TALLINN UNIVERSITY OF TECHNOLOGY
School of Business and Governance
Department of Law

Juho Kivihuhta

THE PRINCIPLE OF DISTINCTION BETWEEN CIVILIANS AND COMBATANTS IN CYBER OPERATIONS

Bachelor's Thesis

Programme HAJB08/14 – Law, Specialisation European Union and international law

Supervisor: Agnes Kasper, Ph.D.

Tallinn 2018

I declare that the I have compiled the paper independently and all works, important standpoints and data by other authors have been properly referenced and the same paper has not been previously been presented for grading. The document length is …….. words from the introduction to the end of summary.

Juho Kivihuhta ……

(signature, date)

Student code: HAJB145796

Student e-mail address: juho.kivihuhta@live.fi

Supervisor: Agnes Kasper, PhD.:

The paper conforms to requirements in force

……

(signature, date)

Chairman of the Defence Committee:

Permitted to the defence

……

(name, signature, date)

Table of Contents

Abstract

The creation of internet during the 1980’s has revolutionized distribution of information and altered the functions of businesses, society and individuals. It is quite possible for cyberspace to become the next battlefield for a conflict. The current international humanitarian law has been in effect in traditional international and internal armed conflicts. Distinction between combatant and civilian in order to protect civilians is one of the key aspects in the law of armed conflict. The application of traditional criteria of distinction is more complicated in cyberspace than in a real-world situation. This is why there are efforts to interpret and apply international law to cyberspace. These interpretations have however not yet been able to unanimously clarify the legal method of distinguishing between civilian and combatant in cyberspace. Some examples concerning these difficulties are described. Distinguishing between combatant and civilian in cyberspace therefore requires the efforts of governments and development of new legal and technological instruments in the field.

KEYWORDS: international law, cyberspace, cyber conflict, principle of distinction

Abbreviations

IHL International humanitarian law

DoS Denial of service attack

DDoS Distributed denial of service attack

CNA Computer network attack

CNE Computer network exploitation

ICRC International Committee of the Red Cross

1 INTRODUCTION

The principle of distinction between civilians and combatants is an important component of international humanitarian law (from now on IHL). IHL aims to regulate conduct in conflict situations in order to help those who do not take part in the hostilities. The principle of distinction determines the rights, obligations, and requirements for the treatment of those not involved in the hostilities and who are therefore to be protected from the effects of the conflicts. A vast portion of the modern world's functions have been relocated to cyberspace, the internet, including many governmental information functions. It is therefore not surprising that conflicts between nations have started to take place in cyberspace, and the author will later review specific cases of these. Due to these past incidents, there is a need to address the issues of the legal status of cyber conflicts, of how the people taking part in hostilities are recognized, and of how attacks carried out in cyberspace are classified. Currently there are some major efforts underway to interpret modern IHL and apply it to cyberspace. The author has chosen the topic of this thesis in order to take a closer look at these recent interpretations of what are possible "cyber combatants" or direct participation in cyber operations in hostilities and what kinds of attacks fall under the scope of IHL. It is important to take a close look at the status of civilians and combatants in cyberspace.

The main goal of this thesis is to analyze the application of IHL to cyberspace and to see how IHL can effectively answer the challenges that the cyber world poses. The current IHL has been developed to answer the legal questions of real-world armed conflicts, and cyberspace in this sense is still uncovered ground. The author aims to answer how IHL can be applied to cyberspace and what kinds of solutions this can provide.

The main question of this research paper is how the principle of distinction applies to persons in connection to cyber operations. The author will also review the questions of what cyber operation constitutes an attack and how direct participants in cyberspace hostilities are identified. The hypothesis of the research paper is that the current legislative instruments regarding the cyber aspects of international conflicts do not provide sufficient clarity and therefore further legislative and technological measures are necessary.

Firstly, the author will take a brief look at modern IHL in order to introduce the legal characteristics of combatants and civilians and to provide an understanding of how legislation works when analyzing a conflict. Secondly, the aim is to introduce what cyberspace is, to present the basics of applying IHL to cyberspace, what the current weapons used in cyberspace are, and what kinds of examples and interpretations are cyber operations that classify as attacks. Thirdly, this paper will analyze direct participation, with the aim to introduce the legal aspects of direct participation in a cyber operation. Then the author will analyze the identification of combatants in cyberspace during hostilities. Finally, the author will take a look at past cases where the cyber elements of warfare have been present. The aim is to assess the qualities of cyber elements in a conflict and how the principle of distinction is applicable to an actual scenario.

The research method used is qualitative, and the method used to understand the current state consists of reviewing peer-reviewed articles on the subject, case studies of past cyber operations, and current legislation.

The author chose the works published in legal journals and conferences by researchers who are active in the field. The research paper will also refer to current conventions such as the Geneva Conventions, the Additional Protocol I to the Geneva Convention and explanatory materials. The Tallinn Manuals are legal discussions between international experts concerning the application of international law in cyberspace. Both of the Manuals are reviewed throughout the research paper, because they are currently widely acknowledged publications on the subject, front runners in the field of cyber conflict analysis. The author also chose other articles on the subject so that the analysis would not be too one-sided or uncritical.

The fact that the subject is novel is an important reason for conducting research on it. The field is in many ways still theoretical, and there are only a handful of examples that can be used to form a foundation for analyzing possible future events. Based on past interactions of the world's nations, one can say, without wishing to be too cynical, that the next conflict is always around the corner. This, combined with the fact that cyberspace is growing in giant leaps and is continually forming a bigger part of our daily lives, of the personal, commercial and government spheres. This development creates a potential for a new era in conflicts. The possibility of witnessing a conflict in cyberspace is greater than ever. Simply because our lives and important functions take place there, cyberspace has the potential to be the future battlefield.

