Does International Human Rights Law impose constraints on digital manipulation or other cyberwarfare ruses?

Analysis of the Stuxnet Worm Attack on Iranian Nuclear Facilities

Author: Alesia Zhuk

Supervisor: Prof. Matthias Hartwig

Educational Institution: Heidelberg University, University of Chile

15.03.2017

PREFACE

The thesis "Does International Human Rights Law impose constraints on digital manipulation or other cyberwarfare ruses?" has been written to fulfill the requirements of the Master's Degree in International Law (LL.M.) International law, Investments, Trade and Arbitration offered by the Faculties of Law of the University of Heidelberg and the University of Chile, with the academic support of the Max-Planck Institute for Comparative Public Law and International Law and of the Institute of International Studies of the University of Chile.

The program is organized on a yearly basis. Three terms was offered in Santiago de Chile, at the Heidelberg Center for Latin America. A final one month term was offered in Heidelberg, at the Max-Planck Institute for Comparative Public Law and International Law and the University of Heidelberg.

Several persons have contributed academically and with support to this master thesis. I would like to thank my supervisor for his priceless guidance. I also wish to thank Luís Marcelo Flores Medrano and Sofía Eugenia Deferrari for their support.

To my other colleagues at Heidelberg Center for Latin America: I would like to thank you for your excellent attitude.

Heidelberg, March 15, 2017

Alesia Zhuk

TABLE OF CONTENTS

ABBREVIATIONS

ICRC International Committee of the Red Cross

AP I Additional Protocol I to the Geneva Conventions

US United States

NATO North Atlantic Treaty Organization

LOAC Law of Armed Conflict

IHL International Humanitarian Law

DoS Denial-of-Service Attack

DDoS Distributed Denial-of-Service Attack

SDoS Single-Source Denial-of-Service Attack

PDoS Permanent Denial-of-Service Attack

APDoS Advanced Persistent Denial-of-Service Attack

USB Universal Serial Bus

PLC Programmable Logic Controller

SCADA Supervisory Control and Data Acquisition

ICCPR International Covenant on Civil and Political Rights

EFF Electronic Frontier Foundation

INTRODUCTION

In 2010 a malicious computer worm attacked Iranian nuclear facilities in Natanz. It was the first computer worm that caused physical damage, and because of this, Iran had to suspend its nuclear program approximately for two years. The case caused great concern among the international community and raised the issue of protecting the population. This paper will address the issues of cyber war and its relationship with International Humanitarian Law and International Human Rights Law.

International law provides two legal regimes for the protection of individuals: International Humanitarian Law - during wartime, and International Human Rights Law - during both wartime and peacetime. The main difference between two legal regimes is that humanitarian law protects only those who is not a combatant and does not directly participate in hostilities, i.e. civilians. While human rights law extends its protection to all people without any discrimination. Both international legal regimes are based on such sources of international law as international treaties and custom. While international treaties apply only to parties to the treaty, customary international law applies to all states. Core treaties of International Humanitarian Law represent customary law; moreover, experts of the International Committee of Red Cross have compiled all norms of customary law in one source. International Human Rights Law does not have a single source of customary law. Certain customary laws are contained in the Universal Declaration of Human Rights, International Covenant on Civil and Political Rights and International Covenant on Economic, Social and Cultural Rights. In this way, people enjoy the protection of custom and international treaties that are binding on their state.

Both legal regimes seem to be similar in view of the fact that they are aiming to protect people, however, such significant differences in object of protection, legal norms, and circumstances when regime is applied, make it important to distinguish which regime is applied.

Cyberwar is a relatively new concept within the framework of international law. It causes debate both about its nature and about the basic definitions, for example, what is cyber space, what is cyber attack. Nevertheless, cyberwar has a huge impact on people, invading their private space and even causing physical damage. In this regard, it seems necessary to determine whether a cyber warfare falls under any of the legal regimes and, if so, which rules of law are applicable.

If cyberwar is a war in its conventional sense, then the rules of humanitarian law should be applied. This means that individuals who are civilians will be protected in most cases from cyber attacks. This protection extends to both the individual and his property. If cyber warfare does not fall under the definition of war or armed conflict, then humanitarian law does not apply, which means that people lose their right to protection. They can be killed, and their property can be destroyed with impunity. However, there is another legal regime - the human rights regime. Customary human rights

law enshrines the right of everyone to life and property, therefore, any arbitrary deprivation of life or property is prohibited. These standards are applied both during the war and in peacetime. Nevertheless, it is not widely recognized that human rights apply to cyber warfare. Thus, one of the main problems is the existence of a debate concerning the cyber war.

Despite the fact that there are different opinions about the application of the norms of humanitarian law and human rights to the situation of cyber war, in this paper we will hold the opinion that both regimes apply to cyber war, because modern cyber attacks are almost identical with kinetic attacks: they can kill, wound or destroy, and because many international instruments state that human rights apply in real and cyber spaces.

In this paper we would like to consider norms that could be applied in both regimes to the situation of cyber war. International humanitarian law, for example, has a relatively large number of principles that protect civilians among which two core principles are the principle of military necessity and humanity. The principle of military necessity includes three other principles: distinction, discrimination and proportionality. The principle of humanity is divided in human treatment and prohibition against the infliction of unnecessary suffering. Humanitarian law also provides for the protection of civilians the principle of neutrality and prohibition of perfidy.

However, the question of what human rights standards are applicable to the situation of cyber warfare is more complicated. If in the case of humanitarian law we can apply the principle of analogy, since cyber attack is a type of armed attack, in the case of human rights analogy is not applicable because cyber war is an absolutely new concept. To cyber attack cannot apply the same human rights that apply to an armed attack, because they affect different rights and freedoms. Cyber attack as a type of armed attack affects the so-called “digital rights” or Internet-related rights. The issue is absolutely new and consequently controversial. In this regard, before considering which human rights are applied and possibly violated in cyber war, we will consider how cyber war and humanitarian law interact.

First, we will consider what types of weapons are used in cyberwar. The main ones are malicious programs or malware and digital manipulation tools. The main malicious programs are viruses, worms, and Trojan horses. This type of malware penetrates into computer devices, systems or networks to collect information, to send information to the attacker, to provide access of the infected system to the attacker and for the suspension of operation of the infected system. Malicious programs can even destroy not only the internal processes of the computer system, but also cause physical damage to the computer itself. There are other methods and tactics of cyber attack, for example, digital manipulation, denial of service attack, logic bomb, and IP spoofing. If the last three cyber attacks are aimed to disable the computer systems, digital manipulation is aimed more at

spreading false information, which is not prohibited by humanitarian law. However, some authors believe that manipulation is a form of sabotage, and sabotage directed against civilians is a violation of humanitarian law.

Secondly, we will consider how cyber weapons violate the norms of humanitarian law. In particular, we will analyze the Stuxnet worm attack on Iranian nuclear facilities – the first cyber attack that caused physical damage. This case was the starting point for the debate over whether humanitarian law should be applied.

Finally, we will turn to the main issue of this paper whether human rights norms apply to cyber warfare. Since, as already mentioned above, we believe that human rights are always applied during the war and in peacetime, in real space and cyber space, we will determine what human rights and freedoms can be violated during cyber war. Thus, in the line with described theoretical frame, the working hypothesis is determined as follows: International human Rights Law imposes restriction on digital manipulation and other cyber warfare ruses.

Thus, general objectives of the present paper are:

- To determine the scope of protection provided by humanitarian law for civilians in the case of armed conflict.
- To demonstrate that despite the fact that cyber warfare seems to be something new in terms of humanitarian law, it is just a new kind of armed attack. And this implies the application of the norms of humanitarian law.
- To demonstrate various types of cyber weapons and determine how they interact with the norms of humanitarian law.
- To analyze the Stuxnet worm attack on Iranian nuclear facilities in the context of customary humanitarian law principles.
- To discuss whether human rights apply to cyber warfare. And if so what are the applicable norms.

In order to accomplish the operational objectives, different working methodologies will be applied: comparative, descriptive, and a case-study methodology. For the theoretical kind of work, the relevant bibliography will be used, mainly consisting of doctrine and international humanitarian and human rights instruments such as the Geneva Conventions.

This paper is divided into 5 chapters. Chapter I reviews basic customary law principles of humanitarian law. Chapter II examines the notion of cyber space and cyber attack and the relationship between humanitarian law and cyber warfare. Chapter III will provide an overview of cyber weapons. Chapter IV will analyze the Stuxnet worm attack applying the customary rule of humanitarian law.

Chapter V will examine how human right could be applicable to the cyber warfare. In conclusion, we will sum up all of the above.

As a result of this work, we plan to demonstrate that human rights norms are applicable to cyber wars, we will also provide some examples of how a specific norm of human rights can be violated by the cyber attack..

CHAPTER I

BASIC PRINCIPLES ON INTERNATIONAL HUMANITARIAN LAW FOR THE PROTECTION OF CIVILIANS

International Humanitarian Law provides certain level of protection for civilians. In accordance with the Geneva Law, combatants must direct their operations only against military objectives because "civilians enjoy a general protection against danger and attacks unless they participate directly in hostilities".[1] However, damaging or destroying them is permitted if it might lead to military advantage.[2] It is not always clear whether civilians can rely on any protection especially when it comes to conflict classification. Even if humanitarian law applies still there are questions under discussion with respect to whether a particular action is a violation of the law of war. In which cases civilians may be eligible for protection and then in such cases what rules are applicable?

In this chapter, for the protection of civilians, we chose the basic rules of humanitarian law, i.e. customary rules that apply to all states regardless of whether the state has signed certain conventions. We will begin with the introduction to customary international law, then we will discuss a core principle of military necessity, and then we will focus on three other principles that contribute to the fulfillment of the last one: distinction, discrimination and proportionality. The principle of humanity is the second core principle that includes the principle of human treatment and prohibition against the infliction of unnecessary suffering. Then we will look at the principle of neutrality, which has no direct relation to the civilians of belligerents, but which nevertheless has great impact on protection of neutral state's citizens. Finally, we will consider the principle of the prohibition of perfidy.

Customary international law

International humanitarian law as a branch of public international law is governed by the traditional sources contained in Article 38 of the Statute of the International Court of Justice. Article

[1] Article 51, 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 13, Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II) 8 June 1977.
[2] Jimena M. Conde Jiminián, "The Principle of Distinction in Virtual War: Restraints and Precautionary Measures under International Humanitarian Law," *Tilburg Law Review* 15, no. 1 (2010): 81.

38 contains "authoritative but incomplete listing of the sources of international legal obligation"[3], among which primary sources are international treaties and custom. While international treaties oblige only the parties to the agreement, custom is binding for all states. However, treaties may form an important material source if they reflect customary law.[4] Article 38 (b) gives the following definition of international custom: "evidence of a general practice accepted as a law". Thus, international custom has two criteria to be met state practice and *opinion iuris*.

State practice does not imply practice of all states, even a "complete consistency is not required"[5]. In the North Sea Continental Shelf cases the International Court of Justice (the Court) noted that state practice, "including that of states whose interests are specially affected", had to be "both extensive and virtually uniform in the sense of the provision invoked".[6] In this way, it means that the practice of states, whose interest are involved, should be extensive and uniform. However, the absence of practice does not always mean that the custom does not apply. Moreover, the absence of a reaction to the practice of customs means the acceptance of the practice and the custom. In the Nicaragua v. United States case the Court emphasized that "the conduct of states should, in general, be consistent with such rules, and that instances of state conduct inconsistent with a given rule should generally have been treated as breaches of that rule, not as indications of the recognition of a new rule".[7] Therefore, in order to avoid be bound by customary law, a state should protest against the rule of customary law in the period of its formation, i.e. to be a persistent objector.

In the Nicaragua case the Court stated that "for a new customary rule to be formed, not only must the acts concern 'amount to a settled practice', but they must be accompanied by the *opinio juris sive necessitatis*. Either the States taking such action or other States in a position to react to it, must have behaved so that their conduct is 'evidence of a belief that this practice is rendered obligatory by the existence of a rule of law requiring it. The need for such a belief, i.e., the existence of a subjective element, is implicit in the very notion of the *opinio juris sive necessitatis*'".[8] Thus, the term "accepted as a law" means that the states regardless of their participation in custom practice formation should believe that the practice is a reflection of existing law.

A distinctive feature of customary law is the fact that in most cases it is not codified and in order to apply customary rules it is necessary to prove their existence. Norms of customary law

[3] Terry D. Gill and Dieter Fleck, *The handbook of the international law of military operations*, 2nd ed. (Oxford, United Kingdom: Oxford University Press, 2011). 10.
[4] James Crawford, *Brownlie's principles of public international law*, 8th ed. (Oxford, United Kingdom: Oxford University Press, 2012). 22.
[5] Ibid., 26.
[6] North Sea Continental Shelf, "Case ICJ Reports 1969," *41 ILR* (1969): 43.
[7] Nicaragua v. United States, "case ICJ Reports 1986," *76 ILR* (1986): 98.
[8] Ibid., 14; North Sea Continental Shelf, "Case ICJ Reports 1969," 6.

applicable to armed conflicts are mostly codified in the ICRC investigation on customary international law[9] and some of them in international treaties. In order to consider the norms, we will apply both of them.

Military necessity

International Humanitarian Law in its protection of civilians is based on two basic principles: military necessity and humanity.[10] The principle of military necessity was first mentioned in the St. Petersburg Declaration of 1868 where in the Preamble were stated that "the only legitimate object which States should endeavour to accomplish during war is to weaken the military forces of the enemy".

During the armed conflict the principle could be applicable in two different ways and the first one is for justifying certain acts of violence[11]. For example, applying the same principle to the situation of armed attack we could say that such measure should be described as necessary[12] or "indispensable for securing the ends of the war[13], and which are lawful[14] according to the modern law and usages of war"[15]. The use of such force should be aimed at "the complete submission of the enemy with the least possible expenditure of time[16], life[17], and money[18"19]. The second one is the

[9] Jean-Marie Henckaerts, Louise Doswald-Beck, and Carolin Alvermann, *Customary international humanitarian law*, vol. 1 (Cambridge: Cambridge University Press, 2005).

[10] Jeremy Richmond, "Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?," *Fordham International Law Journal* 35, no. 3 (2012): 891.

[11] Francoise Bouchet-Saulnier, *The practical guide to humanitarian law*, trans. Laura Brav and Camille Michel, Third ed. (Maryland: Rowman & Littlefield Publishers, 2014). 396; D.M. Drew, "Air Force Manual: Basic Aerospace Doctrine Of The United States Air Force. Volume I," (Washington: Department of the Air Force, 1992), 46.

[12] Office of the Chief of Staff War Department, *Basic Field manual: Rules of Land Warfare* (Washington1914). 9-11."A belligerent is justified in applying any amount and any kind of force which is necessary for the purpose of the war".

[13] UK Manual, "Joint service manual of the law of armed conflict," ed. UK Ministry of Defence (2004); NATO, "Glossary of Terms and Definitions," (APP-06, 2009). "successful conclusion of a military operation". FM 27 - 10 War Department Field Manual, "Basic Field manual: Rules of Land Warfare," (Washington1940). (Change No. 1 1976); War Department, *Basic Field manual: Rules of Land Warfare*. "The complete submission of the enemy"

[14] UK Manual, "Joint service manual of the law of armed conflict." "Not forbidden by the laws of war".

[15] The Lieber Code of April 24, 1863.

[16] FM 27 - 10 Department of the Army Field Manual, "The Law of Land Warfare," (Washington1956). *"As soon as possible"*. UK Manual, "Joint service manual of the law of armed conflict." *"At the earliest possible moment"*.

[17] UK Manual, "The Law of War on Land, Being Part III of the Manual of Military Law," (London: Her Majesty's Stationery Office, 1958).¶ *"men"*. UK Manual, "Joint service manual of the law of armed conflict." "*With the minimum expenditure of life*".

[18] UK Manual, "Joint service manual of the law of armed conflict." *"Resources"*. UK Manual, "The Law of War on Land, Being Part III of the Manual of Military Law." *"resources and money"*.

[19] War Department Field Manual, "Basic Field manual: Rules of Land Warfare." 4a Morris Greenspan, *The Modern Law of Land Warfare* (Berkeley: University of California Press, 1959). MODERN LAW OF LAND WARFARE 313-14.

application of the principle for the prohibition of acts of violence. Here we could not say directly that the principle prohibits certain measures since both the principle of military necessity and the principle of humanity are "abstract in nature"[20] and their application is based on the law of war principles such as the principle of distinction and proportionality from one side, but from the other human treatment and the prohibition against the infliction of unnecessary suffering respectively.[21] Thus, any sort of violence such as destroying and seizing people and property or any other alternative means of subduing the enemy[22] or other incidental harm[23] on the part of the belligerents which could be described as unnecessary, disproportionate, indiscriminate or aiming at spreading terror among the civilian population[24] would be considered as a violation of the principle of military necessity. Such infringements cannot be justified and are punishable by the law of war rules.

Distinction

The principle of distinction is the fundamental principle of humanitarian law[25] which states that "the parties to the conflict must at all times distinguish between civilians and combatants"[26]. The same principle prohibits direct attacks against civilians. It means that all civilians should be protected in any time and from any armed attack whether it is an attack aimed at weakening the enemy forces or aimed directly at civilians. The principle of distinction is applicable to all states regardless of whether they are parties to the Geneva Conventions since the rule is a norm of customary international law[27]. It was firstly established in the St. Petersburg Declaration[28] and then in Additional Protocol I[29]

[20] Richmond, "Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?," 872.
[21] Ibid.
[22] Drew, "Air Force Manual: Basic Aerospace Doctrine Of The United States Air Force. Volume I," 53.
[23] Article 15 of the Lieber Code of April 24, 1863 and United States v. List, *et al.* (The Hostage Case) United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran).
[24] Bouchet-Saulnier, *The practical guide to humanitarian law*: 369.
[25] Article 22 of the 1863 Lieber Code, Article 1 of the 1880 Oxford Manual, Article 1 of the 1880 Oxford Manual, Section 5.1 of the 1999 UN Secretary-General's Bulletin, UN General Assembly, Res. 2444 (XXIII), 19 December 1968, § 1(c), UN General Assembly, Res. 2675 (XXV), 9 December 1970, § 2, UN General Assembly, Res. 2673 (XXV), 9 December 1970, preamble, ICJ, Nuclear Weapons case, Advisory Opinion, 8 July 1996, §§ 78–79, ICTY, Blaˇski.c case, Judgement, 3 March 2000, § 180, ICTY, Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia, The Hague, 14 June 2000, § 29, IACiHR, Case 11.137 (Argentina), Report, 18 November 1997, § 177. QUE?
[26] Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary international humanitarian law*, vol. 1 (Cambridge: Cambridge University Press, International Committee of the Red Cross, 2005). Rule 1.
[27] Ibid.
[28] St. Petersburg Declaration, preamble The Saint Petersburg Declaration of 1868 or in full Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight.
[29] Article 48, Additional Protocol I to the Geneva Conventions, 1977.

and in Additional protocol II[30] to the Geneva Conventions, thus, it allowed applying the norm to both international and non-international armed conflicts.

Article 48 of Additional Protocol I establishes two types of obligations for the belligerent parties. First, "parties to [a] conflict shall at all times distinguish between civilian population and combatants" and correspondingly between civilian and military objectives, and secondly, parties "shall direct their operations only against military objectives". Thus, according to the principle civilians and civilian objects are protected against direct attack during the armed conflict.

To begin with, a person should be a civilian. The definition of a civilian contains in Additional Protocol I[31]. Further, civilians should belong to the side of the enemy, they should be on land, at sea and in the air and last there should be attack regardless of offensive or defensive.

As stated in the definition of a civilian, "civilian" is a person who is not a combatant, thus, when civilian becomes a combatant it loses the right to protection. Definition of combatant provides a number of criteria which vary depending on whether the conflict is international or non-international. Nevertheless, a number of international instruments enshrine a broader range of requirements to qualify for the right to protection: civilians should not "directly participate in hostilities"[32]. As stated above, there is other possibility for state to cause harm to civilians without bearing responsibility and it is a case of collateral damage. The concept of damage which could be caused "beyond the intended objectives of an attack on a target"[33] is closely related to the principle of proportionality which we will discuss below.

The distinction must also be made between civilian and military objectives. The definition of civilian objects is carried out in the same way as the definition of civilians, namely by contradiction: civilian objects are "all objects that are not military objective"[34]. Civilian objects are generally protected against direct attack of the enemy "unless and for such time as they are military objectives"[35]. As soon as a civilian object begins to be used for military purposes, or it is determined that it is necessary to achieve a military advantage, the right to protection against direct attack is voided. Such protection may seem to be ineffective due to the fact that the concept of military advantage is quite uncertain. However, taking into account the concept as it was determined by the

[30] Article 48, 51(2), 52 (2) of Additional Protocol I to the Geneva Conventions, 1977.
[31] Article 50 of Additional Protocol I to the Geneva Conventions, 1977.
[32]Henckaerts and Doswald-Beck, *Customary international humanitarian law*, 1.Rule 5
[33] Article 15 of Additional Protocol I to the Geneva Conventions, 1977.
[34] Henckaerts and Doswald-Beck, *Customary international humanitarian law*, 1.Rule 9), Additional Protocol I, Article 52(1), Amended Protocol II to the CCW, Article 2(7).
[35] Ibid. Rule 10.

law[36] "military advantage" means overall advantage[37] for the entire war and not the advantage for particular military operation.[38] It means that the main objective and the main purpose of any military operation or attack should is to "terminate conflicts swiftly with a minimum loss of life"[39]. Quoting the Lieber Code "The more vigorously wars are pursued, the better it is for humanity"[40].

