International Journal of Humanities & Social Science Studies (IJHSSS)
A Peer-Reviewed Bi-monthly Bi-lingual Research Journal
ISSN: 2349-6959 (Online), ISSN: 2349-6711 (Print)
Volume-I, Issue-II, September 2014, Page no. 76-81
Published by Scholar Publications, Karimganj, Assam, India, 788711
Website: http://www.ijhsss.com

Cyber-attacks and Jus Ad Bellum

Dr. Alireza Hojatzadeh[1] **& Afshin Jafari**[2]
Assistant professor at Faculty of Law, Payame Nour University, Iran[1]
Student of Ph. D in International Law, Payame Nour University, Iran[2]

Abstract

One of the new issues that have nowadays been the center of attention in the area of international law are those legal cases related to cyberspace. Thus, while elaborating on the legal concept of cyber-attacks, this research also studies the significance of this relatively new concept in the current order of international community and taking into account the main question of research on applicability of jus ad bellum principles in cyber-attacks, the research concludes that while some experts assert that these principles apply to cyber-attacks, the applicability of these principles depends upon "type, intensity and impacts of attacks" and that they may only be applied in cases where the severity and threshold of an armed attack have been met. Therefore, it is necessary to not only study the current principles, but also the principles required for conclusion of an international contract and such mechanisms must be established.

Keywords: Cyber Space, Jus Ad Bellum, Cyber Attack, Law of Armed Conflicts.

Introduction: During the past century, an attempt has been made on the one hand to formulate the use of force for settlement of international disputes (jus ad bellum) and on the other hand some explicit and measurable restriction be applied within the framework of humanitarian laws in case an armed conflict breaks out (jus in bello). Some principles have been designed during the course of this process that on the one hand abide by the principle of states refraining from use of force in general and on the other hand, apply restrictions to the rituals of combat in the light of humanitarian approaches dominating the human relationships at both international and domestic levels. This process has resume during the past century but with the advent of third millennium, rapid and amazing evolutions have taken place in all aspects of life among which the information technology has been a major factor in these evolutions. In line with these evolutions one of the new issues that has become the center of attention in international law are the legal cases related to cyberspace including concepts such as cyber war, cyber-attack or even cyber-crimes that are sometimes misinterpreted in other judicial texts while these types of operations legally differ from one another. Due to the growing trend of cyber-attacks and the possibility of abuse of international humanitarian laws as a result of these attacks and since these cyber-attacks may become widespread, thus the principles of armed conflicts laws such as jus ad bellum and jus in bello need to be considered in the study of applicability of cyber-attacks. Due to wide range of cyber-attacks, the extent of damages incurred by such attacks may perhaps be more than conventional and classic attacks both quantitatively and qualitatively. Therefore, one of the important notions is that some states consider cyber-attacks a subject article 2(4) of the UN charter for use of force by states and as a result deem the legitimate self-defense stipulated in article 51 of charter as necessary. Although many countries are yet to explicitly announce their stance on this but the previous trends with regards to broad interpretation of article 51 by Americans along with recent decisions made by U.S and publication of Tallin Manual on these attacks suggest the possibility of using legitimate self-defense and armed attack in response to these attacks. So, the main question in this research is whether these principles of armed conflict laws and especially the jus ad bellum may be applied in cyber-attacks.

To this end, this article tries to examine some of legal principles applied in cyber-attacks and since the information technology and virtual space are the basis and foundation of all these attacks, the study of these elements is also another essential part of this research.

Chapter 1: Legal Nature of Cyber-attacks: Cyberspace as a global infrastructure for communications and digital information has incorporated all the political, economic, religious, social, military, environmental and legal areas and aspects of work and life. Thus, this space calls for its particular principles and we are indeed facing a different community referred to as virtual society which is closely related to and affects the real society.

(Schmitt, 2012:5)

In addition to provision of abundant accommodations, this technology may sometimes even threaten the human lives such as disruption in international aviation traffic control systems, production lines, power transmission and distribution, and railway switching system.

(Hanafieh Rajabi, 2008:8)

Some jurists such as Harold Coh believe that there is no need to neither create new conventional international law in the cyberspace nor to alter the existing norms as the ratified principles of international law may also be applied in the cyberspace. (Schmitt, 2012:6)

A. Definition of Cyber Attack: Military analysts have recognized virtual domain as a new area in the domain of war the significance of which is currently overtaking that of others.
But the initial challenge in assessment and definition of cyber-attacks is the nature and territory of these operations.

