DOKUZ EYLÜL UNIVERSITY

GRADUATE SCHOOL OF SOCIAL SCIENCES

DEPARTMENT OF INTERNATIONAL RELATIONS

INTERNATIONAL RELATIONS PROGRAM

MASTER'S THESIS

THE PLACE OF THE CYBER WARFARE IN THE INTERNATIONAL LAW

Bahadır İNCE

Supervisor

Assoc.Prof.Dr.Deniz KIZILSÜMER ÖZER

İZMİR – 2015

MASTER THESIS/PROJECT
APPROVAL PAGE

University : Dokuz Eylul University
Graduate School : Graduate School of Social Sciences
Name and Surname : BAHADIR INCE
Title of Thesis : The Place of the Cyber Warfare in the International Law

Defence Date : 22/06/2015
Supervisor : Assoc Prof.Dr.Deniz KIZILSUMER OZER

EXAMINING COMMITTE MEMBERS

Title, Name and Surname	University	Signature
Assoc Prof Dr Deniz KIZILSUMER OZER	DOKUZ EYLUL UNIVERSITY	
Assist Prof.Dr Yaşar Metin OZDEMIR	DOKUZ EYLUL UNIVERSITY	
Assist Prof.Dr.Gokay OZERIM	YAŞAR UNIVERSITY	

Unanimity (X)
Majority of votes ( )

The thesis titled as "The Place of the Cyber Warfare in the International Law" prepared and presented by BAHADIR INCEis accepted and approved

Prof.Dr. Utku UTKULU
Director

DECLARATION

I hereby declare that this master's thesis titled as "The Place of the Cyber Warfare in the International Law" has been written by myself in accordance with the academic rules and ethical conduct. I also declare that all materials benefited in this thesis consist of the mentioned resources in the references list. I verify all these with my honour.

..../..../....

Bahadır İNCE

ABSTRACT

Master's Thesis

The Place of the Cyber Warfare in the International Law

Bahadır İNCE

Dokuz Eylül University

Graduate School of Social Sciences

Department of International Relations

International Relations Master Program

The concept of "cyber warfare" has appeared as a new threat to the international peace and security since the last decades of the 20th century. Everything connected to the computer networks in the world, such as personal information, bank accounts, top – secret government data, weapon systems, and power plants are highly vulnerable to "cyber attacks". This risk makes the cyber warfare one of the most problematic areas of international relations. The rapid technological advance in computer systems and Internet enables state and non – state actors to be able to take actions in cyberspace. Their activities sometimes cause asymmetric effects which are much more than expected. In this point, how the victim states of cyber attacks protect themselves and how to respond these attacks have still remain ambiguous because of the different interpretations of international law arrangements. In order to fill this loophole, the legal status of cyber warfare must be related with the concepts of prohibition of "use of force", the exceptions of use of force, self – defense, and "armed attack" which are exist in the current international law. For this reason, in this thesis, the legal aspects of cyber warfare are examined in the light of "*jus ad bellum*" in international law.

Keywords: Cyber Warfare, Cyber Attack, *Jus ad Bellum*, Use of Force, Armed Attack.

ÖZET

Yüksek Lisans Tezi

Siber Savaşın Uluslararası Hukuktaki Yeri

Bahadır İNCE

Dokuz Eylül Üniversitesi

Sosyal Bilimler Enstitüsü

Uluslararası İlişkiler Anabilim Dalı

İngilizce Uluslararası İlişkiler Programı

"Siber savaş" kavramı, 20. yüzyılın son yıllarından itibaren, uluslararası barış ve güvenliğe karşı yeni bir tehdit olarak ortaya çıkmıştır. Dünyada kişisel bilgiler, banka hesapları, çok gizli devlet bilgileri, silah sistemleri, güç santralleri gibi bilgisayar ağlarına bağlı olan her şey "siber saldırılara" karşı çok hassastır. Bu risk, siber savaşı, uluslararası ilişkilerin en sorunlu alanlarından birisi haline getirmiştir. Bilgisayar sistemleri ve internetteki hızlı teknolojik gelişmeler, devlet ve devlet dışı aktörlerin siber ortamda harekete geçebilmesini sağlamaktadır. Bu hareketler bazen beklenenin çok üzerinde asimetrik etkilere yol açmaktadır. Bu noktada, siber saldırı kurbanı olan devletlerin kendilerini nasıl koruyacakları ve siber saldırılara nasıl karşılık verecekleri, uluslararası hukuk düzenlemelerinin farklı yorumlanmasından dolayı hala muğlak kalmıştır. Bu boşluğu doldurmak için, siber savaşın yasal statüsü, uluslararası hukukta var olan "kuvvet kullanımının" yasaklanması, kuvvet kullanımının istisnaları, meşru müdafa ve "silahlı saldırı" kavramlarıyla ilişkilendirilmelidir. Bu nedenle, bu tezde, siber savaşın hukuki boyutları, uluslararası hukuktaki "*jus ad bellum*" kuralları ışığı altında incelenmiştir.

Anahtar Sözcükler: Siber Savaş, Siber Saldırı, *Jus ad Bellum,* Kuvvet Kullanımı, Silahlı Saldırı.

THE PLACE OF THE CYBER WARFARE IN THE INTERNATIONAL LAW

CONTENTS

CHAPTER TWO

CYBER WARFARE IN INTERNATIONAL LAW

CHAPTER THREE

WEAPONS OF CYBER ATTACK AND RECENT INSTANCES OF CYBER WARFARE

ABBREVIATIONS

CCDCOE	Co – operative Cyber Defense Centre of Excellence
DDoS	Distributed Denial of Service
DoS	Denial of Service
EU	European Union
ICJ	International Court of Justice
ICTY	International Criminal Tribunal for the Former Yugoslavia
IP	Internet Protocol
NATO	North Atlantic Treaty Organization
UN	United Nations
UNSC	United Nations Security Council
UK	United Kingdom
USA	United States of America
USSR	Union of Soviet Socialists Republics
WWII	World War Two

INTRODUCTION

History is a process in which countless conflicts and rivalries have never ended. From past to present, very few of these conflicts and rivalries have been solved in peaceful ways. Unfortunately, most of them have been converted into wars. The means of these wars have wide spectrum that ranges from primitive techniques, such as arrows, to the latest style of modern weapons. Within the rapid technological advance, in the 20th century, humanity witnessed disastrous faces of conflicts called conventional wars. But, in the past thirty years, another type of warfare has appeared: "cyber warfare".[1]

Cyber warfare has been accepted as a new evolution in the concept of war after nuclear weapons and intercontinental missiles had come into scene.[2] This new evolution increases the risk and makes "cyber era" more dangerous than the Cold War era. Even though cyber activities conducting in cyberspace seem intangible, their effects can be worse than the conventional wars.[3] Because of the fact that the cyber activities have potential to ruin the social life and cause great depression in society, the disastrous effects of these attacks seem in various parts of life, such as finance system, transportation system, medical system, political system etc.[4]

A new facet is added to the warfare concept. The ways of conducting war have changed drastically. Attacks no longer have to be conducted by military troops firing at visible targets. Anyone who has very few knowledge about computer systems can easily attack to government computer network systems by using complicated computer programs produced by hackers. These programs have become

[1] "Cyber war is an extension of policy by actions taken in cyber space by state or non-state actors that either constitute a serious threat to a nation's security or are conducted in response to a perceived threat against a nation's security." Paulo Shakarian and others, **Introduction to Cyber Warfare,** Syngress, Boston, 2013, p. 2.
[2] Randall R. Dipert, "The Ethics of Cyberwarfare", **Journal of Military Ethics**, Vol. 9, No. 4, 2010, p. 385.
[3] Bradley Raboin, "Corresponding Evolution: International Law the Emergence of Cyber Warfare", **Journal of the National Association of Administrative Law Judiciary**, Vol. 31, No. 2, 2011, p. 605
[4] Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", **Columbia Journal of Transnational Law**, Vol. 37, 1999, (Normative), p.886.

new types of weapons[5] and make computer users bad faith "potential cyber combatants".[6]

This new type of warfare has not only changed the weapons of war, but also the battlefield. In most widely known wars, two or more armed forces come up against each other on the grounds, air, or sea. Soldiers with rifles as members of military troops, and warships or warplanes with explosive bombs and missiles make an effort to kill or destroy each other, at least make their enemies "hors de combat".[7] On the contrary, in this new type of warfare, no soldiers, troops, and warplanes or warships are used. Enemies do not see each other and missiles on the battlefield. They can attack thousands of kilometers away from the target. The attackers conduct the war on the computer network systems, most generally called "cyberspace".[8] Cyberspace therefore has become a new battlefield.

---

[5] Cristopher D. DeLuca, "The Need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors", **3 Pace International Law Review Online Companion**, 2013, p. 279.

[6] Dipert, p. 385.

[7] "A person is *hors de combat* if: He is in the power of an adverse party; He clearly expresses an intention to surrender; he has been rendered unconscious or is otherwise incapacitated by wounds or sickness, and therefore is incapable of defending himself; provided that in any of these cases he abstains from any hostile act and does not attempt to escape." Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Article 41, available at https://www.icrc.org/ihl/WebART/470-750050?Open Document, (11.03.2015).

[8] Cyberspace is described as "global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." Department of Defense Dictionary of Military & Associated Terms 141, 2001, quoted by Raboin, p. 608. It is also defined in the United States Military Strategy for Cyberspace Operations as "a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures." The United States Military Strategy for Cyberspace Operations, the United States Department of Defense, December 2006, http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf, (09.10.2014). "Cyberspace is all of the computer networks in the world and everything they connect and control. It's not just the Internet. Let's be clear about the difference. The Internet is an open network of networks. From any network on the Internet, you should be able to communicate with any computer connected to any of the Internet's networks. Cyberspace includes the Internet plus lots of other networks of computers that are not supposed to be accessible from the Internet." Richard Clarke, "Cyber War", Harper Collis, New York, 2010, quoted by Papanastasiou Afroditi, "Application of International Law in Cyber Warfare Operations", 2010, http://dx.doi.org/10.2139/ssrn.1673785, (18.11.2014). "Cyberspace can be defined as the space in which information circulates from one medium to another and where it is processed, duplicated and stored. It is also the space in which tools communicate, where information technology becomes ubiquitous. So in effect, cyber space consists of communication systems, computers, networks, satellites, and communication infrastructure that all use information in its digital format. This includes sound, voice, text and image data that can be controlled remotely via a network…" Thomas A. Johnson, **Cyber-security Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare**, CRC Press, Boca Raton, 2015, p. 157.

This new arena of warfare involves all around the world with just a simple internet access. For this reason, even if it is supposed to be protected very well, all the networks that have access from outside are vulnerable to the "cyber attacks".[9]

The speed of the cyber attack cannot be compared to any other armed attacks in which conventional weapons are used. Cyber attacks may reach the target just in seconds regardless of whether the target is in another continent or not. This high speed makes states thunderstruck. They cannot react against the cyber attacks immediately. Moreover, they cannot understand what is going on. Thus, they become more vulnerable to the cyber attacks than the armed attacks.[10]

Another originality of the cyber warfare is its cheapness. It is claimed by an expert that "to bring the US to its knees" with one million dollars and twenty individuals is not impossible. This extraordinary thought comes from the reality of cyber warfare mentioned as "war on the cheap".[11] Huge land forces, enormous armies, millions of soldiers, and thousands of tons of bombs are no longer needed to attack states. Sending navy to the enemy shores or air force to dominate the battlefield airspace become needless.[12] It is enough to explode fuel refineries, or jam air – traffic control system by just a mouse click.[13] There is no need other than computer and internet access. A group of hackers whether supported by a state or not, or even just individuals have capability to attack states' critical national infrastructures that produce kinetic energy in everyday life. Hence, critical national infrastructure is getting more vulnerable to cyber attacks.

Moreover, they conduct their attacks by just keystroking on a computer keyboard in their office far away from the target state. So, it is nearly impossible to

---

[9] In the National Research Council document, "cyber attack refers to deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or network or the information and/or programs resident in or transiting these systems or networks." William A. Owens and others, **Technology, Policy, Law, and Ethics Regarding US Acquisition and Use of Cyber attack Capabilities**, The National Academies Press, Washington, 2009, p. 1. In the US Army Handbook, it is defined as "the premeditated use of disruptive activities, or the threat there of, against computers and/or networks, with the intention to cause harm or to further social, ideological, religious, political or similar objectives. Or to intimidate any person in furtherance of such objectives". The US Army Training & Doctrine Command, DCSINT Handbook No: 1.02 Critical Infrastructure Threats and Terrorism, 2006.

[10] Michael N. Schmitt, "The Law of Cyber Warfare: *Quo Vadis*?", **Stanford Law & Policy Review,** Vol. 25, 2014, (*Quo Vadis*), p. 276.

[11] Schmitt, Normative, p. 896.

[12] Walter Gary Sharp, **Cyberspace and the Use of Force**, Aegis Research Corporation, Virginia, 1999, p. 19.

[13] "Hype and Fear", **The Economist**, 08.12.2012, http://search.proquest.com/docview/1223834330?accountid=10527, (03.09.2013).

trace the attack and to find the attacker. This reality gives an asymmetric opportunity to weak states and non – state actors to cause destruction in powerful states. Because of the reason of "high gain with low risk", conducting warfare in cyberspace by both states and non – state actors has been highly increased.[14]

Furthermore, the remote control of cyber weapons is another biggest advantage of cyber attacks. The remote control systems of unmanned missions enable the technologically developed states not to put a single boot on the ground. The attackers therefore may conduct warfare without any risk of being responded.[15] Additionally, using cyber weapons have less risk than using conventional military weapons. Because of the lack of real soldiers and military vehicles in the battlefield, the risk of having casualties in cyber attack is also very low. Conversely, the militarily, economically, and morally gains of the cyber attacks are very high.[16]

In addition to the remoteness, the complexity of the cyber attacks gives another advantage to the attackers. They may deny an allegation of conducting a cyber attack even if the victim state is sure that the origin of the cyber attack comes from the territory of the attackers. Because of the fact that determining the main source of the cyber attack is very difficult, the attacker state may claim not to be aware of that the cyber attack is conducting in its own territory. This situation causes a problematic debate, an "attribution problem".[17]

Cyber attacks do not affect every state equally. The greater dependence on computer network systems a state has, the more vulnerable to cyber attacks it is. In technologically advanced states, both the governmental, military and private enterprise services are rely upon the internet and computer based networks so heavily that they become desired targets for cyber attackers.[18] Although the United States of America (USA) is the most capable state in cyber attack, the defense capability is three out of ten.[19] A senator's speech of "Americans like to think that this country

[14] Jonathan A. Ophardt, "Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield", **Duke Law & Technology Review**, Vol. 3, 2010, p. 12.
[15] Charles J. Dunlap, "Some Reflections on the Intersection of Law and Ethics in Cyber War", **Air & Space Power Journal**, Vol. 27, No. 1, 2013, p. 33.
[16] Schmitt, Normative, p. 13.
[17] Dipert, p. 385
[18] Scott J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law", **Berkeley Journal of International Law**, Vol. 25, No. 3, 2009, p. 198.
[19] "Hype and Fear", **The Economist**, (08.12.2012), http://search.proquest.com/docview/1223834330?accountid=10527, (03.09.2013).

has not been invaded since 1812 – in fact we are invaded every day." clearly expresses that the USA has been worried about the activities in cyberspace for a long time.[20] For this reason, the Cyber Command was established in the Pentagon in order to maintain the security of the military networks of the USA and, when needed, to assist the national private sectors.[21]

Armed forces dependent on technology are also more vulnerable than others that are less dependent. Cyber weapons can be used against the developed states' military systems based on computer network systems. For example, although the inter-continental missiles directed by satellite signals are protected very strictly, it is possible to misdirect them by jamming signals. Military communication systems and even conventional artillery weapons related to computer systems are very open to the harm of cyber attacks. While the troops that are not equipped with technological weapons are supposed not to be in danger, they are still under the risk of enemy weapons controlled by computer network systems, such as drones.[22] So, even in the battlefield of the conventional wars, it is very probable to encounter the problems of cyber weapons in recent years.

Because of these reasons, cyber attacks have been one of the most effective and cheapest ways for weak states to attack against the powerful ones. Industrialized and powerful states therefore have changed their resistance to the proposal of weak states about the interpretation of the Article 2(4) of Charter of the United Nations (UN). Recently, these states which are more vulnerable to cyber attacks have begun to widen the interpretation of this article by adding the cyber attacks. However, they do not permit weak states when the economic and political pressures were alleged to be interpreted within the framework of the Article 2(4).[23]

Cyber warfare is distinguished from other activities conducted in cyberspace. We cannot define all cyber activities as cyber warfare. While their situation seems similar to cyber warfare, they are legally different. Most of them are engaged in domestic law whereas cyber warfare is a subject of international law. Although I

[20] Dan Lerner, "Cyber-Attack Defense Plan Faces Criticism", **Financial Times (London)**, 02.02.2000, http://search.proquest.com/docview/248916398?accountid=10527, (08.09.2013).
[21] Ellen Nakashima, "Pentagon Is Debating Cyber-Attacks", **The Washington Post**, 16.11.2010, http://search.proquest.com/docview/762549546?accountid=10527, (06.10.2013).
[22] Andrew Liaropoulos, "Cyber-Security and the Law of War: The Legal and Ethical Aspects of Cyber-Conflict", **Working Paper of Greek Politics Specialist Group**, No. 7, 2011, p. 4.
[23] Schmitt, Normative, p. 886.

refer to cyber crime, cyber espionage, and cyber terrorism[24] in some part of my study, they are outside of the context.

In my study, I will analyze whether the cyber attacks constitute use of force and armed attack within the framework of the current international law in terms of *jus ad bellum.* I divide my study into three chapters. The Chapter I reflects the normative approach to the international law. In this chapter, debatable definition of prohibition of "use of force" is explained. The principle of non – use of force is very flexible because of the inadequacy of the clear definition of the term "force". Because of this reason, state officials stretch the rules and norms of the UN in parallel with their benefits. This also makes the situation more complex. I take the UN Charter as the point of origin. However, I also study in different international legal arrangements, such as the judgments and advisory opinions of the International Court of Justice (ICJ), in order to interpret the norms created by the UN Charter.

I begin with the process of codification of the prohibition of use of force. I bring this process from the past, nearly the beginning of the 20th century, to the present time. In this process, the attempts intended to prevent wars are explained. After the failure of these attempts, I mean two world wars, the UN established international law system which would also be a customary law in the future. The system created by the UN Charter is the main source of my research which is supported with other international documents.