Discrimination

The principle of discrimination is one of the core principles of humanitarian law embodied in the article 51 (4) of Additional Protocol I, in the article 3(8) of the Amended Protocol II to the CCW and in the article 3(3) of the Protocol II to the CCW where stated that states during conduct of military operations must (a) target their attacks only against military objectives and (b) only by means and methods which can be directed at a specific military objective[41] (c) the effects of which can be limited. The principle of discrimination is similar to the principle of distinction since both of them oblige state to differentiate between targets during the conduct of hostilities. However, the principle of distinction directly imposes the obligation to distinguish between civilians and combatants, while the principle of discrimination goes further requires a certain level of selectivity in the choice of target and means and methods.

Thus, taking into account all of the above it can be concluded that while performing an armed attack belligerent must direct it only against military objectives of other belligerent and only if it is convinced that the consequences of such attack will not be non-discriminatory. Some armed attacks are specifically designed for compliance with such principle in view of the fact that their effects predictable with a high probability, however, we should not exclude completely the opposite result. For example with a dual-use facilities such as power plants which can also be a target of attack, if its destruction would give definite military advantage.[42] However, any sort of damage caused to such installations could trigger a chain reaction, for example, attack on a water power plant may result in flooding of nearby civilian objects and then it would be a so-called "knock-on effect". Knock-on

[36] Rules concerning the Control of Wireless Telegraphy in Time of War and Air Warfare. Drafted by a Commission of Jurists at the Hague, December 1922 Art. 24 (1).
[37] The Rome Statute of the International Criminal Court of 1998, Article 8(2) (b)(iv).
[38] Drew, "Air Force Manual: Basic Aerospace Doctrine Of The United States Air Force. Volume I," 57.
[39] Department of Defense, National Military Strategy of the United States, 10 (Jan. 1992).
[40] Article 40, the Lieber Code.
[41] ICTY, Marti ´c case, Review of the Indictment. The Trial Chamber judgment of June 2007 and the Appeals Judgment of October 2008 by the International Criminal Tribunal for the former Yugoslavia (ICTY) in the case of the Prosecutor v. Milan Martić (IT-95-11).
[42] Richmond, "Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?," 875.

effects are those that lead to unexpected consequences of an armed attack.[43] But in the present case the cause of damage is not the core circumstance, the responsibility of commander or any other responsible for the attack person will completely depends on whether he or she has taken sufficient precaution measures. The obligation of take precautions is also the basic principle of humanitarian law and will be discussed below.

To conclude, the principle of discrimination represents by itself implementation both the principle of distinction[44] and consequently the principle of military necessity.

Proportionality

The principle of proportionality prohibits attacks that could cause excessive damage to civilians in relation to the concrete and direct military advantage which is expected. Moreover, humanitarian law prohibits launching such an attack even it is only anticipated that incidental damage could occur. This rule is recognized as customary norm.[45] Thereby, at the stage of operation planning responsible people such as commander must analyze all possible variations of attack outcome taking into account available information at that moment.[46] And if the number of civilian victims is disproportionate to gained military advantage then such an attack would be a violation of the principle of proportionality.

Based on foregoing, we could assume that the possibility of collateral damage could not be considered as violation of humanitarian law only if death, damage or injury of civilian population were proportional to a concrete and direct military advantage.

The principle is codified in Additional Protocol I[47] and it is applicable to both international and non-international armed conflict although it is not contained in Additional Protocol II to the Geneva Conventions, however, it is mentioned in the Amended Protocol II and the Protocol II to the Convention on Certain Conventional Weapons[48] and in both Nicaragua[49] and Nuclear Weapon cases

[43] Eric Talbot Jensen, "Unexpected consequences from knock-on effects: a different standard for computer network operations?," *American University International Law Review* 18, no. 5 (2003): 1150.
[44] Henckaerts and Doswald-Beck, *Customary international humanitarian law*, 1: 43.
[45] Ibid. Rule 14.
[46] Ibid., 50.
[47] Article 51(5)(b), Article 57(2)(a)(iii), Additional protocol I to the Geneva Conventions, of 12 August 1949.
[48] Protocol II to the CCW, Article 3(3); Protocol II to the Convention on Certain Conventional Weapons Amended Protocol II to the CCW, Article 3(8) Amended Protocol II to the Convention on Certain Conventional Weapons.
[49] Bouchet-Saulnier, *The practical guide to humanitarian law*: 14.para 176.

of the International Court of Justice[50]. Moreover, International Criminal Court in its Statute has determined non-application of the principle of proportionality as a war crime.[51]

Concrete and direct military advantage in accordance with the Commentary to Additional Protocols means "substantial and relatively close, and that advantages which are hardly perceptible and those which would only appear in the long term should be disregarded"[52].

There is assumption[53] that modern means and methods of warfare could cause minimum collective damage or almost zero due to the fact that most of the attacks carried out against the specific target. Nevertheless, we should not exclude the possibility of causing unintentional damage to civilians. For instance, the attack on nuclear power plant evidently could provoke serious damage to the civilian population as a result of uncontrollable nuclear forces. Moreover, we should not exclude the possibility of collateral damage in respect of staff-members, for example, computers maintenance engineers, electricians or plumbers, who are not involved in the conduct of hostilities but who are vital for the maintenance of the power plant system. In fact, any person may become a victim of an attack just by being close to a military facility.[54]

Precautions

In the case when the commander after weighing all available information make a decision about the attack on the basis of military necessity, he or she is faced with the obligation to take all feasible precautions in order to mitigate or to avoid civilian losses. The principle of precautions also derives from the norm of customary international law[55] and it is applicable for both types of armed conflict. The duty for belligerent parties to take all feasible measures is established in article 58 (c) of the Additional Protocol I and in the article 8 of the Second Protocol to the Hague Convention for the Protection of Cultural Property. Moreover, International Court of Justice in its decision recognized the nature of this obligation as customary rule due to the fact that "it specified and fleshed out general pre-existing norms"[56]. In its investigation on customary international law ICRC gives an example of

[50] ICJ, Nuclear Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion.
[51] The Rome Statute of the International Criminal Court of 1998, Article 8(2)(b)(iv).
[52] Claude Pilloud et al., *Commentary on the additional protocols: of 8 June 1977 to the Geneva Conventions of 12 August 1949*, ed. Yves Sandoz, Christophe Swinarski, and Bruno Zimmermann (Geneva: Martinus Nijhoff Publishers, 1987). 2209.
[53] Jiminián, "The Principle of Distinction in Virtual War: Restraints and Precautionary Measures under International Humanitarian Law."
[54] Yoram Dinstein, "The Principle of Distinction and Cyber War in International Armed Conflicts," *Journal of Conflict and Security Law* 17, no. 2 (2012).
[55] Henckaerts and Doswald-Beck, *Customary international humanitarian law*, 1.Rule 22.
[56] Henckaerts and Doswald-Beck, Customary international humanitarian law, 1: 70.

possible precaution measures such as "the construction of shelters, digging of trenches, distribution of information and warnings, withdrawal of the civilian population to safe places, direction of traffic, guarding of civilian property and the mobilization of civil defense organizations"[57].

The ICRC in its investigation has determined the meaning of "feasible" measure as "practicable or practically possible, taking into account all circumstances ruling at the time, including humanitarian and military considerations"[58].

Some examples or a list of possible feasible precautions is provided by the ICRC Customary Law and the US Air Force Manual[59] where stated that effective advance warning before an attack, adjusting the timing of the attack, identifying "military" zones and choice between several military objectives can be used for the purpose of protecting the civilian population. Thus, in a case where a state is going to attack military objectives of the enemy it must provide warning information in order to the civilian population be kept away from military objectives to avoid collateral damage. It may seem pointless since one of the main tactics of war is unexpected attack. But this practice has already had a number of codifications[60] and it is recognized as a norm of customary international law[61]. However, this principle is not considered necessary to apply in cases where there is no threat to the civilian population or where surprise of the attack is necessary for the effectiveness of a military operation. On the same principle to choose the most suitable time for an attack may help to avoid incidental harm. Apart from the choice of the time, choice of the military objective also seems as an important issue. If the belligerent has the opportunity to select an object for the attack then it should choose the one that will cause the least damage to the civilian population. This rule is set forth in Article 57(3) of Additional Protocol I, in the Article 6 of the Second Protocol to the Hague Convention for the Protection of Cultural Property and it is also the norm of customary law[62], although the United States does not recognize the rule as customary[63]. Nevertheless, US Air Force Manual establishes an obligation for a state to choose such zones for an attack in which military objective are more likely to be expected and civilian object are more likely to be absent.[64] Thus, during the armed attack belligerents must give preferences to the military objectives that may cause the least damage to the

[57] Ibid. 70, Rule 22.
[58] Ibid., 70.
[59] Drew, "Air Force Manual: Basic Aerospace Doctrine Of The United States Air Force. Volume I," 237-40; Henckaerts and Doswald-Beck, *Customary international humanitarian law*, 1: 58.
[60] Lieber Code, Article 19; Brussels Declaration, Article 16 *Project* of an *International Declaration concerning* the *Laws* and *Customs* of *War*. *Brussels*, *27 August 1874*; Oxford Manual, Article 33 *The Laws of War on Land*. Oxford, 9 September *1880*.
[61] Henckaerts and Doswald-Beck, Customary international humanitarian law, 1. Rule 20.
[62] Henckaerts and Doswald-Beck, Customary international humanitarian law, 1. Rule 21.
[63] Henckaerts and Doswald-Beck, Customary international humanitarian law: 67.
[64] Drew, "Air Force Manual: Basic Aerospace Doctrine Of The United States Air Force. Volume I," 240.

civilian population or according to the United States to military objectives only. To date this question becomes very important since the dual-use facilities such as power plants may be attractive targets for attack (as an example, nuclear facilities in Iran).

Listed above examples are not exhaustive. In accordance with the ICRC investigation on customary international law there are other rules that states must apply. First of all, a state must verify that an objective of the attack is military[65], a state must take all feasible precautions in order to avoid or minimize incidental loss of civilian life, injuries or damages to civilian objects[66], must assess the impact of the attack that it would not be excessive to the concrete and direct military advantage anticipated[67], otherwise a state must cancel or suspend an attack[68].

The principle of precautions is closely related with the principle of distinction because it imposes an obligation on the belligerents to avoid locating military objectives near densely populated civilian objects. Thus, both parties to the conflict are under obligations arising from the principles: the attacking State must take precautions before the attack such as the warning the civilian population and the protecting State against which the attack is carried out should protect its civilians by locating military objectives far away from civilian objects.[69] But if after all civilians are located near of military facility anyway they remain under the protection of customary international law, which in this case establishes the obligation for States to move these people out of the war zone.[70] This rule is also application of the principle of distinction.

Humanity

The principle of humanity is aimed to protect civilians against unnecessary suffering, injury and damage to their property. It is codified in the four Geneva Conventions and in the both Additional Protocols[71], it is mentioned in the Martens clause and the principle represents by itself a core principle of humanitarian law and a fundamental principle of the ICRC. Thus, the principle prohibits any sort

[65] Henckaerts and Doswald-Beck, *Customary international humanitarian law*, 1. Rule 16.
[66] Ibid. Rule 17.
[67] Ibid Rule 18.
[68] Ibid Rule 19.
[69] Ibid Rule 23.
[70] Ibid Rule 24.
[71] Article 3, common to the four Geneva Conventions of 1949, Article 12 of the Geneva Convention I, Article 12 of the Geneva Convention II, Article 13 of the Geneva Convention III, Article 27 of the Geneva Convention IV. Article 11 of Additional Protocol I, Article 4 of Additional Protocol II of 1977.

of "violence [that] are not necessary for the overpowering of the opponent"[72] or in other words, the principle is always applied when it is not applied the principle of military necessity. This principle should be applied always when a belligerent party chooses as a target for its attack personal computer of civilian or computer system of civilian object, or when indiscriminate weapons are used.

The principle of humanity is implemented by the two other principles: human treatment and the prohibition against the infliction of unnecessary suffering.[73]

Human treatment

The implementation of the principle of human treatment is expressed by the prohibition of inhuman treatment. Breach of this principle constitutes a serious violation of the Geneva Conventions and the Rome Statute.[74] This rule is also the norm of customary international law[75], it is applicable to both international and non-international armed conflicts and it had a wide practical application in the International Court of Justice[76]. Under the principle all civilian population is protected against any action that could be qualified as "inhuman".

The International Criminal Court has identifies "inhuman treatment" as "severe physical or mental pain or suffering"[77] and the International Criminal Tribunal for the Former Yugoslavia has determined it as "causes serious mental or physical suffering or injury or constitutes a serious attack on human dignity"[78].

Considering the armed attack, it is important to take into account the consequence of the attack rather than the direct effect. Thus, if we imagine a situation where an armed attack was the cause of functioning failure of "hospitals, ambulances, food preparations or similar facilities"[79] such as water

[72] Department of Defense, "Law of War Manual," (Washington: Office of General Counsel, Department of Defense (DoD), 2015), 58.

[73] Richmond, "Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?," 872.

[74] First Geneva Convention, Article 50; Second Geneva Convention, Article 51; Third Geneva Convention, Article 130; Fourth Geneva Convention, Article147; The Rome Statute of the International Criminal Court of 1998, Article 8(2)(a)(ii) and (iii) and (c)(i).

[75] Henckaerts and Doswald-Beck, *Customary international humanitarian law*, 1. Rule 90.

[76] ICJ, Nicaragua case (Merits), Judgement; ICTY, Tadi´c case,SecondAmended Indictment and Judgement, Mrkˇsi ´c case, Initial Indictment, Delali´c case, Judgement, Furundˇ zija case, Judgement, Jelisi ´ccase, Judgement, Kupreˇski´c case, Judgement, Blaˇski´c case, Judgement, Kunarac case, Judgement and Kordicˇ and Cˇ erkez case, Judgement.

[77] Elements of Crimes for the ICC, Definition of inhuman treatment as a war crime (The Rome Statute of the International Criminal Court of 1998, Article 8(2)(a)(ii)).

[78] ICTY, Delali´c case, Judgement and Kordic´ and Cˇ erkez case,Judgement.

[79] Yaroslav Radziwill, *Cyber-Attacks and the Exploitable Imperfections of International Law* (Boston: Brill, 2015). 183-84.

supply network that consequently provoked significant and widespread suffering among the civilian population due to the absence of medical aid, food or water, then we could say that the attack is a primary reason if inhuman treatment.

Prohibition against the infliction of unnecessary suffering

Any means and methods of warfare which cause superfluous injury or unnecessary suffering are prohibited. This is also a norm of customary international law[80] and it is applicable both for international and non-international armed conflict. This rule also has its origins in the St. Petersburg Declaration[81] and other early instruments[82]. The prohibition of unnecessary suffering is contained in such recent legal instruments as the Additional Protocol I, the Convention on Certain Conventional Weapons and its Protocol II and Amended Protocol II.[83] International Court of Justice in Nuclear Weapon case[84] had also reaffirmed that the principle constitute a core basis for international law.

The International Court of Justice in its decision mentioned above had determined the definition of "unnecessary suffering".[85] In accordance with to which any suffering that is greater than it is necessary for archiving legitimate military objectives should be prohibited, since the main purpose of any war is the neutralization of the enemy rather than the infliction of the most serious damage. Thus, as well as in the previous case considering an armed attack without direct effect we cannot say that the attack was harmful in the sense of the principle of humanity. However, the consequences incurred by the attack could be. For example, in the case where death or serious permanent disability is inevitable, such as an attack on nuclear power stations that could be equated to the use of nuclear weapons[86].

Due to the same principle international customary law prohibits the use of weapons which are indiscriminate by its nature.[87] Professor Michael Schmitt in its research mentioned that indiscriminate weapons are prohibited". This prohibition is effective for both types of armed conflict and it is

[80] Henckaerts and Doswald-Beck, *Customary international humanitarian law*, 1. Rule 70.
[81] St. Petersburg Declaration The Saint Petersburg Declaration of 1868 or in full Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight.
[82] Hague Declaration concerning Asphyxiating Gases; Hague Declaration concerning Expanding Bullets; 1899 Hague Regulations, Article 23(e); 1907 Hague Regulations, Article 23(e).
[83] Additional Protocol I, Article 35(2) (adopted by consensus), CCW, preamble; Protocol II to the CCW, Article 6(2); Amended Protocol II to the CCW, Article 3(3).
[84] ICJ, Nuclear Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion.
[85] ICJ, Nuclear Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion.
[86] Henckaerts and Doswald-Beck, *Customary international humanitarian law*, 1: 244.
[87] Ibid. Rule 71.

enshrined in the Additional Protocol I[88], in the Rome Statute[89], in the International Court of Justice decision[90] and in the Amended Protocol II to the Convention on Certain Conventional Weapons[91].

Neutrality

International Humanitarian Law extends the scope of protection not only to persons belonging to the belligerent parties, but also to those who are not involved in military conflict, namely, the neutral states and their citizens. The principle of neutrality that protects states that are not involved in armed conflict from the attack take its origins from customary international law and it set forth in the Hague Conventions V[92] and XIII[93] which represent a customary law[94], in the San Remo Manual[95] and in the Handbook[96] and other instruments[97]. The concept of neutrality is also used in all Geneva Conventions and in Additional Protocol I. Moreover, the International Court of Justice in both its decision[98] has recognized the rule as a norm of customary international law. But we have to mention that in comparison with other principles this is applicable only to international conflicts.

The principle of neutrality provides absolute protection to the territory and sovereignty of neutral states by means of Article 1 of the Hague Conventions. It means that penetration into neutral territory of belligerent parties with military purposes is prohibited. The concept of "territory" should be interpreted broadly, i.e. it includes the territory, as well as all objects located in the area, regardless

[88] Additional Protocol I, Article 51(4).

[89] The Rome Statute of the International Criminal Court of 1998, Article 8(2)(b)(xx).

[90] ICJ, Nuclear Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion.

[91] Amended Protocol II to the CCW, Article 1(2).

[92] Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land,The Hague, 18 October 1907, 2 AJIL Supp. 117-127 (1908), art. 8.

[93] Convention (XIII) Concerning the Rights and Duties of Neutral in Naval War, The Hague, 18 October1907, 2 AJIL Supp. 202-216 (1908), supra note 24.

[94] Marco Roscini, *Cyber operations and the use of force in international law* (Oxford: Oxford University Press, 2014). 248.

[95] ICRC, "San Remo Manual on International Law Applicable to Armed Conflicts at Sea," ed. Louise Doswald-Beck (Cambridge: International Committee of the Red Cross (ICRC), 1994).

[96] Alan Cole, *Rules of engagement handbook* (International Institute of Humanitarian Law, 2009).

[97] UN General Assembly Resolution 58/80 of 1995, ILA, Helsinki Principles on the Law of Maritime Neutrality, ILA Report of the Sixty-Eighth Conference, at 497 et seq. (London 1998).10 Program on Humanitarian Policy and Confl ict Research at Harvard University, Manual on International Law Applicable to Air and Missile Warfare, Section X (Bern 2009), Schmitt, *Tallinn manual on the international law applicable to cyber warfare : prepared by the international group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence.* Rule 91-95.

[98] ICJ, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 8 July 1996, 226. ICJ, Case concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America), Merits, Judgment, 27 June 1986, 14.

of the nationality of their owners.[99] Thus, for example, Article 3 of Hague V prohibits the use of "apparatus for the purpose of communicating with belligerent forces" or "any installations of this kind" in the territory of neutral state with military purpose. In case if a belligerent party will use a computer system of a neutral state in order to send a virus to the enemy it will constitute the violation of the Article 1 since computer are also a part of territory of the neutral state and they are under its jurisdiction.

