Indian Journal of Fundamental and Applied Life Sciences ISSN: 2231– 6345 (Online)
An Open Access, Online International Journal Available at www.cibtech.org/sp.ed/jls/2015/02/jls.htm
2015 Vol. 5 (S2), pp. 1667-1670/Ebrahim
Review Article

CYBER ATTACKS IN INTERNATIONAL LAW

***Ebrahim Hosseini Zabet**
Department of International Law, Payam-e Noor University, Tehran, Iran
**Author for Correspondence*

ABSTRACT
International law has frequently been used by many governments as a shield against legal standards and a mechanism to escape and get free from legal obligations by giving an excuse or referring to vital national interests and security, so that governments imposed restrictions on the rules of international law and at the same time, they claim complying with international law by legitimating their actions. Cyber attack is a new phenomenon which can change the conducting method of modern war by governmental and nongovernmental actors. Unique nature of these threats and the ability of cyber war attackers in harming, killing and physical persuasion through cyberspace have changed traditional definitions of the use of force, that is, "it provides imminent armed attack with conventional weapons that we can do legal self-defense".

Keywords: *International law, Cyber Attack, Self-Defense, Cyberspace, Vital National Interest, Armed Attack*

INTRODUCTION

Current societies depend increasingly on computer, networks, and internet services. However, the countries developed in technology are also vulnerable against cyber attacks. Cyber attacks will be more important in a near future.

Concepts

Cyber attacks fall within a wide range of what is called "informational operations". Informational operations which informational war is one of its sub-sets and is used during armed attacks (Schmitt, 1998) is the integrated use of electronic warfare capabilities, computer network operations, mental operations, military deceptions and integrated operations with logistic capability that are done to influence, prevent, destruct or thieve enemy's information as well as to support the decision-making processes in national institutions (www.dod.gov). Cyberspace is an immaterial and intangible space created by computers and computer networks and has generated a virtual world beside the real world (Fazeli, 2010). This space has been developed beyond the internet. Cyberspace has naturally been created for freedom of information flow and thus any limitation in this space is meaningless (Pakzad, 2011). Exploitation operations of related computer networks may be done for spying and stealing important information from computers. Although international law does not prohibit espionage, most of the world's legal systems criminalize it (Dinstein, 2001). The present paper, away from exploitation operation of related computer networks that are for stealing information and spying, merely studies computer network attacks and computer network defense, that is, computer network attacks that is broader than spying and stealing the information and is done with hostile intention. It also investigates the operations which are done in order to change or remove the information of a target computer or a computer network and to disable directly the enemy's information and control headquarter and to inflict damage beyond the target computer network (Dinstein, 2005).

2. Cyber Attacks and Prohibition of the Threat and the use of Force in International Law

Cyber attack attributed to a state is the violation of the common rule about non-intervention in affairs that each state, based on the governing principle of the state, has the right to take freely its economic, social and cultural systems about them (Para, 1986; Nicaragua, 205). The situations described in UN General Assembly Declaration in 1981on non-intervention cover cyber attacks, that is, in determining whether cyber attacks are equal to the use of force in international relations, Article 2 (4) of United National Charter defines the threat by force as following:

© Copyright 2014 | Centre for Info Bio Technology (CIBTech)

"Explicit threat or implicit-verbal or practical threat to use the armed forces illegally against one or more states in the future, which its realization depends on the decision of the threatening person or stat. Threatening to do cyber attacks is considered an illegal threat and depends on assuming cyber attacks as legal or illegal".

Assuming that, the acceptance of Article 2 (4) of the UN Charter only prohibits the use of armed force rises question that what is meant by term "armed"? Can we assume cyber attack as armed force? The answer is that "armed" refers to equip to a weapon or to create riot using a weapon. Weapon is also a tool used or designed to harm or kill another person. Almost all objects may be used as a weapon if the user's intention is hostile.

3. Reaction to Cyber Attacks

Assuming that the victim county could identify the location of cyber attack and attribute it to a state, it may have several options.

3.1 Appealing to UN Security Council

According to Article 35 (1) of the UN Charter, the victim state can report the situation to the United Nations Security Council, and the Council may recommend the appropriate ways to resolve the dispute, based on Article 36 (1) of the Charter. If the Council considers the situation as a threat to the peace, violation of peace or act of aggression, it can apply its abilities according to the Chapter seven of the UN Charter. However, according to the drafters of the UN charter, threat to the peace is limited to use of traditional armed forces (Osterdahl, 1998), but its scope was gradually developed, so that the council may, regarding specific circumstances of each case, consider any action as a threat to the peace. If the UN Security Council considers a cyber attack as a threat to the peace, according ton article 39 of the UN Charter, it can provide recommendations, and in order to prevent the worsening of the crisis and also according to Article 40 of the Charter, propose some actions. Therefore, by the strength of Articles 41 and 42 of the UN charter about actions based on applying force or lack of applying force, the Council takes decisions. The Security Council may also impose a cyber blockade on the state responsible for cyber attacks in order to prevent continuation of attacks or reoccurrence.