For instance, the National Research Council of U.S has defined cyber-attack as a conscious measure taken to replace, disrupt, deceive, alter or damage computer systems or their data. On the other hand, the Shanghai Cooperation Organization, proposing a dentition from a different perspective, calls it "an extensive brainwashing to destabilize and endanger domestic community and coerce the government to adopt decisions in favor of the opposition party". (Hathaway, 2012:3)

But the definition proposed by the authors of "laws of cyber-attacks" seems to be more comprehensive and complete. According to these authors, "Any action taken either with a political purpose or aimed at the national security which would debilitate the function of computer networks of a country" is a cyber-attack. (Hathaway, 2012:4)

B. Technical Typology of Cyber Attack: Identification of type of attacks and implementation of a safe protective system against them is one of the most important responsibilities of IT and computer network experts. Knowing the enemies and awareness of their attacking options would increase the chance of success in encountering them. Therefore, it is required to find out more about various types of attacks and raids directed at computer networks. The following table presents some of these common attacks:

Table 1. Some of common attacks

Common attacks	
Denial of Service (DoS) & Distributed Denial of Service (DDoS)	
Back Door	Spoofing
Man in the Middle	Replay
TCP/IP Hijacking	Weak Keys
Mathematical	Password Guessing
Brute Force	Dictionary
Birthday	Software Exploitation
Malicious Code	Viruses
Virus Hoaxes	Trojan Horses
Logic Bombs	Worms
Social Engineering	Auditing
System Scanning	

B-1: DOS attacks: The purpose of DoS attacks is to disrupt resources or services that the users are seeking access to or try to use (devitalizing the services).

B-2: Backdoor Attacks: Backdoor is a program whereby access to a system without any security check is facilitated. Programmers usually predict such potentials in the software to enable troubleshooting and editing of codes during trial version or application of software and this has turned into an Achilles heel for the computers and software.

B-3: Interception Attack or Eavesdropping Hackers: The attacker in this method may secretly transcribe all the data.

B-4: Modification of Data: The attacker manipulates and changes the data.

B-5: Fabrication of Data: The attacker adds to the original information.

B-6: Interruption: The attacker causes disturbance in networks and exchange of data.

C: Various Threats Arising from Cyber-attacks

C-1: Espionage and Violation of National Security: Cyber espionage refers to an action taken in order to acquire information (crucial, particular or classified data) on individuals, competitors, groups, governments and enemies through application of illegal operation methods on the internet, networks, computers, or via software for military, political or economic purposes.

C-2: Sabotage: Military activities taking place with the use of satellites and computers to impair the equipment of enemy are referred to as sabotage. Electricity, water, fuel, communications and transport infrastructures may be prone to cyber-attacks. Other threats may include decryption of credit card data, disruption of train schedules or even causing disorder in the stock exchange market.

C-3: Power Network: Power transmission networks are among the most important targets of cyber-attacks due to their dependence upon cyberspace and internet. The U.S government claimed in 2009 that China and Russia had planned to disrupt its electric power networks via software penetration. On the other hand, military attacks on electric power transmission networks are highly considered in wars and cyber-attacks in order to disrupt the internet.

D: Samples of Cyber-attacks:

- During Hezbollah and Israel conflict in 2006, the Israeli government announced to have been cyber attacked by Middle East nations and Russia.
- This time it was Estonia in 2007 that reported being cyber attacked.
- The elections website of Kazakhstan underwent failure during a cyber-attack in 2007.
- Hackers attacked the websites of Russia, Georgia and Azerbaijan during the 2008 conflicts in South Ossetia.
- Public sectors, media and financial websites of U.S and South Korea were widely attacked in 2009.
- In May 2010, as a response to cyber-attack of India, the websites of Indian Missile Organization, Indian National Science Academy and offices of a number of political parties were attacked by Pakistani hackers.
- Iran's nuclear facilities were hacked via Stuxnet Virus in September 2010. This was one of the most advanced computer viruses and opened a new chapter in cyber battles.
- In July 2011, the website of SK telecommunications company of South Korea was hacked as phone number, emails and post addresses of 35 million people were robbed.
- In October 2011, the U.S government admitted to have lost the control of its drone due to a cyber-attack by Iran.
- It was revealed in 2012v that India has hacked the data of bilateral economic commission of U.S and China.

E: Different Types of Hackers in Cyber-attacks

E-1: White hat hackers: Whoever is able to bypass the network security blocks but still does not commit any sabotage is referred to white hat hacker.

E-2: Black Hat Hacker: These are individuals who hack the computers of their victims and manipulate their data, spy on them, disseminate viruses, etc.

E-3- Gray Hat Hackers: People who falls between the two above-mentioned categories.

E-4: Pink Hat Hackers: These are novices that use a number of subverting software who try to irritate and harass others.

E-5: Red Hat Hackers: A number of experts who enter wrong data onto internet networks.