After the historical background of the attempts to prevent wars, I focus on what constitutes use of force in accordance with the international law. The threshold of use of force is explicated according to the different perspectives of state officials. I give place two different approaches that are opposite to each other. On one hand, there are states claiming that soft powers, such as economic, political, and diplomatic pressure, constitute use of force. On the other hand, it is claimed that just armed force constitutes use of force. These two opposite arguments are covered in their own point of view. Moreover, in order to interpret the meaning of use of force more

[24] *Cyber crime* is desired to steal money or information, gain personal fame and attention, be intellectually challenged, and/or experience illicit pleasure. *Cyber espionage* is gathering secret data which enables strategic advantage. *Cyber terrorism* threatens or causes violence and fear in order to influence an audience. Natasha Solce, "The Battlefield of Cyberspace: The Inevitable New Military Branch-The Cyber Force", **Albanian Law Journal of Science**, Vol. 18, pp. 301,306.

clearly, I receive support from the Vienna Convention on the Law of Treaties which is the main international arrangement in interpretation of the international treaties.

The Article 2(4) of the UN Charter must be interpreted with its exceptions: measures taken by the UN and self – defense. In the first exception, in which conditions the UN can decide to take action is the written in the Article 39. The Article 41 and 42 also show the way of how the UN can exercise its authority. According to these articles, the authority of the UN increases gradually from the measures which do not constitute armed attack to operations by air, sea, or land forces.

The second exception is "self – defense". The Article 51, which is one of the most important articles of the UN Charter, allows using force in dire need of protection of territorial integrity and political independence against armed attacks. Of course, if your subject is self – defense, it absolutely gets moving to "armed attack". It is nearly impossible to explain self - defense without explaining armed attack. I therefore assess how use of force rises to the level of an armed attack, and which weapons are used in armed attack. In this point, the decision of the ICJ in the Nicaragua case sheds light on the matter. Therefore, in the first Chapter I, the relation between use of force and armed attack is also reviewed.

The Chapter II is about which place cyber warfare has in international law system. I assessed the cyber attacks in the light of the UN Charter. Whether cyber attacks constitute use of force or armed attack depends on the Article 2(4), Article 51 about self – defense, and measures taken by the UN Security Council. With respect to these articles, scholars produce some approaches about what are needed to establish use of force and armed attack. While all these three approaches are explained, one of them, effect – based approach, is focused on. In this approach, Michael Schmitt's seven criteria constitute significant place. While explaining these criteria, I also study in Tallinn Manual which is established by a group of experts of which chief is Michael Schmitt. Furthermore, real – world examples given by the scholars also become very useful in explaining the approach.

In the Chapter III, while I mainly discuss the cases about cyber attacks in recent years, I also describe how cyber attacks are developed in order to understand the cases easily. In the first part of the Chapter III, cyber weapons, which are indeed

computer programs or counterfeiting activities in cyber space, are described. Although this subject is needed technical substructure, which is out of my study, I try to give just summary information which can be understood easily. I need to discuss this subject because it would be difficult to understand the cyber attack instances mentioned in the following part. This chapter also helps us to comprehend the real – world examples.

The second part of the Chapter III brings the theoretical argument to the concrete instances. In this chapter, real – world cyber attacks are examined. The cyber attacks in which states are involved are the subject of this chapter. While there are so many cyber attacks worldwide, I focus on the state – sponsored attacks, at least supposed like that, to the critical national infrastructure systems because of the fact that it is possible to apply the international law to the state actors.

I mainly explain three instances. First instance that I explain is Estonia case. The cyber attacks to Estonia are the most effective ones that the world has ever witnessed. Both the Estonian government and people felt the effects of the cyber attacks in every part of their life. This instance displayed the destructive face of cyber attacks. Another instance I explain is Iran case. This attack's main point was that the real nuclear power plants which had huge potential physical threat were attacked. If it had been intended to destroy the power plants, it could have been a catastrophe of region. There could have been too many deaths and effected people. The last instance is Georgia case. Georgia's situation is slightly different from the others. Because cyber attacks to Georgia had begun before conventional armed conflict began. These cyber attacks also continued during the armed conflicts. This makes the cyber attacks to Georgia unique.

CHAPTER ONE
JUS AD BELLUM IN INTERNATIONAL LAW

1.1. HISTORICAL BACKGROUND

The legitimacy of war has been very controversial through the history. Because of this controversy, to arrange what makes war legal has become a necessity. This necessity created a new branch of international law interested in whether the reasons of war are lawful or not, which is called *jus ad bellum.*[25]

It had not been prohibited to initiate a war until 1900s. The first regulation about initiating a war was established in the Hague Convention III relative to the Opening of Hostilities, 1907. The Article 1 of the Convention holds that;

> *The contracting Powers recognize that hostilities between themselves must not commence without previous and explicit warning, in the form either of a declaration of war, giving reasons, or of an ultimatum with conditional declaration of war.*[26]

However, this article was about a formal declaration of war. It did not systematize the legal requirements of initiating war.[27]

Another attempt to arrange the legality of initiating war was tried by the League of Nations established after the World War I. This attempt was also unsuccessful to prohibit initiating a war. The international society realized the deficiency of the League of Nations and established the 1924 Geneva Protocol for the Pacific Settlement of International Disputes, which was never ratified. In this Protocol, to resort to war was banned with the exception of two situations: self – defense and collective enforcement measures. Although the Protocol did not come into force, it was accepted as a turning point of use of force.[28]

Another attempt was the Briand – Kellogg Pact which changed the meaning of *jus ad bellum* drastically. The principle of prohibition of war was adopted by the

[25] Sharp, p. 28.
[26] "Convention (III) relative to the Opening of Hostilities", 18 October 1907, available at https://www.icrc.org/ihl/INTRO/190?OpenDocument, (26.03.2015).
[27] Sharp, p. 30.
[28] Tarcisio Gazzini, **The Changing Rules on the Use of Force in International Law**, Manchester University Press, Mancherster, 2005. p. 20.

states party to the Pact. It was agreed that the settlement or solution of all disputes or conflicts must be based on pacific means.[29] However, the term "use of force" still remained ambiguous. While there were some shortfalls, this Pact became customary law in *jus ad bellum.* [30]

1.2. THE UNITED NATIONS' NORMS

These attempts could not achieve to completely maintain the peace and stability. Humanity experienced two terrible world wars in which millions of people were killed and injured. More than them lost their homes and became refugees. In order not to live these catastrophes again in the future, the United Nations established by the allied forces during the World War II (WWII) constituted "the norms of living in the peaceful world". During the last period the WWII, the UN Charter was signed by the states which had declared war on Germany and its allies.

The main purposes of the UN are to keep and maintain international peace and security. These purposes are expressed in the UN Charter. Especially, there are three articles of the UN Charter, 2(4), 39, and 51, to be covered in the same perspective. All of them collectively constitute the fundamental structure of contemporary *jus ad bellum*. These articles do not allow the threat or use of force unless the inherent right of self – defense and the decision of the UN Security Council exist.[31]

The prohibition of use of force, which is one of the most important issues in the international law, is also based on the UN Charter. The Article 2(4) of the Charter is so significant that it is put in the words as "the single most important fundament of world order".[32] This significance makes it a customary international law applicable for all states in the world, even if there are still some states which are not member of the UN.

---

[29] "Kellogg-Briand Pact, Article 2", 27 August 1928, available at http://www.history.ubc.ca/sites/default/files/courses/documents/%5Brealname%5D/kellogg-briand_pact_1928.pdf, (13.01.2015).
[30] Sharp, pp. 31, 32.
[31] Sharp, p. 34.
[32] John Norton Moore, **Crisis in the Gulf: Enforcing the Rule of Law**, Oceana Publication, New York, 1992, quoted by Sharp, p. 36.

The Article 2(4) of the UN Charter that prohibits threat or use of force expresses that;

> *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 purpose of the United Nations.*[33]

1.3. WHAT CONSTITUTES "USE OF FORCE"

While the Article 2(4) explains the statue of use of force in international law, it brings some confusing questions. The meaning of the "force" has been one of the most blurry areas in international law since the UN Charter signed.[34] It was avoided to use the term "war" instead of the term "use of force" in the Charter. The term "use of force" and "threat of force" were not clearly expressed. In this situation, the scope of the meaning of use of force and whether economic, political and other types of coercions are accepted as parts of the term use of force or not remain ambiguous. Therefore, it causes different interpretations.[35] What the fundamental meaning of the term force is and what constitutes use of force have not been plainly explained yet.

Explaining this debatable part of the UN Charter is very significant owing to the fact that cyber weapons are sometimes used as political or economic force to change the states' policy in parallel with the attacker states' or used to cause a real – world destruction as armed forces can cause. In which situations a cyber attack constitutes non – use of force, use of force, or armed attack may only be considered with an accurate definition of use of force.

Some policymakers and international lawyers, especially in developing and former eastern bloc states, claim that economic and political force applied by developed states must be assessed within the framework of the term use of force.[36] Scholars are divided into two main groups about this issue. First group clearly distinguishes the political and economic force from use of force expressed in the Article 2(4). They interpret the meaning of use of force narrowly which is limiting to

[33] Schmitt, Normative, p. 898.
[34] DeLuca, p. 294.
[35] Mehmet Yayla, "Cyber War and Use of Force against Cyber Attacks in International Law", **Türkiye Barolar Birliği Dergisi**, Vol. 107, p. 205.
[36] Yayla, p. 40.

only "armed force". This group of scholars comment that to use any kind of force is possible except force involving arms. Even though the political and economic pressures are designated as use of force, they are not the ones mentioned in the Article 2(4). So, the attempts to expand the limits of use of force by especially developing states are ignored.[37]

Most widely known example about this attempt is that the Brazilian delegation at the 1945 San Francisco Conference tried to widen the meaning of the term's range to the economic and political coercion. However, the Brazilian delegation's efforts met resistance and became unsuccessful. The voting of 26-2 showed that the majority of the conference did not confirm the demand of the Brazilian delegation. The common thought in the Conference did not support to extend the Article 2(4) to economic, political, and diplomatic pressure.[38]

Although these economic and political pressures to the states constitute threats to international peace and also violate the principle of non-intervention rule of the customary law, the specific meaning of use of force is mostly interpreted as "armed force".[39] The results of the armed force are usually physical destruction or injury, but the results of the economic and political pressures are not. Moreover, the risks of the armed force are more dangerous than the economic or political forces' owing to the fact that the armed force affect the human beings directly.[40]

Another reason why this group of scholars does not extend the meaning of use of force is to prevent different kinds of unlawful measures which are acted as respond to the political and economic threats.[41] For these reasons, the economic and political coercions are not the subjects of use of force. The common view in international society is that the Article 2(4) applies to armed force.[42]

The Nicaragua Case rendered a judgment which became a turning point in the international law. The ICJ decided what kinds of actions are accepted as use of force. In the Nicaragua case, the ICJ held that:

---

[37] Sharp, p. 88.
[38] Schmitt, Normative, p. 902.
[39] Schmitt, Normative, p. 904.
[40] Schmitt, Normative, p. 907.
[41] Daniel B. Silver, "Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter", **International Law Studies**, (ed. Michael N. Schmitt, Brian T. O'Donnell), Vol. 76, 2002, p. 83.
[42] Matthew C. Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)", **Yale Journal of International Law**, Vol. 36, 2011, (Future), p. 427.

> *While the arming and training of the contras can certainly be said to involve the threat or use of force against Nicaragua, this is not necessarily so in respect of all assistance given by the United States government. In particular, the Court considers that the mere supply of funds to the contras, while undoubtedly an act of intervention in the internal affairs of Nicaragua…does not in itself amount to a use of force.*[43]

Accordingly, just funding guerillas or any other non – state actors who were fighting against another state does not constitute use of force. Nevertheless, arming and training them are different from funding. In the event of arming and training them, it exceeds the threshold of intervention in the internal affairs. Therefore, even financing combatant groups do not amount to use of force, other economic pressures of which effects are not direct to armed actions would not either.[44]

However, this does not mean that there is no international law about such unlawful acts. The UN resolutions and ICJ decisions prohibits the inferences with a state's political, economical, or territorial integrity. The ICJ defines these kinds of actions as "less grave forms" of force that does not trigger the Article 51 but violates the principle of non-intervention.[45]

The second group of scholars asserts that to use the term "force" rather than "war" is more beneficial. In their opinion, the meaning of the term use of force is wider than just armed force. The Article 2(4) must also be interpreted in other meanings apart from the armed force. According to Black's Law Dictionary, force literally means "power, violence, and pressure directed against a person or thing". Thus, the meaning may be broadened to different types of coercion other than traditional armed force.[46] Their legal basis is the preamble of the UN Charter. They mention that to mind in just one statement of "…armed force shall not be used except…" is not enough. The extensively meaning of the all parts of the Charter must be taken into account in order not to ignore the main theme.[47]

Additionally, if lawmakers intended to mean just armed force, they could have used it. But they did not. Conversely, they used the term armed force in the

[43] Schmitt, Normative, p. 905.
[44] Silver, p. 81.
[45] Mary Ellen O'Connell, "Cyber Security and International Law", **Meeting Summary**, 29.05.2012, available at http://www.chathamhouse.org/publications/pepers/view/184529, (13.08.2013), p. 7.
[46] Marco Roscini, "World Wide Warfare – *Jus ad bellum* and the Use of Cyber Warfare", **Max Planck Yearbook of United Nations Law**, Vol. 14, 2010, p. 104.
[47] Sharp, p. 89.

Preamble of the Charter, Article 41, 43, 44, and 46 but Article 2(4). Instead of using armed force in the Article 2(4), the term use of force was written owing to the fact that the interest spectrum of the UN is far more than just the armed conflicts.[48]

The 1970 Declaration on Principles of International Law Concerning Friendly Relations and Cooperation among States[49] emphasizes that to refrain from military, political, economic, or any other form of coercion aimed to the political independence or territorial integrity of any state is a duty of states.[50] The Article 32 of the Charter of Economic Rights and Duties of States adopted by the UN General Assembly in 1974 also approves that "No state may use or encourage the use of economic, political or any other type of measures to coerce another state in order to obtain from it the subordination of the exercise of its sovereign rights."[51]

In addition to these two thoughts, some scholars combine them and reach a conclusion that economic and political force, like boycotts, cessation of trade, devaluation, and recall an ambassador, are lawful and do not constitute use of force. These kinds of force are different from those used to force another state to surrender to the will of itself by violating the principles of the "political independence" and "territorial integrity". In contrast to them, the political or economic aggression constitutes use of force when they endanger the fundamental requirements of "territorial integrity" and "political independence".[52]

1.4. INTERPRETATION OF "USE OF FORCE" ACCORDING TO THE VIENNA CONVENTION ON THE LAW OF TREATIES

Another way of clarifying this confusing debate is to look at the Vienna Convention on the Law of Treaties, signed in 1969, which shows the main points of international treaty interpretation. The Article 31(1) of the convention states that;

---

[48] Sharp, p. 89.

[49] Resolution adopted by the General Assembly, "2625 (XXV). Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations", 24 October 1970, available at http://www.un-documents.net/a25r2625.htm, (10.03.2015).

[50] Malcolm Shaw, **International Law**, Cambridge University Press, New York, 2008, p. 1125.

[51] Resolution adopted by the General Assembly, "3281(XXIX). Charter of Economic Rights and Duties of States, Article 32", 12 December 1974, available at http://www.un-documents.net/a29r3281.htm, (22.12.2014).

[52] Sharp, p. 91.

> *A treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose.*[53]

At first glance, the meaning of use of force as used only in the Article 2(4) of the UN Charter is very broad. It includes military, economic, diplomatic and ideological coercions.[54] On the other hand, according to the Article 31(1) of the Vienna Convention, the term force must be interpreted narrowly in its ordinary meaning with respect to the "object and purpose" of the UN. In the preamble of the Charter, the main approach is clearly mentioned that "we the peoples of the United Nations determined to have succeeding generations from the scourge of war...and for these to ensure… that armed force shall not be used..."[55] As written in the Article 1 of the UN Charter, keeping the international peace and security is the main aim of the UN. In order to protect next generations from the scourge of the war, this stability must be maintained.[56] All parts of the Charter have to be consistent with the preamble and the main aim must also be interpreted in parallel with them. Besides, if the political, economic, or diplomatic pressures were intended to mention in Article 2(4), the term "armed force" would not be used in the preamble.[57]

That the term armed force is used in other articles of the Charter is another sign.[58] The Article 41 of the UN Charter also states that "the Security Council may decide what measures not involving the use of armed force…These may include…air, postal, telegraphic, radio, and other means of communication, and…" In the consecutive articles of the Chapter VII, if these measures not involving use of armed force are inadequate, to use armed force would not become illegal in the name of the right of self – defense.[59]

As mentioned in the Vienna Convention, no term can be used contrary to the main purpose of the treaties due to the fact that the misused terms may defeat the

---

[53] "Vienna Convention on the Law of Treaties, Article 31", 23 May 1969, available at https://www.un.org/doc/so...e/publications/THB/English.pdf, (17.11.2014).
[54] Michael Gervais, "Cyber Attacks and the Laws of War", **Berkeley Journal of International Law**, Vol. 30, No. 2, 2012, p. 536.
[55] "The UN Charter, Preamble", 26 June 1945, available at http://www.un.org/en/documents/charter/preamble.shtml, (30.04.2014)
[56] The UN Charter, Article 1.
[57] Schmitt, Normative, p. 901.
[58] Yayla, p. 205.
[59] Russell Buchan, "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions", **Journal of Conflict & Security Law**, Vol. 17, 2012, p.217.

comprehensive "object and purpose" of the treaties. In order to keep the stability, the Charter prohibits using armed force. Instead, the self – defense and collective security systems are established. This purpose of the UN and the historical events indicate that the term "force" is limited to the military acts, especially armed attacks and it states that the term force must be interpreted as "armed force".[60] When considering the historical, textual, and systematic interpretation of the UN Charter, there is no doubt that the expected meaning of the term "force" is nothing but the armed force.[61]

Though the broadness of regular meanings of a use of force encompass both armed and unarmed practices, recently, the majority of the legists agree that the interpretation of the term "force" in the Article 2(4) of the UN Charter means "armed" and "military" force.[62] While the term armed force is mostly understood when the term "force" is used, the specific definition of "armed force" is still not available in the international treaties or agreements.[63]

1.5. EXCEPTIONS OF USE OF FORCE

Use of force is clearly banned with Article 2(4) of the UN Charter except two situations. The first one is measures taken by the United Nations Security Council (UNSC) and the other one is self – defense of states.