2 INTERNATIONAL HUMANITARIAN LAW, CYBERSPACE AND CYBER OPERATIONS

2.1 General scope of the chapter

Modern IHL comprises treaties and customary law that aim to provide a legal solution to issues arising in conflict situations. This research paper focuses on the legal status of participation and nonparticipation of a person in a cyber conflict. In order to do so, the author has chosen to introduce the traditional aspect of conflict legislation, to provide a basic understanding of the topic and how it is legislated. The chapter will the move on to introduce the basics of cyberspace and introduce basics of the means and methods of warfare. The idea is to lay down a foundation for the thesis on basics.

2.2 The principle of distinction between civilians and combatants

The principle of distinction between civilians and combatants is a part of IHL, jus in bello. It was first set out in the Saint Petersburg Declaration (1868), and its aim is to make a clear distinction between civilians and combatants. The aim of war is not to wreak havoc on the enemy's territory but to weaken their military forces in order to gain an advantage over them.[1] The ability to recognize enemy forces is therefore crucial, in order to be able to attack the appropriate targets. The principle of distinction sets out a foundation of law that protects the civilian population. It

1 ICRC Customary IHL Database. Accessible: https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_cha_chapter1_rule1, 23 April 2018.

also considers objects, but for the purposes of this research paper, only persons and their distinction will be reviewed. Regarding the current legislation, the ICRC has set out the distinction between civilians and combatants as the first rule of customary international law. The principle has been added to the first Additional Protocol to the Geneva Conventions protecting the victims of international armed conflicts. The criteria according to which enemy forces are identified and which aim to protect civilians will be reviewed in the next chapter. When combatants are identified clearly, they can be separated from the rest of the population and given legal rights as combatants, but this also separates them as legitimate targets for the opposing forces. The legitimacy of a target is very important since civilians are protected unless they engage in the conflict in certain ways. It is important to emphasize that the distinction is something that gives the possibility to distinguish between civilian and combatants, so it is legally important for the armed forces to make sure that they are distinguishable from civilians.

2.3 Combatants

In order to be recognized as legal combatants in an international armed conflict, combatants need to fulfill four criteria set out in the Geneva Convention III. The first one of the characteristics set out by Article 4 of the Geneva Convention III is that there needs to be a power structure or hierarchy, in which the combatants are subordinate to a higher-ranking member of the armed forces. Secondly, they must carry arms openly. Thirdly, they must have a distinctive emblem or uniform. Fourthly, they must conduct their operations in accordance with the laws and customs of war.

The reasons why it is of essence to be distinctively a part of an army and display it to others, whether civilians or combatants, is that obligations and liberties come with the combatant status. The status is declared through these marks and they give the combatants their rights according to international law to weaken or kill enemy forces and give them rights as prisoners of war, including treatment according to the Geneva Convention III, in case they are captured.

2.4 Civilians

Civilians have the right to stay outside the conflict, and the aim of IHL is to protect civilians from the consequences of a conflict. Civilians can however revoke these rights by legally becoming a 'levée en masse' by spontaneously grabbing arms when enemy forces approach their territory.[2] Through this action the civilians lose their rights as civilians and becomes targets that the enemy forces can attack. After such action or when the battle is over, the civilians return to their civilian status. This is not to be confused with civilians allowing enemies into their village and then after a while attacking them, which is prohibited. In order to be under the protection of international law, the civilians must grab arms spontaneously. A 'levée en masse' also gives prisoner of war status to the civilians in case they carry their arms openly and respect the laws of war.[3]

The difference is that that the spontaneous element is required for a 'levée en masse'. Direct participation in hostilities broadly means that civilians are engaged in the conflict. Civilians directly participating in hostilities do not have protection as prisoners of war, because such activity is not protected by combatant status and is therefore potentially unlawful.[4] Civilians aiding armed forces during hostilities are not considered to be directly participating in case their engagement involves doing something that does not fall under direct participation in a conflict.[5] The author argues that this is an important distinction since these civilians would be accompanying the combatants, therefore it can be deduced that they remain civilians as long as they do not perform an offensive role in these situations.

2 Geneva Convention III Article 4 (A) (6)

3 *Ibid*.

4 Schmitt, M. (2005). Humanitarian Law and Direct Participation in Hostilities by Private Contractors or Civilian Employees. - Chicago Journal of International Law, Volume 5 No. 2, Winter 2005, 511-546, p 520.

5 Melzer, N. (2009). ICRC Interpretive Guidance on the Notion of Direct Participation in Hostilities. Accessible: https://www.icrc.org/eng/assets/files/other/icrc-002-0990.pdf, 23 April 2018, p 39.

2.5 Cyberspace

In most of the modern world it is nearly impossible to be unaware of the internet, which creates cyberspace. Cyberspace is an alternative reality in which people can lead lives that can be separate from the ones they live in the real world. Lessig argues in the article "The Zones of Cyberspace" that cyberspace is a place separate from reality, meaning that it should be governed by its own laws.[6] The concept of cyberspace is extremely important. From a legal point of view, there is some sense in having designating cyberspace as an area with specialized legislation, and some measures have been taken in this direction, for example in the Council of Europe Budapest Convention on Cybercrime.[7]

However, treating cyberspace as a completely separate domain would be extreme since the actions carried out in cyberspace and the automated functions occurring in it are carried out and created by people at this point in time. Cyberspace does however offer a valid example of necessary international harmonization of legislation. The networks of internet allow for a specific network to be moved to another location in case a country is adversary towards that network.[8] Disconnected from geography, cyberspace is a network where everything is within grasp of a person at any time, which implies devastating consequences when turned into a war zone. It is good to keep in mind that cyberspace consists of an immaterial region of activities but is in fact based on purely physical networks and systems.[9]