Chapter 2: Application of Jus Ad Bellum in Cyber-attacks: Since the followers of international law are identified as legal entities in the international judicial system and the main objectives of cyber-attacks such as state organizations, state-led economy and lifeline infrastructures are similar to those of an armed war, it seems better to first evaluate the principle of political sovereignty and sovereign equality in cyberspace before examining the principles dominating the conflicts and then take on other principles.

A: Political Sovereignty (Territorial Integrity) and Sovereign Equality: Simply put, the sovereign equality considers equal right of sovereignty for all the states and this right must be respected by all the governments with judicial bias of this principle found in numerous international deeds. But this principle is reflected in UN charter before anything else and accepted by the international society. The note 1 of article 2 of UN charter reads "the UN is founded on the basis of sovereign equality of all the members" and the sovereign equality is a fundamental principle. Now, let take a look its stance in cyberspace in spite of the latest advances and developments in IT during the 21st century:

A-1: Sovereignty in Cyberspace: The information technology has had a profound impact on development of countries during the past three decades and has amazingly exerted variations to daily lives as these transitions have caused complicated challenges. These challenges include both the effects of natural disasters on this technology and the technical challenges, cyber threats and disturbance of international peace and security. (White House,2011:8-10)

The question that first that comes to mind is about the role of cyberspace in sovereignty of states. In other words, are the countries allowed to claim sovereignty over cyberspace?

According to most jurists, no country may claim to have total dominance over cyberspace. In fact, if a territory is equipped with cyber infrastructures, that may not be regarded as the right of sovereignty in cyberspace. (Schmitt, 2012:15)

And as indicated in Tallin Manual, sovereignty is not only authorizing but also binding.

(Tallin Manual, 2013:5-20)

If we look at it from a different perspective, we realize that one of the inevitable consequences of cyberspace is to debilitate the sovereign and obliteration of physical relationship in this space. This may be an adaptation of John Barlows "Declaring Independence from Cyberspace" wherein the author has addressed the governments of industrial world suggesting that "you have no right of sovereignty in cyberspace". He asserts that the new cyber society is against the traditional sovereignty as it calls for particular conventions and norms. (Betz David, 2011:5-15)

But in spite of the aforesaid opinions, the view of international law on cyberspace sovereignty must be studied.

A-2: International Legal Sovereignty of Cyberspace: According to the conventional principles and stipulations in UN charter, any government once forming an administration and being recognized by the international society would be transformed into a political entity. Now, is it possible for the cyberspace to enjoy an independent international legal sovereignty or not?

Some theorists and political activists believe that cyberspace must be recognized as an independent ruling entity in the international system. They justify their assertion by emphasizing on the unique essence of cyberspace and lack of territorial borders in it as well as the distance nature of its performed activities. To this end, theoreticians suggest that the cyberspace is beyond the traditional judicial sovereignty of countries and underline the fact that the countries must revere the emerging sovereignty of cyberspace.

(Betz David, 2011:5-15)

But considering the current status of cyberspace and as a response to this point of view, one may assert that these opinions are merely theories and no countries has literally recognized an independent legal sovereignty for the cyberspace since this space may not be considered an independent entity as it is well-dependent upon the sovereignty of states. Therefore, the governments relatively dominate this space and other states must respect this sovereignty.

B: Use of Force by States: All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations. Taking this article into account and the fact that the international court of justice in Nicaragua case considered this prohibition a reflection of conventional international law and the international law commission has cited the basis of this prohibition as a jus cogens (peremptory norm), it remains to be seen whether the cyber measures taken against a government are a transgression of these norms and a use of force.

B-1: Judicial Basics of Use of Force: Use of force and/or threats is a reiterated ban stipulated in many international documents. For instance, United Nations General Assembly demanded the nations in 1949 to refrain from any use of threats that would contradict the objectives of UN charter and independence of nations. Also, the League of Arab States, North Atlantic Treaty Organization (NATO), the Warsaw Pact, Vienna Convention on the Laws of Treaties, the Non-Aggression Pact between the Federal Germany and Soviet Union, and other regional and international covenants have altogether forbidden the use of force or threats.(Ziaee Bigdeli,1994:57)
But how does the use of force or threat take place in the cyberspace?

B-2: Use of Force in Cyberspace: The cyberspace has intimidated the governments due to its unique features and distinctions with the real-world conflicts. This fear and horror reminds of Mc Lohan, the communications theoretician. He remarked in 1967 that "creation of a new space lead to new apprehension and horror". Now, how relevant is this feeling of terror and possible use of force in the cyberspace to the article 2(4) of charter?

