BirEx JOURNAL
Budapest International Research in Exact Sciences
Medical, Biological, Argiculture, Engineering
Science and other related areas
e-ISSN : 2655-7827
p-ISSN : 2655-7835
http://www.bircu-journal.com/index.php/birex

Cyber-attacks Based on Legal Requirements and International Relations of Governments

Maryam Sedaghat[1], Mojtaba Mireh Gini[2]
[1] Student of International Affairs, Gilan University, Gilan, Iran
[2] International Law, Islamic Azad University, Central Branch, Tehran, Iran

Abstract : *Nowadays, the change in the scope of power from hard power to soft power has also shifted the process of military attacks to cyberattack. Cyber-attacks, like armed attacks, must fit into the framework of humanitarian law. Therefore, government responsibilities are also determined based on these changes, and as governments have responsibilities in military strikes, their responsibilities for cyberattacks should also be identified. Therefore, the present study makes use of analytical-descriptive method based on existing documents to examine this issue. Ultimately, the present study concludes that a cyberattack could be described as armed use of force in accordance with Article 2 (4) of the United Nations Charter. On the other hand, a widespread cyberattack on the basic infrastructures that causes material damages or casualties comparable to an armed attack with conventional weapons, gives the affected government the right to seek legitimate defense. Also, governments can resort to legitimate defense in response to a cyberattack that does not amount to an armed attack but provides the settings for an impending armed attack with conventional weapons.*
Keywords *: cyberwarfare; governments; international relations; legal requirements*

I. Introduction

The growing phenomenon of cyberattacks in the virtual world has occupied the minds of many politicians and lawyers. Therefore, many papers and lectures have been presented to offer a solution to this international threat. Perhaps in the past, land, sea and air conflicts were the most prominent examples of hostile relations among governments. But today, with the advent of various malware such as Stuxnet and Flame, various virtual networks, media, and so on threaten the security of nations. Cyberattacks, soft warfare and post-modern war are just some of the names given to these threats. Therefore, given the high potential of cyberattack, such as the ability to make changes to tax records in the stock market, sending error messages to shutdown nuclear systems, opening a dam, disrupting the air traffic system to facilitate aircraft accidents, etc., has led governments to establish a narrow and international definition of cyberattack, since achieving this definition can be an effective step in identifying these attacks and the legitimate potential responses to them (Duncan, 2007:1023).

Since these attacks may expose defense, law enforcement, banking, commerce, transportation, and scientific activities, and a large percentage of public and private sector transactions through the network to sabotage by certain individuals who gain unauthorized access to the network, they can disrupt the daily routines of a country. So, the debate on cyberattacks in cyberspace and cybercrime is on the rise every day (Lehman & Potter, 1395:207)

But the legal challenge to address such attacks is a matter of explanation of its nature and interpretation as a type of war. As in the military wars between two or more countries, the concepts of beginning and end of the war, invading and defending sides, the allies, the enemy, and even the neutral and the front are completely clear. However, in the field of cyberwarfare, these concepts are unclear. For example, the beginning and end of cyberwarfare cannot be timed; incidentally, cyberwarfare could be effective when its time is undetermined. The target country in these types of wars becomes aware of an attack when the enemy's goal is almost

achieved and in fact, it becomes aware of the destruction and smoke caused by the attack (Libicki, 2009:170).

There is another ambiguity in this context relating to the invading country or forces. The fact is that because of the virtual nature of the space and the ambiguity in the nature and type of attack, no one can easily identify the invading country or force. The nature of cyberattack does not allow tracing the attacker. While the location of the cyberattack is not known and the dispatched virus or malware does not show any sign of the attacker. Also, due to the multiplicity of actors in the cyberspace, including states, government agencies and NGOs, terrorists, hackers, and even individuals, identification of the attacker is more difficult and complicated. It should be noted that in the cyberattacks that have taken place so far, the country or attacker have not been identified based on the cyberattack and clear evidence, but on the basis of the political atmosphere and the intentions and goals of the countries (Sanger, 2015:1).