---

6 Lessig, L. (1996). The Zones of Cyberspace. - Stanford Law Review 48, 1403-1411, p 1403.

7 ETS No. 185 Convention on Cybercrime, 28 April 2018.

8 Lessig, L (1996), *supra nota* 6, p 1406.

9 Liles, S. Dietz, J. Rogers, M. (2012). Applying Traditional Military Principles to Cyber Warfare. - 4th International Conference on Cyber Conflict, 5-8 June, Tallinn. (Ed.) C. Czosseck, R. Ottis, K. Ziolkowski. Estonia: NATO CCD COE Publications, 169-180, p 172.

2.6 Cyberspace and international law

One problem of trying to apply the rules of IHL to a cyber conflict is that the parties are usually known in physical warfare, but the opposite is usually true in cyberspace. Another big problem arising from the application of IHL is that events may take place in a way that there is no clear sign of a conflict, not to mention no clear identification of the parties involved.[10] The serious issues arising from these problems does however give some credence to the statement made in the previous chapter that cyberspace should be a space with its own separate legislation. The most pressing question regarding IHL is however whether it applies to cyberspace, and the United Nations Group of Governmental Experts concluded in 2015 that international law does apply to cyberspace, however without specifying that IHL is applicable to cyberspace.[11]

Cyberspace functions through cables, servers, and networks that are on land or elsewhere physically present in this world, meaning that claims that cyberspace is a separate entity can only be valid in the sense that its functionality is different from that of the physical world. However, cyberspace is built, initiated, and controlled in the physical world, and it is therefore reasonable to claim that cyberspace exists in the physical world and is not apart from it, which would devalue claims that it is something completely different.

To be classified as an international armed conflict, a conflict has to be international, between nations, and armed. When applying the rules of conflict to cyber operations, the concept of being armed becomes difficult to define. Michael Schmitt argues that even though cyber operations are not violent in a conventional way, they still amount to violence or acts of aggression due to the results that they are able to bring about.[12]

---

10 Droege, C. (2012). Get off my could: cyber warfare, International Humanitarian Law, and the Protection of Civilians. - International Review of the Red Cross, (New Technologies and Warfare), Issue 886, 94, June 2012, 553-578, p 541.

11 "The 2013 report stated that international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment." United Nations Document A/70/174, p 12.

12 Schmitt, M. (2012). Classification of Cyber Conflict. - Journal of Conflict and Security Law, Summer 2012, 17(2), 245-260, p 250.

2.7 Means and methods of cyber operations

Cyberspace, this immaterial zone where the travel time of data has been reduced to seconds, offers a completely new set of methods of conducting operations. These methods are the weapons that possible future 'cyber combatants' might use instead of traditional weapons. The following analysis of the new weapons will focus on the functioning of the weapon but will also try to establish whether or not use of the weapon can be seen as something that can be considered an attack under current international law. Cyber weapons are similar to traditional ones in the sense that their purpose is to cause damage to their targets.[13]

2.7.1 Malware

Malware, malicious software, consists of a large number of different types of infections of computer systems. Such software aims to disrupt the operation of computer systems or to gather information that is processed in the systems. This includes specific forms of malicious programs such as Trojan horses, worms, spyware, and others that function according to the same key principles. Malware includes a vast amount of different methods of affecting systems ranging from intrusion to information gathering to attempts to destroy key features of the operating system and render it dysfunctional.[14]

2.7.2 Distributed denial of service attack

A distributed denial of service attack (DDoS) is different from a malware attack in the sense that it targets a completely different aspect of a computer system. While malware aims to infect a system by penetrating it, DDoS does not require such access to the system. As the name implies, a DDoS overfloods the servers of the target. This is done by sending inquiries to the service host at such a massive rate that it cannot cope with the information request and therefore is unable to handle any of them and is essentially shut down.[15] Distribution of such an attack creates further

13 Rid, T. McBurney, P. (2012). Cyber-Weapons. - The Rusi Journal, 6-13, p 8.

14 *Ibid*., p 8.

15 Mirkovic, J. Prier, G. Reiher P. (2002). Attacking DDoS at the source, 10th IEEE International Conference on Network Protocols 2002, 12-15 November 2002, Paris. The Institute of Electrical and Electronics Engineers, p 312-321, p 312.

difficulty in blocking the false request because they are sent from multiple locations; every malicious request needs to be identified on its own, so blocking them all is time consuming. A DDoS attack does not require more than one computer,[16] which makes it potentially severe threat.

2.8 The classification of cyber operations under IHL

Broadly speaking, cyber operations of an offensive nature can be divided into two categories. The first one consists of computer network attacks (CNA), which aim to deteriorate, destroy, or somehow change a system's functionality or the information stored in it.[17] The second category consists of computer network exploitation (CNE), which may not cause any changes in a network or its information but spies on it or uses it for data transfer.[18] There are also cyber operations that aim to defend against an offensive operation. The distinction is important since the end result achieved is different. In the case of a CNA, there is a clear intention to have offensive and attacking qualities, the operation is designed to have physically destructive qualities, and therefore the attack is comparable to one carried out with traditional means of warfare.

In case of a CNE, the intention is more of an intelligence gathering nature, which is not strictly illegal under international law, and more concern is caused by CNAs.[19] Espionage is mentioned in the Tallinn Manual, where the question of cyber espionage is interpreted in the fashion that espionage is not illegal under international law since it is not an attack. However, cyber espionage

16 Ophardt, J. (2010). Cyberwarfare and the Crime of Aggression: The need for Individual Accountability for Tomorrows Battlefield. - Duke Law & Technology Review, 1-28, p 2.