Moreover, if a belligerent party by means of a person which is within the boundaries of neutral state will try to realize computer strike then it will constitute a violation of two articles: Article 1 and Article 2 of the Hague V. Last prohibits any movement of "troops or convoys of either munitions of war or supplies across the territory of a neutral Power". Among scholars there are two opposing points of view as to whether this provision applies to openly accessible networks. Some argue that this rule does not extend to the uses of the Internet. For example, if a State will send a worm or a virus by means of infrastructure or a platform located in a neutral State to the other belligerent State, then it will not constitute a violation.[100] However, from the other side some scholars as Kelsey argue that "the use of the Internet to conduct cross-border armed attacks violates the principle of neutrality"[101]. After analyzing both situations we would rather agree with the second statement due to the fact that to make an armed attack by means of network a state probably will send it across the Internet nodes of a neutral state, thereby, the attack would fall under the jurisdiction of that State and thus it would violate the right of a neutral State to exercise sovereignty over its infrastructure.[102]

Absolute protection of the territory of the neutral state is also reflected in the rule that "the neutral states must not be affected by collateral effects of hostilities"[103]. For example, if one belligerent party exercising the armed attack against other belligerent caused a damage to neutral state then this attacking state must bear responsibility. Any attack that could cause damage to property, death or injury of persons or just loss of functionality of infrastructure[104] to the neutral state are prohibited. Moreover a belligerent state must not conduct the attack against any other state if such an attack could cause "prejudicial incidental effects on neutral territory"[105]. This question is particularly

---

[99] Eric Talbot Jensen, "Sovereignty and neutrality in cyber conflict," *Fordham International Law Journal* 35(2012).
[100] Ibid., 825.
[101] Jeffrey T. G. Kelsey, "Hacking into international humanitarian law: The principles of distinction and neutrality in the age of cyber warfare," *Michigan Law Review* 1006(2008): 1443.
[102] Michael N. Schmitt, *Tallinn manual on the international law applicable to cyber warfare : prepared by the international group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence.* (Cambridge New York: Cambridge University Press, 2013). Rule 91.
[103] Gill and Fleck, *The handbook of the international law of military operations*: 560.
[104] Roscini, *Cyber operations and the use of force in international law*: 262.
[105] Ibid., 263.

important when the attack is directed against computer systems since the computer infrastructure of various states can be interconnected. For example, the attack against the Iranian nuclear facilities has affected such countries as Azerbaijan, India, Indonesia, Pakistan, United States, and others.[106]

Prohibition of perfidy

International Humanitarian Law prohibits the use of perfidy with the aim of killing, injuring or capturing the enemy. This norm constitute a customary international law[107] and it set forth in Additional Protocol I, the Roman Statute, the Lieber Code, the Brussels Declaration, the Oxford Manual, the Hague Regulations and in the Tallinn Manual.[108] It is applicable to both international and non-international armed conflict. Additional Protocol I in Article 37 (1) determines "perfidy" as "acts inviting the confidence of an adversary to lead him to believe that he is entitled to, or obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence".[109] For example, the use of e-mail with protected or well-recognized domain as "president-of-the-republic-x" (AP I 39), "icrc.com", "un.org" (AP I 37 (d), 38) describing the desire to surrender (AP I 37 (a)), to provide humanitarian aid or assistance or to gain access to the immunities will constitute a violation[110] of the humanitarian law if its real purpose was to send a virus that killed or injured persons. Hypothetically this principle is important in case if someone from the civilians will be killed or injured as a result of collateral damage. The principle of distinction in this case allows the death of civilians, but the prohibition of perfidy strictly prohibits the same thing and thus creates a higher level of civilian protection. Such a conclusion seems logical if we undertake to assert that the use of the domain should be equated with the use of a distinctive or protective emblem. However, there is a debate about this issue. Some argue that only an electronic reproduction of the emblem is a violation of humanitarian law.[111] Thus, the use of the domain "icrc.com" will not

[106] Nicolas Falliere, Liam O Murchu, and Eric Chien, "W32.Stuxnet Dossier," (Cupertino: Symantec. Security Response, 2011), 5-6.
[107] Henckaerts, Doswald-Beck, and Alvermann, *Customary international humanitarian law*, 1. Rule 65.
[108] Additional Protocol I, Article 37(1), The Rome Statute of the International Criminal Court of 1998, Article 8(2)(e)(ix), Lieber Code, Article 101, Brussels Declaration, Article 13(b), OxfordManual, Article 8(b), Hague Regulations, Article 23(b)., Rule 60 Tallinn Manual 2013.
[109] See also Elements of Crimes for the ICC, Definition of killing or wounding treacherously individuals belonging to the hostile nation or army/a combatant adversary as a war crime (The Rome Statute of the International Criminal Court of 1998, Article 8(2)(b)(xi) and (e)(ix)).
[110] Jenny Döge, "Cyber Warfare Challenges for the Applicability of the Traditional Laws of War Regime," in *Archiv des Völkerrechts*, ed. Mohr Siebeck (2010), 798.
[111] Schmitt, *Tallinn manual on the international law applicable to cyber warfare : prepared by the international group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence.* Rule 62.6.

constitute a violation. Another group of experts on the other hand expressed their opposite view arguing that the rule should be interpreted in a broader sense and it should be applied in this case.[112] In our opinion the last statement seems more reasonable due to the fact that both false emblem and the false domain are aimed at misleading the enemy. In this particular case the intention of belligerent party seems more important than the performance of the attack. Tallinn Manual[113] establishes that the prohibition of perfidy includes fourth elements: an act inviting particular confidence of the adversary, intent to betray this confidence, the specific protection granted by international law and the death or injury of individuals. Since receiving an e-mail adversary party relies on the emblem and the belligerent expects it because the emblem provides protection for the particular person or a subject and as a consequence of this trust the adversary party becomes a victim of the attack.

On the same principle it is prohibited to mark military web-sites as civilian aiming to deceive the enemy and kill him or her or injure. However, there is no obligation to mark information technology facilities whether they are military or civilian.[114] Similarly humanitarian law does not require to open the identity of the originator of the attack.[115] If unidentified e-mail cause an injury to the adversary party then they have no right to demand their rights. It will be permissible military ruse.

[112] Ibid. Rule 62.7.
[113] Ibid. Rule 62.3.
[114] Ibid. Rule 60.12.
[115] Ibid. Rule 60.13.

CHAPTER II

THE CONCEPT OF CYBER WARFARE ATTACK AND INTERNATIONAL HUMANITARIAN LAW

The application of the above-mentioned in Chapter I principles of international law for protection of civilians and civilian objects depends entirely on whether International Humanitarian Law applies. International Humanitarian Law applies only to the situation of armed conflict regardless international or non-international. Thus, to apply the principles of international law to the situation of cyber warfare it is necessary in the traditional sense to have a war. Conducting military operations carried out by armed attacks, in this regard, the question arises whether a cyber warfare attack is an armed attack. Neither in international law nor in the doctrine there is no consensus on this issue. Some authors believe that International Humanitarian Law is not applicable to the situation of cyber warfare. Other authors in contrary argue that International Humanitarian Law is completely applicable to the situation of cyber warfare. In addition, if in the last case where humanitarian law is applied everything is clear - that civilians are protected by the principles of international law, in the first case it is not clear to what extent civilians can expect protection and can they?

In this Chapter we would like to determine the definition of the "cyber space" and "cyber attack" which are the core concepts and then to highlight two main points of view on the possibility of the application of humanitarian law.

The definition of cyber space

In order to determine what "cyber attack" is it is necessary to define what "cyber space" is. There is no commonly accepted definition, however, The US Department of Defense defines it as a "'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".[116] This definition together with the other definitions uses in his article Major Arie J. Schaap[117], he also appeals to the definition of

[116] Joint Chiefs of Staff, "Joint Publication 3-13. Information Operations," (United States of America: Armed Forces of the United States, 2012).

[117] Arie J. Major Schaap, "Cyber warfare operations: Development and use under international law," *Air Force Law Review* 64(2009): 125.

Thomas Wingfield[118], "cyber space is not a physical space - it defies measurement in any physical dimension or time space continuum. It is a shorthand term that refers to the environment created by the confluence of cooperative networks of computers, information systems, and telecommunication infrastructures commonly referred to as the World Wide Web". He also provides the definition of a 2001 Congressional Research Service Report for Congress, where cyber space is a "total interconnectedness of human beings through computers and telecommunication of human beings through computers and telecommunication without regard to physical geography".[119] However, the author concedes preference to the last definition of the National Military Strategy for Cyberspace Operations where cyber space is "domains characterized by the use of [computers and other electronic devices] to store, modify, and exchange data via networked systems and associated physical infrastructures".[120]

Lesley Swanson uses the definition of Michael A. Sinks who defines "cyber space" as "the sum of electronic networks including, but not limited to, the Internet, where various information operations occur"[121].

2003 National Strategy to Secure Cyberspace defines cyber space as the "nervous system - the control system of the country… composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work".[122]

Marco Mayer defines that "cyberspace is a global and dynamic domain (subject to constant change) characterized by the combined use of electrons and electromagnetic spectrum, whose purpose is to create, store, modify, exchange, share and extract, use, eliminate information and disrupt physical resources".[123]

Thus, "cyber space" represents by itself a domain composed of computer network in order to perform various information operations. Cyber attack is one of the information operations' options.

---

[118] Walter G. Sharp Sr. and Thomas C. Wingfield, *Law of Information Conflict: National Security Law in Cyberspace* (Falls Church, Va.: Aegis Research Corporation, 1999). 17.

[119] Schaap, "Cyber warfare operations: Development and use under international law," 126.

[120] C. Todd Lopez, "Fighting in cyberspace means cyber domain dominance," *U.S. Air Force. Air Force Print News* (2007).

[121] Michael A Sinks, "Cyber warfare and international law" (Doctoral dissertation, Air University, 2008), 307.

[122] The White House, *President George W. Bush: The National Strategy to Secure Cyberspace* (Washington, DC.: Morgan James Publishing, 2003).

[123] Marco Mayer et al., "How would you define Cyberspace?," *First Draft Pisa* 19(2014).

The notion of cyber attack

The main cause of contention in deciding whether the law of armed conflict applies to cyber war is understandings of the concepts of cyber warfare and cyber warfare attack.[124] There is no also generally accepted definition of "cyber attack", therefore, we will try to consider some of them.

According to the definition of Tallinn Manual[125] "cyber attack is a cyber operation, whether offensive or defensive that is reasonably expected to cause injury or death to persons or damage or distraction to objects"[126]. This definition is applicable to both international and non-international armed conflict and based on the Geneva Law[127]. In addition, it does not matter what is the object of attack whether it is data, system or civilian, in any case, the strike that caused direct damage to a person or an object will be an armed attack. In contrast, cyber operation that caused large-scale adverse consequences without any damage will not be considered as an armed attack.[128] However, if such an operation without inflicting direct damage causes collateral damage, in this way the situation will fall under the definition of the cyber attack.

Major Arie J. Schaap in his article uses the term "cyber operations" based on the US definition that determines it as "the use of network-based capabilities of one state to disrupt, deny, degrade, manipulate, or destroy information resident in computers and computer networks, or the computers and networks themselves, of another state".[129] In differs from the first definition is a more narrow focus on international conflict the purpose of which is the destruction or seizure of enemy information.

The US Joint Publication[130] unlike previous two definitions distinguishes three types of cyber attack: computer network attack, computer network defense and computer network exploitation.

---

[124] Cordula Droege, "Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians," *International Review of the Red Cross* 94, no. 886 (2012): 536.

[125] Michael N. Schmitt, *Tallinn manual on the international law applicable to cyber warfare : prepared by the international group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence.* (Cambridge New York: Cambridge University Press, 2013). Rule 30.1.

[126] See also Gary D. Solis, "Cyber warfare," *Military Law Review* 219(2014): 12.

[127] Claude Pilloud et al., *Commentary on the additional protocols: of 8 June 1977 to the Geneva Conventions of 12 August 1949*, ed. Yves Sandoz, Christophe Swinarski, and Bruno Zimmermann (Geneva: Martinus Nijhoff Publishers, 1987). para. 4783

[128] Schmitt, *Tallinn manual on the international law applicable to cyber warfare : prepared by the international group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence.* Rule 30.12

[129] Schaap, "Cyber warfare operations: Development and use under international law," 127; See also Nicholas Tsagourias, "Cyber attacks, self-defence and the problem of attribution," *Journal of Conflict and Security Law* 17, no. 2 (2012): 1.

[130] Joint Chiefs of Staff, "Joint Publication 3-13. Information Operations."

While two first of them are clear and refer to the direct attack[131] and protection from the attack[132], the third one "exploitation" is an information gathering or intelligence collection[133]. Thus, in comparison with the definition of Tallinn Manual, "attack" in the US understanding is only action that has the aim of assault, whereas experts of NATO Cooperative Cyber Defence Centre of Excellence includes in this concepts both attack and defense. Herbert Lin examines in detail the difference between offensive and defensive tools and techniques of cyber conflict. While offensive attacks "allows a hostile party to do something undesirable", defensive attack allows "to prevent a hostile party from doing so".[134] Defensive tools could be used to identify errors that a hostile party can use as an advantage or in order to prevent damage that could cause cyber attack of hostile party. [135]

We also would like to provide other examples of US definitions that were used by Arie J. Schaap.[136] The department of Defence determined "cyber operations" as "the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace". The same department has also determined the concept of "computer network attack" as "actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves". Air Force policy Directive 10-7 appeals to the concept of "network warfare operations" and defines it as "the integrated planning and employment of military capabilities to achieve desired effects across the interconnected analog and digital portion of the battlespace". The last definition made by A 2006 CRS Report for Congress that defines "computer network attack" as "operations to disrupt or destroy information resident in computers and computer networks".

Alan Backstrom and Ian Henderson determined "cyber operations" as "operations against or via a computer or a computer system through a data stream… [that] can aim to do different things, for instance to infiltrate a system and collect, export, destroy, change, or encrypt data or to trigger, alter or otherwise manipulate processes controlled by the infiltrated computer system…By these

[131] The US National Military Strategy for Cyberspace Operations defines it as "operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves". Chairman of the Joint Chiefs of Staff, "National Military Strategy for Cyberspace Operations," (United States: United States Department of Defense, 2006), GL-1.

[132] The US National Military Strategy for Cyberspace Operations defines it as "actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DOD information systems and computer networks". Ibid.

[133] The US National Military Strategy for Cyberspace Operations defines it as "enabling operations and intelligence collection to gather data from target or adversary automated information systems or networks". Ibid.

[134] Herbert Lin, "Cyber conflict and international humanitarian law," *International Review of the Red Cross* 94, no. 886 (2012): 517.

[135] Ibid., 518.

[136] Schaap, "Cyber warfare operations: Development and use under international law," 126.

means... "targets" in the real world can be destroyed, altered or disrupted"[137]. Together with the definition of Tallinn Manual, these both definitions mentioned that cyber attacks could cause damage "in the real world". The reasons behind this are more likely the consequences of the Stuxnet attack, the first cyber attack that has demonstrated the ability to cause real damage.

Michael N. Schmitt also has defined "cyber operation" focusing on the consequences of the attack rather than on way of implementation, he said that it is "an attack [that] resulting in death or injury of individuals, whether civilians or combatants, or damage to or destruction of objects, whether military objectives or civilian objects"[138]. Moreover, this definition is more precise in terms of humanitarian law, because only cyber attack that causes physical damage may be considered as an attack in terms of armed conflict.

It also may seem that such a difference in the definition of a cyber attack could occur because the various concepts are taken into account: cyber attack, computer network attack and cyber operation. However, they represent a single concept by means of different words. Cordula Droege combines both "cyber operations" and "computer network attacks" in one definition[139] the same that was used above by A. Backstrom and I. Henderson. However, according to Marco Roscini statement on the fact that "'cyber warfare' is narrower than 'cyber operations'"[140], the last definition could be characterized as broad because it does not specify that cyber operation is the concept that should be subject of law of armed conflict. Cyber warfare attack in this way "refers only to the conduct of hostilities in armed conflict using cyber technologies"[141]. M. Roscini argues that the difference between "cyber warfare attack" and "cyber operation" is reflected in the fact that the concept of cyber operation could be applicable to variety of information operations. Where "information operation" is an "integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own"[142].

---

[137] New capabilities in warfare: an overview of contemporary technological developments and the associated legal and engineering issues in ICRC, *New technologies and warfare*, ed. Vincent Bernard, vol. 94, no. 886, International Review of the Red Cross. Humanitarian debate: Law, policy, action (Geneva: International Committee of the Red Cross (ICRC), 2012). 503.

[138] Droege, "Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians," 557.

[139] Ibid., 538.

[140] Marco Roscini, *Cyber operations and the use of force in international law* (Oxford: Oxford University Press, 2014). 11.

[141] Ibid., 12.

[142] Henry Shelton, "Joint doctrine for information operations," (United States: Defense Technical Information Center, 1998), GL-3.

Returning to the definition of Michael N. Schmitt, we would like to mention Nuclear Weapons Advisory Opinion[143] of the International Court of Justice where it says that law of armed conflict applies to "any use of force, regardless of the weapons employed".[144] Thus, we can conclude that for the application of humanitarian law to the situation of the cyber attack, we need to know whether a "cyber attack" causes a real damage rather than its worldwide-accepted definition. Any state or scholar could develop its own doctrine on cyber attack or cyber operation, but it is not necessary for the LAOC application because norms of customary international law already regulate the issue. The position was supported by the US in the 2011 International Strategy for Operating in Cyberspace where it says, "The development of norms for State conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norm obsolete. Long-standing international norms guiding State behaviour - in times of peace and conflict – also apply in cyberspace".

This position is closely connected with the statement that humanitarian law applies to the cyber warfare, however, as we mentioned there is a diametrically opposite opinion. Thus, based on the fact that any attack regardless of the weapon shall entail the application of humanitarian law, we first consider the opinion "for" application the law of armed conflict and then "against" the application.

IHL is applicable

One opinion is that any cyber attack that causes damage constitute an attack within the meaning of LOAC and consequently entails the humanitarian law application. The weakness of this point is that it is too broad; according to the definition, any cyber strike will constitute an attack, for example, interferences with civilian computer systems[145]. However, only cyber attacks aimed at achieving military advantage by legal means could be considered as a part of warfare, other actions would probably go beyond the scope of rules on the conduct of hostilities.

The other opinion is that it is not necessary for cyber attack to cause material damage. Knut Dörmann, for example, based on the Article 52(2) of Additional Protocol I containing the definition

[143] Internationaler Gerichtshof, "Legality of the threat or use of nuclear weapons, advisory opinion," *ICJ Reports* (1996): 39.
[144] Solis, "Cyber warfare," 1.
[145] Droege, "Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians," 559.

of military objectives, states that any destruction, capture or neutralization that brings definite military advantage could be considered as an attack.[146] If the military objective is disabled it does not matter how it was made by means of object destruction or computer system neutralization. In addition, we have to say that if in the first case definition was too broad, then this definition brings even more uncertainty concerning what is cyber attack in terms of cyber warfare. Moreover, it is also the position of the ICRC that "a cyber operation that "disables" an object is also an attack even when it does not cause physical damage"[147]. However, both points of view insist that humanitarian law should be applied to a cyber attack. The only question is, what is the cyber attack. Thus, we are back to where we started. Mark Shulman has specified in its decision on whether LOAC is applicable the type of cyber operation. He said that "defensive [information warfare] operations are subject to the restraints of LOAC and its principle of proportionality", moreover, he added, "information warfare is neither 'armed' in the traditional sense, nor does it necessarily involve conflict'".[148] Roger D. Scott believes that the laws of armed conflict is applied to computer network attacks basing on the intentions of the warring parties and consequences "in determining the constraints imposed on computer network attack by the law of war the focus of analysis must be the intent and likely results of an attack, not the novel method of attack".[149] In addition, Lesley Swanson confirms, "combat no longer consists solely of physical attacks or invasions among nations with distinct military units. This new kind of warfare uses a target nation's own technology against it, in order to bring down vital infrastructure".[150]

However, if before such states as the US, the United Kingdom of Great Britain and Northern Ireland, and Australia have expressed their consent on the application of humanitarian law to cyber warfare[151], right now the quantity of states increased: Australia[152], China[153], Cuba[154], the European

[146] Droege, "Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians," 558.
[147] Michael Schmitt, "Classification of Cyber Conflict," *Journal of Conflict and Security Law* 17, no. 2 (2012): 252.
[148] Mark Rusell Shulman, "Legal Constraints on Information Warfare," (United States: Center for Strategy and Technology, Air War College, Occasional Paper No. 7, 1999).
[149] Roger D. Scott, "Legal Aspects of Information Warfare: Military Disruption of Telecommunications," *Naval Law Review* 45(1998): 57, 59; Heather Harrison Dinniss, *Cyber warfare and the laws of war*, vol. 92 (New York: Cambridge University Press, 2012). 127.
[150] Solis, "Cyber warfare," 304.
[151] Droege, "Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians," 537.
[152] United Nations, "Developments in the field of information and telecommunications in the context of international security (A/66/152)," (Report of the Secretary-General, 2011), 6.
[153] Li Zhang, "A Chinese perspective on cyber war," *International Review of the Red Cross* 94, no. 886 (2012): 4.
[154] United Nations, "Developments in the field of information and telecommunications in the context of international security (A/57/166/Add.1)," (Report of the Secretary-General, 2002), 3.

Union[155], Hungary[156], Iran[157], Italy[158], Mali[159], the Netherlands[160], Qatar[161], the Russian Federation[162], and the United Kingdom[163].[164] Moreover, some scholars make the assumption that at least basic principles of humanitarian law as principles of distinction, proportionality, and precaution should be applicable as a minimum standard to cyber attacks that cause physical damage.[165] Based on the statement that cyber warfare attack is something new and worldwide-accepted conventions that should regulate it was not yet signed[166] and customary law did not crystallize, other scholars argue that all this things are not necessary for the LOAC application.[167] Thus, they hypothetically assume that humanitarian law may be applicable, since the Article 36 of Additional Protocol I establishes that all contracting parties must determine whether new means and methods of warfare is within the scope of humanitarian and international law. Fllowing the logic, everything that is not forbidden is allowed.[168] If exploitation by new methods of warfare is not contrary to the current rules of law then it makes sense to try to apply those rules.