1.5.1. Measures Taken by the United Nations Security Council

The violation of the Article 2(4) gives an authority to the UNSC to approve use of force in order to keep or restore international peace, security and stability. The first point of this authorization is the Article 39 of the UN Charter. The conditions of

[60] Buchan, p. 218.
[61] Katharina Ziolkowski, "*Jus ad Bellum* in Cyberspace – Some Thoughts on the 'Schmitt Criteria' for Use of Force", **Proceeding of the 4th International Conference on Cyber Conflict**, (ed. Christian Czosseck, Rain Ottis, Katharina Ziolkowski), 2012, p. 297.
[62] Nils Melzer, "Cyberwarfare and International Law", **UNIDIR Books and Reports**, United Nations Institute for Disarmament Research, Geneva, 2011, p. 7.
[63] David E. Graham, "Cyber Threats and the Law of War", **Journal of National Security Law & Policy**, Vol. 4, No. 1, 2010, p. 90.

this article, such as threat to the peace, breach of the peace, or act of aggression, have to exist.[64] Only the presence of them crosses the limits as written in the article 39;

> *The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security.*[65]

This exception about use of force is very flexible. Because, less grave forms of domestic violence, human rights violations, terrorist actions, displaced refugees, anti–democratic regimes that persecutes citizens may be reasons of use of force decided by the UNSC.[66] In order not to misuse this exception, the UNSC generally assess these circumstances in combination when they exceed the threshold of negligible level.[67]

What kind of measures can be taken are the subjects of the Article 41 and 42. The Article 41 tasks the member states to stop economic or diplomatic relations, and leave some means of communication in order to make aggressor state obey the international law. The point that makes this article important is that these measures are listed as measures not involving use of armed force[68] as noted that;

> *The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations.*[69]

Contrary to the Article 41, Article 42 follows more active way. If all necessary measures in Article 41 to maintain peace and security are not enough, then, one state or a group of states of the member states may be assigned by the UNSC to use armed force against the aggressor state.[70] Article 42 holds that;

---

[64] Jeffrey Carr, **Inside Cyber Warfare**, O'Reilly Media, California, 2012, p. 49.
[65] The UN Charter, Article 39.
[66] Sharp, p. 50.
[67] Gazzini, p. 32.
[68] Sharp, p. 50.
[69] The UN Charter, Article 41.
[70] Sharp, p. 52.

> *Should the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security. Such action may include demonstrations, blockade, and other operations by air, sea, or land forces of Members of the United Nations.*[71]

1.5.2. Self – Defense

The second exception of use of force is self – defense which means that if any state feels itself in need of self-defense in order to prevent its rights against an armed attack, this state can use of force, which has a defensive character, on its own or collectively as set out in the Article 51;

> *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. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.*[72]

The attacks causing a self-defense must be attributable to a state.[73] A right of self – defense is invoked against only states. However, after the September 11th terrorist attacks, the UN Security Council issued a resolution that non – state actors could perpetrate an armed attack. Thus, it became possible to use a right of self – defense against them. The USA operation to Afghanistan was a striking example of this approach. However, the effects of this development did not have a long run. The ICJ declared that inherent right of self – defense is invoked "by one state against another state" in Advisory Opinion on the Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, in 2004.[74] The Court repeated the

[71] The UN Charter, Article 42.
[72] The UN Charter, Article 51.
[73] O'Connell, p. 6.
[74] ICJ, "Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory", 09 July 2004, available at htttr://unispal.un.org/UNISPAL.NSF/0/3740E39487A5428A85256ECC005E157A, (21.03.2015).

same opinion in the judgment of an Armed Activities on the Territory of the Congo, in 2005.[75]

More important than the attribution problem is that the presence of right to use of force in self – defense is dependent on whether an armed attack occurs or not. Actually, use of force is prohibited with respect to Article 2(4). When Article 51 is assessed together with the Article 2(4), it becomes legal to use of force if the victim state is exposed to an armed attack that violates the Article 2(4). In other words, to be exposed an armed attack gives a right to use of force in self – defense.[76] But, this force must be used as a last resort if peaceful ways do not work and must not exceed the needed level of self – defense.[77]

1.5.2.1. Armed Attack

What constitutes armed attack is also one of the problematic fields of international law. The meaning of the "attack" is a subject of law of armed conflict, *jus in bello*, and codified in the 1977 Additional Protocol I to the Geneva Conventions. The definition of the "attack" is explained in the Article 49(1) of the Additional Protocol I to the Geneva Conventions as "acts of violence against the adversary, whether in offence or in defense".[78] Another part of the article, 49(3), emphasizes that all kinds of attacks coming from air, sea, and land are the subject of the Protocol provided that they affect the civilian population and individual objects.[79]

The UN General Assembly has a resolution, which is called "General Assembly Definition of on Aggression", that lists the acts of aggression. In this resolution, there is no direct definition of armed attack but these acts are generally accepted as examples of armed attack. These are the acts written in the Article 3 of the resolution: "invasion, attack by the armed forces of a state of the territory of another state, bombardment, blockade, an attack by the armed forces of a state on the land, sea or air forces, allowing a state to use own territory for an act of aggression to

[75] Sheng Li, "When Does Internet Denial Trigger the Right of Armed Self-defense?", **Yale International Journal of Law**, Vol. 38, No. 1, 2013, p. 205.
[76] Carr, p. 50.
[77] Li, p. 202.
[78] 1977 Additional Protocol (I) to the Geneva Conventions, Article 49.
[79] Charles J. Dunlap, "Perspectives for Cyber Strategists on Law for Cyberwar", **Strategic Studies Quarterly**, Vol. 5, No. 1, 2011, (Perspective), p. 85.

the third state, breaching of stationing agreements, sending of armed bands, groups, irregulars or mercenaries".[80] If any violent acts occur other than acts mentioned in the Resolution, then, it must be focused on the state acts. Whether these acts constitute an armed force or not is dependent on the inquiry.[81]

On the other hand, according to the definition given by the Dictionary of Contemporary English armed means "carrying weapons, especially a gun".[82] The meaning of "weapon" is also defined in Black's Law Dictionary as "an instrument used in fighting; an instrument of offensive or defensive combat".[83] So, in order to say "armed attack", there must be an act of violence against the adversary, whether in offensive or defensive in which an instrument of offensive or defensive combat is used.

The way of using weapons is also debatable. Previously, it was considered that weapons must produce kinetic energy, such as explosion, in order to violate the Article 2(4) of the UN Charter. In this perspective, the chemical, biological, and even nuclear weapons are excluded because of the fact that their systems are different from conventional weapons and these weapons do not produce conventional kinetic energy. Sir Ian Brownlie criticized this interpretation. He set a standard which was called "the destruction to life and property". According to his approach, any weapon that causes destruction to life and property constitutes use of force regardless of its destruction mechanism. Kinetic energy is not more important than the results, such as death and injury. If the results of the chemical, biological, or nuclear attacks are same as kinetic attacks, it is clear that they fall under the prohibition of the Article 2(4). While these kinds of unconventional weapons do not have kinetic effect on the targets, it is generally accepted as use of force. Every instrument causing death and injury must be interpreted as weapons. This thought was also acknowledged as one of the first signs of "effect – based" approach which we will discuss later. It was also gained significance in international law literature.[84]

[80] Resolution adopted by General Assembly, "3314 (XXIX). Definition of Aggression, Article 3", 14 December 1974, available at http://www.un-documents.net/a29r3314.htm, (02.11.2014).
[81] Sharp, p. 119.
[82] Dictionary of Contemporary English, Longman, 1995, p. 61.
[83] Black's Law Dictionary Free Online Legal Dictionary, available at http://thelawdictionary.org/weapon/, (13.02.2015).
[84] Buchan, p. 218.

This approach was also supported by the ICJ. According to the ICJ, use of force is prohibited irrespective of what kind of weapons is used. The Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons of the ICJ also expressed that "These provisions do not refer to specific weapons. They apply to any use of force, regardless of the weapons employed".[85] In other words, if an attacker's intent is hostile, nearly every object can be used as a weapon.[86] Karl Zemanek also shares the same opinion with the ICJ. He asserts that;

> *It is neither the designation of device, nor its normal use, which make it a weapon but the intent with which it is used and its effect. The use of any device or number of devices, which results in a considerable loss of life and/or extensive destruction of property must therefore be deemed to fulfill the conditions of an armed attack.*[87]

The threshold of the level of damage or injury which occurs as a result of armed attacks is slightly confusing. The ICJ set forth some significant principles considering the "importance of an attack". Not all armed conflicts, such as inconsiderable border disputes that are minor in their "scale and effects", can be a reason of use of force in self-defense. These kinds of actions are defined as "mere frontier incidents" by the ICJ and their level of "gravity" are not as much as armed attacks. It is generally determined by the ICJ that only the acts of aggression of which "scale and effects" are sufficient rise to the level of armed attack. Unless loss of life or important property damage takes part in a use of force, it does not rise to the level of an armed attack.[88]

Nevertheless, it does not mean that a state cannot use force within the right of self – defense as a respond to unlawful use of force. This situation does not make states unable to adopt measures to respond to violations of its territorial integrity and political independence. It is possible to use lawful responses against another state's unlawful use of force. Diplomatic or economic sanctions are the most used means to

[85] ICJ, "Legality of the Threat or Use of Nuclear Weapons", 8 July 1996, available at www.icj-cij/docket/files/95/7497.pdf, (29.03.2015).
[86] Roscini, p. 106.
[87] Karl Zemanek, "Armed Attack", **Max Planck Encyclopedia of Public International Law**, (ed. Rüdiger Wolfrum), 2010, p. 21, quoted by Nils Melzer, p. 13.
[88] Schmitt, *Quo Vadis*, p. 282.

constitute a lawful counter measures. Furthermore, the way of referring the issue to the Security Council of the UN is always an alternative option.[89]

In the judgment of the ICJ in Nicaragua Case, the US supports in financing, organizing, training, supplying, and equipping of the "contras" were revealed by the Court. Although, there is no doubt that the USA's participation to the contras increased the acts of violence, it is obvious that arming and training the armed groups in another state which are less effective than to fight actively against the government forces are not equal to armed attack while they constitute use of force.[90] So, arming and training armed groups who are in trouble with their own government do not reach to the level of an armed attack.[91]

This decision clarifies that not all damaging events may be enough for authorization of the armed attack.[92] Not all the violations of prohibiting use of force amount to armed attack and trigger the inherent right of self – defense. There may be unlawful intrusion but this does not give right to states to respond with armed force within the framework of self – defense.[93] The UN Charter gives a right to the victim states for self – defense provided that not to use armed force if the attacker state's use of force does not involve an armed attack. This is a fundamental rule for states to respond by using armed actions as a self-defense.[94]

With the Nicaragua judgment of the ICJ, a gap between the term "force" and "armed" was recognized. For the ICJ, some measures do not constitute an armed attack but involve a use of force. This means that "all armed attacks are uses of force, but not all uses of force are armed attacks".[95] Whereas the most grave forms of the use of force are rising to the level of an armed force, the less grave forms are not.[96]

[89] Schmitt, Term of Art, p. 287.
[90] Silver, p. 81.
[91] Michael N. Schmitt, "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed", **Harvard International Law Journal Online**, Vol. 54, 2012, (Tallinn Manual), p. 20.
[92] Charles J. Dunlap, Perspective, p. 86.
[93] Christopher J. Joyner and Catherine Lotrionte, "Information Warfare as International Coercion: Elements of a Legal Framework", **European Journal of International Law**, Vol. 12, No. 5, p. 851.
[94] Sharp, p. 76.
[95] Michael N. Schmitt, "Attack as a Term of Art in International Law: The Cyber Operations Context", **Proceeding of the 4th International Conference on Cyber Conflict**, (ed. Christian Czosseck, Rain Ottis, Katharina Ziolkowski), 2012, (Term of Art), p. 287.
[96] Schmitt, Tallinn Manual, p. 22.

Thus, the ICJ expresses that the threshold of the use of force is lower than the threshold of the armed attack.[97]

However, the governments are intended to fill this gap in the light of their interests. According to the declaration of Harold Koh, the former State Department Legal Advisor of the USA, there is no difference between an armed attack and any unlawful use of force. The "armed attack threshold" is invalid for a "use of deadly force".[98] Another speech of him, "when warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states posses an inherent right to self – defense…" also reaffirms the US position.[99]

As a result, the most grave forms of use of force in which any weapon that causes loss of life and property damage is used constitutes armed attack. Walter G. Sharp gives the simplified definition of the "armed attack" within the framework of these international documents. According to his definition, an armed attack is "a use of force that rises to a certain scope, duration, and intensity threshold constitutes an armed attack within the meaning of Article 51 of the Charter of the United Nations that invokes a state's inherent right of self – defense".[100]

1.5.2.2. Anticipatory Self – Defense

Does a state have to wait to defend itself until aggressor state attacks? This question is also one of the most debatable sections of self – defense. Whether an attack to aggressor state of which armed attack has not actually occurred yet can be accepted as self – defense or not is generally assessed within the framework of *Caroline Case*, which is a historical turning point of this subject.

The *Caroline Case* occurred in 1837 when Canada was struggling against the British Army in order to gain their independence. During this struggle era, some of the Canadian troops attacked the British troops from Navy Island where is in the middle of the Niagara River which constitutes a natural border with the USA and Canada were supported by the Caroline, the US ship, in which there were Canadian

[97] Sharp, p. 44.
[98] Schmitt, *Quo Vadis*, p. 284.
[99] Schmitt, Tallinn Manual, p. 21.
[100] Sharp, p. 119.

sympathizers. Thereupon the British troops damaged the Caroline and some US citizens died.[101]

In this case, the British Government claimed that the Caroline was a pirate ship and the United Kingdom (UK) used their right of self – defense. In the British perspective, they had a right to take measures to defend their troops even if they were in the USA territory because of the incapacity of the USA to take action. However, the USA refused this claim and brought the case to the arbitration. The arbitrary decision accepted the legality of anticipatory self – defense in some conditions but not in *Caroline Case*.[102]

In the *Caroline Case,* Daniel Webster who was a Secretary of Foreign Affairs of the USA agreed upon certain conditions that a right of self – defense could be claimed. These conditions were declared as "necessity of self – defense, instant, overwhelming, leaving no choice of means, and no moment for deliberation". Thus, armed attacks within the framework of the right of self – defense become legal in international law, provided these criteria are met.[103]

It has constituted a traditional perspective in international law which is called Webster formula. Professor Cassese also put strict conditions in parallel with Webster formula that,

> *"(i) solid and consistent evidence exists that another country is about to engage on a large – scale armed attack jeopardizing the very life of the target state and (ii) no peaceful means of preventing such attack are available either because they would certainly prove useless to the specific circumstances, or for lack of time to resort to them, or because they have been exhausted."*[104]

If there is an imminent danger or very evident threat of an armed attack and a state foresee to be exposed an armed attack coming soon, then, this state can defend itself by using armed force. A potential attack must be unavoidable and no

[101] Ahmet Buğra Aydın, "Uluslararası Hukukta Önleyici ve Öngörücü Meşru Müdafaa Hakkı", **Genç Hukukçular Hukuk Okumaları**, Vol. 4, 2013, p. 56.
[102] Aydın, p. 57.
[103] Tom Ruys, **Armed Attack' and Article 51 of the UN Charter**, Cambridge University Press, New York, 2010, p. 251.
[104] Horace B. Robertson, "Self-defense against Computer Network Attack under International Law", **International Law Studies**, (ed. Michael N. Schmitt, Brian T. O'Donnell), Vol. 76, 2002, p. 129.

reasonable choice of peaceful means. Armed attacks in these conditions are generally accepted as legal.[105]

[105] Shackelford, p. 226.

CHAPTER TWO
CYBER WARFARE IN INTERNATIONAL LAW

Legal status of cyber attacks has become controversial and problematic issue since the number of cyber attacks began to rise. Although a lot of studies have been revealed, the legal regime for the cyber activities has not been clearly mentioned until now. Tony Blair, former Prime Minister of the UK, also complained about this situation by declaring that "The precedents and the laws on the books are just hopelessly inadequate for the complexity of the global information network".[106]

The main part of this controversy is whether a cyber attack constitutes "use of force" or not. As we discussed in the previous chapter, state officials and scholars are already in trouble to determine the threshold of use of force. When the cyber actions are added to this controversy arena, it becomes more complex and chaotic. Where the threshold of use of force in cyberspace begins causes different views among scholars.[107]

Generally, the legal regime of the cyber actions is assessed within the perspective of the UN Charter. It is a common thought that the main approaches to use of force in the UN Charter are also applicable to cyber actions. On the other hand, special regulations about the cyber actions are also needed. The most extensive study about the activities in cyberspace is the handbook of "Tallinn Manual on the International Law Applicable to Cyber Warfare". The necessity of this kind of legal document proceeded from the Russian cyber attack against Estonia's critical national infrastructure that caused a long - term chaos in the state. The group of experts came together in Co – operative Cyber Defense Centre of Excellence (CCDCOE) of the North Atlantic Treaty Organization (NATO) in Tallinn, the capital city of Estonia.[108] Although this handbook is not an official document or policy of NATO and does not have constitutional authority, a great consensus of scholars on law of cyber warfare makes it very useful as an advisory document. This document is defined by legal

[106] Ellen Nakashima, "Pentagon Is Debating Cyber-Attacks", **The Washington Post**, 16 November 2010, http://search.proquest.com/docview/762549546?accountid=10527, (06.10.2013).
[107] Schmitt, *Quo Vadis*, p. 279.
[108] Johnson, p. 193.

advisors of the NATO as "the most important document in the law of cyber – warfare".[109]

These attempts are in pursuit of seeking an answer of where a cyber attack should be placed in the international law system. Indeed, the definition of the term "cyber attack" is explained in the Tallinn Manual that "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[110] Whether a cyber attack can be accepted as use of force within the framework of the international law is still the main point of these attempts. After the solution of this question, another one comes. Does it range to the level of an armed attack which triggers the right of self - defense?