II. Theoretical Framework

Perhaps, the first cyberattack was the Morris Worm case in 1988. It was one of the first known worms to disrupt cyberinfrastructure across the United States. Therefore, Robert Tappan Morris, currently a professor at the Massachusetts Institute of Technology, was the first creator of computer worms. According to him, he just wanted to measure the size of the Internet. In December 2006, NASA shut down its emails with their attached files before launching the shuttle for fear of hacking. At that time, the Business Week magazine reported that unknown foreign intruders had access to a recent US space launch program (Reverson, 2012:15).

2.1 Tallinn Directive

This directive was set up in Tallinn, Estonia, in 2009 to the review the laws ruling over cyberwarfare. The project was designed by international law experts and researchers and aimed at outlining legal and law norms in these modern wars. The emphasis of this directive on cybercrime actions against cyber-equipment, for example, the use of cyber operations against a state's critical infrastructure or a cyberattack targeting the enemy's command and control systems. So, the purpose of this directive does not pivot around cyber operations against material equipment, such as air raid and bombing of the cyber-control centers. It also does not include traditional military electronic attacks, such as radio jamming. Such actions have already been defined under the law of armed conflicts. Thus, the Tallinn directive includes both international and non-international armed conflicts, and covers the laws ruling over cyberattacks and related items such as the responsibility of governments and the law of the high seas (Schmitt, 2013:16-19).

2.2 The position of cyberattacks from the Perspective of Banning the Use of Force and the Concept of Invasion

The subject of discussion in this section is to include cyber operations in the scope of banning the use of force in international relations. Although it should be noted that the intention to exert pressure to identify and recognize cyber operations as using military force does not suffice. However, military force is nothing but an extreme form of intervention, such as diplomatic and economic pressure, to force a victim country to submit to something. Accordingly, if cyber operations are used for this purpose, it can be easily categorized as a

type of using force (Roscini, 2014:45). Therefore, cyber operations can include cyber-abuse to collect and monitor information, up to cyberattack, as well as from removal, tampering and modification of the software to damaging the infrastructure belonging to properties and individuals. Such a variety of actions in cyber operations has led to various opinions, including the inclusion of it as a form of using force (Roscini, 2014:52).

In this regard, the International Court of Justice, in its commentary on paragraph 4, Article 2 of the Charter which prohibits the use of force against states, has argued in the case of Nicaragua that such a ban is a customary rule of international law. Also, in a verdict regarding military operations, this court sees this clause as the cornerstone of the Charter. Therefore, cyber operations can be subject to this clause, provided that under the law of international responsibility of governments, such actions have been taken by governments or at least attributable to governments. As resorting to force does not necessarily involve using direct military force by the states or groups or individuals under their control, in cyber operations also, for example, malicious software of a rebel group and teaching how to use it can be included under the use of coercion rubric (Weller, 2015: 1112-1114).

2.3 Cyberattack from the Point of View of laws and Elements of War

The prerequisite for the implementation of armed conflict law is the existence of armed conflicts, which despite the growing importance of this issue, is not included in the present discussion, because no international entity has reported any cyberwarfare incident so far. The only example of the use of armed conflict law in cyber operations can be seen in during the international armed conflict between Georgia and Russia in 2008 that was used to continue the war. For example, if a hacking attack occurs after the war between the two countries, then the hackers involved in this cyberattack would effectively have the same legal status as the soldiers in the war (Gladyshev *et al*., 2015:139).

Thus, international law on cyber operations requires military combatants to comply with regulations such as the principle of military necessity, distinction between military and civilian populations, proportionality, respect for protected individuals and objects, impartiality and the prohibition of particular warfare methods, such as the breach of treaty. Although there are doubts regarding the enforcement of cyber operations laws during armed conflicts, but disagreements over the ease or difficulty of evaluating such operations are expressed under these regulations. Failure in the definition of war and statement of various types of warfare, makes it difficult to include cyber operations in the law of war.