3.2 Referring to the International Court

The state responsible for a cyber attack can be summoned to international courts, including international court of justice to compensate the losses resulted due to breach of article 2 (4) of the united nations charter and the principle of non-intervention. However, it should be noted that determining the amount of damage caused by cyber attacks is difficult, because financial institutions may be doubtful in providing accurate information and determining the amount of damages (www.carlisle.army). In addition, the International Court of Justice, as other international courts, does not have a compulsory jurisdiction. Therefore, both parties of the conflict must agree about referring the case to the International Court of Justice. According to Article 96 of the UN Charter, another option can be the request for advisory opinion on legality or illegality of cyber attacks by the International Court of Justice. Such opinions are optional and non-obligatory, however, are effective in forming an international customary rule (Conforti, 2005). Some commentators believe that cyber attacks that are considered as violation lead to state responsibility as well as international criminal responsibility for attackers (Weisbord, 2009).

3.3 Retaliation and Reciprocity

A victim state of cyber attacks can take non-military countermeasures against the actor. According to Article 49 (1) of the ILC's draft articles of the state, the damaged state can take countermeasures against the state responsible for the internationally wrongful act in order to induce that state to comply with its obligations (Helmi, 2008). Cyber attacks and propaganda with the aim of internal unrest and conflict in a target state are illegal and contrary with prohibition of the use of force and intervention in the internal affairs of states. Such interventions enable the damaged state to take appropriate countermeasures compliant with provisions set forth in Articles 50 and 53 of the ILC's draft articles on state responsibility. Now a question is that whether a victim state of cyber attacks can take countermeasures involving the use of force against cyber-attacker? Since, in contemporary international law such countermeasures are considered illegal based on Article 50 (1) of the ILC's draft articles on state responsibility (Helmi, 2008),

© Copyright 2014 | Centre for Info Bio Technology (CIBTech)

therefore, the positive answer to this question is in the case that applying legal defense is allowed in Article 50 (1) of the charter with international customary law against cyber attack. We should note that if the use of force in cyberspace is subject to article 4(2) of UN charter, and is prohibited under it as well as article 50 (1) of the ILC's draft articles on international responsibility of the state, the victim state of the cyber attack would not allowed to react unless the cyber attack is severe with extensive consequences. In this case, the victim state is allowed to react under article 51 of the UN charter. ILC's "travaux preparatoires" imply that article 50 of the draft articles on state responsibility refers to states that use the force against the previous violation of a treaty by another state, e.g., treaty of commerce. Above-mentioned article prohibits such actions because they are not proportional with initial action. In fact, the claim that a victim state of cyber attack cannot retaliate by sending diverting codes unless the cyber attack amounted to an armed attack is an unreasonable claim. Another issue is that the expected consequences of a counter cyber attack must be proportional to the consequences of the initial attack. Such a measurement is difficult because a virus posted in cyberspace might spread in an uncontrollable manner as biological weapons.

CONCLUSION

Today cyber war has become a reality. However, lack of borders in cyberspace enables cyber-attackers to hide themselves behind wrong addresses and internet tricks, i.e., something that makes it difficult to identify the origin of cyber attacks. The main question is whether a cyber attack is an action less than the threshold of the use of force or it is a form of use of force or even can be considered equal to an armed attack? To answer this question, we can say that those cyber attacks that are extensive and against key infrastructures must be considered as armed attacks. According to the Article 51 of United Nations charter, any attack that causes to a main damage or casualty comparable to an armed attack by traditional weapons authorizes the victim state to self-defense. In addition, the allowed defense against cyber attacks which do not amount to an armed attack but provide the imminent armed attack by traditional weapons, are plausible. According to the existence of relative procedures of countries and legal belief, the customary international law can play an important role in this field, especially about legal defense against cyber attack. This procedure continues and can lead to formation of a customary rule in oncoming years. In addition, the international cooperation at regional and global levels can play an important role in fighting against this borderless phenomenon. In this regard, the necessity of conclusion of a particular treaty on prohibition of cyber attacks is felt more than before.

REFERENCES

Conforti B (2005). *The Law and Practice of the United Nations* (Leiden: Martinus Nijhoff).
Delibasis D (2007). *The Right to National Self-Defense in Information Warfare Operations* (London: Arena Books).
Fazeli M (2010). *Criminal Responsibility in Cyberspace*, 1st edition (Tehran: Khorsandi publications).
Helmi N (2008). *Preparation and Development of International Law: International Responsibility of the State and Political Support*, 1st edition (Tehran: Mizan publications).
Militray and Paramilitary Activities in and Against Nicaragua (Nicaragua V. United States), ICJ Reports 1986.
Osterdahl I (1998). *Threat to Peace*, (Uppsala: Lustus Forlag).
Pakzad B (2009). Cyber terrorism, PhD dissertation in Criminal Law and Criminology, Shahid Beheshti University, Law School.
Pakzad B (2011). The nature of cyber terrorism, Shahid Beheshti University. *Journal of Legal Researches* (4).
Randelzhofer A (2002). Article 2(4). In: *The Charter of the United Nations: A Commentary*, edited by Simma B **1**.
Schmitt MN (No Date). *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, translated by Colum JL 1998-1999 (37).

© Copyright 2014 | Centre for Info Bio Technology (CIBTech)

Weisbord N (2009). Conceptualizing aggression, Duke J. Comp & Int'l L., No. 20.
www.carlisle.army.mil/DIME/documents/Georgia pdf200
www.dod.gov/pubs /foi/ojcs/07-F-2105doc1.pdf

© Copyright 2014 | Centre for Info Bio Technology (CIBTech)