Briefing Memo

International Laws on Cyber attacks that Do Not Constitute an Armed Attack

Keiko KONO
Senior Research Fellow, Government and Law Division,
Security Studies Department

Introduction

In February 2017, the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (hereafter, *Tallinn Manual 2.0*) was published. This book follows up on the *Tallinn Manual on the International Law Applicable to Cyber Warfare* (hereafter, *Tallinn Manual*), and like its predecessor, was published as a part of a research project organized by the NATO Cooperative Cyber Defence Center of Excellence (NATO CCD COE). It was in fact drafted by practitioners and researchers in international law invited by the NATO CCD COE to participate in the project. Of particular note is that experts from some Asian countries (including Japan) were also involved in the project of *Tallinn Manual 2.0*.

Neither the *Tallinn Manual* nor *Tallinn Manual 2.0* is an intergovernmental agreement, and the texts are written in the format of academic product. Regardless of that, the *Tallinn Manual* has been criticized by government officials in countries such as China and Russia, as if it represented the official views of Western countries; *Tallinn Manual 2.0* is expected to be confronted with a similar situation. While NATO's true intention in having experts draw up these two documents is unclear, for external parties, there is a strong possibility that the contents of the Manuals would be received as something that is, to a certain degree, a shared perception among the governments of Western countries. The recent circumstances surrounding this issue are considered to be related to the background giving rise to such doubts and misgivings among some countries.

1. Current Situation with Regard to International Regulations on Cyber Operations

Today, no multilateral international conventions truly exist in relation to cyber operations. The 2001 Convention on Cybercrime certainly sets out provisions on cooperation between the parties on the investigation and prosecution of some cybercrimes such as illegal access, but the number of parties (56 countries) as well as the regulatory items are limited. To date, a number of opportunities have been created for the discussion of international regulations over cybercrimes other than these, and the following are some of the representative examples. This issue has been addressed at the following events and conferences: (1) The UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, established

under the umbrella of the First Committee of the UN General Assembly; (2) The International Telecommunication Union (ITU) in the context of international telecommunication law; (3) The UN Human Rights Council in the context of human rights (especially the right to privacy); (4) The G7 Summit (meeting of the key countries) and particularly the 2016 Ise Shima Summit, and of course the NATO summit meetings. Of these, apart from conferences such as the G7 and NATO that are composed only of Western countries, in frameworks such as the Cyber GGE and ITU which China, Russia, and countries that are in concert with the two countries also participate in, the participating countries often fail to reach a compromise on their differing views over the state of international laws and norms on this issue. These conferences have not reached the formulation of an agreement that all the participating countries can approve of. Against this background of a lack of progress and sluggish negotiations between the respective governments, the *Tallinn Manual 2.0*, like the *Tallinn Manual* before it, has established the goal of putting existing international law (*lex lata*) on cyber operations in statutory form. In doing so, it relied on the rules of international law that have developed in fields other than cyber operations.

2. Overview of the *Tallinn Manual 2.0*

The key consideration of the *Tallinn Manual 2.0* was international laws that are applied to cyber operations in peacetime. Here, "peacetime" refers to situations where cyber attacks are occurring without reaching the level of an armed attack (While the invocation of the right of self-defense against an armed attack is recognized, it has been omitted from this paper as a point of debate that comes under the previous work, the *Tallinn Manual*). The following is an overview of how the experts involved in the drafting of *Tallinn Manual 2.0* organized the ways in which countries under attack could respond, as well as the legal basis for espionage operations.

(1) Response to cyber attacks that do not constitute an armed attack

Cyber attacks that do not constitute an armed attack are, in other words, cyber attacks that correspond mainly to threat or the use of force (Rule 68), illegal interventions (Rule 66), and violation of sovereignty (Rule 4). A typical example of the use of force in cyberspace that the experts involved in the drafting of *Tallinn Manual 2.0* kept in mind is the Stuxnet attack discovered in 2010 (destruction of centrifugal separators used for uranium enrichment). The violation of sovereignty through cyber means refers to cases where data that is indispensable to inherent government functions (social security, elections, collection of taxes, diplomacy, national defense, etc.) is modified or destroyed, thereby obstructing work processes. The cyber attack on the Japan Pension Service, discovered in 2015 falls under this category. Illegal interventions refer to forcible changes of the decision-making processes for domestic and international issues through a cyber attack.

