international law as it applies to cyberwarfare, and make

recommendations for Taiwan's policy.

The Tallinn Manual, initially published in 2013 and updated as a "2.0" version in 2017, details how existing international law can apply to all aspects of cyberwarfare. Commissioned by NATO and authored by many experts, it is the most comprehensive guide for policymakers and legal experts alike.

The publication considers the rules of international law governing cyberincidents that countries encounter daily, but fall below the thresholds of the use of force or armed conflict. It makes extensive reference to international treaties, common practices, general legal principles, judicial decisions, international doctrines and other broad sources of international law to elucidate how international law applies to cyberwarfare.

Although the Tallinn Manual is not a formal, legally binding document, its application and interpretation of laws and regulations in cyberspace result from the development of the academic and practical aspects of international law.

Its essence is similar to collections of international law such as the San Remo Manual, which regulates maritime warfare, and the Air and Missile Warfare Manual. Although the Tallinn Manual does not represent the official positions of any country, it nevertheless shows the consensus of major entities in the West led by the US and NATO. It can be used as a guide for Taiwan to prepare for cyberwarfare. Some legal terms in the manual are defined as such:

NATIONAL SOVEREIGNTY

The Tallinn Manual helps determine the fundamental barriers in international law between the state, cyberinfrastructure and cyberbehaviors. In this context, "national sovereignty" means a country can exercise control over network infrastructure and network activities within its territory. Meanwhile, extended sovereignty is when a country has jurisdiction over individuals participating in cyberactivities, the network infrastructure in its territory and the extraterritorial jurisdiction stipulated by international law.

CYBERSOVEREIGNTY

The state enjoys the principle of exclusive sovereignty; even the Internet is no exception. As long as the network infrastructure is in the country's territory, the country enjoys jurisdiction. Countries can freely participate in online activities, but they must be bound by international law to involve activities outside the country. A country's external sovereignty originates from state immunity, demonstrating that its network activities, including the government, citizens, and public and private sectors, are not subject to foreign restrictions as long as they are within its territory.

VIOLATION OF SOVEREIGNTY

The country has sovereignty over network activities, and other countries must not intervene or infringe in a way that violates international law. Suppose the state's activities on the Internet constitute harm to the private enterprise network located in another country.

In that case, it can be deemed an infringement of the sovereignty of that country. The infringed country can exercise its right to self defense. If a country is unable to fight external cyberattacks, it can invite allies to help. As long as the country's consent is obtained, the allies can exercise power within the country's sovereignty. Countries can negotiate the content and intensity of cyberoperations and how much sovereignty the victim country is willing to transfer to cooperate with the alliance; subsequently, the allies cannot go beyond the scope of authorization (Article 4).

RIGHT TO SELF DEFENSE

If a country becomes the target of cyberoperations that reach the attack level, it can exercise its due self defense (Article 71). Attacks carried out through the Internet may also be considered actions that allow the victim country to exercise legal self defense.

When an attack is imminent, the type of defensive behavior is called "anticipatory self defense" in international law. A victim country must reasonably infer that the hostile intention has

developed into a de facto attack decision. Moreover, if the victimized country does not take action on the attack, it will lose its effective self defense capabilities.

When exercising the right to self defense under the “use of force involving cyberoperations,” the behavior must be necessary and reasonable (Article 14). A country may use force to thwart an imminent cyberattack (Article 15). Cyberoperations taken in armed conflicts should be regulated by international humanitarian law (Article 20). The law forbids attacks on civilians, or medical or religious personnel.

CYBERATTACK

Cyberattacks are offensive or defensive cyberoperations that can reasonably foresee injury or death, and damage or destruction of materials. The need to reset the system or specific data to enable the systems under attack to perform their designed functions constitutes an attack. Even when a cyberattack does not cause the desired damage, it could constitute offensive behavior.

Attacks do not need to be successful as long as it can be expected that attackers’ malicious software is intended to cause damage when it is activated. In that situation, an attack can be considered to have occurred. Even if it is successfully interrupted without causing substantial harm, it is considered an attack under the law of armed conflict.

CYBERESPIONAGE

Cyberespionage does not violate international law, just like traditional espionage behavior does not violate international law. Nevertheless, the implementation of cyberespionage may still violate other norms of international law. Cyberespionage could target and collect specific data over a long period of time.

Although cyberespionage violates the principle of national sovereignty, it does not necessarily constitute a cyberattack (Article 32). Cyberespionage can be regarded as an exception that prohibits infringement of sovereignty (Article 4) and international intervention (Article 66) that

are not allowed by international law.

POLICY PROPOSALS

Offense is the best defense. Since Taiwan has never had any effective countermeasures against China's cyberattacks, the latter has carried out audacious attacks with impunity, making the island country a playground for Chinese hackers. Therefore, I make the following policy recommendations for Taiwan's strategy:

1. The US has its "hunt forward" doctrine. Taiwan should invite the US Cyber Command to help defeat and disrupt China's malicious cyberactivities.

2. In order to have a legal basis for joint cyberoperations between Taiwan and the US, the two countries should sign a bilateral agreement to allow US personnel to station in Taiwan during peacetime.

3. Taiwan could lobby the US Congress to pass the US-Taiwan Joint Cyber Security Center of Excellence Act, paving the ground for the two countries to establish a joint cybersecurity center.

4. NATO's Cooperative Cyber Defence Centre of Excellence this year initiated the Tallinn Handbook 3.0 five-year plan. Taiwan should dispatch experts familiar with the field to participate in discussions.

5. The EU Agency for Cybersecurity released the National Capabilities Assessment Framework for its member countries to evaluate strategic cybersecurity objectives. Taiwan could create a similar framework to prepare comprehensive cybersecurity capabilities, incorporating the public and private sectors at the strategic and operational levels.

6. At present, 56 countries have issued cybersecurity strategies. The Ministry of National Defense should also formulate cybersecurity strategies and tactics, and make its pre-emptive

rights to self defense in cyberwarfare known to the world.

7. In addition to revamping its security clearance mechanism for government officials and civilians, Taiwan should also revise the "Government Procurement Law" so that hackers can contribute directly to the national security apparatus through a contractual relationship with the private sector.

8. Infusing capabilities of the private sector in national defense can cultivate a country's cyberwarfare capabilities. In conjunction with updated security clearance mechanisms, Taiwan should revise the National Intelligence Law and related rules to facilitate the private sector's participation in cyberwarfare.

Holmes Liao has more than 30 years of experience in the US aerospace and defense industry, and served as a distinguished adjunct lecturer at Taiwan's War College between 1999 and 2003.

Source: Taipei Times- Editorials 2021/09/11