Some go further and support the position that "cyber warfare is not fundamentally different from conventional, physical warfare"[169]. Gary D. Solis by comparing the kinetic and cyber attacks

[155] European Comission, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace," (Brussels: High Representative of the European Union for Foreign Affairs and Security Policy, 2013), 15, 16.
[156] Budapest Conference on Cyberspace, Opening Session, 4 October 2012, Welcome speech by János Martonyi, Minister of Foreign Affairs. Roscini, *Cyber operations and the use of force in international law*.
[157] Alireza Miryousefi and Hossein Gharibi, 'View from Iran: World needs rules on cyberattacks', The Christian Science Monitor, 14. Ibid.
[158] Governo italiano, La posizione italiana sui principi fondamentali di Internet, 17 September 2012, ibid., 5.
[159] United Nations, "Developments in the field of information and telecommunications in the context of international security (A/64/129/Add.1)," (Report of the Secretary-General, 2009), 7.
[160] AIV/CAVV, "Dutch Government response to the AIV/CAVV report on cyber warfare," (Advisory Council on International Affairs (AIV), Advisory Committee on Issues of Public International Law (CAVV), 2012), 5-6.
[161] United Nations, "Developments in the field of information and telecommunications in the context of international security (A/65/154)," (Report of the Secretary-General, 2010), 9-10.
[162] Ministry of Defense, "Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space," (Russia: Ministry of Defense of The Russian Federation, 2011), 6.
[163] United Nations, "Developments in the field of information and telecommunications in the context of international security (A/65/154)," 15.
[164] Roscini, *Cyber operations and the use of force in international law*: 21-22.
[165] Alan Backstrom and Ian Henderson, "New capabilities in warfare: an overview of contemporary technological developments and the associated legal and engineering issues in Article 36 weapons reviews," *International Review of the Red Cross* 94, no. 886 (2012): 503. Article 36
[166] There is only one treaty 2001 Budapest Convention on Cybercrime, negotiated in the framework of the Council of Europe and entered into force on 1 July 2004.
[167] Droege, "Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians," 540.
[168] Yohannes Eneyew Ayalew, "Cyber Warfare: A New Hullaballo Under International Humanitarian Law," *Beijing Law Review* 6(2015): 210.
[169] Ibid., 212.

concludes that any attack that "kills, wounds, or destroy constitutes an armed attack[170]". However, the notion of cyber warfare should be distinguished from non-related to armed conflict cyber operations as cyber terrorism or cyber intrusion[171], the difference between which is that the last one were "committed in everyday situations that have nothing to do with war"[172].

There is another opinion, which also classifies cyber attacks as an act of war. J. D. Ohlin, K. Govern and C. Finkelstein in their book[173] use such an example as violation of territorial integrity or sovereign immunity that are always equated to an act of war. According to the authors, cyber attack could be characterized as an act of aggression within the framework of Article 1 of Resolution 3314[174]. The fact that cyber attack as well as the kinetic attack invades the territory of the state thereby violating its sovereignty left no difference whether it was physical invasion or computer invasion.

The statement that humanitarian law is applicable to the cyber warfare has many adherents. However, in practice, it has never been implemented. There was no single case of cyber warfare where law of armed conflict was applied. Perhaps this is the one of the strongest arguments against that statement. Moving away from the arguments that support IHL application we would like to consider the criticism of those who do not believe that it is possible.

IHL is not applicable

Two questions arise in the solution whether humanitarian law applies: first, should it be applied to cyber warfare at all, and, if yes, under what conditions. Is it necessary to know the definition of "cyber attack"? Or is the only circumstance the existence of material damage? This uncertainty contributes to the fact that many critics are saying about the impossibility of application of humanitarian law to cyber attack.[175] Some of them appeals to "the technicality of the subject matter [that] results in non-compliance".[176] First of all, there is no generally accepted concept of "cyber

[170] Solis, "Cyber warfare," 17.
[171] Ibid., 11.
[172] Ayalew, "Cyber Warfare: A New Hullaballo Under International Humanitarian Law," 215; See alsoSolis, "Cyber warfare," 22.
[173] Jens David Ohlin, Kevin Govern, and Claire Finkelstein, *Cyber war: law and ethics for virtual conflicts* (Oxford: Oxford University Press, 2015). 8.
[174] United Nations, "United Nations General Assembly Resolution 3314. Definition of aggression A/RES/3314(XXIX)," (United Nations General Assembly, 1974).
[175] Charles J. Dunlap Jr, "Perspectives for cyber strategists on law for cyberwar," *Strategic Studies Quarterly* 5(2011): 81.
[176] Ayalew, "Cyber Warfare: A New Hullaballo Under International Humanitarian Law," 213.

warfare". Frequently, the situation of cyber strike raises questions whether it was "cyber warfare attack" or act of "cyber terrorism" or it was just a general "cyber operation". Who shall determine the terms? The same confusion contributes the concept of "cyber attack". If even those who favor the use of humanitarian law can not come to common decision about what is a "cyber attack", then what should consider persons who oppose? Every state develops its own legal doctrine on what is "cyber attack" or "cyber operation" or "computer network attack", thus, every state has its own opinion on whether the LOAC is applied. Some of states even can not decide exactly, China initially was against, Russia did not expressed its opinion.[177] The US has developed its own doctrine on what is "information operations" and has distinguished three types of them: attack, defense and exploitation. Moreover, each of them has its own types, thus, for example, computer network defense could be passive or active depending on whether it involves "launching a pre-emptive, preventive, or cyber counter-operation against the source", or whether it "does not involve a counter-operation against the source but uses tools like firewalls, honeypots, anti-virus software, and digital forensic tools".[178] Therefore, differences in the basic concepts seem to be an insurmountable barrier to the adoption of a single legal position regarding cyber warfare.

Another counter-argument is that cyberwar is a new kind of war. The creators of the first international documents on humanitarian law could not imagine that such a problem may occur because the very notion of a digital war did not exist due to the lack of development of digital technologies. Opponents argue that by this way humanitarian law should not apply to those concepts that were not envisaged in the original purpose. As we said above, for this argument is easy to find a counterargument that is associated with the obligation of States to test new weapons on the compliance of rules with humanitarian law. However, what is a "weapon"? Is cyber attack a weapon? If we assume that the cyber attack is not a weapon, then there is no rules of humanitarian law, which would have a connection with cyber attacks, including with the word "cyber". However, if cyber attack is a weapon then at least the basic principles of humanitarian law must be applied during cyber attacks. Once again, there is no binding definition of "weapon".[179] Black's Law Dictionary gives such a definition "an instrument used or designed to be used to injure or kill someone"[180]. Based on this definition, the purpose of any virus or worm should be injuring people, although only recently cyber attacks have become detrimental to the real world, since their original purpose is to harm a computer

[177] Droege, "Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians," 537.
[178] Schmitt, *Tallinn manual on the international law applicable to cyber warfare : prepared by the international group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence.*: 15.
[179] Roscini, *Cyber operations and the use of force in international law*: 51.
[180] Ibid., 1730.

system. The HPCR Manual on Air and Missile Warfare also provide some features of weapon: the capability to cause either injury/death of persons or damage/destruction of objects.[181] This definition is more appropriate, since the purposes of any military attack are both people and objects. Estonian Defense Minister Jaak Aaviksoo, for example, after the cyber attack on Estonia in 2007 stated, "NATO does not define cyber-attacks as a clear military action".[182] Scott Borg, director of the U.S. Cyber Consequences Unit, summed it expressing that "we are in a world where governments have not decided yet whether the tools of cyberattacks are weapons".[183] Other authors like Richard Aldrich on the other hand argue that the physical damage is needed, "'armed conflict', as presently understood, seems far less likely to be applied to the simple manipulation of bits inside a computer, although this may soon change since the nefarious manipulation of bits could, in some cases, already cause significantly more harm than could a bomb".[184]

Other scholars also assert that humanitarian law is out of date and may not be applicable to the situation of cyber conflict.[185]

If we still assume that the cyber attack is a weapon, then we should analyze whether cyber attack is in conformity with humanitarian law. However, ahead of the analysis C. Droege gives an example of other development of situation namely that "cyber warfare challenges some of the fundamental assumptions of IHL" such as "the parties to a conflict must be identifiable and be known".[186] Besides the fact that the parties themselves do not support this assumption, because it seems ridiculous that the hostile party will notify about its plans concerning cyber attacks, furthermore, the purpose of the attack may be to remain unidentified in order to avoid responsibility.

IHL also contains the assumption that "means and methods of warfare will have violent effects in the physical world".[187] Likewise, some scholars insist on the presence of real harm from cyber attacks in order to make possible the application of humanitarian law, thereby, only a certain kind of attack is under IHL. Others are convinced that the damage should not necessary be in a real life, consequently, any cyber attack is under IHL.

---

[181] HPCR, *Manual on International Law Applicable to Air and Missile Warfare* (Cambridge, New York: Cambridge University Press, 2013). 49. Rule 1

[182] Schaap, "Cyber warfare operations: Development and use under international law," 144.

[183] Ibid., 145.

[184] Dinniss, *Cyber warfare and the laws of war*, 92: 126; Richard W Aldrich, "The international legal implications of information warfare," (DTIC Document, 1996), 99, 102.

[185] Michael G. Dillon, *The Liberal Way of War: Killing to Make Life Live* (London: Routledge, 2009). 191.

[186] Droege, "Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians," 541.

[187] Ibid.

One of the arguments against the application of the law of armed conflict is the inability to use its norms during the cyber warfare. How can we apply the rule of law, the application of which causes so much controversy?

There are also some fundamental differences that highlight J. D. Ohlin, K. Govern, and C. Finkelstein[188] between cyber warfare and conventional war. The first one is the fact that implementation of cyber attack in reality not associated with crossing the border in the traditional sense. It means that troops of the enemy do not intrude on the sovereign territory of another state again in the conventional sense. In addition, since military operations do not depend on the movement of soldiers, there is no necessity to kill some someone. Based on these two features the authors put forward the hypothesis that a cyber attack by nature is more similar to the economic sanctions rather than to armed conflict.[189] There is also a third point that is associated with the consequences of the cyber attacks. It is assumed that the cyber attack could also "cause great disruption and result in deaths within the target state".[190] Nevertheless, the damage caused by such an attack is not direct, which means it is a result of the virus or worm. The authors brings to a comparison the economic embargo, which may also have serious consequences like the deaths without such intention. Therefore, cyber attacks are to be understood as "a type of international pressure"[191] especially considering the fact that all cyber attack were made without LOAC application. It can be assumed that the aim of those who carried out the attack was political pressure rather than starting a war.

General conclusions

The legal protection afforded to civilians during a cyber conflict is entirely dependent on what kind of legal regime applies. Earlier, during an armed conflict, civilians have always enjoyed the protection provided by the Geneva law. However, the development of technology has led to the emergence of a new kind of attack it is the information attack. With the development of computer technology emerged cyber space and, subsequently, cyber attacks, which are the form of information attack. In order to understand whether humanitarian law is applies to cyber attack, it is necessary to determine,

[188] Ohlin, Govern, and Finkelstein, *Cyber war: law and ethics for virtual conflicts*: 9.
[189] Ibid., 10.
[190] Ibid.
[191] Ibid., 18.

firstly, what is cyber space, and, secondly, what is cyber attack. There is no consensus on this issue as well as on the issue whether LOAC is applied to cyber warfare.

There are two opposing points of view. On the one hand, scholars argue that humanitarian law should be applied to the situation of cyber warfare. This is due to the fact that any cyber attack is a manifestation of aggression, as well as the fact that it violates the sovereignty and the territorial integrity of another state. Thus, cyber warfare does not differ from conventional war and consequently LOAC is needed.

On the other hand, humanitarian law is out of date, cyber warfare is new kind of war and it requires new rules. Moreover, humanitarian law does not mention such situations as cyber strikes/attacks or warfare. It does not mention a word “cyber”. In addition, it is hard to imagine how LOAC could be applied to the cyber warfare, because there is certain kind of inconsistences between them. Cyber warfare challenges core assumption of the LAOC. Many issues remain unresolved because it is difficult to find consent between countries. In this case, humanitarian law is hardly applicable and it means that civilians are outside the protection granted by the Geneva law.

In order to understand better what is the reason of disagreements and the difference between cyber war and conventional, we first will consider the means and methods of cyber warfare, and then we will analyze the Stuxnet attack and its main issues.

In conclusion, of the paper we will try to figure out what is the situation of civilians, in the case if humanitarian law does not provide them the necessary level of protection. The other issue is whether cyber warfare is something new. Is it necessary to create new legal instruments for the legal order regulation?

Representatives of both points of view in this chapter agreed on the opinion that the situation with the war is no longer the same. The only question is what changes it brings.

CHAPTER III

CYBER WEAPONS

The main difference between conventional war and cyber war consist of means and methods of warfare. As was mentioned in Chapter II, major combat operations of cyber war are carried out within the computer network. The main purpose of this war is an attack on a computer system or by means of a computer system. Thus, the main weapon of cyber warfare is malicious programs and other cyber methods to deceive the enemy. In this Chapter, we will try to highlight the main types of them and to identify their connection with the law of armed conflict.

Malicious programs

Malicious programs or malware are those that aim to disable computers, to disrupt computer functions, to gain access or to gather information. Malware allows an attacker to gain control over computer system and to disable it or to make it transmit the same harmful effect on other computers. Clay Wilson defines malicious programs as those that "attack by disrupting normal computer functions or by opening a back door for a remote attacker to take control of the computer… An attack can trigger the automatic transmission of huge volumes of harmful signals that can very rapidly disrupt or paralyze many thousands of other computers throughout the Internet, or severely clog transmission lines with an abundance of bogus messages, causing portions of the Internet to become slow and unresponsive".[192] The Technology Analysis Center as has identified "malware" as a "software or firmware intended to perform an unauthorized process that will have adverse impact on one or more required properties of the targeted system, including (but not limited toy-confidentiality, privacy, integrity, availability, dependability, usability, and performance".[193] Troy Nash provides various types of malware: various forms of adware, dialers, hijackware, slag code (logic bombs),

[192] Clay Wilson, "Computer attack and cyber terrorism: vulnerabilities and policy issues for congress," *Focus on Terrorism* 9(2003): 32.

[193] Chance Cammack, "The Stuxnet Worm and Potential Prosecution by the International Criminal Court under the Newly Defined Crime of Aggression," *Tulane Journal Ofint'l & Comp. Law* 20(2011): 315.

spyware, Trojan horses, viruses, web bugs, and worms.[194] However, the most common examples are worms, Trojan horses and viruses[195], which we will discuss below.

Worms

A warm is malware that uses vulnerability of the computer system or network in order to harm the computer operations. It can spread itself from one computer system to another and a warm can replicate itself within the same computer system. Eugene H. Spafford defined it as "a program that can run by itself and can propagate a fully working version of itself to other machines. It is derived from the word tapeworm, a parasitic organism that lives inside a host and saps its resources to maintain itself".[196]

A worm usually consists of three components: identifier, transmitter and payload.[197] An identifier is a code that searches for targets, for example, it identifies new vulnerable computer systems for the attack; a transmitter serves for worm transfer and a payload identifies malicious actions to be done. Thus, a payload allows the attacker to interfere in the operation of the computer, to collect necessary information and in some cases to control computer system remotely[198].

There are various types of worms, depending on whether they are spreading themselves: those that spread over the Internet, computer network, by means of e-mail or by Internet messaging (IM).[199] Thus, for example, one of the military receptions in cyber war may be a worm send by e-mail. This worm can easily replicate itself using e-mail addresses associated with the infected e-mail. In the case of a computer network attack, the worm begins to replicate itself by running multiple computer processes, it slows down the functioning of the network and it makes sensitive information accessible

---

[194] Troy Nash, "An undirected attack against critical infrastructure," *Technical Report, US-CERT Control Systems Security Center* 1.2(2005): 10.

[195] Arie J. Major Schaap, "Cyber warfare operations: Development and use under international law," *Air Force Law Review* 64(2009): 135.

[196] Eugene H. Spafford, "The internet worm program: an analysis," *ACM SIGCOMM Computer Communication Review* 19, no. 1 (1989): 3.

[197] Hossein Rouhani Zeidanloo et al., "All About Malwares (Malicious Codes)," in *International Conference on Security & Management* (Las Vegas Nevada2010).

[198] Schaap, "Cyber warfare operations: Development and use under international law," 136.

[199] Mihai Trifan, "Cyber-Attacks (Viruses, Trojan Horses and Computer Worms) Analysis," *International Journal of Information Security and Cybercrime* 1, no. 1 (2012): 50.

to the attacker. A worm "consumes too much system memory or network bandwidth, causing web servers, network servers, and individual computers to stop responding".[200]

On November 2, 1988, Robert Morris made one of the first significant worm attacks on the Internet. The Morris worm disabled million computers for several days. Eugene H. Spafford argues that "the worm was deliberately designed to do two things: infect as many machines as possible, and be difficult to track and stop".[201] This assumption causes some concern if we look at the situation from the perspective of humanitarian law. If hypothetically imagine this attack as part of cyber war, the various issues will arise. On the one hand, the worm was directed against a specific group of persons, those who had vulnerabilities such as an error in SEND MAIL, a bug in the "finger demon" program, the "trusted hosts" feature and those who had weak passwords. However, on the other hand the list of victims is quite wide and includes only vulnerable persons. Firstly, it violates the principles of distinction and discrimination, since it does not distinguish civilians and combatants, and secondly, the basic principle of military necessity, since the attack should serve for securing the ends of the war with the least possible expenditure.[202]

The case of the Morris worm is also closely related with the denial of service attack, which is another kind of cyber attack that will be discussed below. There are no strict rules regarding the classification of cyber attack. Attack of R. Morris is a worm attack and at the same time denial of service attack. The difference between them is that a worm attack only vulnerable computers and systems but only once, while denial of service attack sends a large number of requests to the same computer or system. The Morris worm has infected some computers several times. There is also discussion whether it is a worm or a virus. We will take a position of those who say that this is worm since unlike the worm virus cannot exist independently they are in most cases part of another program.[203] Thus, the Morris worm cannot be characterized as a virus because it was independent from other programs and because it replicated itself without human intervention.[204]

[200] Schaap, "Cyber warfare operations: Development and use under international law," 136.
[201] Spafford, "The internet worm program: an analysis," 26.
[202] See Chapter 1.
[203] Spafford, "The internet worm program: an analysis," 3.
[204] Zeidanloo et al., "All About Malwares (Malicious Codes)."

Viruses

Another type of malware which is similar to worm is a virus. Viruses as worms are aiming to harm the computer operations; however, they are very dependent on other programs that maintain their existence and spread. Eugene H. Spafford has defined virus as "a piece of code that adds itself to other programs, including operating systems. It cannot run independently - it requires that its ''host'' program be run to activate it".[205] Unlike the worm virus needs a human intervention – a person who will launch the host program. Fred Cohen identified "virus" as "a program that can 'infect' other programs by modifying them to include a possibly evolved copy of itself… a virus can spread throughout a computer system or network using the authorizations of every user using it to infect their programs… thus the infection grows".[206] As well as the worm virus can be sent by e-mail or transported by removable media as USB drive.

A virus unlike worm usually consists of two parts: insertion code and payload.[207] The first one is a code that sets the virus into other programs, and the second one is a code that programs malicious actions of virus. An attacker, therefore, can program a virus to corrupt or destroy the data.

There are three types of viruses according to the object classification: file investors, boot-sector viruses and multipartite viruses[208], where separation is made depending on the object of attack. File investors are those that damage executable files, boot-sector viruses can affect, for example, boot sector of the hard drive, and multipartite viruses includes both. Thus, cyber attacker can choose between two different way of attack or he or she can use a combination of them thereby increasing the speed of virus spread.

On 5 May, 2000, a virus known as "ILOVEYOU" attacked millions of users by means e-mail. The e-mail contained an infected file at the opening of which virus was passed to the computer. In this case, in contrast to the Morris worm attack the user had a chance to delete the letter and thereby to avoid the attack. Applying the situation of cyber warfare the question whether any humanitarian law principal is applicable here arises. Could we say that once a user has opened the virus he is responsible for the consequences? The answer is no. Regardless whether the attack is direct or depends entirely on actions of civilian, the civilian is protected under the principles of distinction and

[205] Spafford, "The internet worm program: an analysis," 3.
[206] Fred Cohen, "Computer viruses," *Computers & Security* 6, no. 1 (1987).
[207] Zeidanloo et al., "All About Malwares (Malicious Codes)," 4.
[208] Christopher C Elisan, *Malware, Rootkits & Botnets A Beginner's Guide* (New York: McGraw Hill Professional, 2012). 11.

discrimination. This type of attack to some extent can be compared with land mines, which are prohibited since their attacks are indiscriminate. Both examples have harmful effects, which occur after the "touch" of the victim.

Trojan horses

Another type of a cyber attack is a hidden threat of Trojan horse. Usually a malware is contained inside programs or data that seem to be safe, however, a malware can attack files and system information on the computer. Mejor Arie J. Schaap in his article uses the following definition: "Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage".[209] Manuel Bucher defines "Trojan horse" as "a harmless programme or useful file, but is in fact a virus dropper, which carries an independently working spyware source code that mostly executes undesirable, additional functions unknown to the user".[210] Rita C. Summers defines it as "apparently useful program containing hidden functions that can exploit the privileges of the user [running the program], with a resulting security threat. A Trojan horse does things that the program user did not intend".[211] Ed Skoudis and Lenny Zeltser have identified a Trojan as "a program that appears to have some useful or benign purpose, but really masks some hidden malicious functionality".[212] Thereby, a Trojan horse is a malware that may take control over computer, affect computer operations and gather sensitive information. It is completely dependent on host program and cannot spread by itself or replicate itself. A Trojan horse can infect computer system if a user or the attacker will install the malicious program or it can also penetrate by means of worms and viruses[213]. In comparison with viruses and worms, a Trojan horse seems to be more harmful for personal security because it can gather information by using all computer functions, for example, using web camera.