Thus, although there is no credible and legal definition of cyberwarfare or cyberattack in general international law, specific treaties, customary law, and doctrine, there are practical descriptions based on technology and how it operates. The United States Department of Defense has provided definitions of cyber operations concepts and actions, such as attacking computer networks, defending computer networks, and exploiting computer networks. Thus, attacking computer networks as using a computer to disrupt, degrade or destroy information available on computers and computer networks is defined as: protection, monitoring, analysis, detection and response through authorized computer network and The Ministry of Defense intelligence systems activities, and ultimately the exploitation of computer networks to collect data from a target or network or automated information systems. Overall, in the event of military conflicts, these actions can be called cyberwarfare.

Also, the International Committee of the Red Cross (ICRC), in 2005, in explaining the cyber scope in warfare and attacks in the traditional studies of international humanitarian law, stated its position on the legal applicability of international humanitarian law in cyber

operations during armed conflict in two official texts. Similarly, the Red Cross Committee of the United Nations deems cyberwarfare and as a result, the application of international humanitarian law cited by the International Committee of the Red Cross, solely related to the co-existence and interference of armed attacks and cyber operations as follows:
"... the International Committee of the Red Cross (ICRC) drew the attention of countries to the potential implications of international humanitarian law in cyberwarfare, i.e. the attack on computer networks during armed conflict situations, which could include disastrous situations such as intervention in air traffic control systems and consequently, collision and crash of planes, interruption of urban water and electricity supply, or destruction of nuclear and chemical facilities. So, the above committee demands that all parties to the conflict comply with the international humanitarian law regarding the cyberwarfare means and methods in accordance with the principles of separation, proportionality and precaution in the attack." (Saxon, 2013: 210-220)

But the most important issue in cyber operations is the confusion about the scope and definition of the time of occurrence of this phenomenon and the term *attack* in the international humanitarian law and the *military attack* in the law of war. According to the interpretative statement of the International Committee of the Red Cross (ICRC) that takes the term *attack* equivalent to military action, the attack on cyber-networks must definitely take place in this context, so the title *attack* can be applied to it. But the Red Cross, in its recent statement mentioned the uncertainty in the law as such:
"... certainly, in the face of armed conflicts, international humanitarian law will be applied to cyber operations along with traditional weaponry, but the problem will be exacerbated when international humanitarian law seeks to apply only to cyber operations. Can such a situation be called a military conflict under the Geneva Conventions and other humanitarian treaties? Does the applicability change according to the situation? The answer to these questions solely depends on the performance of governments in the future. So, the cyberattack on Estonia in 2007 and the use of Stuxnet Worm against Iran's Natanz Nuclear Power Plant in 2010 cannot be covered by international humanitarian law because the concept of attack has not been realized (*Ibid*: 223).

2.4 Responsibility of Governments in the Event of Cyberattack in International Law

Given the importance of the Internet and computers and cyberinfrastructure for each country and its affiliates and institutions, their improper and hostile use can be extremely dangerous too. Hence, national governments need to be sure of their national security and economic networks. Therefore, in the events of the breach of security and the principle of a state's territorial integrity by a hostile country, it must be held accountable in order to prevent misuse of this useful, inexpensive and accessible tool.
Thus, with regard to the international responsibility of the state, three theories are proposed: the theory of error, risk, and liability arising from prohibited acts. So, the main problem in raising the government's responsibility caused by cyberattacks, due to the complexity of Internet networks and online actors, is the perpetrator of the cyberattack and reliance on risk theory cannot serve the purposes of this theory. In other words, the risk theory is emphasized where the perpetrator is known, and elsewhere, proving fault can help in attributing the action to the assisting government. In fact, by proving the fault, the government related to cyberattack can be found. The fault in this case will be used to attribute the action, and proof of the fault can be one of the means of asserting the attribution, while some also believe the fault can be used in proving the causal relationship in the domestic law. Therefore, the

emphasis on fault or malevolence can to some extent ensure that by finding the *culprit* we find the *perpetrator* as well. Therefore, the theory of fault seems to be more appropriate for invoking the government's responsibility caused by cyberattacks. It should be noted that the basis of international responsibility of the government caused by cyberattacks comes from the theory of *fault*, so the result of liability is not only limited to compensation, but the offending state is required to suspend and refrain from repeating violation of its obligation (*Responsibility of the State for Internationally Wrongful Acts* article, 2001: 30-35).