17 National Research Council, (2009). Technology, Policy, law and Ethics Regarding U.S Acquisition and Use of Cyberattack Capabilities, The National Academies Press, p 80, referenced in Lobel (Lobel, H. (2012). Cyber Warfare Inc.: The Law of War Implications of the Private Sector's Role in Cyber Conflict. Texas International Law Journal, Vol 47(3), 618-640, p 623.)

18 Clark, D. Landau, S. (2010). Untangling Attribution, in Proceedings Of A Workshop Deterring Cyberattacks, National Research Council, p 25-28, referenced in Lobel (Lobel, H. (2012). Cyber Warfare Inc.: The Law of War Implications of the Private Sector's Role in Cyber Conflict. Texas International Law Journal, Summer 2012, 47(3), 618-640, p 623.)

19 Lobel, H. (2012). Cyber Warfare Inc.: The Law of War Implications of the Private Sector's Role in Cyber Conflict. - Texas International Law Journal, Summer 2012 47(3), 618-640, p 623.

can have consequences that make it difficult to conduct without causing results that are similar to an attack.[20]

In the Tallinn Manual a cyber attack is defined as "A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects".[21] The attack is defined as a conventional attack, and due to the lack of legislation, applying international law to these situations seems appropriate.

International law defines an attack as having an aspect of violence in it, and therefore activities such as social engineering, spreading propaganda, and spying on the adversary are not considered attacks.[22] Compared to the traditional methods of psychological warfare and non-violent acts, these methods could be vastly more effective in cyberspace. The Tallinn Manual states that prohibition of causing mental suffering to civilian population is justified through interpretation of the Additional Protocol, where threatening with an attack to cause terror in the population is prohibited.[23] Creating non-violent attacks or misinformation is a lot easier in cyberspace, and they serve a bigger purpose than, for example, attempting to spread misinformation without the use of the web. There is a point to an attack being defined as being an aggressive act of violence because further problems might arise if an information war were legally considered the same as dropping bombs.

Cyberspace is a relevantly new and growing field that offers a completely new battlefield with new weapons and concepts. Even though it is an abstract area, cyberspace functions based on structures present on land, which allows for the possibility of IHL to be applicable. Weapons in cyberspace have the potential of wiping out the electricity of an entire city.[25] The previously introduced weapons also have the potential to create this type of damage, at least theoretically,[26] but they are only part of the force that is used in cyberspace. The key to the legal understanding of

---

20 Schmitt, M. (2013). Tallinn Manual on The International Law Applicable to Cyber Warfare. Cambridge University Press, p 105.

21 *Ibid*., p 106.

22 Schmitt, M. (2011). Cyber Operations and the Jus ad Bellum Revisited, Villanova Law Review, Vol 56, December 2011, 569-606, p 577.

23 Schmitt, M (2013), *supra nota* 20, p 108.

25 Lobel, H. (2012), *supra nota* 19, p 626.

26 *Ibid*., p 625.

the use of these weapons is that the legal consequences for the nations and operatives that use them depend on the purpose of the use and the scale in which they are targeted.

3 THE PRINCIPLE OF DISTINCTION IN CYBERSPACE

3.1 General scope of the chapter

In this chapter, the author will review the current legislation, the possibilities of identifying participants in cyber operations, and the fundamental factors that define the principle of distinction between civilians and combatants in cyberspace. The problem is currently very theoretical, so the focus will be on the academic writings of other authors on the current situation. Combatants are part of the armed forces of a nation, who have rights and obligations according to international law, which means that their active status as a military target continues throughout a military conflict and they therefore do not become civilians at any point and instead remain military targets regardless of their actions. Civilians are by definition those who are not combatants meaning that they do not fit the criteria for a combatant. The aim of this chapter is to clarify the distinction between combatants and civilians and cover international legislation and apply it to a cyber point of view.

3.2 Prohibition of attacking civilians

The law regarding attacks against civilian targets is quite clear, stating that intentional attacks against civilian persons or targets are prohibited.[27] The matter is regulated in multiple instruments like the Geneva Convention and the Rome Statute. The subject is important in discussing combatants because it is necessary to distinguish between civilians and combatants, in order to identify the parties taking part in the conflict. In terms of cyber operations, traditional attacks that would be classified as CNAs are prohibited against the civilian population, for example interference with commercial air traffic.[28]

27 Dinstein, Y. (2012). The Principle of Distinction and Cyber Warfare in International Armed Conflicts - The Journal of Conflicts & Security Law, Oxford University Press, 2012, p 265

28 *Ibid*., p 265.

According to IHL, civilians are protected from attacks that are planned and aimed to cause damage in the physical world, but the civilian population is legal a target of CNE attacks since these do not cause serious harm. Civilians are also legal targets of attacks such as propaganda or other psychologically manipulative attacks.[29] The rules regarding civilian attacks are quite clear in protecting the population from harm, but in cyberspace the effects of a propaganda operation can cause a lot more consequences The author stresses that it is necessary to distinguish clearly that CNE or misinformation have to be independent from the CNA operations in order to be legal. In case the misinformation attacks disrupt or destroy the official information channels of the local government, the nature of the attack changes, making it something that is no longer misinformation or espionage but something that attacks the channels of the local government and their ability to communicate with the population. The author agrees with the discussion of the experts in the field but is concerned about the fine line separating merely spreading misinformation and interfering with the distribution of local official information.