---

[209] Schaap, "Cyber warfare operations: Development and use under international law," 136.

[210] Basil Cupa, "Trojan horse resurrected - On the legality of the use of government spyware," in *Living in surveillance societies: The state of surveillance*, ed. C William R. Webster (Proceedings of LiSS conference 3: CreateSpace Independent Publishing Platform, 2013), 420.

[211] Rita C. Summers, *Secure computing: threats and safeguards* (Hightstown: McGraw-Hill, Inc., 1997). http://www.cert.org/historical/advisories/CA-1999-02.cfm#reference1.

[212] Ed Skoudis and Lenny Zeltser, *Malware: Fighting malicious code* (New Jersey: Prentice Hall Professional, 2004). 251.

[213] Zeidanloo et al., "All About Malwares (Malicious Codes)."

In contrast to previous malware, Trojans seem to be “less unlawful” mean of cyber attack since they do not affect random users, moreover, the attacker can control all their malicious actions. However, taking into account that Trojans masquerade themselves as useful programs, we can say that to some extent it could be a violation of the prohibition of perfidy principle, if the attacker's intention is defrauding the trust of the enemy.

Among malicious actions that can perform a Trojan horse, it is possible to highlight elimination of critical files or processes, redirection of access to security update site, collection of information, and opening ports on computer.[214] In addition, it can install other program, explore vulnerabilities of the infected computer in order to increase the level of access, install viruses, and install other Trojans.[215]

Some examples of possible attack implementation are the use of space to hide the file extension, giving the name of a program, combining two files of software and malware or insert it in a software. Trojans also can be distributed via the Internet by means of web sites and social networks.

Blended threat

In case where the attack has characteristics of various malware, it should be considered as blended, thus, for example, a single attack can combine aspects of viruses, worms and Trojan horses in one code. One of the definitions is that “a blended threat is a sophisticated attack that bundles some of the worst aspects of viruses, worms, Trojan horses and malicious code into one threat”.[216]

Above we have discussed that sometimes it is complicated to distinguish virus and worm, and that the worm may transform into the denial of service attack. We suppose that this is one of the major problems of cyber attacks in the context of humanitarian law, i.e. it is complicated to say exactly what happened, whether it was an act of war, who launch the attack and what kind of attack is this. Moreover, a blended attack can spread quickly and cause widespread damage.[217] This fact could be closely related with the three basic principles of international law mentioned above: the principle of distinction, the principle of discrimination and the principle of proportionality. If the cyber attack will

[214] Ibid.
[215] CERT, Trojan Horses, accessed March 8, 2017, http://www.cert.org/historical/advisories/CA-1999-02.cfm#reference1
[216] Schaap, "Cyber warfare operations: Development and use under international law," 136.
[217] Ibid., 137.

be worm-like or virus-like, i.e. it will aim to attack as many as possible computer systems, and then all of the following principles are violated.

Denial of Service Attacks

One type of the cyber attack is denial of service attack (DoS) that aims to interrupt the operation of another computer. Major Arie J. Schaap uses the following definition: "an assault on a network that floods in with so many additional requests that regular traffic is either slowed or completely interrupted".[218] It means that a person cannot use successfully the network connection because the computer or network is affected by the floods of requests of the attacker. In such situations, it may occur that people cannot use certain sites or services, such as e-mail or accounts.

However, David Moore, Geoffrey M.Voelker and Stefan Savage have identified two types of DoS attacks: logic and flooding.[219] While the first one aims to use vulnerabilities of computer software in order to disable it, the second one tries to send a large number of requests aiming to overwhelm it. In this regard, the definition provided above does not seem comprehensive. Mehmud Abliz has also identified it as "such attacks that aimed at blocking availability of computer systems or services".[220] This determination on the contrary seems to be quite wide. We would likely define a denial of service attack as an attack that aims to slow, interrupt or disable a computer system, network or service by means of massive requests or the use of existing software flaws. Other authors appeal to four examples of DoS: attacks that attempts to flood a network, to disrupt a computer or a system, to prevent access to service and to break the connection.[221]

Additionally, there are different types of denial of service attack, for example, a distributed (DDoS), a single-source (SDoS), a permanent (PDoS), advanced persistent (APDoS) attack and other. Briefly will consider the mentioned ones.

A distributed denial of service attack is one that by means of a large number of hosts whether computer or other device attacks a single one. A single-source denial of service attack in contrary uses only one host for the attack. The only difference between them is that the first type of attack is

---

[218] Ibid., 134.

[219]David Moore et al., "Inferring internet denial-of-service activity," *ACM Transactions on Computer Systems (TOCS)* 24, no. 2 (2006): 2..

[220], Mehmud Abliz, "Internet denial of service attacks and defense mechanisms," *University of Pittsburgh, Department of Computer Science, Technical Report* (2011): 1.

[221] Felix Lau et al., "Distributed denial of service attacks" (paper presented at the Systems, Man, and Cybernetics, 2000 IEEE International Conference on, 2000), 1.

more powerful and consequently "defending against DDoS attacks is proven to be harder than defending against SDoS attacks".[222] PDoS attack unlike DDos and SDoS attacks inflict such a big damage that computer system requires replacement or reinstallation.[223] APDoS attack could be characterized as an action with numerous repeated attacks for a long time.

A DoS attack bears no direct physical harm, since it does not seek to kill or injure people or destroy objects. However, it should be taken into account that in some cases, proper operation of the computer system may play a vital role, for example, in the case of power plants or it may also include any military facility since matters of national security and defense are primary. This kind of attack can also perfectly serve for direct intervention in the civilians computers. During the armed conflict, military advantage from such attacks it is doubtful, however, the possibility of such events should not be excluded. The advantage of this attack is also the fact that it is not necessary to have a powerful computer for the attacker, by means of any computer networks and sophisticated machines may be disabled.[224]

On July 19, 2001, a computer worm knows as "Red Code" attacked more than 359.000 computers in less than 14 hours.[225] This attack was not discriminatory and did not have any particular purpose; it just randomly chose vulnerable computers. Nevertheless, one of the objectives of this attack was the White House Web site. Thus, considering this issue in the context of cyberwar, we can conclude that denial of service attack can endanger international law principles. For example, distinction and discrimination, since the target of attack was not selected on the principle of distinguishing military and civilians; rather it was depending on the server and in this particular case on computer vulnerability. The principle of neutrality may also be affected, in view of the fact that such worm will not make a distinction between a person who direct participation in hostilities and who does not, it will consider neither nationality nor preference of someone to remain neutral in the conflict.

[222] Ibid., 4.
[223] Schaap, "Cyber warfare operations: Development and use under international law," 135.
[224] Ibid., 134.
[225] David Moore and Colleen Shannon, "The spread of the code-red worm (crv2)," (Center for Applied Internet Data Analysis, 2001), accessed Match 01, 2017, http://www.caida.org/research/security/code-red/coderedv2_analysis.xml.

Logic Bomb

Logic bomb is a type of malware which effects are predictable with a high level of probability. The main goal of such attacks is to execute a particular action if some events have occurred or if there is a predetermined time.[226] Stephenie Gosnell Handler defines it as "a piece of code that is intentionally inserted into a software system for the purpose of setting off a malicious function when specified conditions are met"[227]. John Richardson provides the following definition: "A logic bomb is a program, or portion of a program, which lies dormant until a specific piece of program logic is activated. In this way, a logic bomb is very analogous to areal-world land mine"[228]. Some of the consequences of the logic bomb are to disable the computer system, to delete sensitive information, or provoke a denial of service attack with the interruption of computer system operations.[229] A logic bomb attack may also provoke severe consequences, for example, it may activate a DoS attack.[230]

Logic bomb seems to be discriminative kind of cyber weapon since the attacker will exactly determine an object and a time of the attack; however, from the other side it does not. One of the first attacks, for example, was a logic bomb that led to a major pipeline disaster in Soviet Union in 1982.[231] The attack was "the most monumental non-nuclear explosion and fire ever seen from space"[232]; respectively, it was not proportional and discriminative within the meaning of humanitarian law since the time of the attack is hardly predictable and that means the damage will be widespread.[233] Thus, the attack could probably violate basic principles of international law as proportionality, distinction or discrimination.

---

[226] Schaap, "Cyber warfare operations: Development and use under international law," 137; See also McGavran, supra note 36, at 263. Cited atShaun Roberts, "Cyber Wars: Applying Conventional Laws to War to Cyber Warfare and Non-State Actors," *Northern Kentucky Law Review* 41, no. 3 (2014): 542.

[227] Stephenie Gosnell Handler, "New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare," *Stanford Journal of International Law* 48, no. 1 (2012): 228., Note 66.

[228] John Richardson, "Stuxnet as cyberwarfare: applying the law of war to the virtual battlefield," *Journal of Computer & Information Law* 29(2011): 15.

[229] Schaap, "Cyber warfare operations: Development and use under international law," 137.

[230] Coleman, supra note 36. Cited at Bradley Raboin, "Corresponding Evolution: International Law and the Emergence of Cyber Warfare," *Journal of the National Association of Administrative Law Judiciary* 31, no. 2 (2011): 614.

[231]Jack M. Beard, "Legal Phantoms in Cyberspace: The Problematic Status of Information as a Weapon and a Target Under International Humanitarian Law," *Vanderbilt Journal of Transnational Law* 47(2014): 79; Roberts, "Cyber Wars: Applying Conventional Laws to War to Cyber Warfare and Non-State Actors," 542.

[232] Cyberwar: War in the Fih Domain, EcoNoMST,July 3, 2010, at 25. Cited atScott J. Shackelford and Richard B. Andres, "State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem," *Georgetown Journal of International Law* 42(2011): 972.

[233] Raboin, "Corresponding Evolution: International Law and the Emergence of Cyber Warfare," 614.

IP Spoofing

IP spoofing as well as Trojan horse is a way to deceive the trust of the enemy in order to obtain access to a computer system. However, IP spoofing differs from Trojans since it is not a malicious program rather it is a method of deception. Major Arie J. Schaap gave the following definition of IP spoofing, "is a hijacking technique in which hijackers masquerade as a trusted host to conceal their identity, spoof a Website, hijack browsers, or gain access to a network"[234]. Shaun Roberts with reference to the previous author defines IP spoofing as a "trickery whereby a user who enters a legitimate web address is re-directed to a fraudulent web site created by a hacker"[235]. Bradley Raboin also identified IP spoofing as "a kind of hijacking technique that allows the hacking user to operate a computer while appearing as a trusted host"[236]. Phillip Pool uses similar definition where IP spoofing is a "tool that allows a hacker to create a web page that appears identical to a trusted web page online, which deceives the user into entering private information"[237]. Ryan Patterson provides more technical definition limiting the concept only by the intentions of the attacker: "IP spoofing is the creation of data packets with a forged source IP address, with the purpose of concealing the identity of the sender or impersonating another computer system"[238].

Just as Trojan horse, the attack may case a damage or undesirable consequences only if the user will interact with the spoofed page. After gaining access to a computer, the attacker can control a computer or a network and gather sensitive information.[239] Taking into account humanitarian law, we could apply the norm of prohibition of perfidy, since the attacker aims to mislead the victim. From our point of view it is most comprehensive data since the first definition it includes possible targets of the attacker like information gathering or computer access.

[234] Schaap, "Cyber warfare operations: Development and use under international law," 137.
[235] Roberts, "Cyber Wars: Applying Conventional Laws to War to Cyber Warfare and Non-State Actors," 542.
[236] Raboin, "Corresponding Evolution: International Law and the Emergence of Cyber Warfare," 615.
[237] Phillip Pool, "War of the cyber world: The law of cyber warfare," *The International Lawyer* 47, no. 2 (2013): 302.
[238] Ryan Patterson, "Silencing the Call to Arms: A Shift Away from Cyber Attacks as Warfare," *Loyola of Los Angeles Law Review* 48(2015): 980., Note 66.
[239] Schaap, "Cyber warfare operations: Development and use under international law," 137; Raboin, "Corresponding Evolution: International Law and the Emergence of Cyber Warfare," 615; Roberts, "Cyber Wars: Applying Conventional Laws to War to Cyber Warfare and Non-State Actors," 542.

Digital Manipulation

Digital manipulation is another type of cyber attack which is not similar to malware discussed above. While malicious programs represent a combination of certain codes, digital manipulation is not a program by itself it is result of using computer program in order to cause a negative effect on the enemy party. Major Arie J. Schaap appeals to the concept of digital image manipulation and gives the following definition: "Digital image manipulation is the alteration of an image using computer program tools and software to produce a contrived image, which often reflects new meaning".[240] In particular he refers to manipulation of photograph and videos, however, this list is not limited it also includes voice record changing. The main purpose of this type of cyber attack it is not related with disabling enemy's computer system whereas to misinform or deceive the victim.[241]

Currently, the issue of digital manipulation represents considerable interest due to the development or technologies. Why is this so important? First, widespread distribution of videos and photos on the Internet, including those containing speeches government representatives. Second, the possibility of modifying the multimedia files. For example, video can be changed in a real time. No need to spend a large amount of time on it to make a digital manipulation. Third, the low cost of implementation of the cyber attack.Thus, any person with a computer and a specific knowledge hypothetically may cause significant damage to a representative of any state. For example, the attacker may provoke a civil war or a coup d'etat in a particular state only by modifying one of the president's speeches. Pentagon considered this method for the adoption against Saddam Hussein after Iraq's invasion of Kuwait in 1990.[242]

Digital manipulation is not prohibited under humanitarian law and it represents different from Trojan horse and IP spoofing method of cyber warfare since it does not cause harm directly to the enemy. The principle of the prohibition of perfidy is hardly applicable here, however, digital manipulation can significantly influence the actions of particular persons and thus cause indirect damage. George O'Malley classifies actions of informational manipulation to the sabotage and says that "Cyber sabotage involves deliberate and malicious acts that result in the disruption of the normal processes and functions or the destruction or damage of equipment or information".[243] Sabotage are

[240] Schaap, "Cyber warfare operations: Development and use under international law," 137.
[241] Ibid.
[242] "When Seeing and Hearing Isn't Believing", last review March 15, 2017, http://www.washingtonpost.com/wp-srv/national/dotmil/arkin020199.htm, cited in Ibid., 139.
[243] George O'Malley, "Hacktivism: Cyber Activism or Cyber Crime," *Trinity College Law Review* 16(2013): 114.

lawful combat activities until they are directed against legitimate military targets, however, if they are directed against civilians who must not be military targets, it constitute a violation of humanitarian law in particular violation of the principles of distinction and discrimination.

Some important aspects

The main difference between kinetic and cyber war is a weapon. In the first case, the weapon is tangible and its use is perfectly regulated by international instruments. In this case, there is no doubt who carries out the attack; consequently, there should be no problems in order to understand whether the law of armed conflict applies and what kind of norms regulates the particular case. However, in the second case the weapon in its conventional understanding is missing. There is also no direct attack since the object of the attack is a computer system, network or data. A damage which is in this case applied to civilians is not a direct consequence of cyber attacks, it is derived consequence. Therefore, cyber weapons have their own special status. Strictly speaking there is no legal conventional norms that could be applied to it. In this regard, in order to protect civilians, it is necessary to apply a customary law rules such as a prohibition of perfidy, the principles of distinction, discrimination, proportionality and neutrality. However, not all of these principles are applied to each cyberattack or by using any cyber weapon. Thus, for example, if such malware as viruses and worms are eager to steal information or cause any direct damage to the computer or network, electronic manipulation rather seeks to harm the reputation of a person or to mislead.

As we said above, until a certain moment there was no a problem of cyber warfare since the damage caused by the cyber attack was associated exclusively with the data leakage. However, after the cyber attack on Natanz nuclear facilities the issue concerning the safety of civilians emerged. In the next chapter we would like to consider in more detail the Stuxnet worm attack on nuclear facilities of Iran in order to reveal that cyber warfare is a new notion in humanitarian law and it may or may not fall under its rules.

CHAPTER IV

THE STUXNET WORM ATTACK

Stuxnet worm

Stuxnet was a cyber attack sponsored by a state. It was a worm with the ability of self-reproducing by means of the Internet. However, although the worm spread through the Internet, he was uploaded by intermediate devices such as thumb drivers.[244] The worm originally was directed against a specific object namely against the Natanz nuclear facilities, nevertheless, it infected thousands of computer systems. Unlike other worms, Stuxnet was discriminate; it was "designed to perform a specific attack"[245]. First, Stuxnet infected Windows-operating systems, by means of USB devices, and second, it targeted only Programmable Logic Controller (PLC). Jeremy Richmond define PLC as "small computers that typically control simple industrial tasks such as regulating motors and opening and closing valves".[246] They are produced by Siemens and operate in conjunction with Supervisory Control and Data Acquisition (SCADA) systems. According to John Richardson's definition Stuxnet is a "form of malicious software (malware) designed to disrupt a Microsoft Windows-based application employed by an Iranian industrial control system".[247] Ralph Langner identified Stuxnet as a "military-grade cyber missile that was used to launch an 'all-out cyber strike against the Iranian nuclear program'".[248] In this way, "once inside the system, Stuxnet had the ability to degrade or destroy the software on which it operated".[249]

The worm consists of two components: first that inflicts damage and second that covers tracks. While the first component is aimed at infecting the PLC by making changes to the system, the second component is intended to make a copy of the plant system operating at normal conditions.[250] Thus, the worm at the beginning increase in speed of the uranium centrifuges in order to destroy it. Stuxnet increase and decrease the speed of the spinning centrifuges used to enrich uranium, "causing their

---

[244] John Richardson, "Stuxnet as cyberwarfare: applying the law of war to the virtual battlefield," *Journal of Computer & Information Law* 29(2011): 425.

[245] Chance Cammack, "The Stuxnet Worm and Potential Prosecution by the International Criminal Court under the Newly Defined Crime of Aggression," *Tulane Journal Ofint'l & Comp. Law* 20(2011): 316.

[246] Jeremy Richmond, "Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?," *Fordham International Law Journal* 35, no. 3 (2012): 850.

[247] Richardson, "Stuxnet as cyberwarfare: applying the law of war to the virtual battlefield," 425.

[248] Ibid.

[249] Ibid.

[250] Cammack, "The Stuxnet Worm and Potential Prosecution by the International Criminal Court under the Newly Defined Crime of Aggression," 317.

parts to break and thereby crippling the entire uranium enrichment operation".[251] And then it deceives the plant operators installing a rootkit (software that enables undetectable access to a computer)[252] that sends signals to facility operators, who believe that the plant is working properly. Thus, the computers in the operation room just reported normal functioning without any problem.[253]

After the worm penetrates into a computer it attempts to identify whether Siemens SCADA software is present on the computer, if there is no software, Stuxnet "'deactivates' and becomes an inert piece of code".[254] This is the main reason why physical damage was caused only to nuclear facilities without damaging other infected computers, since this type of software is closely related with industrial systems, their hardware and the processes of overseeing and controlling.[255] After determining the type of system the worm examines whether the software is used to control a PLC, whether a certain type of machinery s attached to the PLC, then whether its components are operating under certain conditions such as speed, and finally, Stuxnet delivers its payload.[256] Thereafter, the worm is ready to perform the necessary operations to change the speed of centrifuges and to "hide" these changes.

The origin of the worm shows us that it was an initiative of a state since the project had to require considerable resources such as time and money. Stuxnet took approximately "eight to ten computer programmers up to six month to write"[257]. Peter W. Singer emphasizes that "Stuxnet's makers had enormous resources and wanted to be absolutely certain they would penetrate their target".[258] Moreover, the fact that the target was pretty specific also limits the circle of persons who might be interested in committing the attack, speaking more precisely it is supposed that it was the United Stated or Israel. Initially the origins of the worm were unknown because the United States refused to confirm or deny its participation in the development of Stuxnet.[259] However, on June 1,

---

[251] David Weissbrodt, "Cyber-conflict, Cyber-crime, and Cyber-espionage," *Minnesota Journal of International Law* 22, no. 2 (2013): 351.
[252] Richmond, "Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?," 851.
[253] Weissbrodt, "Cyber-conflict, Cyber-crime, and Cyber-espionage," 351.
[254] Richmond, "Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?," 850.
[255] Ibid.
[256] Ibid.
[257] Cammack, "The Stuxnet Worm and Potential Prosecution by the International Criminal Court under the Newly Defined Crime of Aggression," 318.
[258] P. W. Singer, "Stuxnet and its hidden lessons on the ethics of cyberweapons," *Case Western Reserve Journal of International Law* 47(2015): 81.
[259] Richmond, "Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?," 845.

2012, administration of Barack Obama recognized that the worm was a joint project of the United Stated and Israel aiming to disrupt nuclear program of Iran.[260] It was so cold the "Olympic Games" program that was launched at the presidency of George Walker Bush and continued by Barack Obama's administration.[261]

The worm has some specific features that distinguish it from other, one of them it is its ability to hide from detection. While Stuxnet spreads, it uses a "digital signature" which is necessary for authentication on a new infected computer.[262] The digital signature is a key for identification in situation when a program is transferred from one machine to another. Stuxnet's signature received from Realtek Semiconductor Corporation allows the worm to access to a greater number of computers.[263] Moreover, the worm allows each computer to infect no more than three other computers.[264] The other characteristic is that Stuxnet was programmed to self-destruction on a specific date, i.e. on June 24, 2012.[265] Another feature that distinguishes Stuxnet from other worms and malware is its selectivity in attack. We will discuss it in more detail in the following paragraphs.