In line with this, one of the institutions that has assumed this responsibility for governments is the International Court of Justice, which has repeatedly invoked the international responsibility of states for breach of international obligations. In the most famous of these cases, the Corfu Channel case, the Court ruled that the mere existence of mines in the territory of the Albanian State could not render that state responsible, but the Court for the lack of notification about the existence of a minefield in the territorial sea to the ships of the third-party countries by Albania issued a ruling for its international responsibility. In the Court's view, this commitment rests on three general principles: the basic humanitarian principles, freedom of maritime communications, and the commitment of each state not to allow a state to consciously use its territory for actions contrary to the rights of other countries. In this category, the Court considered other realistic circumstances that if Albania at the last moment - for example, less than 24 hours from the time of the British warships collision - had become aware of minelaying, failure to inform the third-party countries due to difficulty or impossibility could be acceptable. The international responsibility problem has also been raised in other cases, such as Congo *vs*. Uganda, Bosnia Genocide, etc. (Tsagourias, 2015: 67). Moreover, based on the analysis provided, governments can be held responsible for the internationally illegal practices of governments in cyberspace to attempt to violate the rights of other countries in their territory. The attempt of governments to violate the rights of other countries can be assessed in such a way that firstly, the use of the Internet is not illegal *per se*; and secondly, data transmission by computers is not necessarily the source of harmful activities (Tsagourias 2015: 69).

The obligation of the hostile governments is another responsibility of the states. Based on the legal principles of neutrality set forth in the fifth and thirteenth Hague Conventions in 1907, the conflicting parties must respect the inviolability of the territory of neutral states that are prohibited to direct the hostilities, the exercise of hostile party rights and establishing operational bases in the land of neutral states (Hague Convention V,1907: Arts. 1, 2, 3; Hague Convention XIII, 1907: Arts. 1, 2, 5).

2.5 Government Response to Cyberattack

Given that the victim governments can identify the origins of cyberattack and attribute it to a country, they will have several options available to them as follows:

a. The Right to Legitimate Self-defense in Cyberattacks

According to a model drawn up by the law of war, the response of a government to an armed attack by another government must fulfill three conditions to be recognized as self-defense: necessity, proportionality and urgency. To satisfy the condition of necessity, a state should connect the attack to a specific source, specify the attacker's intention of attack, and conclude that the country should use force in response. The principle of proportionality states that the force used to respond to an attack should be proportionate to the initial attack. The principle of urgency prohibits a response to an attack after a long time. Based on the principle

of urgency, there is no other provision for defensive action immediately after an armed attack (Saberi Tilki, 2014:79).

Thus, with regard to the legitimate right of the states to defend themselves, the Article 51 of the United Nations Charter stipulates: "In the event of an armed attack against a United Nations member, until the Security Council takes the necessary action to maintain international peace and security, no provision in this Charter will prejudice the inherent right of self-defense, whether individual or collective. Members must report immediately to the Security Council the actions taken to exercise their right to self-defense. These actions in no way affect the authority and responsibility of the Security Council under this Charter to take action in order to maintain and restore international peace and security when it considers it necessary."

Accordingly, according to this article, in the event of the attack and waging war and resorting to force, by invoking an exception to the prohibition of the use of force set forth by the United Nations, the countries may exercise the right to national self-defense (Committee on Deterring Cyberattacks, 2010:162).

This right is exclusively for the compensation of damages to the victim of military strike, since such attacks subject to paragraph 4, Article 2 of the Charter and customary law to resort to force and its legal requirements. On the other hand, the legitimate self-defense is an effective defense in terms of nature, essence, continuity and scope, which otherwise involves illegal resort to force by a country. Therefore, it can be argued that passive cyber-defense, which only tries to deter attack, is a legal defense. Only in case of proactive defense, whether in cyberspace or physically, the law of legitimate defense is invoked directly by the government or the group involved in the conflict.