Actually, the place of the cyber attack is in a grey zone because of the fact that there is no unambiguous legal identification in international law system. The international society cannot put the case clearly because it is too difficult to categorize the effects of the cyber attacks. It may cause both the traditional armed force consequences and other types of coercion consequences.[111] So, there is no single answer about the statue of the cyber attacks. While not all cyber attacks are equal to the level of use of force or armed attack, scholars emerged three main views that clarify the statue of the use of force: the instrument – based approach, the target – based approach, and the effect – based approach.[112]

2.1. INSTRUMENT – BASED APPROACH[113]

The "instrument – based" approach only takes the conventional military weapons into consideration. In this approach, just these weapons can constitute an armed attack. In the light of this perspective, the instrument – based approach does not accept a cyber attack as an armed attack owing to the lack of the presence of

[109] Owen Bowcott, "Nato Guide Says Nuclear Plants and Hospitals Are Off- Limits in Cyberwar: Online Attacks Could Make 'Hacktivists' Lawful Targets Project Codifies Legal Basis For State-Led Cyber-Warfare", **The Guardian**, 19 March 2013, http://search.proquest.com/docview/1317738187?accountid=10527, (22.07.2013).
[110] Michael N. Schmitt (ed.), **Tallinn Manual on the International Law Applicable to Cyber Warfare**, Cambridge University Press, New York, 2013, (Cyber Warfare), p.106.
[111] Melzer, p. 9.
[112] Oona A. Hathaway et al, "The Law of Cyber-Attack", **California Law Review**, Vol. 100, No. 4, 2012, p. 848, DeDeluca, p. 286, Graham, p. 91.
[113] Schmitt, Normative, p. 1005.

these kinds of weapons. If a cyber attack constitutes an armed attack, weapons used in cyber attacks must be traditional military weapons that cause sufficient kinetic destruction but they are not.[114] For instance, if there was an attack in which military weapons are used at the same time with the cyber attack or a bombing assault against to the computer network systems of any state, it could absolutely constitute an armed attack.[115]

Duncan Hollis also argues that not all cyber attacks are equal to armed attacks because of the lack of the traditional kinetic characteristics of the military efforts. For instance, just interruption of the communication is not enough to constitute an armed attack, different types of aggression that are more severe are required to apply the Article 2(4) of the UN Charter.[116]

In this point of view, the UN Charter provides some support to Hollis's approach. According to the Article 41, as mentioned above, the Security Council may decide which measures may be applied with respect to the threats to the peace, breaches of the peace, and acts of aggression. The measures not involving the use of force are complete and partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio and other means of communication. The "definition of aggression" given by the UN General Assembly also supports this approach. The acts which constitute aggression must involve armed weapons or force.[117] The first article of the Resolution is very similar to the Article 2(4) of the UN Charter but there is a noticeable difference. In this Resolution, aggression is defined as "the use of armed force" as written "Aggression is the use of armed force by a state against the sovereignty, territorial integrity or political independence of another state". In the Article 3 of the Resolution, seven types of aggression are related to the classical military weapons.[118] Besides, the threat of force is not added to the definition of aggression. This means that the aggression comes into being when military armed

[114] Li, p. 186.
[115] Hathaway et al, p. 848.
[116] Duncan B. Hollis, "Why States Need an International Law for Information Operations", **Lewis & Clark Law Review**, Vol. 11, 1997, p. 1041.
[117] Hathaway et al, p. 848.
[118] Arie J. Schaap, "Cyber Warfare Operations: Development and Use under International Law", **Air Force Law Review**, Vol. 64, 2009, p. 143.

forces equipped with traditional weapons are used. In this perspective, the political, economical, cultural, and ideological pressures do not constitute any aggression.[119]

On the other hand, the ICJ had an advisory opinion about the threat or use of nuclear force which was slightly different. In this decision's perspective, in order to interpret the cyber attack as an armed force, just considering the use of traditional military weapons are not enough. As we discussed in the previous chapter, Karl Zemanek noted that "The use of any device or number of devices, which results in a considerable loss of life and/or extensive destruction of property must be deemed to fulfill the conditions of an armed attack."[120]

According to the nuclear weapon advisory opinion, it is very clear that victim states might be affected by the non – traditional military weapons as much as military weapons. Furthermore, non – traditional military weapons sometimes might generate more fatal consequences than the others. The main point lies in the consequences what weapons produce. For example, to open the gates of the dams and let the water release without the control to create a flood, or to fire a light in the forest to spread across border are not traditional military weapons, but their affects might be worse than the bullets, grenades, or bombs. This reality makes the instruments of an armed attack immaterial. Anything that can be used as a weapon can be a weapon.[121]

Another striking examples of weapons causing armed attack are airplanes hijacked by terrorists in 9/11 attacks. After 9/11 attacks, the USA was authorized by the UN Security Council to respond forcefully in self - defense. For this reason, some scholars agree that the Article 2(4) involves these kinds of use of force even if they are not traditional military weapons. Depending on this, it also causes that the right of self – defense mentioned in Article 51 might be triggered against conventional and non – conventional weapons with regards to the "scale and effects" test.[122]

The US Secretary of Defense also shared the same thought. In 1999, Defense Department Assessment of International Legal Issues in Information Operations noted that;

[119] Yayla, p. 213.
[120] Melzer, p. 13.
[121] Sharp, p. 101.
[122] Gervais, p. 543.

> *If we focused on the means we used, we might conclude that electronic signal imperceptible to human senses do not closely resemble bombs, bullets, or troops. On the other hand it seems likely that the international community will be more interested in the consequences of a computer network attack than in its mechanism.*[123]

The most significant specificity of this approach is clearness of the definition because it is very easy to define conventional military weapons. However, the cyber weapons sometimes have more capability to give damages and causalities than military weapons. So, there have been long debates about the usefulness of this approach among scholars for a long time.[124]

2.2. TARGET – BASED APPROACH[125]

In the "target – based" approach, any cyber attack aimed to the critical national infrastructure is determined as armed attack although its severity is not sufficient. In this approach, if a cyber attack affects the critical national infrastructure, even there is no important disruption or there is a cyber operation which is lawful under international law such as espionage, it constitutes an armed attack.[126] Because, the critical national infrastructures are so important that any attack to or even espionage into these systems cause to prevent states from defending themselves. This significance leads states to take an action in the cyberspace or in other ways. Hence, to respond with a necessary and proportional use of force can be lawful.[127]

The state officials are interested in not only data theft but also cyber attacks to power grids, communication systems and other critical structures.[128] According to the UN General Assembly's Resolution of Creation of a Global Culture of Cyber Security and the Protection of Critical Information Infrastructures, "each country will

[123] Waxman, (Future), p. 433.
[124] Yayla, p. 213.
[125] While the term "Aimed – based" can be used, it is preferred using the term "Target – based" as written in the Hollis, p. 1041.
[126] DeLuca, p. 297.
[127] Sharp, p. 130.
[128] John Stephenson and Karla Jones, "Fighting Cyber Warfare at the State Level; While Congress and the President Quarrel over What to Do Next, Governors Join in a Collaborative Defense Effort", **Wall Street Journal**, 22 February 2013, http://search.proquest.com/docview/1296294459?accountid=10527, (03.09.2013).

determine its own critical information infrastructures".[129] The declaration of the President Clinton extensively defined the US critical national infrastructure. This declaration does not only consist of military targets but also commercial institutions and any other economic interests. According to this declaration, either physical or cyber attacks against telecommunications, electrical power plants, gas and oil storage, transportation, banking and finance, water supply system, emergency services, and continuity of government are unacceptable considering the effects on national defense end economic security.[130] Additionally, "public and private institutions in the sectors of agriculture, food, water, public health, emergency services, government, defense industrial base, information, and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping'' are regarded as the US critical infrastructure in the 2003 United States National Strategy to Secure Cyberspace.[131] This perspective expresses how extensive the critical national infrastructure can be interpreted.

The UK categorizes its critical infrastructure as energy, food, water, transport, communications, government and public services, emergency services, health and finance systems.[132] The European Union (EU) also defines the critical infrastructure as "those physical resources, services, and information technology facilities, networks and infrastructure assets which, if disrupted or destroyed, would have a serious impact on health, safety, security or economic well – being of citizens or the effective functioning of governments".[133] It is also agreed by almost all legal commentators that the presence of right of self – defense for these infrastructure systems within a state's own territory, without any distinction between governmental or non – governmental, is indisputable.[134]

---

[129] Resolution adopted by the General Assembly, "58/199. Creation of a Global Culture of Cyber Security and the Protection of Critical Information Infrastructures", 30 January 2004, available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf, (12.04.2015).

[130] Executive Order EO 13010, Critical Infrastructure Protection, 15 July 1996, available at http://fas.org/irp/offdocs/eo13010.htm, (14.04.2015).

[131] The National Strategy to Secure Cyberspace, February 2003, p. 4, available at http://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf, (10.03.2014).

[132] Roscini, p. 117.

[133] Green Paper on a European Programme for Critical Infrastructure Protection, **Commission of the European Communities**, 17 November 2005, p. 20, available at https://marcusviniciusreis.files.wordpress.com/2010/06european-program-to-protect-ci.pdf, (10.03.2014)

[134] Sharp, p. 131.

This approach also justify the right of self – defense to respond against this kind of attacks which is aimed at critical national infrastructures owned by either government or private sector. In this view, the results of cyber attacks aimed at critical national infrastructure meet the requirements of justifying a conventional military response.[135] Although states can protect their critical national infrastructure by means of this approach, it creates risk which causes destructive conventional armed conflicts in virtue of an extensive interpretation of critical national infrastructure that constitutes low threshold of the self-defense by using armed forces. Because of this reason, victim states must follow the principles of proportionality and necessity while responding.[136]

2.3. EFFECT – BASED APPROACH[137]

This final approach categorizes a cyber attack as an armed attack with regards to density of its effects. The idea of that a cyber attack that generates kinetic effect or physical damage to the persons or property constitutes an armed attack is widely acknowledged among the effect – based scholars.[138] On the other words, a cyber attack of which effects are repairable physical damages with no long – term results and that causes no injury to people does not constitute an armed attack.[139]

The cyber operations are divided into two parts. First one is a cyber attack causing important injury and damage. Its consequences are as destructive as bombs or bullets can generate. This makes a cyber attack equal to an armed attack. The Department of Defense Office of General Counsel of the USA also affirmed that;

> *If a coordinated computer network attack shuts down a nation's air traffic control system along with its banking and financial systems and public utilities, and opens the floodgates of several dams resulting in general flooding that causes widespread civilian deaths and property damage, it may well be that no one would challenge the victim nation if it*

[135] Hathaway et al, p. 849.
[136] Yayla, p. 214.
[137] While the term "Act – based" and "Consequence – based" can be used, it is preferred using the term "Effect – based" as written in the Waxman, (Future), p. 434.
[138] Li, p. 188.
[139] James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War", **Survival: Global Politics and Strategy**, Vol. 53, No. 1, 2011, p. 30.

concluded that it was a victim of an armed attack, or of an act equivalent to an armed attack.[140]

The Institute for National Strategic Studies of the National Defense University uses the same approach. In their point of view, if a cyber attack includes sufficient destruction, it constitutes a use of force.[141] The National Research Council also declared that a cyber attack must be assessed under rules of the UN Charter and the principles of *jus ad bellum* with respect to its effects.[142] If the results of a cyber attack cause death and injury to people or destruction of the property, there is no reason not to accept it as an armed attack.[143]

Professor Yoram Dinstein clarifies the effect – based approach by giving examples. He gives an example that an attacker captures the codes of a nuclear power plant and let the radioactive materials out of the reactor without control. Maybe the consequences of this attack would be worse than any armed attack in which conventional military weapons are used. Thousands of people may die, even if they do not, their next generations would carry the negative effects of radioactive materials. Another example of Dinstein is shutting down the computer network systems regulating the water level of dam. In case of sudden releasing water without control, generating flood is inevitable. A village can be easily wrapped of the map by this flood. So, describing these attacks which are producing human being injury and property damage as unlawful use of force is generally accepted view for international lawyers.[144]

Second one is a cyber attack that is not causing directly deaths, injury, or significant property damages. Intelligence gathering, cyber espionage, and distributed denial of service (DDoS) attacks are examples of non - armed attacks in which non - destructive cyber operations are involved.[145] While these kinds of cyber attacks may constitute use of force when the victim state's territorial integrity or political independence is threatened, they do not meet the requirements of an armed

[140] Department of Defense Office of General Counsel, "An Assessment of International Legal Issues in Information Operations", quoted by DeLuca, p. 311.
[141] Robertson, p. 129.
[142] Waxman, (Future), p. 432.
[143] Buchan, p. 218.
[144] Dinstein, p. 105.
[145] Schmitt, *Quo Vadis*, p. 282.

attack. This limits the right of self – defense that makes victim states more vulnerable to cyber attacks. However, non – physical consequences of cyber attacks can affect the society too much.[146]

Professor Michael Schmitt is one of the scholars who adopt the perspective of effect – based approach. He suggests that there must be some criteria which can differentiate armed attacks from political, economic, and diplomatic pressures and any other soft measures. His study is formed under the rules and principles of the UN Charter. For him, a cyber attack must be intended to cause physical damage to both concrete objects and human beings in order to be accepted as armed attack. As a result of physical damage to the human beings and properties, states exposed to the cyber attacks can respond by way of using armed forces insofar as the inherent right of self – defense written in the Article 51 of the UN Charter permits.[147]

He created seven criteria to explain the statue of use of force which rise to the level of an armed attack. His seven criteria that produce a new structure for the international coercion gain recognition in international polls. These criteria can also be applicable for the cyber attacks whether they meet the necessities of being use of force or not.

2.3.1. Severity

The first criterion "severity" is about deaths, wounds, and property damages which are the natural results of the armed attacks that soft measures never produce. A cyber attack which is accepted as an armed attack must produce physical injury to the people and destruction of properties like an armed attack in which military weapons are used.[148] These undoubtedly constitute use of force by all means. It is also expressed in the Rule 11 of the Tallinn Manual that;

[146] Li, p. 189.
[147] Schmitt, Normative, p. 1009.
[148] Dorothy E. Denning, "The Ethics of Cyber Conflict",**The Handbook Information and Computer Ethics**, (ed. Kenneth Einar Himma and Herman T.Tavani), Wiley, New Jersey, 2008, p. 441.

> *…consequences involving physical harm to individuals or property will in and of themselves qualify the act as a use of force…A cyber operation, like any operation, resulting in damage, destruction, injury, or death is highly likely to be considered a use of force.*[149]

This argument is also supported by some state officials and scholars. The key point for the USA government about the cyber operation became the physical effects. According to Harold Koh, "cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force". He asserted that if there is no difference between the consequences of bombing or firing missiles and the consequences of cyber attack, then it is obvious that cyber attack may be considered as use of force. The International Group of Experts agreed with Koh. It is also written in the Rule 11 of the Tallinn Manual that "a cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force". For these experts, to injure persons or damage property means absolutely use of force.[150]

Other than physical damage or injury, a cyber attack may cause any different harmful results, such as severe non – destructive or non – injurious consequences. This situation divides scholars into two groups. The first group's approach is narrow interpretation of international law. In accordance with their perspective, the current international law can only be applied to the physical effects. But the other group of scholars submits that the severity of the attack is as important as the physical consequences of it. This argument also takes part in the same rule: "…In this regard, the scope, duration and intensity of the consequences will have great bearing on the appraisal of their severity".[151]

The current international law of self – defense does not permit to act against non – destructive or non – injuries cyber operations. Nonetheless, with respect to the statements of the states, these kinds of consequences of cyber attacks will be regarded as reasons of resort to use of force if it is seen as sufficient severe. That "a disruptive activity in cyberspace could constitute an armed attack" is claimed by the USA. In 2011, the White House explained official cyber security strategy. According to this strategy, all states have an inherent self – defense right. Thus, it was declared

[149] Schmitt, Cyber Warfare, p. 49.
[150] Schmitt, Tallinn Manual, p. 19.
[151] Schmitt, *Quo Vadis*, p. 283.

that the right to use all necessary means, such as diplomatic, economic, or military, was reserved.[152] Additionally, the Dutch Advisory Council on International Affairs and the Advisory Committee on Issues of Public International Law published an edition which gave a support to the US claim. The Netherlands' broad interpretation of the international law was reported in the edition that;

> *...An organized cyber attack on essential functions must be regarded as an 'armed attack' within the meaning of article 51 of the UN Charter if it causes (or has the potential to cause) serious disruption to the functioning of the state or serious or prolonged consequences for the stability of the state, even if there is no physical damage or injury. In such cases, there must be a disruption of the state and/or society, or a sustained attempt thereto, and not merely an impediment to or delay in the normal performance of tasks''.* [153]

Severity is slightly different from the other criteria. It is so important that only the presence of severity is enough to constitute use of force. That said, even if a cyber attack does not meet the other criteria, it can amount to an armed attack taking just the severity of the attack into consideration. It is also mentioned in the Manual that "…severity is self – evidently the most significant factor in analysis".[154]

2.3.2. Immediacy

The second criterion is "immediacy". The cyber attacks may appear with great immediacy. Its huge potential is released just by entering a key of the computer. Process of the cyber attack, from decision to execution, depends on just a computer transaction. Additionally, the consequences of cyber attacks can easily be measured in seconds, while economic or political coercion are less so. For this reason, states are more concerned about immediate consequences than others.[155] So, with this criterion, cyber attacks are distinguished from the other measures like political or economic ones of which effects may reveal months or years later.

---

[152] Matthew C. Waxman, "Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions", **International Law Studies**, Vol. 89, 2013, p. 113, 114.
[153]Advisory Council on International Affairs, **Cyber Warfare**, No.77, December 2011, available at http://aiv-advies.nl/6ct/publications/advisory-reports/cyber-warfare #advice-summary, (10.03.2015).
[154] Schmitt, *Quo Vadis*, p. 281.
[155] Denning, p. 6.