3.3 Classification of participants in a cyber operation

3.3.1 Combatants in cyberspace

The distinctive signs of combatants are subordinate structure, uniform, emblem, and carrying arms openly, also conducting their operations in accordance with IHL. The author will now review the interpretation of these in cyberspace and their necessity. It is important that the members of the armed forces adhere to the requirements of the Geneva Convention III Article 4, that were listed previously so that their privileged status as prisoners of war is secured.[31] Merely complying with the criteria set out in the Geneva Convention might not be be sufficient. The international experts of the Tallinn Manual agree that belonging to an armed organized group that is not a party to the conflict, will not amount to combatant status regardless of the groups compliance with the

29 Schmitt, M. (2017). Tallinn Manual 2.0 on The International Law Applicable to Cyber Warfare. Cambridge University Press, p 421.

31 Geneva Convention III Article 4

combatant criteria.[32] The author agrees with the experts since there is no direct link to the official armed forces in such a case.

Carrying arms openly is not as easily interpreted in cyberspace as one might imagine. Having access to the internet or using a computer could be interpreted as carrying arms since they are the potential doorway to armed activity. The international experts of the Tallinn Manual however argue that the criteria of carrying arms openly is not essential in cyberspace.[33] The author agrees because what can be interpreted as carrying arms openly in cyberspace, e.g. using a computer and having malicious code on the computer, can be misinterpreted. Malicious code can be stored for other reasons, e.g. for developing antimalware programs, so the author agrees that carrying arms openly cannot be seen as an essential criteria of identifying combatants in cyberspace.

Some interesting points have been raised in the Tallinn Manual concerning the carrying out of cyber operations in accordance with the law. The experts argue that in case a group conducts illegal operations, the members of the group are not complying with the law and therefore cannot be treated as combatants. But by the same logic, the experts argue that if the overall functioning of a group complies with the law and makes it eligible for combatant status, an individual member committing illegal acts does not lose their combatant status.[34]

The costs and benefits to a combatant in a cyber conflict are quite different from those to a combatant in a traditional military conflict.[35] Remote access to cyberspace and the ability to conduct nearly all of the operations from a distance lessen the risk of injury and casualty.[36] Nevertheless, military personnel conducting cyber operations that have targets and seek to weaken the enemy and gain an advantage, would obviously have these operatives considered in the same manner as military personnel that operate on land, at sea, or in the air. This is due to the same legally defined operative nature of and reason for the actions of the military personnel.

---

32 Schmitt (2013), *supra nota* 20, p 98.

33 *Ibid*., p 100.

34 *Ibid*., p 100.

35 Brenner, S. Clarke, Leo. (2010). Civilians in Cyberwarfare: Conscripts. - Vanderbilt Journal of Transnational Law, October 2010, 1011-1076, p 1032.

36 *Ibid*., p 1014.

As previously analyzed, combatant status is difficult to define in cyberspace, but one of the weapons that can more clearly link a combatant or a hostile system to hostile action is a DDoS, or a DoS, if carried out from one location. The difference to malware is therefore quite important. Malware can be used in a way that it spreads through the web through systems without its ultimate purpose being clear until it reaches its intended target, as in the Stuxnet case.[37] Though a malware attack spreads through the web from links set up for that specific purpose, the connection to the perpetrator is tenuous, but a DoS attack clearly links the perpetrator to the action. From the point of view of the principle of distinction, the difference is very important because in the case of an army operation using DoS or DDoS, there are operatives conducting the operation.

3.3.2 Civilian status in cyberspace

IHL is clear in terms of civilian protection and stipulates that they should not be subject to violence or attack conducted by the adverse party, in accordance with the Additional Protocol Article 51. There should be no exception concerning hostilities and operations conducted in cyberspace. Depending on the interpretation of Additional Protocol, certain targets such as the electrical grid or the systems that handle water distribution and filtering could be prohibited targets in cyber operations.[39]

Susan W. Brenner and Leo L. Clarke present an interesting situation where the electrical grid or systems that are used to operate financial functions are attacked by an adverse party, and the civilians working in the space that is attacked naturally have to participate in defensive action against the attack. Their actions taken against the attack can be defensive, e.g. trying to shut down the attack and protect their systems.[40] Their civilian status is a difficult concept since they keep their civilian status only as long as they do not participate in the hostilities. The author agrees that it seems logical for a civilian to abstain from offensive operations in order to remain their status, but defensive measures seem to be within their rights since it is not logical for a civilian to be

37 Richardson, J. (2011). Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield. - The John Marshall Journal of Computer & International Law an International Journal on Information Technology, Fall 2011, 29(1), p 1-27, p 2.

39 Droege, C. (2012), *supra nota* 10, p 553.

40 Brenner, S. Clarke, L. (2010), *supra nota* 35, p 1032.

forced to volunteer or surrender their network functionality for the use or attack of the adverse party.

Another author Logan Lilies has developed two scenarios where the analysis of the status on an actor. One of the scenarios regards whether or not actors, not distinguishable as combatants, taking part in cyber hostilities are combatants during a situation they encounter enemy forces in the real world. In the second scenario private contractors are seized while they are trying to inject malware into air traffic control system. In both cases the analysis leans towards civilian status.[41] The scenarios do not offer much help in providing concrete examples where distinction could be made on a person taking part in a cyber operation.

41 Lilies, L. (2014). The Civilian Cyber Battlefield: Non-State Cyber Operators' Status Under the Law of Armed Conflict. The North Carolina Journal of International Law and Commercial Regulation, Fall 2013, 39(1), 1092-1121, p 1093-1095.