Moreover, only governments have a legitimate right to self-defense, so, private entities such as companies that are subject to cyberattack cannot react in accordance with the right to legitimate self-defense regardless of its severity. Their response will be subject to domestic and international laws. However, an attack against national governments could be considered military strike and the government must effectively defend itself. It should be noted that the requirements for legitimate defense such as urgency, certainty and lack of time for reflection must apply (Committee on Deterring Cyberattacks, 2010:163).

b. Referring to the International Court of Justice

The country responsible for cyberattack can be summoned to an international tribunal, including the International Court of Justice, to compensate for the violation of Article 2 (4) of the UN Charter and the principle of non-intervention. However, it should be noted that determining the amount of damage caused by a cyberattack is difficult because financial institutions may be hesitant in providing accurate information and determining the amount of damages. Likewise, the International Court of Justice like other international courts lacks binding jurisdiction, so both parties must agree to refer the case to the Court. In accordance with the Article 96 of the United Nations Charter, another option may be asking for an advisory opinion from the International Court of Justice on the legitimacy or non-legitimacy of cyberattack. Such opinions are optional and non-binding, although they are effective in creating a customary international rule (Conforti, 2005: 276).

c. Retaliatory Action

The country victim of a cyberattack can resort to retaliation and non-military countermeasures against the attacker. Under Article 49 (1) of the international liability of

governments act, the affected government may take countermeasures against the government responsible for international misconduct in order to force that government to fulfill its obligations. However, according to Article 50 (1) of the plan, such countermeasures that are not proportional to the initial action are prohibited. In fact, the claim that the victim country of cyber operations cannot retaliate by sending fraudulent codes unless a cyberattack has reached the brink of an armed attack, is unreasonable. Another issue is that the expected consequences of a countermeasure cyberattack should be proportional to the consequences of the initial attack. Such a calculation is difficult because, like biological weapons, the virus dispatched to cyberspace may be propagated uncontrollably (Delibasis, 2007: 364).

III. Research Methodology

The research method of this study to investigate and prove the raised hypotheses according to the nature of the subject, is the descriptive-analytical method and the method of collecting information is the library method using written references.

Definition of concepts and terms

Cyberspace

The global grid of computer systems interconnected by the Internet, communications infrastructure, online conference facilities, databases, and information organizations that are generally known as The Network. However, such a system generally means the Internet, but this term may also be used to refer to a specific and limited electronic information space of a company or military and government organization, etc. (Andress *et al*., 2014: 4).

Cyberinfrastructure

Cyberinfrastructure is the communications, storage, and computing resources that act based on that information system. Apparently, this damage should be physical because measures such as supervision seem to stay outside the definition of the expert group of regulators (Schmitt, 2013: 24,25).

Cyberattack

Cyberattack refers to the use of intentional attempt to modify, disrupt, deceive, reduce or eliminate computer systems or networks or information and programs or transmission through these systems or networks. Thus, cyberattack is the expansion of policies in cyberspace by government and non-governmental actors, to start attack or in response to a serious threat against national security (Shakarian, 2013:32).

Cyberwarfare

It is a war that governments as the main actors wage it to destroy the facilities, capabilities, and strengths of the enemy. The purpose of this war is the submission of the enemy to demands of the invading country. It should be noted that in this war, governments can use their cyber-army, non-state actors, or even hackers and individuals. Nonetheless, the main actor and leader is the state (Lee, 2013:105).

IV. Discussion

The new conditions of cyberattacks have created new challenges for the use of customary humanitarian law such as necessity, proportionality, distinction and impartiality. In other words, there are problems with the basic principles of international humanitarian law in dealing with cyberattacks. Also, cyberattacks are often not immediately lethal or destructive and may only create temporary breaches in network systems, it is difficult to assess whether a cyberattack is appropriate or not. On the other hand, the distinction between military and civilian people directly involved in the war and the involved civilians is impossible and ultimately, the hidden source of cyberattack complicates the implementation of neutrality tasks.

Therefore, in the wake of legitimate defense against such attacks, topics such as necessity are not specific to cyberattack, and in general in any attack if the need for the attack is necessary for military purposes, that attack is legitimate, otherwise, any part of the attack which is not necessary for military purposes is illegitimate.