That the consequences of the cyber attack happen immediately differs the cyber attacks from the cyber actions which do not generate immediate consequences as written in the Manual that "…states…are more likely to characterize a cyber operation that produces immediate results as a use of force than cyber actions that take weeks or months to achieve their intended effects". However, some consequences of the cyber attacks may not be understood immediately by the victims. In this situation, it is enough to determine whether a cyber action of which consequences will be seen in the future constitutes a use of force or not.[156]

On the other hand, the long – term harmful consequences may reduce the chance of victim states in order to seek negotiation of a debate.[157] According to the Manual, "The sooner consequences manifest, the less opportunity States have to seek peaceful accommodation of a dispute or to otherwise forestall their harmful effects. Therefore, States harbor a greater concern about immediate consequences than those that are delayed or build slowly over time…" This also inhibits the opportunity to defend itself in the light of self – defense.[158]

2.3.3. Directness

The third criterion is "directness". This means that there must be a connection between an attack and its harmful consequences. For most of the scholars, lawyers, and policymakers, the most effective way of assessing the cyber attacks is focusing on the direct consequences. If the cyber attack causes direct physical damage, injury, suffering, or death, it becomes use of force.[159] Contrary to immediacy interested in the instant outcomes, directness focuses on the chain of causation as noted in the Manual that, "Whereas the immediacy factor focuses on the temporal aspect of the consequences in question, directness examines the chain of causation".[160]

An example whether there is a causal chain between the cause and the ultimate result is very explanatory. For instance, there are two border neighbor states, state A and state B. State A is broadcasting a television channel which encourage the

[156] Silver, p. 90.
[157] Ziolkowski, p. 300.
[158] Schmitt, Cyber Warfare, p. 50.
[159] Gervais, p. 539.
[160] Ziolkowski, p. 300.

illegal terrorist activities in state B's territory and the radio station is very close to the border. State A does not take care of states B's demands to stop broadcast. Ultimately, state B decides to stop this broadcast by using its own cyber capability. State B jams all radio frequencies around the radio station which also cuts the cell phone communication. As a result of this cyber activity, an ambulance helicopter's radio which is going to take a patient who must go to the hospital immediately can be cut. For this reason, the pilot cannot take the patient and this patient can die. Even though it causes loss of life, to determine the causal link between the intended result and the real result is ambiguous because an intention to cause a death may not happen.[161]

Instead of this cyber action, state B leaks to the computer system of only electricity plant around the radio station and cuts the electricity generation suddenly. This kind of cyber activity can cause important results even if it is seen inconsiderable. One of the outcomes of this attack can be that the life support units for the intensive care patients are damaged, and some people can die if there is no any extra electricity supply. In this situation, to foresee the fatal results of this cyber activity is simpler than the first one. So, this cyber activity creates an intention to use of force. However, it is also the most controversial area of this approach.[162]

Different examples strengthen this criterion. For example, there has to be an important difference between the cyber attack that can easily damage the communication network system of airport and make planes crashed, and cyber attack that only blocks bank accounts. The results of these two examples are completely different from each other. Decidedly, the first situation's result, which causes loss of life and property damage, is dependent on the cyber attack. At first sight, blocking bank accounts cannot constitute a use of force due to the fact that it does not cause consequences consisting of damage to persons and property. Although this cyber attack does not result in physical damages, it has huge potential to affect all parts of people's life. The economic, social, mental, and physical life of society are very open to the effects of this cyber attack. In this example, the consequences of the cyber

[161] Sharp, p. 92.
[162] Hathaway et al, p. 850.

attack are not physical, but economic. These kinds of results, such as economic and political, do not rise to the level of use of force under the Article 2(4).[163]

If the results of the latter example go to the physical injury or property damage, such as a significant chaos among society that causes deaths and vandalistic movements in the streets, it becomes a complex case. But even in this situation, a causal link between the initial act and its consequences is not unambiguously direct.[164] This is also expressed in the Manual that;

> *...market forces, access to markets, and the like determine the eventual consequences of economic coercion. The causal connection between the initial acts and their effects tends to be indirect – economic sanctions may take weeks or even months to have a significant effect. In armed actions, by contrast, cause and effect are closely related. An explosion, for example, directly harms people or objects. Cyber operations in which the cause and effect are clearly linked are more likely to be characterized as uses of force.*[165]

Another example of indirect effect is shutting down the internet access of university library. Destroying the network system of the library does not produce a kinetic or physical effect. Hence, the deaths, wounds, or any property damage cannot exist as a result of this action. The consequences of this cyber attack are very different from the effects of battlefield operations. So, this type of example does not meet the criteria of use of force as well.[166]

2.3.4. Invasiveness

The fourth criterion is "invasiveness". The aggressors using military weapons carry out their military operations in the target state's territory. These actions need to cross borders physically whereas the soft measures do not.[167] The effects of the cyber attack are the main point of this approach. Walter Gary Sharp argues that "any state activity in Cyberspace that intentionally causes any destructive effect within the sovereign territory of another state are an unlawful use of force".[168] It is also

[163] Silver, p. 85.
[164] Silver, p. 90.
[165] Schmitt, Cyber Warfare, p. 50.
[166] Silver, p. 91.
[167] Denning, p. 6.
[168] Sharp, p. 102.

mentioned in the Tallinn Manual that "invasiveness refers to the degree to which cyber operations intrude into the target state or its cyber systems contrary to the interests of that state".[169]

In cyber attacks, soldiers or physical objects are not used in the targeted state's territory or airspace. Generally, the means of electronic warfare, such as radio signals, electromagnetic radiation, and electromagnetic pulse, are used.[170] Even if there is nothing visible or concrete penetrating the physical borders of states, the hostile electromagnetic signals, electrons, or photons causing harm violates the principal of territorial integrity by leaking into the target state's network systems.[171] But this situation happens constantly. In this era, airspace of the world is full of radio signals and most of the foreign radio signals use other states' airspace without any complaint.[172]

States, apparently or surreptitiously, make an effort to get information about other states which are rival or threat for themselves. There is no international law to prohibit these attempts which are called espionage. It is already known by every state that the "cyberspace infrastructures" are generally used for getting information to implement them in the operation field.[173] Some scholars who consider the cyber attacks as a new method of modern espionage assert that cyber espionage conducted by just using signals to get information does not meet the requisites of use of force unless armed warships or war planes cross the borders physically in order to collect intelligence.[174] The Tallinn Manual also expressed that "…computer network exploitation is a pervasive tool of modern espionage. Though highly invasive, cyber espionage does not rise to the level a use of force due to the absence of a direct prohibition in international law on espionage".[175]

Especially in the most dangerous era of the Cold War, lots of air craft were shot by the Union of Soviet Socialists Republics (USSR). The most widely – known one is the U – 2 incident. In 1960, the American reconnaissance plane U – 2 was shot by the Soviet weapons during taking pictures 1200 miles inside the Soviet territory.

[169] Schmitt, Cyber Warfare, p. 50.
[170] Dipert, p.397
[171] Silver, p. 90.
[172] Dipert, p.397.
[173] Sharp, p. 125.
[174] Ziolkowski, p. 300.
[175] Schmitt, Cyber Warfare, p. 50.

The USSR brought the incident to the UNSC. The USSR claimed that this incident was an act of aggression.[176] The Security Council admitted that the U –2 flight violated the Soviet airspace integrity, but denied that this incident could constitute a use of force mentioned in the Article 2(4) of the UN Charter. From the point of this example, it is certain that collecting information by leaking the networks of any states do not rise to the level of a use force within the meaning of the Article 2 (4) of the UN Charter seeing that the U – 2 incident did not constituted use of force.[177] Nevertheless, the territorial state's right of jurisdiction in accordance with domestic law maintains.[178]

2.3.5. Measurability

The fifth criterion is "measurability". In armed conflicts, the consequences of armed attacks can easily be measured. At the end of the armed conflicts, the number of deaths, wounds, or loses can be quantified. Even the monetary value of the property damages can be calculated.[179] In the Tallinn Manual, this criterion is defined as;

> *…the armed forces carried out operations that qualified as uses of force and the effects of the operations were generally measurable. In the cyber realm, consequences may be less apparent. Therefore, the more quantifiable and identifiable a set of consequences, the easier it will be for a State to assess the situation when determining whether the cyber operation in question has reached the level of a use of force…*[180]

On the other hand, measuring the outcomes of the economic, political, or diplomatic pressures or other soft measures are not so easy because these do not generate physical consequences. So, the consequences which are not physical do not draw a real conclusion.

[176] Robertson, p. 134.
[177] Schaap, p. 143.
[178] Sharp, p. 128.
[179] Denning, p. 6.
[180] Schmitt, Cyber Warfare, p. 51.

2.3.6. Presumptive legitimacy

The sixth criterion is "presumptive legitimacy". As a nature of law, if an action is not banned in the law, people are free to do it and they cannot be punished because of their actions. In other words, an action which is not prohibited in the law is permitted. This means that an action which is not prohibited is presumptively legal.

For example, mostly all states have penal law about spy actions. Should a person is caught while getting information illegally; he or she can be tried according to the domestic law. However, the spy may be a subject of exchange with the spy of apprehending state or declared as a persona non grata having regard to diplomatic identification. According to the domestic law, spying is banned and not permitted. This makes it illegal action.[181] But almost all states do not take the cyber espionage into consideration while legislating. So, cyber espionage operations are presumptively legitimate in most states.[182]

Additionally, while international law forbids using of force and armed force, propaganda, psychological operations, espionage, or mere economic pressure are not clearly prohibited. So, these kinds of actions are presumptively legal, even in cyberspace.

2.3.7. Responsibility

The last criterion is "responsibility". This criterion is slightly different from the others. States are much more interested in use of force if the operation is conducted by a state due to the fact that international stability becomes more vulnerable when a state has a leading role in conflicts. Therefore, there is an apt to attribute the consequences of actions to the states.[183] Moreover, the proof of state responsibility constitutes a statutory basis that enables victim states to defend their rights in the light of the Article 51 of the UN Charter. Thus, if the attacker state is

[181] Sharp, p. 126.
[182] Ziolkowski, p. 300.
[183] Ziolkowski, p. 300.

known, the victim states can make a response to the attacker state without giving any extra damage to the innocent states.[184]

The Article 4 of the Responsibility of the States for Internationally Wrongful Acts established by the International Law Commission emphasizes that the conduct of state's legal organs can be clearly attributed to the states. It is understood that all individual and collective entities that take part in state organizations make out state's legal organs as noted that;

> *The conduct of any State organ shall be considered an act of that State under international law, whether the organ exercises legislative, executive, judicial or any other functions, whatever position it holds in the organization of the State, and whatever its character as an organ of the central Government or of a territorial unit of the State.*[185]

Even the non – state actors' actions are attributed to the states. The Article 8 of the same treaty mentions that;

> *The conduct of a person or group of persons shall be considered an act of a state under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that state in carrying out the conduct.*[186]

Thus, states may be automatically responsible for the actions of person or group of persons working for the state, called as "state agents".[187]

Some decisions of the ICJ also strengthen this thought. In the Armed Activities on the Territory of the Congo, it was held that "…a party to an armed conflict shall be responsible for all acts by persons forming part of its armed forces". If people or entities who are not a legal organ of states act under an authority of state must be thought in this statement.[188] In another case, Caire Claim, the Mexican

[184] Raboin, p. 641.
[185] Resolution adopted by General Assembly, "56/83. Responsibility of States for International Wrongful Acts, Article 4", 12 December 2001, available at http://legal.un.org/ilc/texts/instruments/english/draft%20articles/9_6_2001.pdf, (22.03.2015).
[186] Resolution adopted by General Assembly, "56/83. Responsibility of States for International Wrongful Acts, Article 8", 12 December 2001, available at http://legal.un.org/ilc/texts/instruments/english/draft%20articles/9_6_2001.pdf, (22.03.2015).
[187] Raboin, p. 643.
[188] Gervais, p. 545.

government was found responsible for the actions of its soldier, despite the fact that he disobeyed the orders and acted independent from the command – chain.[189]

For the actions of non – state actors, the ICJ and International Criminal Tribunal for Yugoslavia (ICTY) have two competing criteria. The "effective control" standard articulated in *Nicaragua Case* attribute the non – state actor's act to state if the act is dependent on state before the action occurs.[190] These non – state actors are called as *de facto* state organs.

The non – states actors' cyber attacks attributable to the states enable victim states to respond forcefully. The non – state actors conducting the cyber attacks and states to which cyber attacks are attributable share the responsibility and can be exposed to the victim state's use of force. It is clearly noted in *Nicaragua Case* by the ICJ that;

> *…an armed attack must be understood as including not merely action by regular forces across an international border, but also 'the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to' an actual armed attack conducted by regular forces, or its substantial involvement therein…*[191]

On the other hand, in the Tadic case, the ICTY set forth the "overall control" standard, which is less restrictive.

> *…Plainly, an organized group differs from individual in that the former normally has a structure, a chain of command and a set of rules as well as the outward symbols of authority. Normally a member of the group does not act on his own but conforms to the standards prevailing in the group and is subject to the authority of the head of the group. Consequently, for the attribution to a state of acts of these groups it is sufficient to require that the group as a whole be under the overall control of the state.*[192]

---

[189] French – Mexican Claims Commission, Estate of Jean – Baptiste Caire (France) v. United Mexican States, 5 R.I.A.A. 516, 7 June 1929, available at http://legal.un.org/riaa/cases/vol_V/516-534_Caire.pdf, (11.04.2015).

[190] Li, p. 203.

[191] ICJ, "Case Concerning Military and Paramilitary Activities in and Against Nicaragua", 27.06.1986, available atwww.icj-cij.org/docket/files/70/6503.pdf, (10.03.2015).

[192] ICTY, "International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia since 1991, Article 120", 15 July 1999, available at http://www.icty.org/x/cases/tadic/acjug/en/tad-aj990715e.pdf, (11.03.2015).

According to this standard, equipping, financing, and training constitutes state responsibility for acts of non – state actors. Thus, the scope of state responsibility is broadened. This approach makes the non – state actors *de jure* state organ.[193]

Due to the fact that "effective control" requires unambiguous and clear evident, which is very difficult to determine the responsibility in cyberspace, and the technical difficulty of identifying the attacker, the "overall control" is preferred to the Nicaragua test for some scholars.[194] However, some of them do not share the same perspective. Because being accused of a cyber attack becomes very easy with the overall test. So, the threshold of the right of self – defense for the victim states decreases which can cause more destructive conflicts.[195]

The third state whose territory is used by one state to attack another one is under charge of use of force. The UN General Assembly has a Resolution about third state acts which constitutes customary international law. It is provided in "1970 Declaration on Principles of International Law Concerning Friendly Relations among States in Accordance with the Charter of the United Nations" that;

> *Every state has the duty to refrain from organizing or encouraging the organization of irregular forces or armed bands, including mercenaries, for incursion into the territory of another state. Every state has the duty to refrain from organizing, instigating, assisting or participating in acts of civil strife or terrorist acts in another state or acquiescing in organized activities within its territory directed towards the commission of such acts, when the acts referred to in the present paragraph involve a threat or use of force.*[196]

For third state, allowing its own parts of territory or infrastructure system to be utilized by other states or groups to act in violence constitutes "use of indirect force". This is also assessed within the framework of the Article 2(4). Moreover, considering the effects of the cyber attack on the victim state, the level of this consent can cause an armed attack.[197]

---

[193] Michael N. Schmitt, "Classification of Cyber Conflict", **Journal of Conflict & Security Law**, Vol. 17, No. 2, 2012, p. 252.
[194] Li, p. 204.
[195] Roscini, p. 100.
[196] Resolution adopted by the General Assembly, ''2625 (XXV). Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations'', 24 October 1970, available at http://www.un-documents.net/a25r2625.htm, (10.03.2015).
[197] Sharp, p. 112.

Indeed, the more disputable matter is the cyber actions conducted by non – state actors who are independent from states. The cyber attacks may be conducted by individuals in different states from different continents by using computer network. Although the armed attacks producing kinetic energy and causing injury or property damage are hardly conducting by individuals, it is easy to conduct cyber attack of which consequences may be more destructive.[198] For example, some cyber attackers defines themselves as "patriotic hackers" or "hacktivists" which means private citizens who attack on their own initiative with motives of nationalism and ideological feelings.[199]

In these situations, as far as the host state is informed, precautions must be taken in order not to host cyber attacks within its own territory. The Corfu Channel decision about the state responsibility given by the International Court of Justice brings a necessity of "not to allow knowingly its territory to be used for acts contrary to the rights of other states".[200] Taking this decision into consideration, the Rule 5 of the Tallinn Manual also states that "a state shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other states".[201] This rule is based on the principle of territorial sovereignty. The independent states must respect the territorial sovereignty of others as written in the Nicaragua judgment "…between independent States, respect for territorial sovereignty is an essential foundation of international relations".[202]

A State in which cyber attack is carried on has to prohibit such actions in its own territory. If host state does not answer the requirements, deliberately or not, a victim state has a right to take counter measures to defend its own benefits.[203] The unwillingness or inability of host state to stop unlawful actions in its own territory gives a right to the victim state to solve the problem by own force, including cross –

[198] Schmitt, *Quo Vadis*, p. 287.
[199] "Masters of the Cyber-Universe; Cyber-Hacking", **The Economist**, 06 April 2013, http://search.proquest.com/docview/1324420283?accountid=10527, (03.09.2013).
[200] ICJ, "Corfu Channel Case (Preliminary Objection)", 25 March 1948, available at http:/www.icj-cij.org/docket/files/1/1571.pdf, (10.03.2015).
[201] Schmitt, Cyber Warfare, p. 26.
[202] Schmitt, *Quo Vadis*, p. 276.
[203] Yoram Dinstein, "Computer Network Attacks and Self-Defense", **International Law Studies**, (ed. Michael N. Schmitt, Brian T. O'Donnell), Vol. 76, 2002, p. 104.

border operations.[204] If host state were willing and able to struggle with the threat, it would be unnecessary to adopt measures as a right of self – defense.[205]

The United States Diplomatic and Consular Staff in Tehran case is an obvious example about this situation. The Iran government's approval of the seizure of the USA embassy and its personnel by terrorists caused a state responsibility. The US intervention to Afghanistan in name of self – defense after the 9/11 attacks is another instance for the responsibility of non – state actors. The "inherent right" of the USA to respond forcefully within the framework of the Article 51 was legalized by the Resolution 1368 of the UN General Assembly.[206] In this Resolution, the responsibility of state extended to knowingly harboring perpetrators of attacks regardless of the state's "effective control" over the attackers.[207]

Recently, the US Government also repeated that it is necessary to take action against these kinds of states in the light of self – defense. In 2010, Hillary Clinton, the Secretary of Foreign Affairs, declared that;

> "*States, terrorists, and those who would act as their proxies must know that the US will protect our networks…Those who engage in cyber attacks should face consequences and international condemnation. In an interconnected world, an attack on one nation's networks can be an attack on all".*[208]

In this perspective, in the USA, the rules of engagement for cyber warfare has been tried to be more permissive which leads the allies to follow.[209]

In order to hold a state responsible for a cyber attack, the material evidences for attribution have to be explicit and unambiguous. Although the technological means of tracking cyber attackers are very developed, it is also too difficult to impeach a state with responsibility of cyber attack. The victim state may trace back to the source of cyber attack, but this is not sufficient to claim that any state is guilty.[210] Even if the victim state is very sure which computer is indeed behind the