Stuxnet worm attack raised global concern relatively to cyber attacks. Although the attack did not cause any damage to civilians or civilian objects[266] it showed that worms, viruses and other means of cyber warfare have a great potential in modern wars. Such manipulations with the centrifuges caused a physical destruction of property, and Stuxnet damaged approximately 1,000 centrifuges.[267] It means that from this point onwards it is possible to damage any object that is operated by a computer systems including civilian objects or dual-use objects. Such destructions "rises above the level of a 'minor inconvenience or irritation'"[268].

Although the worm was design to attack a specific purpose it was distributed to more than 100,000 computer systems by occasionally.[269] Stuxnet's target was Iran but infected operational systems also were found in India, Indonesia, the United States and other countries. According to Symantec Corporation's study 62,867 in India, 13,336 in Indonesia, 6,552 in India, 2,913 in the

[260] Weissbrodt, "Cyber-conflict, Cyber-crime, and Cyber-espionage," 351.
[261] Ibid.
[262] Richmond, "Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?," 851.
[263] Ibid., 852.
[264] Singer, "Stuxnet and its hidden lessons on the ethics of cyberweapons," 81.
[265] Weissbrodt, "Cyber-conflict, Cyber-crime, and Cyber-espionage," 351.
[266] Allison Arnold, "Cyber "Hostilities" and the War Powers Resolution," *Military Law Review* 217(2013): 188.
[267] Ibid., 187.
[268] Weissbrodt, "Cyber-conflict, Cyber-crime, and Cyber-espionage," 377.
[269] Richmond, "Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?," 888.

United States, 2,436 in Australia, 1,038 in Britain, 1,013 in Malaysia, and 993 in Pakistan.[270] According to other sources among infected countries are also China, Finland, and Germany.[271]

Thus, taking into account all the characteristics of Stuxnet we can conclude that "it represents a major new development in warfare technology".[272] It may seem that Stuxnet is the next stage in the development of the weapon, due to the fact that it can perform functions of the kinetic weapon but with great accuracy.[273] Peter W. Singer asserts that Stuxnet is new kind of weapon design to cause physical damage in the real world by means of digital networks.[274]

Applicability of IHL

The issue of the applicability of humanitarian law to Stuxnet worm attack is closely related to the matter of dispute whether humanitarian law should apply to the cyber warfare. And there is no consensus on this matter. The debate embodies several questions as to whether a cyber attack is an act of war, which is the threshold, whether a cyber attack in conformity with humanitarian law, and the problem of attribution.

To begin with it is necessary to understand if the attack on Natanz marked the beginning of armed conflict. According to the Article 49 of Additional Protocol I an armed attack is "acts of violence against the adversary, whether in offence or in defence". Michael N. Schmitt argues that the concept of "violence" includes violent consequence where "significant human suffering or mental anguish is included in the concept of injury, as does loss of assets (investments, savings, and the like) constitute damage or destruction. However, mere inconvenience or discomfort is insufficient".[275] Humanitarian law, thus, applies in situation where a cyber attack can be attributed to a state which had the intention to inflict injury, death, damage, or destruction to adversary. Before the Stuxnet worm attack the issue had a special significance since cyber attack did not cause a physical damage, however, in the present case the worm destroyed the centrifuges that according to the United States set back the Iranian nuclear program from eighteen months to two years.[276] Thus, it may seem that

[270] Richardson, "Stuxnet as cyberwarfare: applying the law of war to the virtual battlefield," 6.
[271] Ibid., 425.
[272] Richmond, "Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?," 852.
[273] Ibid.
[274] Singer, "Stuxnet and its hidden lessons on the ethics of cyberweapons," 84.
[275] Richardson, "Stuxnet as cyberwarfare: applying the law of war to the virtual battlefield," 9.
[276] Weissbrodt, "Cyber-conflict, Cyber-crime, and Cyber-espionage," 377.

the threshold of the armed conflict is reached since the was an act of violence and moreover since the United Stated confessed to the attack and its intentions to stop Iranian nuclear program. Nevertheless, the doctrine provides other criteria to be met in order to characterized the situation as an armed conflict. Jean Pictet, for example, argues that the armed conflict must have "the sufficient scope, duration and intensity".[277] However, this approach is also criticized by scholars since it does not determine whether a cyber attack is an armed attack.[278]

Additionally, there are three models developed to apply Pictet's Use of Force Continuum for assessing different unconventional attacks such as cyber attacks.[279] First model is an instrument-based approach, which consider whether the damage caused by an unconventional attack could have ben achieved previously by the kinetic weapon. The destruction of centrifuges could be carried out by different types of kinetic weapon and in the case of Stuxnet there is no doubts. However, if we take into account all cyber attacks, this approach may be inappropriate since it "does not account for attacks that damage or destroy data while leaving hardware intact".[280]

Second model is an effect-based or consequence-based approach, which considers overall effect of the attack on the state-victim.[281] Considering the Stuxnet attack on Iran we can conclude that it affected only state's nuclear program. The target was quite specific and the consequence of the attack fairly controversial. The question is whether the attack has affected the well-being of the state to be considered as an armed attack? It can be argued that the attack had no much influence on the state and its population, however, the opinion of the state and the reasons for which the program was developed should be considered additionally. Some authors believe that this model better address the complexities of cyber attacks and consequently it is better applicable.[282]

Third model is a strict liability approach, which asserts that any attack against critical infrastructure of the states is automatically treated as an armed attack.[283] For example, any attack against water supply, electricity generation or security services could be described as an armed attack. Two questions arise, first, what was the purpose of the attack, and second, whether the nuclear facilities are critical infrastructure. Considering the first issue it is necessary to note that Stuxnet

---

[277] Richardson, "Stuxnet as cyberwarfare: applying the law of war to the virtual battlefield," 10.
[278] Ibid.
[279] Jeffrey Carr, *Inside cyber warfare: Mapping the cyber underworld* (Beijing Sebastopol, CA: "O'Reilly Media, Inc.", 2011). 59.
[280] Richardson, "Stuxnet as cyberwarfare: applying the law of war to the virtual battlefield," 10.
[281] Carr, *Inside cyber warfare: Mapping the cyber underworld*: 59.
[282] Richardson, "Stuxnet as cyberwarfare: applying the law of war to the virtual battlefield," 10.
[283] Carr, *Inside cyber warfare: Mapping the cyber underworld*: 59.

attack was not destructive, it disrupt the nuclear plant. The difference between two notion is that in the first case the main goal of the attack is to destroy a whole plant while in the second case the attack may destroy only internal computer system without causing the complete destruction. Taking into account the second issue, we would assert that nuclear facilities are critical infrastructure since the functioning of the nuclear plant is closely related to the issues of security and electricity supply. The answer, thus, is not straightforward. Other authors, for example, emphasize that damage on a smaller scale as disruption of a municipal water or sewage facility does not constitute an armed attack.[284] Thus, the present model is also quite specific and could not be applicable to all cyber attacks.

Nevertheless, there is an opinion that humanitarian law applies to the situation of cyber war only by analogy since "cyber attacks do not constitute armed attacks".[285] On the one hand, scholars argue that cyber weapons go beyond humanitarian law, and from the other side, other scholars approve that rules of the of armed conflict is outdated since the creators of the rules could not means a weapon that at that time did not exist. In this regard, we would like to notice that, first, such rules as norms of customary international law could not be out of date and must be applicable to any situation of armed conflict. And second, the law of armed conflict includes new means and methods of warfare. Moreover, in 2003 the International Committee of the Red Cross stated that "the existing legal framework is sufficient to deal with present day conflicts".[286] Additionally, some persons argue that cyber warfare needs additional regulation such as new treaty. However, there is also no consensus: some scholars say that such a treaty due to the cyber capabilities cannot be "enforceable or workable", and others that treaty "is not only workable, but necessary".[287] From our point of view, the application of humanitarian to the situation of Stuxnet possible and even to some extent necessary.

Cyber attack may initiate international armed conflict[288]; however, it does not mean that every cyber attack must lead to the war and consequently to the automatic application of humanitarian law. Stuxnet attack, in our view, although it was an armed attack, did not lead to the emergence of armed conflict. Nevertheless, this does not prevent us from applying the norms of humanitarian law to the attack, since "international humanitarian law principles apply whenever computer network attacks can be ascribed to a State… and are either intended to cause injury, death, damage or destruction".[289]

---

[284] Richardson, "Stuxnet as cyberwarfare: applying the law of war to the virtual battlefield," 10.
[285] Jordan Peagler, "The Stuxnet Attack: A New Form of Warfare and the (In) Applicability of Current International Law," *Arizona Journal of International & Comparative Law* 31, no. 2 (2014): 409.
[286] Peagler, "The Stuxnet Attack: A New Form of Warfare and the (In) Applicability of Current International Law," 428.
[287] Ibid., 429.
[288] Gary D. Solis, "Cyber warfare," *Military Law Review* 219(2014): 18.
[289] Ibid.

By this standard, the cyber attack on Iranian nuclear facilities by agents of the United States would implicate humanitarian law.

The Stuxnet worm attack arise several issues, for example, whether such principle as distinction, discrimination and the principle of proportionality are applicable. In particular, whether the worm can distinguish between possible civilian objects and military objectives, and whether the attack was performed in a manner to minimized possible damage to civilians.[290] We will consider each of these principles below.

Distinction

The principle of distinction includes two elements: obligation to distinguish civilians and combatants, and obligation to distinguish civilian objects and military objectives. Application of the principle of distinction in the present case is closely related with the notion of military objective. Is Iranian nuclear plant a legitimate military objective? Does Stuxnet distinguish military objectives and civilian objects? We will not consider first element since it is not applicable to Stuxnet because no persons were target by the attack.[291]

According to customary international law Natanz nuclear facilities to be legal military objective must "by their nature, location, purpose or use make an effective contribution to military action and whose partial or total destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage"[292]. The first thing worth determining is whether Natanz nuclear plant make an effective contribution to military action. There are two hypothetical options when it is possible. The first one is that the purpose of uranium enrichment at Natanz was the creation of a nuclear weapons.[293] In this case Natanz could be a legitimate military target. The second one is that the centrifuges could be enriching uranium for Iranian nuclear power plants.[294] Legitimate military targets include installations providing energy, for example, plant producing gas or electricity. However, attacks on nuclear power plants are generally prohibited. International customary law says

[290] Richardson, "Stuxnet as cyberwarfare: applying the law of war to the virtual battlefield," 17.
[291] Richmond, "Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?," 874.
[292] Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary international humanitarian law*, vol. 1 (Cambridge: Cambridge University Press, International Committee of the Red Cross, 2005).Rule 8
[293] Richmond, "Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?," 884.
[294] Ibid.

that "particular care must be taken if works and installations containing dangerous forces, namely dams, dykes and nuclear electrical generating stations, and other installations located at or in their vicinity are attacked, in order to avoid the release of dangerous forces and consequent severe losses among the civilian population".[295] The Legal Adviser of the US Department of State in 1987 stated that attack on military objectives which can release the radiation and cause severe civilian causalities must be prohibited. Although customary international law does not prohibited directly the attack on nuclear installations, humanitarian law instruments such as Additional protocol I Article 56 and Additional Protocol II Article 15 protect these types of installations which in accordance with custom are legitimate military objectives. There are some exceptions from this rule, thus, if a nuclear power plant is used "in regular, significant, and direct support of military operations" in the form of electric power, it loses it protection. This can also include "production of arms, ammunition, and military equipment". The Legal Adviser of the US Department of State also stated that the electricity produced in nuclear power plant may also be used by civilians and usually it is impossible to say who the customer is. In this regard, "a nuclear power plant that is being used to produce plutonium for nuclear weapons purposes would not lose its protection". Thus, even if we do not know the real purpose of Natanz nuclear station, anyway it does not lose its protection. Even if the goal is the production of weapons and electric power for military objectives Natanz is protected under humanitarian norms.

However, exist other opinion, Jeremy Richmond, for example, asserts that in both cases Natanz is military legitimate target. In accordance with his point of view, the possibility of uranium enrichment for nuclear weapons creation or for fuel render Natanz as acceptable military target. [296] He bases the position on the facts that such actions constitute an effective military contribution and thus it is possible to say that nuclear power plant is military objective. The opinion is also supported by the fact than no damage was caused to civilians. However, if Stuxnet infected civilian computers as a "stepping-stone" to infecting Natanz, then it will constitute violation of the principle of distinction. This is applicable even in the case where civilians suffered no harm.[297]

The second part of the question is whether Stuxnet distinguished between military objective and civilian objects. The harmful effect of the worm was quite discriminative due to the fact that it was directed against a specific computer system. Moreover, its spread among civilian computers was a coincidence and not a planned attack. But even this case Stuxnet did not cause damage to civilians.

---

[295] Henckaerts and Doswald-Beck, *Customary international humanitarian law*, 1. Rule 42.

[296] Richmond, "Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?," 884.

[297] Ibid., 885.

All this demonstrates that the worm acts within the principle of distinction. There is an opinion that cyber attacks against civilian objects may be considered lawful "if it did not cause the destruction or if its effects are reversible".[298] However, the International Committee of the Red Cross stated that it does not matter whether the cyber attack caused any destruction, since "only those objects, which make an effective contribution to military action and whose total or partial destruction, capture or neutralization offers a definite military advantage, may be attacked".[299] Thus, any attack even accidental and without any damage is prohibited.

Some authors argue that Natanz nuclear plant was legitimate military target since it was dual-use object, i.e. the object that serves both civilians and military. John Richardson says that there is no evidence against whom the attack was directed, and even if we assume that the attack was against civilians, "the dual-purpose of the Natanz facility makes it a legitimate target".[300] With regard to this argument, we must object since there are circumstances when it is not lawful to target such dual-use objects. For example, targeting against power grids can have a huge impact on civilian population. Thus, before the attack it is necessary to consider all consequences that would cause the attack and especially its impacts on civilian population.[301]

The Tallinn Manual also establishes that the principle of distinction applies to cyber attacks.[302] Rule 37 of the Manual says that civilian objects shall not be an object of the attack while "computers, computer networks, and cyber infrastructure may be made the object of attack if they are military objectives". As we stated above, Natanz nuclear plant can hardly be called a military objective. However, even if we assume that the nuclear plant is a military objective, there is Rule 80 that prohibits attacks against installations containing dangerous forces. Thus, we can conclude that "determination that Natanz was not a valid military objective would render Stuxnet illegal, regardless of the worm's adherence to the principles of discrimination and proportionality".[303]

---

[298] Richardson, "Stuxnet as cyberwarfare: applying the law of war to the virtual battlefield," 16.
[299] Ibid., 17.
[300] Ibid., 23.
[301] Angelina Harutyunyan, "Dilemma of Targeting: Dual-Use Objects in Military Operations," *Law of Armed Conflict* (n.d.): 4.
[302] Henckaerts and Doswald-Beck, *Customary international humanitarian law*, 1. Rule 31.
[303] Richmond, "Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?," 883.

Discrimination

As we mentioned in Chapter I the principle of discrimination consists of three components. First, Stuxnet must be directed only against military objectives, second, means and methods of the cyber attack must be directed only against specific objective, and third, the effects of the cyber attack must be limited. The main distinguishing feature of the worm is that Stuxnet was created specifically for particular computer system attack. In comparison with other worms, it is quite discriminative. Initially, it was directed only against Natanz nuclear facility, the worm did not try even to infect as many computer systems as possible. Moreover, it was directed against specific objective. Stuxnet was not intended to attack different Iranian objects, it even did not intend to attack other nuclear stations in Iran. The main purpose was Natanz facility. And finally, it is assumed that the worm was programmed specifically to avoid the possible destruction of other objects. It seems that the attack was conducted in accordance with the principle of discrimination. However, the principle of discrimination should also be considered in conjunction with the possibility of Stuxnet to distinguish military objectives and correlated things. With a traditional weapon that implies collateral damage or physical area surrounding the target, while with cyber weapon that means "potential damage to connected computers or computer networks".[304] Michael Schmitt argued that if a worm cannot limit its transmission, then it should be prohibited as indiscriminate.[305] Stuxnet from the one side is absolutely indiscriminative in spreading because it infected more than 100,000 computers. Moreover, the fact that no damage was caused should not be considered as mitigating factor, since "the damage actually done by Stuxnet is not what must be considered when analyzing the principle of discrimination"[306]. Two factor that should be considered are what the commander expected at the time of deployment and if everything feasible was done to gather information before launching the attack.[307] However, due to the fact that there is no any available information related to the expectations of the commanders or whether they took all feasible measures to gather necessary information before the attack, it seems impossible to make any conclusion on this matter. The only thing that can be analyzed is the worm itself and they it performed the attack.

Thus, for example, as we mentioned bellowed, Stuxnet was created for the purpose of causing damage only to a specific objective – Natanz nuclear facilities. Despite the fact that the worm was distributed across all Windows systems, it did not damage other facilities outside of the Natanz. This

[304] Ibid., 885.
[305] Ibid.
[306] Ibid., 886.
[307] Ibid.

fact is of greater importance in view of the fact that with such a large-scale distribution, the worm caused damage only to one objective. On the one hand, it can characterize the worm as quite discriminating, from the other side; it demonstrates that creators of Stuxnet, who invested a lot of time and money in its creation, tried to create the worm in accordance with the norm of humanitarian law. Or at least, they took all measures at the development stage to prevent the spread of damage across other computer systems. The developers also had to conduct large-scale research in this area both regarding the Natanz facilities and relative to other similar facilities that could have been accidentally damaged. The same point of view is also held by other authors, for example, by Jeremy Richmond. Moreover, in his article he also affirms that according to US policy there is a requirement for all commanders "to full investigate possible unintended consequences of malware".[308]

Considering the situation from the other side, the worm was limited since its destructive effects affect only intended target. Indeed, although it is unknown whether civilian computer systems suffered some sort of damage, it is supposed that even if the damage was caused, it was minimal. Additionally, it should be mentioned that even the spread of worm was restricted by the creators, thus, it could not replicate itself indefinitely. Moreover, the worm after the execution of the attack was programed to self-destruction. This indicated that, to some extent, certain precautions have been taken.

If the application of the principle of distinction raises some doubts as to whether Stuxnet is in conformity with humanitarian law, with the application of the principle of discrimination there seems to be no doubt although the information to which it is worthwhile to operate in second case is rather meager. This is due to the fact that the application of the first principle is related to the question of doctrine while the application of the second principle is more connected with facts and intentions of the attacking party.

The application of the principle of discrimination is perfectly demonstrates that Stuxnet could be considered as lawful cyber attack under humanitarian law. It also demonstrates that any cyber weapon regardless of the type of malicious program could be created and programed in accordance with the norms of humanitarian law. This fact can serve as a counter-argument against those who claim that humanitarian law is outdated or that cyber attacks go beyond the scope of humanitarian law. Stuxnet had a great potential for destruction not only centrifuges but entire Natanz nuclear facility and other similar facilities. Jeremy Richmond concludes that the creators of Stuxnet took into account the principles of humanitarian law although the law of armed conflict did not apply and that

[308] Ibid., 887.

"the application of the principle of discrimination to Stuxnet assured that civilian objects were not harmed and that the overall level of destruction caused by the worm was minimalized".[309]

The Tallinn Manual also specifically mentions Stuxnet-like malware and assures that such malware does not violate the principle of discrimination since although it spreads widely the harmful effects of worms extends only to a specific objet.[310]

Nevertheless, if the situation with cyber attacks was so clear and simple then there would be no controversy. But there are debates. Indeed, some authors agree that Stuxnet had a particular objective of the attack and therefore it can be described as discriminative weapon. However, if we look beyond such worm attacks demonstrate vulnerabilities of a huge amount of computer systems. Such cyber attacks threaten the subsequent existence vulnerable computer systems regardless of whether they are military or civilian object. The vulnerability information may be reused in a peacetime and in war time.[311] Thomas Cross makes the assumption[312] that the use of such vulnerability may fall under Rule 43 of the Tallinn Manual, where it says that the use of weapons that by their nature are incapable of being controlled in particular that create an uncontrollable chain of events should be prohibited[313], where the reuse of vulnerability can be correlated with uncontrollable chain of events. However, considering the issue in more detail, he notices that this would be incorrect. Each creator of the malware makes a choice of a type of the attack and the consequences that entails the attack. And each case should of cyber attack should be analyze separately. Thomas Cross proposes in the present case to use Rule 51 of the Tallinn Manual related to the principles of proportionality, however, even applying this principle to Stuxnet attack he concludes that the damage caused to other parties did not meet the threshold.[314]

Proportionality

According to the principle of proportionality the commander of the Stuxnet worm attack after weighting all available information had to take all feasible precautions in order to mitigate or to avoid

[309] Ibid., 889.
[310] Henckaerts and Doswald-Beck, *Customary international humanitarian law*, 1. Rule 43.5
[311] Thomas Cross, "Legal Implications of Vulnerability Disclosure in International Conflict," *Journal of Law and Cyber Warfare* 4(2014): 103.
[312] Ibid., 104.
[313] Henckaerts and Doswald-Beck, *Customary international humanitarian law*, 1. Rule 43.4
[314] Cross, "Legal Implications of Vulnerability Disclosure in International Conflict," 105.

civilian causalities[315]. In humanitarian law, civilian lives "are given greater weight in the proportionality analysis than civilian property".[316] In case of Stuxnet attack it means that even the worm has affected civilian property i.e. civilian computer systems, the fact that it avoided civilian loses makes the worm attack legitimate in terms of the principle of proportionality. In addition, the fact that Israel and the United States have chosen a cyber attack instead of the kinetic attack shows their foresight. Indeed, if the United Stated or Israel had decided to attack Natanz nuclear facilities by means of bombing, for example, it could provoke more serious consequences both for the nuclear plant and for civilians who worked at the station and who were outside of the nuclear plant.[317] In this regard, the choice in favor of a cyber attack seems to be more rational and in conformity with the principle of precautions. This also demonstrates some advantage of cyber attack before the kinetic attack. Instead of destroying entire nuclear plant and causing irreversible consequences cause by radiation release, the creator of Stuxnet just disabled centrifuges for a certain period of time.