4 PERSON'S STATUS AND DIRECT PARTICIPATION IN CYBER HOSTILITIES

4.1 General scope of the chapter

In this chapter the focus will be on the status of people who are or are claimed to be connected with cyber hostilities. The author will review situations where a person's status is unclear, how a person can be a lawful target of an attack, and what constitutes direct participation. The analysis is based on the negative definition of a civilian, that everyone who is not a combatant is a civilian. Cases are not always clear-cut, so this chapter aims to determine where this is applicable and what kind of actions cause doubt, justify attack, and revoke civilian protection in cyberspace.

4.2 Doubt as to person's status

When trying to identify an actor as a civilian or as a combatant in cyberspace, the question is how should the two be distinguished from one another? In fact, in IHL there is always a presumption according to which the most beneficial interpretation should be applied, in this case the status of a civilian. The international experts concluded that in case there is doubt as to the status of a person, the attacker do not bear the burden to prove that their assessment of the situation was correct and the target was in fact lawful but the defensive side must take precautions to distinguish themselves.[42] The law that was in question was the Article 50(1) of the Additional Protocol that states "In case of doubt whether a person is a civilian, that person shall be considered to be a civilian". The opinion of the experts seems more practical than the actual legal text since the Article 50(1) is quite clear that doubt is something that in fact should not exist in the target.[43] The difference is quite large considering the earlier two scenario examples, where the bottom line was that the preferential interpretation is to be used. There is also an important distinction in the

42 Schmitt, M. (2017), *supra nota* 29, p 424.

43 Additional Protocol I, Article 50(1)

repercussions of the attack; an attack that destroys system functionality is very different than an attack with lethal force.

It is argued that cyber warfare would be likely to pose a threat to the infrastructure of a nation and that civilians would therefore end up being affected by attacks.[44] The same argument goes on to state that these attacks on critical infrastructure might not be automatically illegitimate. This argument raises a legal problem in the area since there might be the possibility that civilians cannot be distinguished or are likely to suffer from the conflict. The current legislation regarding distinction relies on the fact that civilians and combatants are distinguished. The legal problem would be that in case distinction is impossible or meaningless due to the nature of the attacks, then the application of IHL to cyber conflicts may become impossible. However, this would not be a good development because the use of cyber methods is more than likely in modern conflicts, so ruling out IHL is not an option. One of the interpretations that can be drawn is that in case there is doubt about combatant status in a cyber conflict, the protection of civilians may not be as strong. If the argument is that there is no certainty that attacks on critical systems are unlawful and that they are very likely targets in cyberspace, their protection might also not be as strong in cyberspace. Having legislation that permits attacks on civilians is of course barbaric, but the nature and consequences of these attacks do not have the same effects as traditional weapons so it is not impossible to have an interpretation that in case of doubt is more lenient. The author cannot decide in favor of either choice but the problem will likely raise a potential gap in the application of current legal instruments to cyberspace.

The international experts were not able to settle on what is a 'precise threshold' or 'sufficient threshold' to assessing when there is doubt as to a target's identity, and they also noted that civilian and military networks can be interlinked in cyberspace rendering them indistinguishable from each other when observed from the outside.[45] There is also a technique called "IP spoofing" which allows for hostile actors to masquerade as on non-threatening ones.[46] The distinction between that and the traditional battlefield is that a combatant is always a combatant; they do not have the choice

44 *Ibid*., p 1029.

45 *Ibid*., p 1029.

46 Schaap, M. (2009). Cyberwafare Operations: Development and Use Under International Law. - Air Force Law Review, (64), 121-174, p 137.

of returning to civilian status after a conflict situation as would a civilian taking directly part in hostilities.

4.3 Persons as lawful targets

There certain groups that can be considered legal targets of an attack in cyberspace. The persons that fall under this category are members of the armed forces, members of organized armed groups, civilians for the duration of time they take directly part in the hostilities, and the participants in a 'levée en masse'.[47] The situation is clear in terms of armed forces in combat unless they are injured, hors de combat, or medical or religious personnel.[48] The international experts had interpretive differences in their discussions as to what is the legal duration for a combatant to be a target in the conflict. Persons fitting two criteria are lawful targets. The two groups are those who have a 'continuous combat function' according to the Interpretive Guidance and those who take part in hostilities and are lawful targets for the duration of their involvement in combat.[49] Some of the legal experts were opposed to this and argued that only membership in the armed forces fulfills the criteria of being a lawful target.[51]

The author argues that there is vast similarity between a civilian taking part in hostilities and a combatant who does not have the continuous function. This means that there can be a combatant function in a nation's use that is hidden with the exception of certain operational use. This could be seen as a stretched function of the civilian status, and there can be an armed force that is not subject to an attack for most of the time. The author would argue that belonging to the armed forces seems like a more reasonable assumption because it makes the principle of distinction more easily applicable. The easier application in a conflict situation guarantees greater protection for the civilian population, which would make it easier to assess conflicts legally.

47 Schmitt, M.(2017), *supra nota* 29, p 425.

48 *Ibid*., p 426.

49 Crawford, E. (2013). Virtual Battlegrounds: Participation in Cyber Warfare. - A Journal of Law and Policy for The Information Society, 9 (1), 1-19, p 11.

51 Schmitt, M.(2017), *supra nota* 29, p 425.

As far as an ongoing situation is concerned, assessing whether or not someone is directly participating is very difficult. Assessing the level of their involvement as constituting direct participation is obligatory in order for them to lose their civilian status and become a lawful target of an attack. Locating certain activities and then linking them to the people who have committed them would legally permit an actor's capture or an attack against them. The author of this paper recommends a solution to this legal problem, cyber activity should be met with a cyber response. Real-world weapons might bring irreversible unlawful results but rendering an attacking system dysfunctional would be more proportionate and less destructive in case of error. A benefit to this approach would keep cyberspace and the real-world battlefield separate, since the two have different problems arising in their legal interpretation. The approach is not flawless, this way of interpreting would separate the conflict into two different legal situations. The approach is suggested in the spirit of reducing the harm of a conflict but might be impossible in reality. One problem would be cyber-physical systems like the autonomous car, for which the application of the approach would be difficult.