---

[204] Schmitt, *Quo Vadis*, p. 288.
[205] Li, p. 205.
[206] Resolution adopted by the Security Council, "Resolution 1368", 12 September 2001, available at http:/daccess-dds-ny.un.org/doc/UNDOC/GEN/N013382.pdf?OpenElement, (2.2.2015).
[207] Gervais, p. 548.
[208] Waxman, Future, p. 433.
[209] "Hype and Fear", **The Economist**, 08 December 2012, http://search.proquest.com/docview/1223834330?accountid=10527, (03.09.2013).
[210] O'Connell, p. 7.

cyber attack, only this fact cannot make anyone or any state responsible for the cyber attack.[211]

The tricks of detecting the source of cyber attacks make victim states reluctant to blame any state.[212] This anonymity constitutes one of the most significant advantages for cyber attackers. This advantage makes it easier to deny the responsibility of conducting cyber attack. A cyber analyst expressed the easiness of attackers by writing this speech in his column: "They do not care if they caught".[213] So, this causes a time consuming process owing to the fact that any other government organizations or even individuals may create "zombies" by using innocent systems. So, this process may not be enough for accusation.[214]

2.3.8. General Assessment of the Criteria

Although these criteria are very informative, they are not inherently enough to explain all events. In other words, some new criteria may be added to effect – based approach and some of them may be assessed more significant than others.[215] The severity criterion has more important place in these criteria. It is more applicable to physical injury and property damage. So, severity comes first among these criteria to clarify cyber events. Even if the other criteria are not met, only the severity criterion can be enough to constitute an armed attack.[216]

Schmitt, himself, gives an explanatory example about these criteria. It is an intervention to the electronic communication systems of airports and airplanes. Consider a cyber attack that can easily affect the air traffic control systems. An attacker can misdirect the airplanes. Because of this, these planes can enter the same air traffic corridor and crash. As a result of this, many passengers can die. In this situation, there is no kinetic force that destroys the airplane, no rockets, no bullets,

[211] Jack Goldsmith, "How Cyber Changes the Laws of War", **European Journal of International Law**, Vol. 24, No. 1, 2013, p. 134.
[212] "Hype and Fear", **The Economist**, 08 December 2012, http://search.proquest.com/docview/1223834330?accountid=10527, (03.09.2013).
[213] "Masters of the Cyber-Universe; Cyber-Hacking", **The Economist**, 06 April 2013, http://search.proquest.com/docview/1324420283?accountid=10527, (03.09.2013).
[214] Graham, p. 92.
[215] Yayla, p. 215.
[216] Silver, p. 91.

and no missiles. But the main factor of the air crash is the cyber attack that cannot be seen by eyes explicitly.[217]

Assessing this example within the framework of the criteria would be more explicit. The example meets exactly the severity criteria. The crashed airplanes become wreckage and most probably they are never used again. It is also nearly impossible to survive from an air crash. There would be lots of deaths. Moreover, so many people would experience psychological problems. So, there is no doubt that the physical injury and the property damage exist. Immediacy is very high even though the time between the attack and the crash is longer than the time between the missile attack and the crash. As to the directness criteria, it is very clear that the reason of the crash is misleading action of the attacker by leaking to the computer system. The causal chain is established with link between the act of cyber operation, misleading the airplanes and the effect, and crash. With respect to measurability, it is also very high. The deaths, wounds, and property damage are easily countable. However, the non - physical effects, like public confidence to air transportation system or psychological problems of survivors and relatives of victims cannot be quantified. As for the presumptive legitimacy, to cause an airplane crash and deaths cannot be legalized in any law system. It is absolutely illegal to kill civilians even in *jus in bello*. These five criteria meet standards that cross the threshold of constituting an armed attack, and automatically use of force. The remained two criteria are slightly ambiguous. It is sometimes difficult to claim that to send electromagnetic signals is a way of invasion rather than physical weapons. In terms of responsibility, the attacker may be anyone who acts independent from any state. But in reality, it is very difficult to realize such a kind of cyber attack without any help from states.[218]

Consequently, this example expresses that the new attacking techniques through computer network systems does not change the reality. It is obvious that the attacker's intend is to aim the airplane directly and the consequences of the attack is severe. So, taking the result of the air crash into account, the cyber attack is equal to the level of armed attack.[219] Although this cyber attack is determined as an armed attack by Schmitt, some scholars are not in the same point with him. Walter G. Sharp

[217] Schmitt, Normative, p. 911.
[218] Denning, p. 6.
[219] Schmitt, Normative, p. 911.

thinks that this kind of cyber attack constitutes use of force but not armed attack. For him, not all cyber attacks, even if they are so destructive, and meeting the threshold of the armed attack, as mentioned in the Nicaragua Case that "all armed attacks are uses of force, but not all uses of force are armed attacks". He interprets this crash as a single incident caused by Internet. If the attacker keeps attacking in the same way in a long time, or causes one major destruction which effects the all units of the state, then use of force goes up to the level of an armed attack.[220]

[220] Sharp, p. 103.

CHAPTER THREE
WEAPONS OF CYBER ATTACK AND RECENT INSTANCES OF CYBER WARFARE

3.1. WEAPONS OF CYBER ATTACK

During the armed conflicts, while states fight against each other in the battlefield, they also seek to take information about their enemy's position. Besides, they try to camouflage their own position. These are espionage and disinformation attempts that all military commanders need in order to defeat their enemies. In the past, these attempts included cutting the communication cables and jamming the radio signals. However, in recent years, with the high technological changes in the world, new kinds of cyber weapons has come into being. These new weapons are not only used to get information from enemy but also to damage them.[221] The most important ones used in recent significant cyber instances are explained below.

3.1.1. Denial Of Service

There are so many techniques to stop the legitimate access to networks. A denial of service (DoS) is one of them. This cyber weapon is an assault on a computer that decreases the computer systems' performance or even makes them completely interrupted by too much overwhelming requests and data. The most usual way of DoS attack is to flood the computer network system with lots of unnecessary information incapacitating to work properly.[222]

Due to the fact that the computer systems can only operate a certain amounts of requests at the same time, the system fails when an excessive amount of data requests are sent. Thus, the access to the information services, such as e-mail, websites, and personal accounts of the legitimate users are prevented.[223] However,

[221] Dipert, p.386.
[222] Shakarin, p. 14.
[223] DeLuca, p. 283.

the attacker is not able to leak to the software of the targeted computer network system.[224]

One of the most significant advantages of this kind of attack is that an attacker can damage the targeted computer system with his less qualified and slower computer system. It is possible to disable the more complicated and developed computer systems in very cheap way.[225]

3.1.2. Distributed Denial of Service

A distributed denial of service (DDoS) attack is very similar to DoS attack. Its process and tactics are almost the same. In other words, DDoS attack is an attack which is converted from DoS. However, they are slightly different. The first difference between them is the number of computers using in the attack. The DDoS attack must be well planned, coordinated, and synchronized because many pre-infected computers are used to damage just a computer system. Namely, attackers exploit these pre-infected computers, which are called "zombies" or "botnets", by taking control of and forcing them to send large amounts of requests in order to disable the targeted computer system.[226] In other words, the targeted computer is exposed to a bombardment of too much e – mail or requests. This creates slave computers that attack to the computers targeted by the attacker.[227] Moreover, the third computer owners cannot realize that their computers are utilized by an attacker to attack somebody's targeted computer system.

The other difference is the way of protection against the attacks. In simple DoS attacks, to block undesirable messages is sometimes possible because there is only one Internet Protocol (IP) address although it may be spoofed. But in DDoS attacks, to block the messages and to protect the computer systems are nearly impossible due to the fact that it is ambiguous where the flooding data comes from and there are too much varied IP addresses from all around the world.[228]

[224] Dipert, p.387.
[225] Schaap, p. 134.
[226] Raboin, p. 612.
[227] Dipert, p.388.
[228] Dipert, p.388.

3.1.3. Viruses

Viruses are the most known malicious programming by most of the computer users. It is also one of the easiest ways of cyber attacks. It is intentionally written by programmers and sent to the targeted computers. It has two important distinctive abilities. First, it can easily attach itself to a computer programs or files. Second, it is capable of replicating itself. Thus, a virus can circulate on computer networks and leak into another computers to strike them.[229]Moreover, the viruses contain payloads. They can be programmed by attacker to cause side effects, such as damaging data, destroying programs, and incapacitating the software of computers etc.[230]

The purpose of the attackers using viruses is to damage computer systems without knowledge of the owners of computers. After leaking to the targeted computer system, the viruses can become unforeseen. This means that viruses exist on the computer, but it cannot be recognized. During this period, the owner of the computer may not realize that he is in danger of a cyber attack. Once they run the programs or open the files which the virus is attached to, the destructive effects of it come into being.[231]

The computer users have been in trouble with the effects of the viruses since the using internet became widespread. The first known virus was the Creeper Virus. The attacker sent this virus with the message of "I am the Creeper: Catch me if you scan!" But just after the virus had been given a free run, an anti-virus program, "the Reaper", was written and it could eradicate that virus.[232] Moreover, the cyber attacks in which viruses are used cost expensive. For instance, in 2000, the cost of the harm of the "I Love You" virus created by a lone Filipino amounted to more than 6 billion US Dollars.[233]

[229] DeLuca, p. 282.
[230] Schaap, p. 136.
[231] Raboin, p. 613.
[232] Gervais, p. 531.
[233] DeDeluca, p. 282.

3.1.4. Worms

Worms can replicate itself onto other computers as an independent program which does not revise the existing programs.[234] They can easily spread from one computer to another one. While worms are similar with viruses with regard to the traveling among computers, they do not need any help from the individual computer users. The unaided way they use is to utilize the transportation system of file and information.[235]

Worms have an ability to copy itself thousands of times on a system which is more harmful than viruses for computer systems. They consume massive amounts of memory or network bandwidth of system. Thus, server or individual computers lose their capacity to respond.[236] For example, the Morris Worm released by a young man who wanted to demonstrate security vulnerabilities damaged ten percent of computers connected to Internet in 1988.[237]

3.1.5. Trojan Horses

Trojan Horses are the malicious programs that seem useful like the "Trojan Horses" which carried Greek soldiers as though they were supposed to carry presents. Today's Trojan Horses are very similar to the mythological Trojan Horses because the Trojan Horses, as a malicious program, contain harmful codes inside the so-called innocent programs, such as mails, or program files downloaded from internet etc. It is too difficult to differentiate innocent programs from disguised programs that have harmful codes. Thus, the Trojan Horses are distributed by way of leading individuals to use a program as if it came from a legal source. For example, an e-mail may be sent to the targeted computer in order to be readby the victim. When the victim opens the e-mail without the knowledge of harmful programs, then the Trojan Horses become active.[238]

[234] DeLuca, p. 284.
[235] Schaap, p. 143.
[236] Schaap, p. 136.
[237] Gervais, p. 531.
[238] Schaap, p. 136.

A Trojan Horse can involve viruses. However, a Trojan Horse, itself, is not a virus. The most important difference between them is that a Trojan Horse does not reproduce by damaging other files and replicate itself.[239]

A Trojan Horse enables an attacker to leak to and command the targeted computer remotely. This access may not be recognized by the computer owner. For instance, the attacker can access to the user's personal files and send them out to the third-party by using internet. Besides, anyone can connect remotely to the targeted computer which makes Trojan Horse a server. This creates a "back door" on computers. Therefore, the victim's all data become open to the access for anyone who knows to exploit a Trojan Horse leaked to the targeted computer.[240]

3.1.6. Logic Bombs

Logic bomb is a kind of malicious code design. It is deliberately loaded into computer software system but it does not work as soon as loaded. It can stay silent for a long time. Some pre-determined events have to occur in order to activate the logic bomb. So, its malicious effects are recognized later on. But these effects are so destructive that the infected computer can become completely spoiled. The specific data can be deleted, the computer can be unusable, even worse DDoS attacks can be triggered when a logic bomb takes into action.[241]

3.1.7. IP Spoofing

Internet Protocol (IP) spoofing is generally understood as a dispatch of mails from anyone's IP address in internet. Actually, it is a way of creation of IP packets without using an original IP address. When an attacker takes the control of internet browser, any computer using this browser is directed to the tricky webpage. The individual who uses the forged webpage cannot understand whether it is created by the real IP address or not. He can suppose that the webpage is legitimate. But when

[239] Schaap, p. 136.
[240] DeLuca, p. 285.
[241] Schaap, p. 137.

the targeted computer transact with the tricky webpage created by the attacker, the attacker can access to the information existed in the targeted computer.[242]

3.2. RECENT INSTANCES OF CYBER WARFARE

Cyber attacks have come into being since the uptrend of internet usage. This time nearly falls on 1990s. With the rise of the cyber threats, especially the USA, the UK, Russia, China, and Israel have been developing their cyber attack capabilities in order to both defend their critical national infrastructure and integrate them into military operations. The intent of these states is to use cyber weapons before or during the conflicts, even in the military operations. Thus, damaging the adversary's network, hitting the target, and defeating the enemy become easier without giving any casualty.[243]

One of the first highly - organized hostile use of cyberspace is the cyber attack against non-governmental organizations of Ireland that is cutting off the Internet service of 3000 people on January 1999.[244] Nearly at the same time, the USA was placed in difficult circumstances because of multiple attacks which were supposed that China conducted the operations. These attacks, called "Titan Rain", mostly affected the defense contracting companies' security systems. With these attacks, it was intended to evaluate the US countermeasures capability against cyber attacks.[245] Another cyber attack, the "Moonlight Maze", was one of the most extensive computer attacks which effected the US government, such as Pentagon, the NASA, the Department of Energy, and some universities. Thousands of files about military and technological developments which are top – secret for the US government were revealed. Russia was alleged that it sponsored the hackers, but it could not be proved. Russian government also denied any involvement in such a cyber activity.[246]

---

[242] Raboin, p. 615.
[243] "A New Kind of Warfare", **New York Times**, 10 September 2012, http://search.proquest.com/docview/1038573240?accountid=10527, (11.10.2013).
[244] Sharp, p. 22.
[245] Ophardt, p. 11.
[246] Gregory Vistica, "We're in the Middle of Cyberwar", **Newsweek**, 20 September 1999, available at http://www.newsweek.com/were-middle-cyberwar-166196, (10.01.2015).

Not only the state organizations but also the private sector organizations are subjected to the cyber attacks. One of the biggest defense companies of the USA, Lockheed Martin, is worried about the cyber attacks in which the attackers' purposes are to get top – secret military information. Even one of the biggest brands of the Internet, Google, is also in trouble with cyber attacks threatening the important government officials' mail accounts.[247]

In the first decade of the 21st century, the cyber warfare began to become one of the most important issues for the international security specialists. The new – independent post – Soviet states were much more in trouble with cyber attacks. Lithuania was also exposed cyber attacks in 2008 just after outlawing the use of Soviet and communist symbols like the Soviet hammer and sickle. This attack involved the DoS kind of cyber attacks. The Lithuanian officials claimed that the attacks were conducted by Russia. Their claim was based on the fact that relations between Russia and Lithuania had already been deteriorated because of compensation of Lithuanian victims of Soviet labor camps and the Lithuanian blockage on the EU- Russia partnership.

Kyrgyzstan was also attacked in 2009. Some websites and email services were deactivated by DoS attacks. The origin of the cyber attacks went to the Russia. However, it could not be clearly proved whether the Russian government was behind the attacks. However, before the attacks, Kyrgyzstan had been in trouble with Russia because of the airbase used by the USA to supply logistic support to the troops in Afghanistan.[248]

The cyber attack against Estonia in 2007 consolidated the fears of the specialists. Just after this attack, another cyber operation took place in Georgia during the armed conflict with Russia. In addition to these two important cyber attacks, the Iran attack is also explained below.

[247] Con Coughlin, "The Cyber Warriors Are Preparing for Battle", **The Daily Telegraph**, 03 June 2011, http://search.proquest.com/docview/869762229?accountid=10527, (06.10.2013).
[248] William C. Ashmore, "Impact of Alleged Russian Cyber Attacks", **Baltic Security & Defense Review**, Vol. 11, 2009, p. 11.

