Briefing Memo

Cyber Security and the Tallinn Manual

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

Preface

Are states subject to cyber attack allowed to retaliate with military action under international law? Or as with cyber-crime cases, do they have to rely on law enforcement? The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), which was established following the cyber attacks on Estonia in 2007 in order to enhance NATO's cyber defence capability, published "The Tallinn Manual on the International Law Applicable to Cyber Warfare" (hereinafter referred to as the Manual) last year as a result of a three-year study, answering to the former question in the affirmative.

Article 51 of the Charter of the United Nations provides that states may respond in self-defense if an armed attack occurs. However opinions are divided as regards the scope of an armed attack. Although the Manual examines the existing laws applicable to cyber warfare (lex lata), the approach can be seen as quite ambitious in that it copes with a challenging task concerning the interpretation of the right of self-defense. Here I would like to draw attention to the following three issues of the Manual, and explore to what extent the Manual represents lex lata; first, should anticipatory self-defense be allowed in response to a cyber armed attack? Secondly, what cyber-operation constitutes a use of force? Thirdly, can the victim state attack terrorists based in Pakistan and Yemen without the consent of territorial states?

The Manual is a research product drafted by the independent International Group of Experts consisting of lawyers and practitioners who sit in personal capacity, and is not meant to represent the views of the NATO CCD COE. Therefore the Manual does not qualify as a source of law in the formal sense. However, as is the case with the "San Remo Manual on International Law Applicable to Armed Conflicts at Sea," which has been extensively referenced in the *The UK Manual of the Law of Armed Conflict*, the Manual may be adopted into the practice of states in the future.

The requirement of the right of self-defense

The UN Charter prohibits the threat or use of force against any state. However the victim state is allowed to exercise the right of self-defense only when it is against the most grave form of the use of force constituting an armed attack. In other words, there is a considerable gap between "use of force" and "armed attack." A dominant view is that in the case of less grave forms of use of force, the victim state is prevented from adopting military countermeasures, with the Security Council taking measures under

Chapter VII of the UN Charter. Secondly, even if an armed attack occurs, it does not imply that the victim state has an unlimited right to use force, and it must adhere to the conditions of necessity or proportionality based on customary international law. These points are adopted in the Manual.

(1) Anticipatory self-defense against a cyber-armed attack

Article 51 of the UN Charter provides the right to engage in self-defence when "an armed attack occurs." The theory of pre-emption is the view that self-defense can be taken if the risk of an armed attack is imminent, even before it takes place. According to the Commentary, anticipatory self-defense is the current law established before 1945, and is still in force. Nevertheless, some maintains that if an armed attack has begun, then it is imminent even before its effect has not yet materialized. This proposition approximates the interpretation on the scope of an armed attack, and there is not much reason to hold discussions on the validity of the theory (in case of Japan, it is necessary to establish that there is an imminent and illegitimate act of aggression against Japan). The Manual goes even further in that it judges imminence on the basis of whether it is the last window of opportunity or not for the victim state to take effective defensive measures, and allows anticipatory actions even before an armed attack has actually been launched. Although this approach has already been proposed in relation to the weapons of mass destruction, demand for it has grown even more in view of the characteristics of cyber attacks, the process of which from the launch of an attack to damages being caused is completed instantaneously.

Furthermore, cyber attacks against air traffic control systems and nuclear-related facilities have been referred as examples of a cyber armed attack. This is based on the argument that these types of cyber attacks can cause serious damages comparable to those caused by conventional weapons, such as airplane collisions and radiation diffusion. Although the Manual presents "scale and effects" as a factor to measure an armed attack, experts were not able to agree on whether a cyber operation, which has an adverse effect but does not accompany physical damages such as loss of human life and destruction of property, constitutes an armed attack.

For comparison, the Manual sees cyber-to-cyber operation, stricto sensu as a focal point, and makes no reference to cyber attacks in combination with conventional weapons (for example the Israeli air-defence manipulation before its air raid against Syria in 2007). Nevertheless, given the basic ideas of the Manual, such an operation can be qualified as part of an armed attack when it is an integral part of the whole attack, even if it does not cause physical harm.