The principle of proportionality established that the number of affected civilians should not disproportionate to gained military advantage or otherwise the attack would not be legitimate. As we mentioned, Stuxnet worm destroyed more than 1000 centrifuges and this damage is "extensive and multifaceted".[318] Further consideration should be given a military advantage that Israel and the United States have received. From the point of view of the attackers, the main purpose of the attack was to prevent the development of nuclear weapon by Iran. After the attack, Iran stated that it would take about two years to recover from the damage. If we consider the situation from this point of view, then a significant military advantage was achieved. The same opinion is held by Jeremy Richmond.[319]

The second point is that the principle of proportionality prohibits excessive damage to civilians in the relation to the concrete and direct military advantage which is expected. Stuxnet worm attack has caused a minimal damage to civilian population since "the payload was never delivered to civilian computers; the 'inert' worm caused little to no damage to civilian computers; and the worm has a self-destruct deadline".[320] And the military advantage that the United States and Israel have gained by deploying Stuxnet "was significantly greater than the harm to civilian objects" since it

[315] Henckaerts and Doswald-Beck, *Customary international humanitarian law*, vol. 1, Rule 22.
[316] Richmond, "Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?," 889.
[317] Ibid.
[318] Ibid., 890.
[319] Ibid.
[320] Ibid., 891.

could stop for two years Iranian nuclear program.[321] Thus, the damage cause by the cyber attack was not excessive to the concrete and direct military advantage that was gained.

General conclusions

Stuxnet worm attack was the first demonstration of the cyber weapon's power. This cyber attack was really revolutionary because it raised new issues in the field of the application of humanitarian law to modern wars. Stuxnet was the first worm that caused physical damage to the real world and thus brought the worm to the new level of regulation. It is worth to mention that Stuxnet cyber attack could be attributed to the armed attack and consequently this will entail the application of humanitarian law principles, such as distinction, discrimination and proportionality. There are different opinions whether the worm violates this principles. We could possible argue that Stuxnet violates the first and more important principle – the principle of distinction. However, according to our analysis there is no any doubt that the worm attack was in conformity with other customary law principles.

In the previous chapters, we considered the notion of cyber attack together with the humanitarian law and in particular with the customary law principles. However, as we mentioned, there is no consensus on application of the humanitarian law, although, from our point of view, humanitarian law is perfectly applicable and it is being demonstrated by the example of Stuxnet, nevertheless, we should not completely exclude other point of view. In this regard, the last chapter we will devote the last chapter to the application of the human rights law to the cyber conflict. The main difference between human rights and humanitarian law constitutes the fact that humanitarian applies only to armed conflict (and we have no agreed opinion whether Stuxnet attack is armed attack) while human rights law applies both during the peace time and the war time. Thus, it seems more rational try to apply norm or human rights law.

[321] Ibid.

CHAPTER V

HUMAN RIGHTS CONSTRAINT AGAINST CYBER WEAPONS

International Human Rights Law

Human rights apply both offline and online; it is widely enshrined in international human rights instruments[322], the International Group of Experts (the Experts) also recognized this in the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations[323]. In additions, they also agreed that treaties and customary international human rights law are both applicable to cyber activities.[324] Just as in the case of humanitarian law, the norms of international human rights treaties apply only to the parties to the treaties. Moreover, most of them have a regional character and depend on the regional system for the protection of human rights. The customary laws that are contained in the Universal Declaration of Human Rights and some of them in the International Covenant on Civil and Political Rights and International Covenant on Economic, Social and Cultural Rights does not have any single source where all customary laws would be listed. Therefore, the application of human rights to cyber warfare in the form of a global standard seems somewhat problematic. In addition, the Experts also agreed that the implementation of human rights should be carried out at the regional and national level, taking into account "different political, economic, legal, social, cultural, historical and religious backgrounds".[325]

International humanitarian law and human rights law are both applicable to the situation of cyber war.[326] However, international humanitarian law applies as *lex specialis*. This means that in case of contradictions between legal norms, the norms of humanitarian law will prevail over human

[322] The Promotion, Protection and Enjoyment of Human Rights on the Internet, para. 1, UN Doc. A/HRC/32/L.20 (27 June 2016); The Right to Privacy in the Digital Age, GA Res. 68/167, para. 3, UN Doc. A/RES/68/167 (18 December 2013); EU Human Rights Guidelines on Freedom of Expression Online and Offline, Council of the European Union, para. 6 (12 May 2014); UN GGE 2013 Report, para. 21; UN GGE 2015 Report, paras. 13(e), 26; NATO 2016 Warsaw Summit Communiqué, para. 70; Convention on Cybercrime, pmbl., Art. 15.1; Deauville G8 Declaration: Renewed Commitment for Freedom and Democracy, para. IIи(10) (26–27 May 2011); Agreement between the Governments of the Member States of Shanghai Cooperation Organization on Cooperation in the field of International Information Security, Art. 4(1), 16 June 2009.

[323] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations: Prepared by the International Group of Experts at the Invitation of the Nato Cooperative Cyber Defence Centre of Excellence* (Cambridge New York: Cambridge University Press, 2017): 179.

[324] Ibid.

[325] Ibid., 180.

[326] Ibid., 181.

rights. For instance, the right to life and the prohibition of arbitrary deprivation of life are violated during the armed conflict.

Moreover, human rights may be a subject of limitation by sates in certain circumstances as matter of national security. Most international instruments on human rights also provide for a state the possibility of derogation to a certain extent but only if it does not violate international law. This means that in order for a state to violate the human rights norm it should be bound by the treaty, cyber-related activities of a person must fall within the scope of particular legal norm, the act of state is contrary to the norms of international law, and there is no lawful limitations on that particular norm.[327]

Nevertheless, all states must respect and protect human rights. The obligation to respect obliges state to "refrain from unlawfully interfering with human rights that individual enjoy".[328] While the obligation to protect imposes the legal requirement to take all possible measures to "ensure third parties do not interfere with the enjoyment of human rights".[329] States are also responsible for all violations of human rights that they committed.[330]

Human rights and cyber warfare

The discussions concerning human rights application during cyber warfare are not a new phenomenon. As well as disputes over the application of humanitarian law, the issue of "digital rights" is widely discussed by the public and scholars. Some of them believe that the development of technologies in particular, computer systems, networks, malware, is the cause of the emergence of a new kind of war - "World Wide War".[331] This new kind of war unites states, non-state actor, hackers, and just civilians. Thus, the main purpose of the "wide war" is to control the access to data[332] instead of destroying enemy's military forces. On the one hand, the state tries to protect the civilian population by signing international instruments on the protection of human rights; on the other hand, the state is some sort of enemy that tries to take advantage of the vulnerability of civilians. In this

[327] Ibid., 182.
[328] Ibid., 181.
[329] Ibid.
[330] Ibid. Rule 34
[331] Anja Mihr, "Cyber Justice: Cyber Governance through Human Rights and a Rule of Law in the Internet," *US-China Law Review* 13(2016): 319.
[332] Ibid., 320.

regard, here are various rights to protect a human being, to prevent abuse of private data, to provide a free access to information; however, none of them is effective since cyber warfare casts doubt on their effectiveness. We will consider human rights that should be applicable to the situation of cyber war and "the challenge will be to assess how human rights can be fully guaranteed under the arrangements and agreements".[333]

There are a large number of rights and freedoms that can be affected by cyber conflict, for example, basic rights: right to life if the cyber attack caused death, to food or to medicine if the cyber attack was performed against critical infrastructure and damaged the food production and distribution or hospitals and ambulances. However, in this paper we will not consider the application of these rights within the framework of cyber war since the situations in which these rights apply are quite exceptional.

There is another type of rights namely "digital rights", or rights and freedoms relevant to the Internet. Such rights include freedom of expression, data protection, and privacy, freedom of association, intellectual property rights, right to be forgotten, right to Internet and right of access to information. In the present chapter, we will consider some of them those that are more applicable to cyber attacks.

The main difference between humanitarian law and human rights law is that in the second case "human person is the central subject of human rights and fundamental freedoms, and consequently should be the main beneficiary and should participate actively in the realization of these rights and freedoms".[334] While in the first case, well-being and security of a person can be evaluated less that of the society as a whole. Human rights are also applicable to everyone without any discrimination whether based on "nationality, place of residence, sex, national or ethnic origin, color, religion, language, or any other status". Rights granted by humanitarian law on the contrary are discriminatory, some of them are provided only to a defined group at a particular time and under certain conditions. That is why there are questions about the possibility of applying humanitarian law to a cyber attack.

Human rights are generally guaranteed by treaties, customary international law, general principles of law and other sources of international law.[335] They provide rights and freedoms of

[333] Ibid.
[334] Ibid., 321.
[335] Statute of the International Court of Justice, San Francisco, 26 June 1945

individuals and obligations and duties of governments, companies, individuals and others.[336] Every state or company has to respect and protect human rights, although most of them originate in international agreements such as International Covenant on Civil and Political Rights (ICCPR), they are still closely related the customary international law. Thus, for example, ICCPR is the legal-binding embodiment of Universal Declaration on Human Rights, and therefore all members of the first convent must respect declaration.

Many representative of non-governmental organizations have expressed their concern about the fact that human rights are not protected during cyber conflict. Thus, for example, the Electronic Frontier Foundation (EFF) has stated, "technologies can open a Pandora's Box of previously unimaginable site surveillance intrusions and metadata can reveal sensitive information that can be easily accessed, stored, mined and exploited".[337] In addition, still "there is no internal cyber law to combat cyber-attacks or the dissemination of private data and secret files".[338] Probably the absence of of the law or any treaty on cyber matters is justified by the fact that the existence of humanitarian law and human rights is sufficient to address the issue. Anja Mihr adheres to the same opinion and considers that "there is no need… to establish a separate set of human rights standards for cyberspace or for the Internet. Human Rights apply offline as well as online".[339]

Data-protection issues

Data-protection is a part of personal privacy and the rights developed out the right to respect for private right.[340] According to the definition of the Council of Europe Convention[341], "personal data" is any information relating to an identified or identifiable individual, for example, name, address, date of birth and national insurance number. Article 8 (1) of the European Convention of Human Rights sets forth "everyone has the right to respect for his private and family life, his home and his correspondence". Article 12 of the Universal Declaration of Human Rights also establishes that "no one should be subjected to arbitrary interference with his privacy, family, home or

[336] Mihr, "Cyber Justice: Cyber Governance through Human Rights and a Rule of Law in the Internet," 321.
[337] Ibid., 324.
[338] Ibid., 325.
[339] Ibid., 336; Schmitt, *Tallinn manual on the international law applicable to cyber warfare : prepared by the international group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence.*
[340] European Union Agency for Fundamental Rights, *Handbook on European data protection law* (Luxembourg: Publications Office of the European Union, 2014). 37.
[341] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg, 28/01/1981, Article 8.

correspondence, nor to attacks upon his honour and reputation". The right is applicable only to human beings and therefore only natural persons may have rights, however, national organs of a state may freely regulate this subject.[342]

According to European Union regulation, information contains personal information if: an individual is identified in this information, or if an individual is described in a way, which makes it, possible to find out who the data subject is.[343] This fact was also confirmed in the European Court of Human Rights.[344] Moreover, a person may be considered as identifiable if "a piece of information contains elements of identification through which the person can be identified, directly or indirectly".[345]

The right to data-protection covers different types of information including personal life information, and additionally professional or social life information.[346] In Volker and Markus Schecke and Hartmut Eifert v. Land Hessen case, the European Court of Human Rights said, "the term 'private life' must not be interpreted restrictively". Additionally, the form in which the data is stored does not matter, this may be an image, IP address, sounds, closed-circuit television footage and etc.[347] Under European Union law there is special category of personal data that by its nature may endangered the data subject. Thus, the processing of such data revealing racial or ethnic group, political opinions, religious or other beliefs, and concerning health and sexual life[348] must be allowed only with a specific precautions or safeguards.

Article 2 of the Convention on Cybercrime establishes that every state-party "shall adopt such legislation and other measures as may be necessary to establish as criminal offences under its domestic law, when committed internationally, the access to the whole or any part of computer system without right. A Party may require that the offence be committed… with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system".

International humanitarian law does not prohibits such actions during wartime, in view of this, the emergence of Stuxnet worm, which showed all the danger of the malware and the entire level of

[342] European Union Agency for Fundamental Rights, *Handbook on European data protection law*: 38.
[343] Ibid., 39.
[344] Ibid.
[345] Ibid., 40.
[346] Ibid., 42.
[347] Ibid., 43.
[348] Ibid.

harm that it can inflict, caused worldwide concern. The collection of information during the war is not something forbidden, therefore worms or viruses that simply spied or gathered information were legitimate weapons. However, human rights law impose constraints on such intrusion in private life. For example, a state that by means of cyber attack gather private data of individual would probably violate the right to private life.

Certain types of malware violate the right of data-protection, for example, worms or viruses that collect and make sensitive information available to the attacker, or Trojan horses that can gather information by different means bot inside of computer and outside (using web camera, for example). IP spoofing besides that it can collect information goes further and offers users to enter personal information by deceiving their trust.

It seems difficult to apply human rights to the situation of cyber conflict, first of all, due to the fact that humanitarian law is *lex specials* and even if human rights protect right to life, humanitarian law provides exemptions when the right could be violated. Therefore, if there is a military conflict, it is always possible to claim that human rights are *lex generalis*.

Moreover, the application of human rights is also connected with certain problems. First, the problem of attribution when states do not recognized that they carried out the attack. In the case of an attack on Iranian nuclear facilities, initially neither Iran nor the United States recognized their participation in the creation and development the worm. The application of human rights does not depend on whether it is known who committed the attack, unlike humanitarian law human rights applied automatically. However, in order to demand rights and freedoms and in order to say that they were violated it is necessary to know from whom to demand observance from the law.

Perhaps, it is impossible to say with a high degree of probability that the right to data-protection is applicable and will be applied to cyber warfare, nevertheless, the right to privacy has not been cancelled and it means that this can be a starting point for development and implementation personal privacy right at a higher degree.

Freedom of expression, the right to information and the right to Internet

Article 19 of the Universal Declaration on Human Rights states that “everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless

of frontiers". Freedom of expression is also protected by Article 11 of the Charter of Fundamental Rights of the European Union, Article 10 of the European Convention on Human Rights, Preamble Convention on Cybercrime. There is a certain relation between the right to privacy and the freedom of expression and it may seem that they contradict. However, Article 9 of the Data Protection Directive provides derogations or limitations to the protection of data and consequently to the principle of privacy. Nevertheless, these derogations are provided solely for journalistic purposes or the purpose of artistic or literary expression.[349]

In Magyar Helsinki Bizottsag v. Hungry case of the European Court of Human Rights[350] the applicant (NGO) claimed the implementation of the right to freedom of expression in particular the right to receive information. The required information was related to ex-official of the Hungarian authorities. Authorities had the position that the information is private under the right to privacy and could not be a subject of dissemination. However, the Court confirmed that such refusal to provide information is a violation of Article 10 of the Council of Europe Convention and the freedom of expression.[351]

The relationship between cyber war and the right to freedom of expression is not clear. From the one side we have situation of armed conflict with the application of humanitarian law and from the other side the freedom to express personal opinion. However, although it is not obvious there is a connection between them. We will try to imagine two hypothetical situations.

A state A. launched a cyber attack against state B. by using a malicious program namely Trojan horse hidden in the other program. The malware spread across of thousands civilians computers, however, without causing any physical damage. The only purpose of the attacker is to gather information. The state B. knowing about Trojan prefers to keep silence and forbids discussing the situation in order to avoid panic in mass median explaining that it is protection of the national security. Trojan horse violates the right to data-protection by collecting sensitive information of users, and additionally, state B. violates indirectly the freedom of expression since, it prohibits to disseminate information which is necessary for computer users.

The second hypothetical situation is associated with the cyber attack on civilians by means of denial of service attack. State X. has a civil war between different political parties, therefore, in order

[349] Ibid., 23.
[350] European Court of Human Rights, "Personal data protection," *Press Unit*, accessed 16, February 2017, http://www.echr.coe.int/Documents/FS_Data_ENG.pdf.
[351] Ibid.

to stop disturbances among the population and at the same time to prevent the spread of information by means of infecting the main web site of one of the two political parties, state X. launched denial of service attack and disabled tens of thousands of user's computers. From the one side, it is clear that the attack is not discriminatory since it affects everyone who visits the web page. From the other side, the attack discriminates people in accordance with their political views. The attack on the web page of the one of political parties constitutes a violation against the freedom of expression and rights to seek, receive and impart information.

The right to freedom of expression should be also considered together with the right to information. According to Principle 1 of the Tshwane Principles on National Security and the Right to Information, "everyone has a right to seek, use, and impart information held by or on behalf of public authorities, or to which public authorities are entitled by law to have access". Principles three of the same document provides criteria for the exceptions for the restrictions of the right to information on national security grounds: it should be prescribed by law, it should be necessary for democratic society or it can be protection of a legitimate national security interest.

In the case Ltd v. United Kingdom, the European Court of Human Rights said, "The Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information generally". Moreover, the realization of the right to freedom of expression and also the right to information seems impossible without the Internet and the right to Internet access. In May 2011, the United Nations Special reporter stated that all states have to "ensure that Internet access is maintained at all times, including times of political unrest".[352] Further, the Special Reporter emphasizes, "The Internet has become an indispensable tool for realizing a range of human rights… the Internet should be priority for all States".[353] In 2016, the Unite Nations Human Rights Council in its resolution condemned International disruption of internet access by states.[354] The Resolution affirms, "The same rights that people have offline must also be protected online, in particular the freedom of expression".[355]

---

[352] "VI. Conclusions and recommendations", *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, Human Rights Council, Seventeenth session Agenda item 3, United Nations General Assembly, accessed 20 February 2017, para 79. http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

[353] Ibid., para 85

[354] United Nations, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue (A/HRC/17/27)," (Human Rights Council, 2011).

[355] Ibid.

Intellectual property rights

Article 2 (viii) of the Convention Establishing the World Intellectual Property Organization stated that intellectual property shall include rights relating to: literary, artistic and scientific works, phonograms, broadcasts "and all other rights resulting from intellectual activity in the industrial, scientific, literary or artistic fields. Intellectual property is divided into two groups: industrial property, such as inventions and trademarks and copyright, such as art works.[356] Why is it important and how do intellectual property rights work during armed conflict?

It is worth starting with the copyright and related rights. Copyright is a form of property applicable to creative works, for example, photographic works. In order to become a copyright holder the only thing a person have to do is create an artistic work. Several exclusive rights realize the holder of copyright: to produce copies or reproductions, to perform or display the work publicly, to transmit or display by radio or video.[357] This means that only copyright holder may exercises such rights while other persons only with the holder's permission.

Cyber space contains many art works such as photos, videos or sounds recordings, and most of them are used and reproduced without the copyright holder's permission. Cyber warfare may include various methods of warfare including digital manipulation. Digital manipulation is the only weapon that as it may seems that does not cause a physical harm or at least the harm that it can cause does not fall under any norm or rule. For example, we will create a situation where a head of a state X. in the midst of conflict with the other state Z. delivered a video message with the help of a private television company to the citizens of state X. Cyber attackers of state Z. stole the video a video and changed it content. The video was shown to the public; however, the speech was changed radically. The enraged population of the country began the riots within the house of the head of state. Summarizing we can conclude that, first, copyrights rights of television company were violated since it property was stolen, altered and demonstrated to the public. The head of state Z. could also be a victim of copyright violation since his speech was changed, moreover, changes in speech let to adverse consequences for his dignity and probably property.

[356] WIPO, "What is intellectual property?,", accessed 10 March 2017, http://www.wipo.int/edocs/pubdocs/en/intproperty/450/wipo_pub_450.pdf.

[357] Peter K. Yu, *Intellectual property and information wealth : issues and practices in the digital age.* (Westport, Conn: Praeger Publishers, 2007).

In 2006 there was an incident related to photo manipulation between Israel and the Lebanese Hezbollah group.[358] In 1990 after Iraq's invasion of Kuwait, the United States military decided to create and distribute "a compute-faked videotape of Saddam Hussein crying or getting caught in a sexually compromising situation".[359]

Industrial property rights are those that include patents, trademarks, industrial designs and geographical indication.[360] Unlike copyright, industrial property, rights require registration. Thus, for example in the Internet it is possible to register an exclusive domain name. However, it is also possible to steal it. The European Court of Human Rights in the case of Paeffgen Gmbh v. Germany[361] expressed the opinion that the right to domain name by its nature is property right because it has economic value. In theory, a violation of the right to a domain may occur when a malicious program such as IP spoofing creates a web page that appears identical to trusted one. The attacker may abuse the registered trademark or domain in order to mislead users and infect their computer systems.