According to the *Tallinn Manual 2.0*, the country under attack may implement countermeasures against the country carrying out the attack, in order to make the latter comply with the legal obligations

owing to the former (Rule 21). In short, the country under attack is permitted to carry out a cyber operation that violates the sovereignty of the country carrying out the attack, and moreover, the illegality of that act is precluded, and therefore justified. However, this countermeasures must not involve the use of force.

According to the *Tallinn Manual*, the use of force in cyberspace is qualified by the occurrence of the death or injury to persons, or physical damage to objects. Comparing the situations where a military aircraft violates the territorial airspace of another country and where personnel involved in cyber operations hack into an information network that lies within the domain of another country (electronic virtual intrusion), the former will commonly be regarded as an illegal use of force, while the latter will not be deemed as use of force. This is because, unlike a physical intrusion, the act of hacking through cyber means cannot necessarily be described as an infringement of the territorial integrity of the country. Of course, among countries that are party to the Convention on Cybercrime, such acts would correspond with the crime of illegal access as stipulated by the Convention. However, neither Russia, China, nor North Korea are party to the Convention. While such acts may also be deemed as criminal acts under domestic law for countries that are not party to the Convention (in the case of Japan, unauthorized access), unauthorized access may not necessarily be equated to violation of sovereignty.

Next, with regard to whether or not any cases apart from the aforementioned (infringement of inherent government functions) can be described as a violation of the sovereignty of the country that has been subjected to the cyber attack, *Tallinn Manual 2.0* was not able to identify any clear standards or criteria. The only point that the experts agreed on was that damages that require the replacement of cyber/infrastructural components are equivalent to the infliction of physical damage, and therefore, correspond to violation of sovereignty just like in cases where physical damage have been incurred. However, in cases where the replacement of component parts is not particularly required and where the damage incurred only reaches the extent of temporary loss in the functions of infrastructure, such as in the case of a distributed denial-of-service attack (DDoS), experts involved in the *Tallinn Manual* did not consider such cases as a violation of the sovereignty of the country under attack. Hence, for cyber attacks that do not infringe on the inherent government functions of the target country, nor violate other international agreements, are regarded as legal acts under international law even if they result in the loss of infrastructural functions that are recovered easily, such as temporary power outages. In the context of physical domain, it has been pointed out that attacks in the form of retorsion, which are hostile but not illegal retaliatory acts, have traditionally existed. Theoretical examples of retorsion include the interception of foreign military aircrafts in response to the intrusion of the said aircraft in the territorial airspace, forcible expulsion of foreign warships involved in non-innocent passage in the territorial waters, or navigation operations carried out to verify the right of vessels to pass through. Similarly for cyber means, *Tallinn Manual 2.0* suggests that certain cyber measures could be deemed as legal response undertaken by the country under attack.

(2) Serial cyber attacks related to North Korea

According to some reports, the US President has signed and issued an (undisclosed) executive order permitting cyber attacks to be carried out against North Korea, and it is said that the Cyber Command had carried out DDoS attacks by the end of September 2017. Hypothetically, if these reports are factually accurate, would these cyber attacks against North Korea constitute a countermeasure against the series of nuclear and missile development as well as cyber attacks by North Korea? (For example, the leak of operational plans against North Korea by the U.S. and South Korea military is suspected to be the result of actions carried out by North Korea. With regard to this point, refer to (3) below.) Although the UN Security Council has already acknowledged that North Korea's nuclear missile development plans as a threat to international peace and security, and put in place economic sanctions, cyber-related measures have not been included as a part of these sanctions. Furthermore, the implementation of countermeasures by the United States alone, based on the violation of a series of Security Council Resolutions as its justification, may not necessarily be approved. *Tallinn Manual 2.0* also demonstrates a passive stance with regard to tolerance of countermeasures based on such pretexts (Commentary for Rule 24, paragraph 4 and 5).

In that case, can cyber attacks on North Korea by the U.S. Cyber Command be justified as a countermeasure undertaken by the United States in retaliation to direct damage it has incurred through North Korea's actions (not limited to cyber attacks), or can that be categorized as a legal act of retorsion to begin with? In 2014, soon after a series of cyber attack on Sony Pictures Entertainment (SPE) was found, reports were circulated that the Internet was temporarily blocked in North Korea; according to rumors, that was the result of a countermeasure carried out by the United States. Even if that were true, hypothetically, that measure itself would be a legal response as far as an assessment made based on standards set out in *Tallinn Manual 2.0*. Similarly, the DDoS attacks carried out by the U.S. Cyber Command against North Korea, rumored to have been carried out recently, would also be legal as long as the damage was restricted to temporary inconvenience, and no physical damages were incurred. On the other hand, while it is unclear if the reports are true, it is difficult to explain operations to halt missile launches by North Korea through cyber operations as a means of retorsion, because such operations clearly inhibit inherent government processes in light of the aforementioned criteria for the violation of sovereignty. Putting aside the question of what the preceding illegal acts carried out by North Korea were, theoretically, the only main basis for justification that can be identified would be countermeasure.