(2) The scope of cyber attacks and the use of force

Although use of force in itself does not invoke self-defense as aforementioned, an armed attack cannot exist without a use of force. To put it simply, it is prerequisite for an armed attack to exist. The Manual focuses on "the scale and effect" approach with which to determine when an act amounts to the use of force. The Commentary states that under existing law cyber operations that bring about death or injury of persons or physical destruction of objects are unambiguously a use of force. But other cyber

operations without any physical damage may be identified as a use of force as well. The Commentary lists eight factors that could serve to assess such acts (1. severity, 2. immediacy, 3. directness, 4. invasiveness, 5. measurability of effects, 6. military character, 7. State involvement, 8. Presumptive legality. These are illustrative lists and there may be others), but some of experts argue such tendency has already been seen among several states. For example, according to the Joint Report of the Advisory Council on International Affairs and Advisory Committee on Public International Law of the Netherlands (2011), a cyber attack on essential functions of the state that could or did lead to serious disruption of the functioning of the state or serious and long-lasting consequences for the stability of the state could be qualified as an armed attack.

The above mentioned argument will not evoke practical problems in cyber-to-cyber operations, althogh none of the countries are discounting military countermeasures using conventional weapons. Therefore it is desirable that there is a common understanding beforehand concerning what kind of cyber operations constitute a use of force and also an armed attack, in order to avoid the outbreak of war or its escalation based on over estimation.

(3) Self-defense against third state

Intense criticism is being made in recent years against targeted killings conducted by drone aircrafts in Pakistan, Yemen, and so forth. The U.S. Government explains that all of these operations are justified by self-defense, when the territorial states are either unwilling or unable to control terrorists by itself. The Manual is right to say that the state does not have responsibility just because data merely pass through its cyberspace. But what about the case when the state is aware of the fact that the cyber infrastructure located within its territory or other places under its exclusive control (such as military bases abroad, high seas and its airspace, or diplomatic premises abroad) is being used to carry out actions that could have a harmful effects on other countries, but fails to take appropriate measures? The Manual seems to be following the same pattern as the U.S. government's view on the drone campaign, insisting that the victim state is entitled to exercise the right of self-defense in the latter case.

Supposing that a civil war has already erupted in Yemen and the U.S. military actions were due to a request from Yemen's government, there may be no legal issues whether a terrorist organization based in Yemen carries out a cyber attack, or the U.S. deploys drones. Conversely, there are authors that argue against military actions when there is no civil war in another state and the territorial state has not given consent. As the Manual does not cite specific international case law or national practices, it seems slightly premature to consider that test as existing law.

Nevertheless there are points to take note of when we listen to the various criticisms. One is that a terror attack by a non-state armed group is always classifiable as a crime as long as it is not attributed to the host state, and the victim state may not use force in self-defense, even if a cyber attack by terrorists is comparable to the 9/11 attacks. Since 2001, however, the issue of whether a non-state actor can engage an armed attack without any support or involvement on the part of states has been receiving interest among states and academia. As we recognize a certain tendency

across the countries to view the point in a positive light, therefore, it is hoped that more discussions are done widely.

Conclusion

I dealt with the issue of what is existing law applicable to a cyber attack in light of jus ad bellum, and focused on the three main points of the Manual; anticipatory self-defense, scope of the use of force and the right of self-defense against states that are unwilling or unable to repress terror attacks. Although all the issues reflect the recent inclination of a group of states, they cannot be concluded yet as existing law. Nonetheless, regardless of whether to support the Manual or not, there is no doubt that the Manual will exert substantial influence on an international agreements on cyberspace to be developed in the future, bearing in mind legal issues prominent in the cyberspace are covered comprehensively in the Manual. Whether anticipatory self-defense should be allowed in view of the specific characteristics of cyberspace, how cyber terrorism by non-state actors should be evaluated under international law, and when military countermeasures should be allowed or not; all these agendas are waiting for swift and satisfying solutions.

(Completed on October 8, 2013)

References

・Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of The NATO Cooperative Cyber Defence Centre of Excellence /General Editor Michael N. Schmitt (Cambridge University Press, 2013) <http://www.ccdcoe.org/249.html>.