Also, on prohibition relating to proportionality of the attack, where attacks have caused the loss of civilian lives and damage them, damage to non-military objects, or a combination of them is more than the predicted benefits of warfare, it prohibits the attack. In the analysis of proportionality, it should be considered that a military decision-maker must not exaggerate assessment of potential civilian casualties, destruction of non-military property and the loss of necessary non-military assets to achieve military ends. Here we are faced with a unique challenge on proportionality assessment of cyberattack. It's very hard to assess whether this attack, with regard to categories of objects, could be considered as a direct effect of instances of non-fatal temporary or severe cyberattack.

Also, there is a challenge in examining the distinction principle in these attacks. This principle claims there is a distinction between military individuals and objects or else, and targeting of military personnel in the battlefield. Also, military commanders should use a tool to correctly distinguish between military and non-military personnel and objects, and in other words, humanitarian law prohibits cyberattacks that are uncontrollable, without anticipation or without distinction between military and non-military personnel and objects (Schmitt, 2013:178). In some cases, there are situations where cyberattacks are legitimate, because the target is specifically military personnel and the principle of distinction is applicable, such as when cyberattack targets a military air traffic control system and this impedes military transportation. Similarly, there are situations in which the cyberattack is easily illegal, such as attacking some targets like hospitals, museums, and places of worship. These places, even if they are a part of targets and benefits of military strikes, still deserve the necessary protection. Of course, things are not always that simple. Moreover, the traditional support of the above-mentioned objects needs a complicated analysis of cyberattack because attacks occur in cyberspace and definitely attack on networks that steer those places should also be illegal, but due to the large number of military and non-military actors, the likelihood of using these seemingly civilian targets by military personnel increases and because of the double standard in this case, the required protection will not arise in the discussion of distinction.

Also, the neutrality principle refers to a situation in which a state can permanently, like Switzerland, or temporarily at a particular time of conflict, declare neutrality relative to the conditions of war and consequently assume rights and responsibilities (Heinegg, 2012:35). The challenge that is posed is to assess the lawfulness of these attacks, primarily because the cyberspace is without boundary. In this regard, since the space is used by both military and

civilian personnel, and because of interconnectedness of the cyberinfrastructure across the globe there is no boundary and it is not under the jurisdiction of any state (Lobel, 2012: 630); thus, the duty of the hostile states to respect the neutral territory should be considered in a broad manner, i.e. the prohibited acts include all actions and operations that have a negative effect on the functionality of cyberinfrastructure and computer networks, or render them useless (Talbot Jensen2012:822).

V. Conclusion

Cyberspace is an Internet space, in which the countries hide many of their intelligence data, and even in some cases, make them inaccessible to conduct their national and military affairs. In this context, a concept such as cyberwarfare is a term that is being used in the military literature of the world today, replacing the international conflict concepts in the past. Cyber-attacks have created a new challenge in the field of humanitarian law principles and the legal obligations of governments. Most cyberattacks cause temporary handicaps to achieve the results of the attack, making it difficult to assess whether a cyberattack was appropriate or not. The dual use of Internet infrastructure and the potential participation of civilians together with the military, complicates the distinction between them in cyberattacks and ultimately, the use of zombie computers and host servers raises many questions about the rights and obligations of neutral countries. Therefore, the present study examined the legal obligations of states in dealing with cyberattacks in their international relations, as well as their privileges to other non-governmental organizations in the face of cyberattacks, and ultimately examined the responses of the affected state against these attacks. In this regard, following the statement of hypotheses, questions and challenges relating to government legal requirements in cyberattack, the introduction discussed the background of the subject, history of cyberattacks, Tallinn directive, the position of cyberattacks in terms of prohibition of the use of force and the concept of invasion, cyberattacks from the perspective of laws and elements of war, responsibility of the governments in the face of cyberattacks in international law, and the response of governments to cyberattack. Finally, the data of the present research were analyzed. The results of the research showed that the cyberattack, in accordance with Article 2 (4) of the United Nations Charter, can be described as the use of armed force. On the other hand, a widespread cyberattack attack on the basic infrastructure that causes material damage or casualties comparable to an armed attack with conventional weapons, gives the victim government the right to seek legitimate defense. Also, governments can resort to legitimate defense in response to a cyberattack that does not amount to an armed attack but provides the settings for an impending armed attack with conventional weapons.