4.4 Direct participation in hostilities

According to the ICRC Interpretive Guidance on the notion of Direct Participation in Hostilities, a person can be seen as directly participating in a conflict if the actions they take fulfill three conditions of a cumulative criteria. Firstly, they must cause harm of a military nature, meaning interference or damaging for example communication devices of the military. Secondly, the harm needs to be caused in one causal step, there needs to be a direct link between a participant's actions and the harm caused that fits criteria of the first step. Lastly, the "belligerent nexus" requires that the harmful action that directly affects the adverse party needs to be done in a supportive manner to the nation on behalf of which the action is carried out.[52] In addition the Interpretive Guidance has the concept of 'continuous combat function'. This means that a combatant is targetable for a prolonged duration, and not simply while taking part in operation or situation, to further distinguish

52 Melzner, N. (2009), *supra nota* 5, p 46.

combatant from directly participating civilian.[53] The three main criteria rule out quite a bit of activity related to cyber operations.

The requirement of an operation having a military nature rules out other types of harm done during the conflict so that such actions violating the law would fall under the jurisdiction of national courts or other competent authorities. As to the second requirement, the causal link creates interpretational difficulty in cyberspace. The persons developing the software might not be participating directly in the cyber operations even though they create the prerequisites for the operations. This may make software development a military target in case it is located in a qualifying place, where the purpose is to create military programs. However, civilians do not qualify as combatants under the definition of the principle of distinction, and the ICRC states that according to military manuals, civilians working in facilities that are military targets work there knowing the risk but still do not qualify as combatants.[54] The logic here is that a person is taking a risk while working in such a place but if an armed attack is conducted that aims to capture the location, the people working there should be treated as civilians, and should therefore not be subject to capture or physical attack on their person. Concerning cyber aspects, the military targets might be extended to facilities where internet capabilities are handled or where data is stored. The topic of locations is different but it would concern the people working there, so that if cyber warfare was to occur, the internet capabilities would have similar characteristics as weapon or ammunition factories or storages and would therefore be likely targets of attack.

Taking directly part in hostilities becomes more difficult in case cyberspace is considered an active battlefield. In past cases like Georgia, the analysis has not shown any links to the government but only involvement of Russian hackers.[56]. The case lacks enough clarity so it could be stated with certainty who in particular was behind the operation and where the it came from. The problem of applying modern IHL is that in case those who take part in the hostilities cannot be located, the

53 Prescott, J. (2012). Direct Participation in Cyber Hostilities: Terms of Reference for Like-Minded States. - 4th International Conference on Cyber Conflict, 5-8 June, Tallinn. (Ed.) C. Czosseck, R. Ottis, K. Ziolkowski, Estonia: NATO CCD COE Publications, 251-266, p 254.

54 Henckaerts, J. Doswald-Beck, L. (2005). Customary International Law, International Committee of the Red Cross, Vol 1, Cambridge University Press, p 29.

56 Swanson, L. (2010). The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict. - Loyola of Los Angeles International and Comparative Law Review, Winter 2010 Volume 32 (1), 303-333, p 320.

ability to apply the law seems like a rare occasion. There is a need to apply law to conflict situations, otherwise cyberspace would exist as a lawless realm for international conflicts. The problem is that there is no certainty as to how a person behind an attack can be located during or even after the attack.

Direct participation in hostilities can consist of belonging to a group and conducting cyber operations with them. If the person does not belong to a party to the conflict they are not guaranteed combatant immunity and instead qualifies them as an "unprivileged belligerent", meaning that they are not entitled to the same treatment as combatants.[57] As a person engages in a conflict in the traditional battlefield, their status will be return to civilian after they have stopped engaging in the attack. In cyber terms, if a person takes part in a cyber operation, their involvement ends after the operation. In a case like this, the legal question arises that in case the operation concerns something like spreading malware, the malware will not cease to act when the person does. The whole idea of malware is that it will continue the attack as long as needed or as long as the systems have been immunized or patched against it. In traditional conflict there is a clear distinction that when arms are laid down and the person has ceased to take part in the hostilities they should return to their civilian status. Would this be the case if the person was spreading malware? Would their participation be seen as the presence of malware and therefore continue to make them subject to capture? There is a logic that speaks for saying that the person continues to participate even after shutting their own computer down, meaning that there is an objective to malware and as long as it continues to pursue to objective, it is reasonable to say that the person's participation continues. There has not been any real-world necessity to answer this question because the perpetrators in cases such as Stuxnet could never be fully identified.

Direct participation in hostilities in the real world would be clear in the sense that it is of damaging nature to the enemy forces, as we have previously assessed. However, direct participation in hostilities in a conflict can occur as either CNA or CNE.[58]

There is also the question whether direct participation in a conflict could be illegal in the first place, because the notion of "combatant privilege" does not concern civilians. The argument is that only when a person directly participates in hostilities is it possible that the law may not

57 Schmitt, M (2013), *supra nota* 20, p 98.

58 Crawford, E. (2013), *supra nota* 49, p 13.

recognize the person as someone with the legal right to take those actions.[59] This is of course to rule out the 'levée en masse' function which is justified by the spontaneous nature of the participation. The argument creates further hardship since belonging to a group of 'unprivileged belligerents' could be seen as not only being cast out from the beneficial treatment upon capture but their actions could later be ruled completely unlawful.