(European Security Reviw, 2013:5)

Some international experts who contributed to writing of Tallin Manual have tried to demarcate a threshold for use of force in cyber-attacks. For instance, factors such as intensity, speed and purposefulness of attacks may be used to interpret cyber activities stipulated in article 2(4). For example, the scale and intensity criteria were considered in Nicaragua case. Thus, for cyber-attacks to become subject of use of force, the intensity and impacts must be such that leads to injury or casualties or extensive destruction of properties and not merely to partial damages or cyber larceny. (European Security Review, 2013:4)

According to the Red Cross International Committee and the 1949 Quadruple Geneva Conventions, it may also be inferred that all the disputes leading to armed conflicts or alike can be regarded as a military challenge and use of force.

C. Legitimate Defence in Cyber-attacks: Any response to cyber-attacks is basically difficult because as opposed to traditional battles, the cyber-attacks are invisible. Cyberspace is the opposite pole of physical space since unlike the physical space the variations in this space happen at the speed of light and therefore the cyberspace is more in favor of the attacker and indeed one of the attractive things about this space is the unanimity of the attacker and one of the main problems with regards to legitimate defence is to affiliate and identify the invader as a distinction should be made between cyber-crimes, cyber-attacks and their agents. The reason for this distinction is based on the international rules and regulations, the legitimate defence is only allowed when the invader are affiliated with a certain state and other principles such as necessity, distinction and proportionality are met. Article 51 of UN charter reads:

> "Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security".

According to the pattern designed by the law of armed conflicts, the response of a government to an armed attack by another state must include three principles to be considered self-defense: necessity, proportionality and distinction. As for necessity, the attack must be attributed to a certain source, the intent of assailant must be distinguished and a conclusion must be made on using force as a response. Proportionality indicates that the force used as a response to an attack must be proportional to the initial attack. And distinction forbids response to an attack after a long time has elapsed.

Attributing a cyber-attack to a certain source and discerning the intent of assailant are of high significance in cyber-attacks. Ascription of an attack to a particular suspect allows for a state to not

attack an innocent country. In addition, a government should establish a link between as attack and its source since the laws dominating the legitimate response to an attack differ in cases of state or non-state invaders. The ban stipulated in article 2(4) is applicable to states and not individuals i.e. according to the international laws the states are barred from use of threat or force against one another but similar actions committed by individuals may be judged under criminal laws.

Where it is difficult to identify the invader, figuring out the intent and stimulus of attack would even become more challenging in order to adopt preventive measures. For a government to be able to respond to actions of another state, the belligerent intent of the assailant state must first be verified. As opposed to conventional physical battles, the instantaneous and immediate nature of cyber-attacks deprives the victim of an attack from appropriate response. Walter Gary Sharp proposed all the nations ordain a law whereby they would be allowed to use force in order to jump the gun against any country that poses threats through penetration in crucial computer systems of another nation. (Sharp, 2013:3-13) Yet again, we face the challenge of affiliation and that is why some IT and military specialists believe that states may better focus on strategic cyber defence and establishment of cyber security instead of identification of the hackers. (Klimburg, 2011:5)

Achievements: A movement has increasingly taken place in the past two decades with regards to application of cyberspace as a means of attack on information networks of countries which has led to confusion of international jurists and politicians since they consider cyber-attack on computer networks as a use of force and they find the legitimate defence permissible according to article 51 of UN charter. But some others only consider this article allowable when the intensity and impact of attacks are proportional and similar to those of an armed one. Thus, we may conclude that the rules and regulations dominating the armed conflicts may not be applicable in case of cyber-attacks under any condition as they require new rules or conclusion of an international pact.

References:

1. Betz David,Stevens Tim," Cyberspace and Sovereignty", In Cyberspace and the State, Toward a Strategy for Cyber Power, The International institute for Strategic Studies, 2011.
2. European Parliament, "Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU", 15 April 2011.
3- European Security Review," Regulation of Cyber Warfare", Esr 70, Dec 2013.
4. Hanafieh Rajabi; Mohammad, "Jus ad bellum In Computer Network Attacks (CNA)", Payame Noor University, 2008.
5. Hathaway Oona and Crootof Rebecca, Levitz Philip, "The Law of Cyber Attack", California Law Review, 2012.
6. Klimburg Alexander and Tirmaa-Klaar Heli,"Cyberspace and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU", European Parliament, 15 April 2011.
7. Schmitt Michael, "International Law in Cyberspace", Online: www.harvardilj.org, 2012.
8. Sharp, Walter Gray,"Cyberspace and the Use of Force", Stanford University Libraries, 2013.
9. White House, "International Strategy for Cyberspace", The White House, May 2011.
10. Ziaee Bigdeli, Mohammad Reza, "The law of Armed Conflicts", Allame Tabatabaee University, 1994.

***