3.2.1. Estonia

3.2.1.1. General Assessment

In April 2007, the statue of a Russian soldier, which is known as Bronze Soldier, commemorating the Soviet soldiers who fought against the Nazi Germany during the WWII became an international problem between Estonia and Russia. The Estonian Government announced that the statue would be moved to out of the Tõnismägi Park in centrum of the capital, Tallinn, because of the fact that it was perceived as a symbol of foreign occupation. The large Russian population in Estonia reacted against the government's decision. The protests and some violent actions appeared on the streets of Tallinn.[249]

Just after these protests, a comprehensive cyber attacks targeting Estonian government websites came into being on April. Hackers started to attack by way of DDOS. In a few hours, almost all of the government, newspapers, universities, hospitals, fire services, banks network systems were flooded with too many unnecessary requests which came from all around the world.[250]

The attack became more planned and complicated in a very short time. The attackers hijacked too many computers in all around the world. Almost 85.000 computers were used by the hackers to send messages. The cyber attackers used the botnets of "zombie" computers without the knowledge of these computers' owners.[251] While the normal capacity of government and bank websites are almost 1000 visits a day, it raised to 2000 visits a second during the cyber attacks.[252] Within a very short time, the packet traffic exceeded four million. Computer network systems of Estonia could not resist to so much request. Therefore, access to the network systems in Estonia by the legitimate users became impossible.[253]

These cyber attacks did not end in a short time, it lasted for days. They caused chaos within the society. The economic system became upside-down. People

[249] Buchan, p. 219.
[250] DeLuca, p. 286.
[251] Buchan, p. 219.
[252] Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses", **Journal of Strategic Security**, Vol. 4, No. 2, 2011, p. 52.
[253] Shackelford, p. 203.

and commercial organizations could not use the bank accounts. Some of the bank accounts, especially in two major banks, were deleted. The budgets of the government and private sector got mixed up. The government organizations could not meet the public requirements; even hospitals' paramedic services were out of order for some time. The telecommunication system crashed both domestically and internationally. Worse than this, 150 people were injured and one Russian citizen died. Almost all of the people in Estonia were affected negatively.[254]

Estonia is one of the highly wired and most Internet – dependent states in the world. 99 % of the citizens were using Internet for banking and 86 % of them were completing their taxes online. Moreover, Internet was used as a way of election which made Estonia the world's first web – based election state. 5.5 % of the votes sent by Internet. This rate increased to the 25 % of the votes in 2011. Nearly, there is no state in the world like Estonia with regards to dependence on Internet for commerce, communication, and other services. Further, this reliance leads the Estonian government to be called as "paperless government".[255] This cyber dependence and the small size of the country are establishing the main reasons of high cyber vulnerabilities of Estonia.[256]

3.2.1.2. Legal Assessment

The Estonian officials stated that this cyber attack was as destructive as an armed attack. Estonian Defense Minister, Jaak Aaviksoo, compared it with closing down the ports by using military force.[257] Besides, Ene Ergma, a member of the parliament of Estonia, used an exaggerated speech that "When I look at a nuclear explosion, and the explosion that happened in our country in May, I see the same thing…Like nuclear radiation, cyber war does not make you bleed, but it can destroy everything."[258]

After the attack, no state or non – state organization took the responsibility. But it was clear that the complexity of attack required a cooperation of a state. So,

[254] DeLuca, p. 286.
[255] Herzog, p. 51.
[256] Li, p. 200.
[257] O'Connell, p. 4.
[258] Shackelford, p. 194.

the Estonian officials charged Russia with conducting these cyber attacks. The cyber attacks on post – Soviet states already have some similarities. All of them happened after an opposition to Russia had begun. Additionally, Russia did not take the responsibility of the attacks, and the victim states could not prove the situation with facts because it is nearly impossible to trace back to the origin of the DDos attacks. Albeit the Russian officials denied any responsibility of the attacks, it is obvious that such an attack cannot be organized by just individuals who have no connect with any state.[259]

While minds about the responsible of this cyber attack were blurred, Estonia also called upon the NATO to activate the Article 5 of the treaty about the collective self – defense. But the NATO officials did not assess that the cyber attacks constituted an armed attack and triggered the most important article of the organization taking the Article 41 of the UN Charter into consideration.[260]

The Estonian critical national infrastructure, such as fire services, hospitals, and banking system, were exposed to massive DDoS attacks. With regards to the "target – based" approach, some scholars argue that it is possible to assess these attacks as use of force.[261]

The other group of scholars hold that it falls short of the use of force regarding the "effect – based" approach. For them, these cyber attacks did not increase to the threshold of an armed attack. The results were not assessed as severe as an armed attack generates. Although attacks were presumptively illegitimate, the results of the attacks generated no physical damage or measurable suffering. Also, the physical damage was not enough to establish an armed attack. The rate of people injury and property damage left under the level of which traditional military weapons could produces. Even if it had an immediate result and created measurable suffering like not being able to access to emergency services, such as police or ambulance, the relation between reason and cause seem indirect. Another reason was that the attackers could not be found. Although the Estonian government claimed that they had evidences, the responsibility of the cyber attacks is still uncertain.[262]

[259] Raboin, p. 618.
[260] Schaap, p. 145.
[261] DeLuca, p. 298.
[262] Gervais, p. 540.

Consequently, these cyber attacks were assessed as cyber operations which did not constitute use of force. This also shows that it is very difficult to respond in the light of self – defense to the attackers in a short time due to the lack of strong legal evidences which are generally accepted internationally. Neither Estonia nor the NATO responded to any state in consideration of self – defense.

This instance is very important because it was the first cyber attack that was conducted as a coercive instrument in an international political conflict between two states. With this cyber attack, Russia, which was rejected the charges, tested both its cyber capacity and the counter reaction of the NATO in case of a cyber attack to one of its members.[263] Thus, the international society realized the importance of this new type of war. At the end of the cyber attacks, the NATO established the CCDCOE in order to make the member states be conscious about the protection means against the cyber attacks. Additionally, Estonia itself make an organization consisted entirely of volunteer cyber experts. Thus, Estonia became one of the most active states against the cyber attacks.[264]

3.2.2. Georgia

3.2.2.1. General Assessment

In 2008, Georgia was in trouble with minority problem located in the north part of the country. After the South Ossetian officials had declared their independence from Georgia, the Georgian troops attacked to the capital city of the South Ossetia, Tskhinvali. An armed conflict began but did not remain between just Georgia and its semi – dependent state, the South Ossetia. This armed conflict ranged over a wide field including the Russian Army. Just after the armed conflict had begun, the Russian military troops counter attacked to the Georgian troops. The course of the war changed drastically in very short time. The Georgian government decided to cease – fire and negotiation period began.[265]

[263] Schaap, p. 145.
[264] O'Connell, p. 4.
[265] O'Connell, p. 4.

Georgia was not only invaded on the ground, through the air, and by sea, but also via cyberspace. A conventional military invasion coordinated with a cyber attack. The conventional means of war were conducted with forth front. Thus, it was added a new phase to the warfare history and cyber warfare became a necessary element in the modern conduct of war. This was the first known combination of the cyber and traditional armed attack which was more destructive than only one.[266]

Before the war began, the first signals of cyber attack had been already realized by the Georgian officials. According to the statement "…three weeks before the shooting war between Georgia and Russia began; online attackers started assaulting Georgia's websites. Since then, researchers have tried to find out who masterminded the network strikes – military electronic warriors, patriotic hackers, cyber – crooks – without finding anything definitive."[267]

The difference between the armed conflict coordinated with cyber warfare and classical military armed conflict is that the Georgian government's computer network systems and private sector internet infrastructure, such as media, communications, and transportation companies, were attacked both before and during the armed conflict. However, Georgia was not as affected as Estonia because of the fact that Georgian cyber infrastructure was not so complicated as Estonia. Some government and private organizations' websites which were cyber – attacked were loaded with the pictures of Georgian President and Adolf Hitler. In this way, the government's authority on the state institutions decreased. This did not only affect the domestic structure, but also the international relations with foreign states.[268]

3.2.2.2. Legal assessment

Although it is debatable to determine whether a mere cyber attack constitutes a use of force or an armed attack, the combination of cyber and traditional armed attack dispel doubts because this combination meets all the criteria that constitute a use of force and an armed attack. Even if the people injury, wounds and deaths, and

[266] Raboin, p. 620.
[267] David Hollis, "Cyberwar Case Study:Georgia 2008", **Small Wars Journal**, Vol.7, No.1,2011, p. 2.
[268] DeLuca, p. 286.

the property damage are the direct results of the armed attack, the cyber attack coordinated with the armed attack can be assessed as a way of military tactics.

While coordinated attacks produce physical destruction, the situation of the cyber attack before the armed attack began is also disputable. If a causal chain between cyber and armed attacks cannot be established, it is too difficult to claim that there was a use of force. Because the first cyber attacks were independent from armed attacks and did not cause physical destruction such as injury to people and property damage. The consequences produced by cyber attacks were not as severe as physical destructive effects generated by armed forces.

3.2.3. Iran

3.2.3.1. General Assessment

Iran has been having an entanglement with nuclear enrichment program for several years. The western states, especially the USA, have come out against this project which may enable Iran to produce nuclear weapons in the future. Besides, Israel which perceives this program as a dreadful threat for itself is the major supporter of the USA. On the other hand, Iranian government has been denying these claims. According to the Iranian officials, the nuclear enrichment program was initiated just for peaceful purposes, such as generating nuclear energy.[269]

Although some sanctions were applied against Iran, an armed attack did not happen. However, western states always tried to hinder Iran producing nuclear weapons. In 2010, the computer systems of Iran's two important nuclear enrichment power plants located in Bushehr and Natanz were attacked.[270] At first, Iran did not admit the cyber attack but later a malware virus, which was called "Stuxnet", was discovered by the computer experts.[271]

Actually, Stuxnet invaded computer systems not only in Iran, but also all around the world. More than 60.000 computers were infected; nearly half of them were in Iran. It was first detected in the software of the German company, Siemens.

[269] Buchan, p. 220.
[270] Raboin, p. 624.
[271] Buchan, p. 220.

The removable memory stick was the first source. This worm leaked to the system by way of USB ports and used Microsoft Windows operating system to spread. It was copying itself and able to be hidden. The worst handicap of this worm is not to be realized for a period of time. While "Stuxnet" easily distributes itself to thousands of computer systems, it can remain invisible for a long time. During this period of time, although it did not directly damage the computer network system, an attacker easily exploited data in the software and took the control of the system.[272] These characteristics make the "Stuxnet" one of the most sophisticated and complex computer worms in cyberspace.

The attack against Iran was almost the same. The worm, Stuxnet, penetrated high – secure computer systems of specific nuclear research facilities. Although they were not connected to Internet, the virus uploaded into Iran's complex computer system by using simple removable memory stick. It took the control of the main computer of the reactor and changed the speed of the centrifuges in which uranium spins at a stabile speed, temperature and pressure in order to be enriched. With that intervention, the speed increased and decreased vehemently. A researcher said that "Stuxnet changes the output frequencies and thus the speed of the motors for short intervals over a period of months. Interfering with the speed of the motors sabotages the normal operation of the industrial control process."[273] Worse than this was that Stuxnet affected the system thanks to ability of concealing itself perfectly as if everything was working fine. Therefore, the experts could not understand that the reactor was under a cyber attack for a period of time.[274]

The drastic alternation of the speed caused that the centrifuges expanded. They could have touched each other and destroyed the system. Fortunately, the reactor did not explode and no nuclear leakage came into being.[275]However, the uranium enrichment efforts of Iran set back to several years. The Iranian officials met this event calmly. The initial comments expressed that the Stuxnet was not so significant to affect the Iran's nuclear research program. The Chief of Iran's Atomic Energy Organization, Ali Akbar Salehi, declared that "…we discovered the virus

[272] DeLuca, p. 288.
[273] Farwell and Rohozinski, p. 25.
[274] Buchan, p. 220.
[275] DeLuca, p. 289.

exactly at the same spot it wanted to penetrate because of our vigilance and prevented the virus from harming equipment…" With this declaration, it might be intended to magnify Iran more than it was but the reality was not like that. Even though the Stuxnet did not cause a catastrophe, it shook Iran's self – confidence. The President, Ahmadinejad, accepted this reality by giving a statement to the media that "…they succeeded in creating problems for a limited number of our centrifuges with the software they installed in electronic parts…"[276] With this cyber attack, attackers gave a message to Iran that they possessed potential cyber capability. Although Iran officials denied this claim, they were impressed to stop nuclear enrichment program.[277]

3.2.3.2. Legal Assessment

The threat of the Stuxnet was more severe than its results. According to the Institute of Science and National Security, the strong change of the speed of rotation was enough to produce overflowing vibrations that contact the centrifuges. It could have destroyed the centrifuges and caused a real – world explosion.[278] General Michael Mayden, former director of the CIA, mentioned the importance of the situation with these words: "Stuxnet is the first time where we have seen significant physical damage created by a cyber attack."[279]

The Stuxnet became so important due to the fact that it was the first - known cyber attack aimed at a real – world concrete infrastructure system, such as power stations, water plants, and industrial units. It was a nuclear power plant that hosted huge potential energy that could kill thousands of people. This kind of a professional cyber attack to Iran confuses the minds because of the fact that Iran has been under international pressure for a long time about the uranium enrichment program. It seems remote possibility that this cyber attack was conducted by an independent hacker. Ralph Langner, a German computer security expert, claimed that "This is not some hacker sitting in the basement of his parents' house. To me, it seems that the

[276] Buchan, p. 221.
[277] Johnson, p. 174.
[278] DeLuca, p. 288.
[279] DeLuca, p. 289.

resources needed to stage this attack point to a nation state." The thoughts about the responsibility of this cyber attack focuses on the USA and Israel.[280] However, these states have not accepted the responsibility of the attack yet and no clear proof has been emerged until now.

While this attack has drawn considerable international attention, the results have not been lightened clearly up to present. No injury to people was officially reported, and property damage was limited to only power plants. Just some parts of important enrichment equipment were destroyed. So, whether the Article 2(4) of the UN Charter comes into force is unambiguous.

As we understand from the speech of the Iranian officials, the Stuxnet caused just some inconsiderable problems. These problems were just the alternation of the speed of rotation, and they did not result in people injury and property damage. There were no severe consequences to constitute an armed attack. In this point of view, there is no legal evidence to assert the presence of a use of force and an armed attack.[281]

[280] O'Connell, p. 4.
[281] Buchan, p. 222.

CONCLUSION

Appearance of every innovation is inspired by the requirements of the humanity. In the 19th and the first half of the 20th century, there were so many blurry areas in *jus ad bellum* and *jus in bello*. After world wars had caused destructive results, international society felt an absence of legal arrangements that restore the international order. This absence led international society to establish new and global law system. This law system has lived until now and become international customary law. Thus, the blurry areas are nearly clarified, and the requirements of international society are almost met. After the usage of Internet had become widespread all around the world in the last decades of the 20th century, international society began to feel another legal absence - legal arrangement about cyber activities.

With the Article 2(4) of the UN Charter, "use of force" and "threat of force" are prohibited, but the term "force" has not been clearly expressed. There is a dichotomy among scholars about what constitutes use of force. One group claims that political, diplomatic, or economic pressures are also regarded as elements of use of force. According to them, lawmakers could have used the term "armed force" instead of the term "force", if they had want. But they did not. Thus, it is impossible to limit the meaning of force to only armed force.

The opposite group clearly distinguishes political, diplomatic, or economic force from the term "force" expressed in the Article 2(4). They interpret the meaning of use of force narrowly which is limiting to only "armed force". Because the armed force produce usually physical destruction or injury, but political, diplomatic, or economic force do not. Additionally, the results of armed force are more dangerous owing to the fact that armed force affects the human beings directly. For these reasons, the common view in international society is that the Article 2(4) states only armed force.

While use of force is prohibited in the UN Charter, two exceptions are legally under guarantee. Firstly, the UNSC can take measures in order to keep or restore the international peace, security and stability. The UNSC has an authority to approve use of force to maintain or restore international peace and security within the framework of Article 39. What kind of measures can be taken is mentioned in the Article 41 and

42. While measures not involving use of armed force can be applied, other operations by air, sea, or land forces of members of the UN can be taken into consideration as other options.

Secondly, the prohibition of use of force is also concerned with "self – defense". This exception means that if any state feels itself in need of self-defense in order to prevent its rights against an armed attack, this state can use force on its own or collectively until the UNSC takes measures necessary to maintain international peace and security as set out in the Article 51 of the UN Charter.

States can apply to the Article 51 of the UN Charter only when they are exposed to an armed attack. The legal situation of armed attack is another debatable area of international law system. Although the meaning of armed attack is defined in the 1977 Additional Protocol I to Geneva Conventions as "acts of violence against the adversary, whether in offence or in defense", it does not become satisfactory. For instance, there is no consensus on what kind of weapons constitutes armed attack.

In the past, the meaning of weapon used to be only conventional military weapon, but recent meanings involve more than the past. The effects of the weapons, whether conventional or not, are more important than how they work. If any weapon causes loss of life and property damage, it constitutes armed force regardless of what it is. Nuclear energy was invented for humans' benefit, but nuclear bombs killed thousands of people in Japan. So, it would be irrational to claim that a nuclear bomb do not constitute an armed force because of the fact that it does not produce physical energy as conventional weapons generate. This approach is also supported by the ICJ with the Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons.

While injury and property damage are signs of an armed attack, the threshold of the level of damage or injury is important. Not all damaging events rise to the level of an armed attack. Whereas most grave forms of the use of force amount to an armed force, the mere frontier incidents do not. An obvious definition of an armed attack is mentioned by Walter G. Sharp as "a use of force that rises to a certain scope, duration, and intensity threshold constitutes an armed attack within the meaning of Article 51 of the Charter of the United Nations that invokes a state's inherent right of self – defense".

The cyber warfare has to be assessed in the light of current international law due to the fact that there is no specific law system applicable to only cyber warfare. Three approaches are developed to decide what constitutes use of force rising to the level of an armed attack. When the cyber attacks are put in this frame, it became more comprehensible. The first one, instrument – based approach, does not accept a cyber attack as an armed attack owing to lack of presence of conventional military weapons. If a cyber attack constitutes an armed attack, weapons used in cyber attacks must be traditional military weapons that cause sufficient kinetic destruction but cyber weapons are not like that. However, cyber weapons sometimes have more capability to give damage and causality than conventional military weapons. For this reason, this approach does not reflect the reality of cyber warfare.

In the second one, target – based approach, while severity of cyber attacks is not sufficient, it is enough aiming to the critical national infrastructure to constitute an armed attack. In this approach, if a cyber attack affects the critical national infrastructure, even there is no important disruption or a cyber operation which is lawful under international law such as espionage, it constitutes an armed attack. In this view, the results of cyber attacks aimed at critical national infrastructure meet the requirements of constituting an armed attack. States can protect their critical national infrastructure thanks to this approach; it creates risk which may cause destructive conventional armed responses because of the fact that an extensive interpretation of critical national infrastructure decreases the threshold of the self-defense. So, this approach is not so practical to interpret the position of cyber warfare in international law system, too.

The third one, effect – based approach, categorizes cyber attacks into two groups. In the first group, a cyber attack can cause important injury and damage. Its consequences are as destructive as bombs or bullets can generate. This clearly makes a cyber attack equal to an armed attack. The second group involves cyber attacks causing injury and damage but they are not as important as armed attacks cause. Then, the question of how to decide which one is more important and constitutes armed attack appears.

Michael Schmitt's seven criteria explain the statue of use of force which rises to the level of an armed attack to answer this question. The first criterion severity

means that a cyber attack which is accepted as an armed attack must produce physical injury to the people and destruction of property like an armed attack in which military weapons are used. This criterion is the most significant one because only the presence of severity is enough to constitute armed attack as mentioned in the Tallinn Manual that "severity is self – evidently the most significant factor in analysis". The second one is immediacy. The cyber attacks may appear with great immediacy. This criterion distinguishes cyber attacks from the other measures like political or economic ones of which effects may reveal months or years later. The third one is directness. There must be a direct connection between an attack and its harmful consequences. If the cyber attack causes direct physical damage, injury, suffering, or death, it becomes use of force. The fourth one is invasiveness. A cyber attack that intentionally causes any destructive effect within the sovereign territory of another state is an unlawful use of force. The fifth one is measurability. At the end of the armed conflicts, the number of deaths, wounds, or loses can be quantified. Even the monetary value of the property damage can be calculated. The measurable results of cyber attacks help to determine whether the cyber operation has reached the level of a use of force. The sixth one is presumptive legitimacy. If an action is not banned in the law, people are free to do it and they cannot be punished because of their actions. In other words, an action which is not prohibited in the law is permitted. Although international law forbids using of force, propaganda, psychological operations, espionage, or mere economic pressure are not clearly prohibited. So, these kinds of actions are presumptively legal, even in cyberspace. The last criterion is responsibility. The actions of state's legal organs and non – state actors can be clearly attributed to the states. A State in which cyber attack is carried on has to prohibit such actions in its own territory. If host state does not prevent hostile cyber activities, a victim state has a right to take counter measures to defend its own benefits. However, to hold a state responsible for a cyber attack is not so easy. The material evidences for attribution have to be explicit and unambiguous. Although the technological means of tracking cyber attackers are very developed, it is also too difficult to impeach a state with responsibility of cyber attack. The victim state may trace back to the source of cyber attack, but this is not sufficient to claim that any state is guilty.