Another violation when worms, viruses and Trojan horses are hiding in other programs to penetrate user computer and to carry out malicious act. We dare to say that all of them violate industrial property rights of the holders since each program has it patent and each holder has exclusive right to make, use and sell program. When a worm or a virus is attached to the program, it had in fact altered it. Moreover, the attacker uses the program for its own purposes. In a computer system, there are many different components to which a patient may be obtained, for example, algorithms, and functions embodied in a software product: user-interface features, program algorithms, operating system techniques, menu arrangements etc.[362]

Regarding programs they are also protected under copyright, for example, protection extends to the source and object code, as well as to the user interface.[363] Many features of software are considered as trademarks, for example, codes, ideas and concepts. Therefore, the use or modification

---

[358] Arie J. Major Schaap, "Cyber warfare operations: Development and use under international law," *Air Force Law Review* 64(2009): 138.
[359] Ibid., 139.
[360] WIPO, "What is intellectual property?.", accessed 15 March 2017, http://www.wipo.int/edocs/pubdocs/en/intproperty/450/wipo_pub_450.pdf.
[361] European Court of Human Rights, "Personal data protection," *Press Unit*, accessed 23 February 2017, http://www.echr.coe.int/Documents/FS_Data_ENG.pdf.
[362] Freibrun Law, "Intellectual Property Rights in Software – What They Are and How to Protect Them", accessed 28 February 2017, http://www.freibrun.com/intellectual-property-rights-software-protect .
[363] Ibid.

of programs to infect as many computer systems as possible constitutes a violation of patent/ copyrights/ trade secrets holder industrial property rights.

Conclusion

In 2012, the United Nations Human Rights Council approved the Resolution on the promotion, protection and enjoyment of human rights on the Internet. This document promotes human rights both outside and inside cyberspace and appeals to such notions as right to freedom of opinion and expression, right to privacy in the digital age, right to Internet, right to information etc. The importance of cyberspace as a source of information and communication for individuals has grown significantly over the last twenty years.[364] A harmful effect of the cyber attack is also grown over the past 17 years. In this connection, "the nexus between cyber warfare and human rights is an urgent need to be addressed by the political agenda, so as to aid the enforcement of law in cyberspace".[365] Perhaps there is no single example in which a certain right or freedom is applied to a particular cyber attack. However, if we consider each situation separately for the existence of human rights violations, then such a practice could form a new legal regime for cyber space where both humanitarian law and human rights are interrelated and where they function effectively to protect individuals.

[364] Andresa da Mota Silveira Rodrigues et al., "Cyber Warfare. Establishing instruments to deal with a new world threat," *Simulação das Nações Unidas para Secundaristas* (2013).
[365] Ibid. 379

CONCLUSION

During cyber warfare both International Humanitarian Law and International Human Rights Law impose constraints on the conduct of hostilities. International Humanitarian Law by means of international treaties and custom imposes obligations on states. Two principles of customary law should be specifically taken into account: military necessity and precautions.

The principle of military necessity is implemented by three other principles such as distinction, discrimination and proportionality. The principle of distinction require to distinguish between civilians and combatants and between civilian objects and military objectives. The principle of discrimination establishes that only military objective can be targeted, and only by means and methods which can be directed against specific objective, which effects can be limited. The principle of proportionality prohibits attacks that can cause excessive damage to civilian population in relations to concreate and direct military advantage. These principles of humanitarian law are applicable in most cases and can serve a sufficient basis for the protection of people during cyber warfare.

The principle of precautions requires from command staff of the armed forces of the state to take all feasible precautions in order to mitigate or to avoid civilian losses.

International Human Rights Law International law gives all people certain rights and freedoms, deviation from compliance which is permissible only if a state is not bound by the treaty which establishes the right or freedom, or if cyber-related activity does not fall under the rule of law, or if the act of state is not contrary to international law, and finally, if in the treaty there is a specific provision concerning the possibility of lawful limitation of the norm.

The rules of human rights law that may be violated include right to privacy, in particular, right to data-protection, right to freedom of expression, right to information, right to Internet access and intellectual property rights. The right to privacy prohibits the interference into a private life of a person and the right to data-protections protects personal life information. The right to freedom of expression allows every person to hold opinion and the right to information gives the right to seek, receive and impart information and ideas without any interference by authorities of any state. The right forbids to prevent access to the Internet. And finally, intellectual property rights protects interest of authors and patent right holders in case if their rights are violated by the third parties.

All the rules of law including rights, freedoms and duties listed above apply to the situation of cyber warfare. In this regard, the answer to the question whether International Human Rights Law

impose constraints on digital manipulation or other cyber warfare ruses is affirmative. International Human Rights Law which contains a set of rights and freedoms imposes restrictions on states' actions during cyber warfare. However, there is no exhaustive list of these restrictions. Therefore, every case of cyber war should be considered separately. It is possible that in the future custom or judicial practice will allow talking about "more established" rules applicable to cyber wars.

REFERENCES

Abliz, Mehmud. "Internet Denial of Service Attacks and Defense Mechanisms." *University of Pittsburgh, Department of Computer Science, Technical Report* (2011): 1-50.

AIV/CAVV. "Dutch Government Response to the Aiv/Cavv Report on Cyber Warfare." Advisory Council on International Affairs (AIV), Advisory Committee on Issues of Public International Law (CAVV), 2012.

Aldrich, Richard W. "The International Legal Implications of Information Warfare." DTIC Document, 1996.

Arnold, Allison. "Cyber "Hostilities" and the War Powers Resolution." *Military Law Review* 217 (2013): 174 - 92.

Ayalew, Yohannes Eneyew. "Cyber Warfare: A New Hullaballo under International Humanitarian Law." *Beijing Law Review* 6 (2015): 209 - 23.

Backstrom, Alan, and Ian Henderson. "New Capabilities in Warfare: An Overview of Contemporary Technological Developments and the Associated Legal and Engineering Issues in Article 36 Weapons Reviews." *International Review of the Red Cross* 94, no. 886 (2012): 483-514.

Beard, Jack M. "Legal Phantoms in Cyberspace: The Problematic Status of Information as a Weapon and a Target under International Humanitarian Law." *Vanderbilt Journal of Transnational Law* 47 (2014): 67 - 144.

Bouchet-Saulnier, Francoise. *The Practical Guide to Humanitarian Law*. Translated by Laura Brav and Camille Michel. Third ed. Maryland: Rowman & Littlefield Publishers, 2014.

Cammack, Chance. "The Stuxnet Worm and Potential Prosecution by the International Criminal Court under the Newly Defined Crime of Aggression." *Tulane Journal Ofint'l & Comp. Law* 20 (2011): 303 - 25.

Carr, Jeffrey. *Inside Cyber Warfare: Mapping the Cyber Underworld*. Beijing Sebastopol, CA: "O'Reilly Media, Inc.", 2011.

Chairman of the Joint Chiefs of Staff. "National Military Strategy for Cyberspace Operations." United States: United States Department of Defense, 2006.

Cohen, Fred. "Computer Viruses." *Computers & Security* 6, no. 1 (1987): 22 - 35.

Cole, Alan. *Rules of Engagement Handbook*. International Institute of Humanitarian Law, 2009.

Crawford, James. *Brownlie's Principles of Public International Law*. 8th ed. Oxford, United Kingdom: Oxford University Press, 2012.

Cross, Thomas. "Legal Implications of Vulnerability Disclosure in International Conflict." *Journal of Law and Cyber Warfare* 4 (2014): 94 - 108.

Cupa, Basil. "Trojan Horse Resurrected - on the Legality of the Use of Government Spyware." In *Living in surveillance societies: The state of surveillance*, edited by C William R. Webster, 419 - 28: Proceedings of LiSS conference 3: CreateSpace Independent Publishing Platform, 2013.

Department of the Army Field Manual, FM 27 - 10. "The Law of Land Warfare." Washington, 1956.

Dillon, Michael G. *The Liberal Way of War: Killing to Make Life Live*. London: Routledge, 2009.

Dinniss, Heather Harrison. *Cyber Warfare and the Laws of War*. Vol. 92: Cambridge University Press, 2012.

Dinstein, Yoram. "The Principle of Distinction and Cyber War in International Armed Conflicts." *Journal of Conflict and Security Law* 17, no. 2 (2012): 261-77.

Döge, Jenny. "Cyber Warfare Challenges for the Applicability of the Traditional Laws of War Regime." In *Archiv Des Völkerrechts*, edited by Mohr Siebeck. 486-501, 2010.

Drew, D.M. "Air Force Manual: Basic Aerospace Doctrine of the United States Air Force. Volume I." Washington: Department of the Air Force, 1992.

Droege, Cordula. "Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians." *International Review of the Red Cross* 94, no. 886 (2012): 533-78.
Dunlap Jr, Charles J. "Perspectives for Cyber Strategists on Law for Cyberwar." *Strategic Studies Quarterly* 5 (2011): 81 - 99.
Elisan, Christopher C. *Malware, Rootkits & Botnets a Beginner's Guide*. New York: McGraw Hill Professional, 2012.
European Comission. "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace." Brussels: High Representative of the European Union for Foreign Affairs and Security Policy, 2013.
European Court of Human Rights. "Personal Data Protection." *Press Unit* (2017): 1 - 22.
European Union Agency for Fundamental Rights. *Handbook on European Data Protection Law*. Luxembourg: Publications Office of the European Union, 2014.
Falliere, Nicolas, Liam O Murchu, and Eric Chien. "W32.Stuxnet Dossier." Cupertino: Symantec. Security Response, 2011.
Gerichtshof, Internationaler. "Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion." *ICJ Reports* (1996): 226 - 593.
Gill, Terry D., and Dieter Fleck. *The Handbook of the International Law of Military Operations*. 2nd ed. Oxford, United Kingdom: Oxford University Press, 2011.
Greenspan, Morris. *The Modern Law of Land Warfare*. Berkeley: University of California Press, 1959.
Handler, Stephenie Gosnell. "New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare." *Stanford Journal of International Law* 48, no. 1 (2012): 209 - 37.
Harutyunyan, Angelina. "Dilemma of Targeting: Dual-Use Objects in Military Operations." *Law of Armed Conflict* (n.d.).
Henckaerts, Jean-Marie, and Louise Doswald-Beck. *Customary International Humanitarian Law*. Vol. 1, Cambridge: Cambridge University Press, International Committee of the Red Cross, 2005.
Henckaerts, Jean-Marie, Louise Doswald-Beck, and Carolin Alvermann. *Customary International Humanitarian Law*. Vol. 1, Cambridge: Cambridge University Press, 2005.
HPCR. *Manual on International Law Applicable to Air and Missile Warfare*. Cambridge, New York: Cambridge University Press, 2013.
ICRC. *New Technologies and Warfare*. International Review of the Red Cross. Humanitarian Debate: Law, Policy, Action. edited by Vincent Bernard. Vol. 94, no. 886, Geneva: International Committee of the Red Cross (ICRC), 2012.
———. "San Remo Manual on International Law Applicable to Armed Conflicts at Sea." edited by Louise Doswald-Beck. Cambridge: International Committee of the Red Cross (ICRC), 1994.
Jensen, Eric Talbot. "Sovereignty and Neutrality in Cyber Conflict." *Fordham International Law Journal* 35 (2012): 815 - 41.
———. "Unexpected Consequences from Knock-on Effects: A Different Standard for Computer Network Operations?". *American University International Law Review* 18, no. 5 (2003): 1145 - 88.
Jiminián, Jimena M. Conde. "The Principle of Distinction in Virtual War: Restraints and Precautionary Measures under International Humanitarian Law." *Tilburg Law Review* 15, no. 1 (2010): 69-91.
Joint Chiefs of Staff. "Joint Publication 3-13. Information Operations." United States of America: Armed Forces of the United States, 2012.
Kelsey, Jeffrey T. G. "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare." *Michigan Law Review* 1006 (2008): 1427-51.

Lau, Felix, Stuart H Rubin, Michael H Smith, and Ljiljana Trajkovic. "Distributed Denial of Service Attacks." Paper presented at the Systems, Man, and Cybernetics, 2000 IEEE International Conference on, 2000.

Lin, Herbert. "Cyber Conflict and International Humanitarian Law." *International Review of the Red Cross* 94, no. 886 (2012): 515 - 31.

Lopez, C. Todd. "Fighting in Cyberspace Means Cyber Domain Dominance." *U.S. Air Force. Air Force Print News* (2007).

Mayer, Marco, Luigi Martino, Pablo Mazurier, and Gergana Tzvetkova. "How Would You Define Cyberspace?". *First Draft Pisa* 19 (2014): 2014.

Mihr, Anja. "Cyber Justice: Cyber Governance through Human Rights and a Rule of Law in the Internet." *US-China Law Review* 13 (2016): 314 - 36.

Ministry of Defense. "Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space." Russia: Ministry of Defense of The Russian Federation, 2011.

Moore, David, and Colleen Shannon. "The Spread of the Code-Red Worm (Crv2)." Center for Applied Internet Data Analysis, 2001.

Moore, David, Colleen Shannon, Douglas J Brown, Geoffrey M Voelker, and Stefan Savage. "Inferring Internet Denial-of-Service Activity." *ACM Transactions on Computer Systems (TOCS)* 24, no. 2 (2006): 115 - 39.

Nash, Troy. "An Undirected Attack against Critical Infrastructure." *Technical Report, US-CERT Control Systems Security Center* 1.2 (2005): 1 - 10.

NATO. "Glossary of Terms and Definitions." APP-06, 2009.

Nicaragua v. United States. "Case Icj Reports 1986." *76 ILR* (1986): 98 - 432.

North Sea Continental Shelf. "Case Icj Reports 1969." *41 ILR* (1969): 3 - 29.

O'Malley, George. "Hacktivism: Cyber Activism or Cyber Crime." *Trinity College Law Review* 16 (2013): 137 - 60.

Ohlin, Jens David, Kevin Govern, and Claire Finkelstein. *Cyber War: Law and Ethics for Virtual Conflicts*. Oxford: Oxford University Press, 2015.

Patterson, Ryan. "Silencing the Call to Arms: A Shift Away from Cyber Attacks as Warfare." *Loyola of Los Angeles Law Review* 48 (2015): 969 - 1016.

Peagler, Jordan. "The Stuxnet Attack: A New Form of Warfare and the (in) Applicability of Current International Law." *Arizona Journal of International & Comparative Law* 31, no. 2 (2014): 399 - 434.

Pilloud, Claude, Jean De Preux, Yves Sandoz, Bruno Zimmermann, Phillippe Eberlin, Hans-Peter Gasser, and Claude F. Wenger. *Commentary on the Additional Protocols: Of 8 June 1977 to the Geneva Conventions of 12 August 1949*. edited by Yves Sandoz, Christophe Swinarski and Bruno Zimmermann Geneva: Martinus Nijhoff Publishers, 1987.

Pool, Phillip. "War of the Cyber World: The Law of Cyber Warfare." *The International Lawyer* 47, no. 2 (2013): 299 - 323.

Raboin, Bradley. "Corresponding Evolution: International Law and the Emergence of Cyber Warfare." *Journal of the National Association of Administrative Law Judiciary* 31, no. 2 (2011): 602 - 68.

Radziwill, Yaroslav. *Cyber-Attacks and the Exploitable Imperfections of International Law*. Boston: Brill, 2015.

Richardson, John. "Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield." *Journal of Computer & Information Law* 29 (2011): 1 - 28.

Richmond, Jeremy. "Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?". *Fordham International Law Journal* 35, no. 3 (2012): 842 - 94.

Roberts, Shaun. "Cyber Wars: Applying Conventional Laws to War to Cyber Warfare and Non-State Actors." *Northern Kentucky Law Review* 41, no. 3 (2014): 535 - 72.

Rodrigues, Andresa da Mota Silveira, Carolina Carvalho Tavares, Henrique Mendonça Torres Sottovia, and Márcio Nascimento Costa Carvalho. "Cyber Warfare. Establishing Instruments to Deal with a New World Threat." *Simulação das Nações Unidas para Secundaristas* (2013): 357 - 84.

Roscini, Marco. *Cyber Operations and the Use of Force in International Law*. Oxford: Oxford University Press, 2014.

Schaap, Arie J. Major. "Cyber Warfare Operations: Development and Use under International Law." *Air Force Law Review* 64 (2009): 121 - 73.

Schmitt, Michael. "Classification of Cyber Conflict." *Journal of Conflict and Security Law* 17, no. 2 (2012): 245-60.

Schmitt, Michael N. *Tallinn Manual on the International Law Applicable to Cyber Warfare : Prepared by the International Group of Experts at the Invitation of the Nato Cooperative Cyber Defence Centre of Excellence.* Cambridge New York: Cambridge University Press, 2013.

Schmitt, Michael N. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations : Prepared by the International Group of Experts at the Invitation of the Nato Cooperative Cyber Defence Centre of Excellence.* Cambridge New York: Cambridge University Press, 2017.

Scott, Roger D. "Legal Aspects of Information Warfare: Military Disruption of Telecommunications." *Naval Law Review* 45 (1998): 57 - 273.

Shackelford, Scott J., and Richard B. Andres. "State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem." *Georgetown Journal of International Law* 42 (2011): 971 - 1016.

Sharp Sr., Walter G., and Thomas C. Wingfield. *Law of Information Conflict: National Security Law in Cyberspace*. Falls Church, Va.: Aegis Research Corporation, 1999.

Shelton, Henry. "Joint Doctrine for Information Operations." United States: Defense Technical Information Center, 1998.

Shulman, Mark Rusell. "Legal Constraints on Information Warfare." United States: Center for Strategy and Technology, Air War College, Occasional Paper No. 7, 1999.

Singer, P. W. "Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons." *Case Western Reserve Journal of International Law* 47 (2015): 79 - 86.

Sinks, Michael A. "Cyber Warfare and International Law." Doctoral dissertation, Air University, 2008.

Skoudis, Ed, and Lenny Zeltser. *Malware: Fighting Malicious Code*. New Jersey: Prentice Hall Professional, 2004.

Solis, Gary D. "Cyber Warfare." *Military Law Review* 219 (2014): 1 - 52.

Spafford, Eugene H. "The Internet Worm Program: An Analysis." *ACM SIGCOMM Computer Communication Review* 19, no. 1 (1989): 17-57.

Summers, Rita C. *Secure Computing: Threats and Safeguards*. Hightstown: McGraw-Hill, Inc., 1997.

The White House. *President George W. Bush: The National Strategy to Secure Cyberspace*. Washington, DC.: Morgan James Publishing, 2003.

Trifan, Mihai. "Cyber-Attacks (Viruses, Trojan Horses and Computer Worms) Analysis." *International Journal of Information Security and Cybercrime* 1, no. 1 (2012): 46 - 54.

Tsagourias, Nicholas. "Cyber Attacks, Self-Defence and the Problem of Attribution." *Journal of Conflict and Security Law* 17, no. 2 (2012): 229 - 44.

UK Manual. "Joint Service Manual of the Law of Armed Conflict." edited by UK Ministry of Defence, 2004.

———. "The Law of War on Land, Being Part Iii of the Manual of Military Law." London: Her Majesty's Stationery Office, 1958.

United Nations. "Developments in the Field of Information and Telecommunications in the Context of International Security (a/57/166/Add.1)." Report of the Secretary-General, 2002.
———. "Developments in the Field of Information and Telecommunications in the Context of International Security (a/64/129/Add.1)." Report of the Secretary-General, 2009.
———. "Developments in the Field of Information and Telecommunications in the Context of International Security (a/65/154)." Report of the Secretary-General, 2010.
———. "Developments in the Field of Information and Telecommunications in the Context of International Security (a/66/152)." Report of the Secretary-General, 2011.
———. "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue (a/Hrc/17/27)." Human Rights Council, 2011.
———. "United Nations General Assembly Resolution 3314. Definition of Aggression a/Res/3314(Xxix)." United Nations General Assembly, 1974.
War Department Field Manual, FM 27 - 10. "Basic Field Manual: Rules of Land Warfare." Washington, 1940.
War Department, Office of the Chief of Staff. *Basic Field Manual: Rules of Land Warfare*. Washington1914.
Weissbrodt, David. "Cyber-Conflict, Cyber-Crime, and Cyber-Espionage." *Minnesota Journal of International Law* 22, no. 2 (2013): 347 - 87.
Wilson, Clay. "Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress." *Focus on Terrorism* 9 (2003): 1 - 32.
WIPO. "What Is Intellectual Property?". Geneva: World Intellectual Property Organization, n.d.
Yu, Peter K. *Intellectual Property and Information Wealth : Issues and Practices in the Digital Age.* Westport, Conn: Praeger Publishers, 2007.
Zeidanloo, Hossein Rouhani, Farzaneh Tabatabaei, Payam Vahdani Amoli, and Atefeh Tajpour. "All About Malwares (Malicious Codes)." In *International Conference on Security & Management*, 342 - 48. Las Vegas Nevada, 2010.
Zhang, Li. "A Chinese Perspective on Cyber War." *International Review of the Red Cross* 94, no. 886 (2012): 801 - 07.