References

A-Book

Lehman, Michael & Gray, Potter (2016). Terrorism as an Organized Crime, translated by Qasem Zamani, Law, 3rd ed., Tehran, Ney publ.

B-Article

Andress, J & Winterfeld, S (2014), Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, second edition, USA, Elsevier

Conforti, B.(2005), The Law and Practice of the United Nations, Leiden: Martinus Nijhoff.

Duncan B. H (2007), Why States Need an International Law for Information Operations, 11 Lewis & Clark Law Review.1023, 1042.

Delibasis, D.(2007), The Right to National Self-Defence in Information warfare Operations, London: Arena Books.

Gladyshev, Pavel; Marrington, Andrew & Baggili, Ibrahim (2015), Digital forensics and cyber crime, New York, Springer International Publishing.

Heinegg, W. H. (2012, June). Legal implications of territorial sovereignty in cyberspace. In *Cyber Conflict (CYCON), 2012 4th International Conference on* (pp. 1-13). IEEE.

Jensen, E. T. (2013). Cyber attacks: Proportionality and precautions in attack. Int'l L. Stud. Ser. US Naval War Col., 89, i.

Jensen, E. T. (2013). Cyber attacks: Proportionality and precautions in attack. Int'l L. Stud. Ser. US Naval War Col., 89, i.

Kodar, Erki (2013). "Applying the Law of Armed Conflict to Cyber Attacks : From the Martens Clause to Additional Protocol 1", ENDC Proceedings, Vol 15, 107-132.

Libicki C. Martin (2009) Cyber deterrence and Cyber war, at: http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf

Lee, D(2013) "China Dismisses U.S. Accusations of Cyber-Spying", Los Angeles Times, May 7, 2013 http://articles.latimes.com/2013/may/07/world/la-fg-wn-china-uscyber-spying-20130507 .

Lewis, James A., "Multilateral Agreements to Constrain Cyber Conflicts", Arms Control Today.

Lobel, H. (2012). Cyber war inc.: The law of war implications of the private sector's role in cyber conflict. *Tex. Int'l LJ*, *47*, 617.

Markoff, John & Kramer, Andrew E.(2010), "U.S., Russia Disagree on Need for Cyber Treaty" , The New York Times, June 28, 2009 cited in:

Reverson, Derek S. (2012), Cyberspace and national security: threats, opportunities, and power in a virtual world, USA, Georgetown University Press.

Responsibility of state for internationally wrongful acts article, 2001: 30-35

Responsibility of state for internationally wrongful acts وarticle 30-31.(2001).

Roscini, Marco (2014), Cyber Operations and the Use of Force in International Law, first Edition, USA, Oxford University Press.

Schreier, Fred (2015), On Cyberwarfare, DCAF Horizon 2015 Working Paper No. 7.

Spinello, Richard A. (2014), Cyberethics: Morality and Law in Cyberspace, fifth edition, USA, Jones & Bartlett Learning

Saxon, Dan (2013), International Humanitarian Law and the changing technology of war, Netherlands, Koninklijke Brill NV.

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

Sanger E. David (2015), Document Reveals Growth of Cyberwarfare between the U.S. and Iran, at: http://www.nytimes.com

Shakarian, Paulo; Shakarian, Jana & Ruef, Andrew (2013), Introduction to Cyber warfare: A Multidisciplinary Approach, USA, Elsevier.

Tsagourias, Nicholas & Buchan Russell (2015), Research Handbook on International Law and Cyberspace, UK, Edward Elgar Publishing Limited.

Weller, Marc (2015), The Oxford Handbook of the Use of Force in International Law, first Edition, UK, Oxford University Press.

C-Theses

Saberi Tilki, Moazameh (2014). Cyberattacks on Iran's Nuclear Facilities from the Perspective of International Law (Stuxnet Virus), Master's thesis, Pardis, University of Gilan.