The recent cyber attacks help to explain how the international law system is practiced. Although a global cyber crisis which is as much destructive as conventional armed conflicts has not happened until now, some states have suffered heavy damage. *The Estonia, Iran, and Georgia Cases* have different characteristics. *The Estonia Case* is the most comprehensive cyber attack that international society has ever witnessed. The cyber attacks in Estonia did not end in a short time; it lasted for days, and caused absolute chaos within the society. Moreover, this instance has another important aspect that it was the first cyber attack to be conducted as an instrument in an international political conflict between two states. In *the Georgia Case*, cyber attacks were coordinated with conventional military invasion. This is the first known combination of the cyber and traditional armed attack which is more destructive than only one. *The Iran Case*'s important characteristic is to be the first - known cyber attack that aimed at a real – world concrete infrastructure system, such as power stations, water plants, and industrial units. While none of these cyber attacks was accepted as an armed attack and legalized any armed response, they called attention to new phenomenon of warfare history. These cyber attacks also indicated that cyber warfare obviously will take conventional warfare's place in the future.

The weapons used in these cyber attacks are not like conventional weapons that have explosive effects. They are some kinds of computer programs, but the intention of creating these programs is to damage other systems. In recent years, with the high technological changes in the world, new kinds of cyber weapons has come into being. These new weapons are not only used to get information from enemy but also to damage them.

Cyber attacks are one of the most problematic fields of international conflicts. Although the presence of cyber activities is very young compared to the conventional armed conflicts, they have huge potential to affect humanity as much as military weapons have. In order to struggle with cyber attacks, international law system must be implemented by international society, even if most of the states have domestic law systems about cyber activities, such as cyber crime, cyber espionage. They are not sufficient to be applied for international cyber conflicts.[282] The USA President

[282] DeLuca, p. 306.

Barack Obama also recognized this fact in a White House report which stated, "The Nation also needs a strategy for cybersecurity designed to shape the international environment and bring like-minded nations together on a host of issues, such as technical standards and acceptable legal norms regarding territorial jurisdiction, sovereign responsibility, and use of force."[283]

It is nearly impossible to solve all the problems about cyber activities because of the fact that the cyberspace has been changing every moment. Humanity will most probably face more sophisticated and complex cyber weapons than ones used in Estonia, Iran and Georgia. Although it seems impossible to establish completely secure cyber system in the world, to come together and make a new international law system before most of the world are affected would be the best in lieu of to establish a legal systematization after destructive results come into being.

[283] "White House Cyberspace Policy Review", 2009, available at http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf, (22.01.2015).

BIBLIOGRAPHY

Books

Carr, Jeffrey. **Inside Cyber Warfare Mapping the Cyber under World**, O'Reilly Media, California, 2012.

Johnson, Thomas A. **Cyber-security Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare,** CRC Press, Boca Raton, 2015.

Moore, John Norton. **Crisis in the Gulf: Enforcing the Rule of Law**, Oceana Publication, New York, 1992.

Owens, William A, Kenneth W. Dam, Herbert S. Lin. **Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities**, The National Academies Press, Washington, 2009.

Ruys, Tom. '**Armed Attack' and Article 51 of the UN Charter**, Cambridge University Press, New York, 2010.

Shakarian, Paulo, Jana Shakarian, Andrew Ruef. **Introduction to Cyber Warfare,** Syngress, Boston, 2013.

Sharp, Walter Gary. **Cyberspace and the Use of Force**, Aegis Research Corporation, Virginia, 1999.

Shaw, Malcolm. **International Law**, Cambridge University Press, New York, 2008.

Schmitt, Michael N. (ed.). **Tallinn Manual on the International Law Applicable to Cyber Warfare**, Cambridge University Press, New York, 2013.

Articles

Ashmore, William C. "Impact of Alleged Russian Cyber Attacks", **Baltic Security & Defense Review**, Vol. 11, 2009, pp. 1-53.

Aydın, Ahmet Buğra. "Uluslararası Hukukta Önleyici ve Öngörücü Meşru Müdafaa Hakkı", **Genç Hukukçular Hukuk Okumaları**, Vol. 4, 2013, pp. 52-64.

Buchan, Russell. "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions", **Journal of Conflict & Security Law**, Vol. 17, 2012, pp. 212-227.

DeLuca, Cristopher D. "The Need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors", **3 Pace International Law Review Online Companion**, 2013, pp. 278-315.

Denning, Dorothy E. "The Ethics of Cyber Conflict", **The Handbook Information and Computer Ethics**, Wiley, New Jersey, 2008, pp. 407-429.

Dinstein, Yoram. "Computer Network Attacks and Self-Defense", **International Law Studies**, (ed. Michael N. Schmitt, Brian T. O'Donnell), Vol. 76, 2002, pp. 99-119.

Dipert, Randall R. "The Ethics of Cyberwarfare", **Journal of Military Ethics**, Vol.9, No. 4, 2010, pp.384 – 410.

Dunlap, Charles J. "Perspectives for Cyber Strategists on Law for Cyberwar", **Strategic Studies Quarterly**, Vol. 5, No. 1, 2011, pp 81-95.

Dunlap, Charles J. "Some Reflections on the Intersection of Law and Ethics in Cyber War", **Air & Space Power Journal**, Vol. 27, No. 1, 2013, pp. 22-38.

Farwell, James P. and Rafal Rohozinski, “Stuxnet and the Future of Cyber War”, **Survival: Global Politics and Strategy**, Vol. 53, No. 1, 2011, pp. 23-40.

Gervais, Michael. “Cyber Attacks and the Laws of War”, **Berkeley Journal of International Law**, Vol. 30, No. 2, 2012, pp. 525-579.

Goldsmith, Jack, “How Cyber Changes the Laws of War”, **European Journal of International Law**, Vol. 24, No. 1, 2013, pp. 129-138.

Graham, David E. “Cyber Threats and the Law of War”, **Journal of National Security Law & Policy**, Vol. 4, No. 1, 2010, pp. 87-102.

Hathaway, Oona A. et al. “The Law of Cyber-Attack”, **California Law Review**, Vol. 100, No. 4, 2012, pp. 817-885.

Herzog, Stephen. “Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses”, **Journal of Strategic Security**, Vol. 4, No. 2, 2011, pp. 49-56.

Hollis, David. ‘‘Cyberwar Case Study: Georgia 2008’’, **Small Wars Journal**, Vol.7, No. 1, 2011, pp. 1-9.

Hollis, Duncan B. “Why States Need an International Law for Information Operations”, **Lewis & Clark Law Review**, Vol. 11, 1997, pp. 1041-1061.

Joyner, Christopher J. and Catherine Lotrionte, “Information Warfare as International Coercion: Elements of a Legal Framework”, **European Journal of International Law**, Vol. 12, No. 5, pp. 842-865.

Kesan, Jay P. and Carol M. Hayes. “Migitative Counterstriking: Self-Defense and Deterrence in Cyberspace”, **Harvard Journal of Law & Technology**, Vol. 25, No.2, 2012, pp. 415-432.

Li, Sheng. “When Does Internet Denial Trigger the Right of Armed Self-defense?”, **Yale International Journal of Law**, Vol. 38, No. 1, 2013, pp. 179-216.

Liaropoulos, Andrew. “Cyber-Security and the Law of War: The Legal and Ethical Aspects of Cyber-Conflict”, **Working Paper of Greek Politics Specialist Group**, No. 7, 2011, pp. 1-6.

Melzer, Nils. “Cyberwarfare and International Law”, **UNIDIR Books and Reports**, United Nations Institute for Disarmament Research, Geneva, 2011, pp. 1-36.

Ophardt, Jonathan A. “Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow’s Battlefield”, **Duke Law & Technology Review**, Vol. 3, 2010, pp.1-28.

Raboin, Bradley. “Corresponding Evolution: International Law and the Emergence of Cyber Warfare”, **Journal of the National Association of Administrative Law Judiciary**, Vol. 31, No. 2, 2011, pp. 603 – 668.

Robertson, Horace B. “Self-defense against Computer Network Attack under International Law”, **International Law Studies**, (ed. Michael N. Schmitt, Brian T. O’Donnell), Vol. 76, 2002, pp. 121-145.

Roscini, Marco. “World Wide Warfare – *Jus ad bellum* and the Use of Cyber Warfare”, **Max Planck Yearbook of United Nations Law**, Vol. 14, 2010, pp. 87-130.

Schaap, Arie J. “Cyber Warfare Operations: Development and Use under International Law”, **Air Force Law Review**, Vol. 64, 2009, pp. 121-1.

Schmitt, Michael N. “Attack as a Term of Art in International Law: The Cyber Operations Context”, **Proceeding of the 4th International Conference on Cyber Conflict**, (ed. Christian Czosseck, Rain Ottis, Katharina Ziolkowski), 2012, pp. 283-293.

Schmitt, Michael N. “Classification of Cyber Conflict”, **Journal of Conflict & Security Law**, Vol. 17, No. 2, 2012, pp. 245-260.

Schmitt, Michael N. “Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework”, **Columbia Journal of Transnational Law**, Vol. 37, 1999, pp. 1-48.

Schmitt, Michael N. “International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed”, **Harvard International Law Journal Online**, Vol. 54, 2012, pp.13-37.

Schmitt, Michael N. “The Law of Cyber Warfare: *Quo Vadis*?”, **Stanford Law & Policy Review,** Vol. 25, 2014, (*Quo Vadis*), pp. 269-299.

Shackelford, Scott J. “From Nuclear War to Net War: Analogizing Cyber Attacks in International Law”, **Berkeley Journal of International Law**, Vol. 25, No. 3, 2009, pp. 191-250.

Silver, Daniel B. “Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter”, **International Law Studies**, (ed. Michael N. Schmitt, Brian T. O’Donnell), Vol. 76, 2002, pp. 73-97.

Solce, Natasha. “The Battlefield of Cyberspace: The Inevitable New Military Branch-The Cyber Force”, **Albanian Law Journal of Science**, Vol. 18, pp. 293-324.

Waxman, Matthew C. “Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions”, **International Law Studies**, Vol. 89, 2013, pp. 109-122.

Waxman, Matthew C. “Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)”, **Yale Journal of International Law**, Vol. 36, 2011, pp. 421-459.

Yayla, Mehmet. “Cyber War and Use of Force Against Cyber Attacks in International Law”, **Türkiye Barolar Birliği Dergisi**, Vol. 107, pp. 199-220.

Ziolkowski, Katharina. “Jus ad Bellum in Cyberspace–Some Thoughts on the ‘Schmitt Criteria’ for Use of Force”, **Proceeding of the 4th International Conference on Cyber Conflict**, (ed. Christian Czosseck, Rain Ottis, Katharina Ziolkowski), 2012, pp. 295-309.

International Documents

“Convention (III) relative to the Opening of Hostilities”, 18 October 1907, available at https://www.icrc.org/ihl/INTRO/190?OpenDocument, (26.03.2015).

French – Mexican Claims Commission, “Estate of Jean – Baptiste Caire (France) v. United Mexican States, 5 R.I.A.A. 516”, 7 June 1929, available at http://legal.un.org/riaa/cases/vol_V/516-534_Caire.pdf, (11.04.2015).

Green Paper on a European Programme for Critical Infrastructure Protection, **Commission of the European Communities**, 17.11.2005, available at https://marcusviniciusreis.files.wordpress.com/2010/06european-program-to-protect-ci.pdf, (10.03.2014).

ICJ, “Case Concerning Military and Paramilitary Activities in and Against Nicaragua”, 27 June 1986, available at www.icj-cij.org/docket/files/70/6503.pdf, (10.03.2015).

ICJ, “Corfu Channel Case (Preliminary Objection)”, 25 March 1948, available at http:/www.icj-cij.org/docket/files/1/1571.pdf, (10.03.2015).

ICJ, “Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory”, 09 June 2004, available at http://unispal.un.org/UNISPAL.NSF/0/3740E39487A5428A85256ECC005E157A, (21.03.2015).

ICJ, “Legality of the Threat or Use of Nuclear Weapons”, 8 July 1996, available at www.icj-cij/docket/files/95/7497.pdf, (29.03.2015).

ICJ, “Reparation for Injuries Suffered in the Service of the United Nations”, 11 April 1949, available at www.icj-cij.org/docket/files/4/1837.pdf, (10.03.2015).

ICTY, “International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia since 1991”, 15 July 1999, available at http://www.icty.org/x/cases/tadic/acjug/en/tad-aj990715e.pdf, (11.03.2015).

“Kellogg-Briand Pact”, 27 August 1928, available at http://www.history.ubc.ca/sites/default/files/courses/documents/%5Brealname%5D/kellogg-briand_pact_1928.pdf, (13.01.2015).

“Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I)”, 8 June 1977, available at https://www.icrc.org/ihl/WebART/470-750050?Open Document, (11.03.2015).

Resolution adopted by the General Assembly, “2625 (XXV). Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations”, 24 October 1970, available at http://www.un-documents.net/a25r2625.htm, (10.03.2015).

Resolution adopted by the General Assembly, "3281(XXIX). Charter of Economic Rights and Duties of States", 12 December 1974, available at http://www.un-documents.net/a29r3281.htm, (22.12.2014).

Resolution adopted by General Assembly, "3314 (XXIX). Definition of Aggression", 14 December 1974, available at http://www.un-documents.net/a29r3314.htm, (02.11.2014).

Resolution adopted by General Assembly, "56/83. Responsibility of States for International Wrongful Acts", 12 December 2002, available at http://legal.un.org/ilc/texts/instruments/english/draft%20articles/9_6_2001.pdf, (22.03.2015).

Resolution adopted by the General Assembly, "58/199. Creation of a Global Culture of Cyber Security and the Protection of Critical Information Infrastructures", 30 January 2004, available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf, (12.04.2015).

Resolution adopted by the Security Council, "Resolution 1368", 12 September 2001, available at http:/daccess-dds-ny.un.org/doc/UNDOC/GEN/N013382.pdf?OpenElement, (2.2.2015).

UN, "Charter of the United Nations", 26 June 1945, available at http://www.un.org./en/documents/charter/, (11.03.2014).

"Vienna Convention on the Law of Treaties", 23 May 1969, available at https://www.un.org/doc/so...e/publications/THB/English.pdf, (17.11.2014).

Articles of Magazine and Newspaper

"A New Kind of Warfare", **New York Times**, 10 September 2012, http://search.proquest.com/docview/1038573240?accountid=10527, (11.10.2013).

Bowcott, Owen. "Nato Guide Says Nuclear Plants and Hospitals Are Off- Limits in Cyberwar: Online Attacks Could Make 'Hacktivists' Lawful Targets Project Codifies Legal Basis For State-Led Cyber-Warfare", **The Guardian**, 19 March 2013, http://search.proquest.com/docview/1317738187?accountid=10527, (22.07.2013).

Coughlin, Con. "The Cyber Warriors Are Preparing for Battle", **The Daily Telegraph**, 03 June 2011, available at http://search.proquest.com/docview/869762229?accountid=10527, (06.10.2013).

"Cyber Warfare: More Must Be Done", **Telegraph**, 24 May 2013, http://search.proquest.com/docview/1319400151?accountid=10527, (22.07.2013).

"Hype and Fear", **The Economist**, 08 October 2012, http://search.proquest.com/docview/1223834330?accountid=10527, (03.09.2013).

Lerner, Dan. "Cyber-Attack Defense Plan Faces Criticism", **Financial Times (London)**, 02 February 2000, http://search.proquest.com/docview/248916398?accountid=10527, (08.09.2013).

"Masters of the Cyber-Universe; Cyber-Hacking", **The Economist**, 06 April 2013, http://search.proquest.com/docview/1324420283?accountid=10527, (03.09.2013).

Nakashima, Ellen. "Pentagon Is Debating Cyber-Attacks", **The Washington Post**, 16 November 2010, http://search.proquest.com/docview/762549546?accountid=10527, (06.10.2013).

Stephenson, John and Karla Jones. “Fighting Cyber Warfare at the State Level; While Congress and the President Quarrel over What to Do Next, Governors Join in a Collaborative Defense Effort”, **Wall Street Journal**, 22 February 2013, http://search.proquest.com/docview/1296294459?accountid=10527, (03.09.2013).

Vistica, Gregory. “We’re in the Middle of Cyberwar”, **Newsweek**, 20 September 1999, available at http://www.newsweek.com/were-middle-cyberwar-166196, (10.01.2015).

Other Sources

Advisory Council on International Affairs, **Cyber Warfare**, No. 77, December 2011, available at http://aiv-advies.nl/6ct/publications/advisory-reports/cyber-warfare #advice-summary, (10.03.2015).

Afroditi, Papanastasiou. “Application of International Law in Cyber Warfare Operations”, 2010, available at http://dx.doi.org/10.2139/ssrn.1673785, (18.11.2014).

Black’s Law Dictionary Free Online Legal Dictionary, available at http://thelawdictionary.org/weapon/, (13.02.2015).

Dictionary of Contemporary English, Longman, Barcelona, 1995.

Executive Order EO 13010, Critical Infrastructure Protection, 15 July 1996, available at http://fas.org/irp/offdocs/eo13010.htm, (14.04.2015).

O’Connell, Mary Ellen. “Cyber Security and International Law”, Meeting Summary, 29 May 2012, available at http://www.chathamhouse.org/publications/pepers/view/184529, (22.02.2015).

The National Strategy to Secure Cyberspace, February 2003, available at http://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf, (10.03.2014).

The United States Department of Defense, "The United States Military Strategy for Cyberspace Operations", December 2006, available at http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf, (09.10.2014).

The US Army Training & Doctrine Command, DCSINT Handbook No: 1.02 Critical Infrastructure Threats and Terrorism, 2006, available at https://fas.org/irp/threat/terrorism/sup2.pdf, (13.08.2013).

"White House Cyberspace Policy Review", 2009, available at http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf, (22.01.2015).