(3) Cyber espionage

The criteria for the recognition of a violation of sovereignty, as examined in (1) above, is closely related to the legality of cyber espionage. Under international law, the legality of cyber espionage is determined based on the following two points. The first is the legality of the espionage itself, and the second is the legality of the method of the espionage. With regard to the first aspect, the *Tallinn Manual*

2.0 concluded that there are no rules under international law that prohibits that (Rule 32). Secondly, in the event that an espionage operation is carried out through means that are deemed illegal under international law, such as the violation of sovereignty, the overall espionage operation would be perceived as an illegal act. However, depending on the way that the question of what constitutes a violation of sovereignty is perceived, the judgement on the second point may vary (in the sense that no particular physical damage is incurred). The majority view put forth in *Tallinn Manual 2.0*, which indicate that hacking alone does not even constitute a violation of sovereignty, have in fact already been shared among some countries such as Estonia (a member of the UN Cyber GGE since 2009), and could also be described as an approach that is easily accepted by the governments of countries that are concerned about cyber espionage. Reading the *Tallinn Manual 2.0*, we would see that cases involving the invasion of networks categorized as inherent government functions (the aforementioned stealing of data on plans related to attacks on North Korea by the U.S. and South Korea military) are, for the most part, regarded as violation of sovereignty; however, for cases that do not fall under that category, such as hacking of organizations that do not form a part of inherent government functions or industrial infrastructure, and the stealing of information, the *Tallinn Manual 2.0* suggests the conclusion that such acts are not illegal either from the perspective of methodology. On the other hand, if the criteria for the violation of sovereignty were an infringement of inherent government functions, then the interception of electronic communications between a (sending) country and its embassies located overseas would always fall under that definition of violation of sovereignty. While the 1961 Vienna Convention on the Law of Treaties has also established provisions on the inviolability of archives, documents, and official correspondence of the diplomatic mission, *Tallinn Manual 2.0* also applies this rule to cyber communications (Rule 41). Diplomatic mission's cyber communications are inviolable regardless of the physical location, and the espionage of such communications is deemed to be illegal even in cases where the communications are carried out via infrastructure placed within the territory of the country carrying out the espionage. While it may be true that the method is illegal, whether the respective countries will hesitate to carry out cyber espionage operations, or suspend such operations, remains a separate question.

Conclusion

Today, cyber attacks are carried out between countries on a regular basis, but the relevant countries involved may not necessarily have clarified the legality of such acts under international law. Against the background of such a situation, *Tallinn Manual 2.0*, which explicitly sets forth the international laws concerning cyber operations that do not constitute an armed attack, is acknowledged to offer a certain degree of usefulness. On the other hand, it is important to note that both the *Tallinn Manual* and the *Tallinn Manual 2.0* contain law-creating descriptions (particularly in reference to the criteria on the use of force) and unresolved points of contention. Furthermore, the mechanical application of the *Manuals*, even for contents that have been presented as the majority view by experts, must be

carefully avoided. Even if the term "DDoS attack" were to be applied universally, there are differences between the extent to which inherent government functions in Estonia and North Korea are dependent on cyber infrastructure. For this reason, the extent of the damage is also expected to vary significantly. The assessment of whether cyber operations undertaken by state actors are legal under international law, including assessments based on such facts, will be called for in the future, and the *Tallinn Manual 2.0* is likely to offer helpful hints when that time comes.

Reference

• Terry D. Gill, "Non-Intervention in the Cyber Context," in Katharina Ziolkowski, ed., *Peacetime Regime for State Activities in Cyberspace* (NATO CCD COE, 2013), pp. 217-238.

• Marina Kaljurand, "United Nations Group of Governmental Experts: The Estonian Perspective," in Anna-Maria Osula and Henry Rõigas, eds., *International Cyber Norms: Legal, Policy & Industry Perspectives* (NATO CCD COE, 2016), Chapter 6.

• Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017).

(Completed on October 20, 2017)

Please contact us at the following regarding any questions, comments or requests you may have.

Planning and Management Division, Planning and Administration Department, NIDS

Telephone: 03-3260-3011 ext.: 8-6-29171

FAX: 03-3260-3034 *NIDS Website: http://www.nids.mod.go.jp/