59 Schmitt, M. (2005), *supra nota* 4, p 520.

5 CYBER OPERATIONS: STUXNET, ESTONIA AND GEORGIA

5.1 General scope of the chapter

In evaluating recent cyber operations, their characteristics are best recognized by analyzing the most visible examples. By reviewing the three different cases in the subheading, the author will attempt to analyze the legal aspects of the attacks and the legal status of the attackers. First, we will take a look at Stuxnet, at what happened and how can it be analyzed in legal terms. The Estonia and Stuxnet cyber operations did not happen in an armed conflict situation. The reason for using them as an example in this research paper, is that there are fortunately currently only few examples of cyber hostilities that have had an impact on a governmental level. However, the situations are legally speaking good examples to analyze what an offensive cyber operation looks like and what type of consequences it can have. The events of the Stuxnet and Estonia cyber operations were hostilities conducted through cyberspace and are therefore used as examples of what real-world cyber operations look like and what they may look like in conflict situations.

As the author will review cases, it is important to clarify the definition and regulation of an attack in IHL. This is done in the Additional Protocol to the Geneva Conventions of 1949. The Additional Protocol I Article 49 lists among the criteria for an activity to be considered an attack that it must be an act of violence against an adversary.[60] The attacks need to have been done on land, at sea, or in the air,[61] so the argument could be made that cyberspace is a dimension in itself and therefore is not inside the scope of the Article 49, but the UN GGE declaration has made international law applicable to cyberspace, the important aspect being what kind of cyber operation would constitute an attack under the Article 49 definition.

The author will analyze the questions whether the attacks fulfilled the criteria of Article 49 and how the status of the participants can be classified according to the principle of distinction. The principle of distinction has been reviewed but in this chapter the author will try to analyze whether

60 Additional Protocol I Article 49 (1)

61 Additional Protocol I Article 49 (2)

or not the status of the participants can be pinpointed from the facts of the cases. The author will also create a hypothetical legal analysis applying the relevant laws and rules to the situation for the sake of testing the application of IHL to cyberspace and what type of problems this may cause.

5.2 Stuxnet

Stuxnet was a cyber operation in which a computer worm was spread throughout the internet and it was in fact designed to reach a certain operating system, an Iranian nuclear facility, in which the virus was activated and gas centrifuges used to enrich uranium were destroyed.[62] An attack of this sophistication had never been seen before and had experts baffled. The worm used a program that was used in nuclear and other facilities to gain access to the internal network of the facility and then proceeded to destruct the centrifuges.[63]

5.2.1 Legal analysis of the situation

The Stuxnet worm was later linked to targeting the specific facility and damaged the functioning of the reactor.[64] The worm also stole information from the facility.[65] The characteristics of the attack entail elements of both CNA and CNE. It can be said that the Stuxnet worm was an offensive cyber operation constituting an attack according to the Additional Protocol 1. The main purpose of the worm was to destroy and delay the facility's operations, and it is clear that the damage would have been similar in the physical world if the attack had been carried out with physical force. There is also the question of the legality of the operation since the nuclear facility had been stated to be in use for peaceful purposes.

62 Richardson, J. (2011), *supra nota* 37, p 3.

63 *Ibid*., p 2.

64 *Ibid*., p 2.

65 Lobel, H.(2012), *supra nota* 19, p 624.

5.2.2 What is the legal status of the attackers?

The list of possible perpetrators is quite limited in the Stuxnet case,[66] but the biggest problem in the cyber world is that proving conclusively who was the perpetrator of an attack can be extremely difficult. The situational analysis is conducted from the perspective of the law of war, meaning that a person's status is analyzed as if they were in a conflict situation.

It can be stated that there was a group of people who planned and developed the attack, even though it's unknown who they were. In case it was a governmental action, then the attackers would qualify as combatant but there is no clear reason why such an assumption should be made. In case such a weapon was developed by a private contractor, this would affect their status. If a group or company was hired to develop this type of malware, they would be civilians at least in terms of the civilian combatant distinction. The experts of the Tallinn Manual state that private contractors are seen as directly participating for the duration of their involvement, and a majority stated that a company would be seen to fit the criteria of an organized armed group in case they were to conduct cyber operations for a state.[67]

In case the Stuxnet worm was developed by a company or personnel with technological knowledge the question would be what their status would be under IHL in case their identity was revealed. The causal link, introduced from the ICRC Interpretive Guidance, requires that the damage be one causal step away from the person who is directly participating, so in the case of the company or technician who developed the worm, they would have had to press the button to deploy it themselves, otherwise their status would be that of civilians that are not directly participating. In case the worm was developed as a military project by military personnel their status would be that of combatant since they are would be acting under orders of a state. Regardless of who sent the worm, their status would be that of a combatant or civilian directly participating in hostilities. In case of direct participation, the legal problem would be to define the length of the participation. In a hypothetical conflict situation if a similar worm were to attack a system, the question would be how long, the person who deploys the worm, remains as a legal target for the opposing forces. If it were defined by how long the worm affects the targeted system, their participation would be

66 *Ibid*., p 624.

67 Schmitt, M.(2017), *supra nota* 29, p 426.

defined by the technological capabilities of those who operate the targeted system. This would result in certain degree of absurdity since the length of their participation would be decided by the abilities of the opposing government or their ambition to stop the attacker's participation.

5.3 Estonia

An important feature of the cyber operation against Estonia is that it was not legally classified as an attack. This is because the targets of the hostilities were governmental institutions and commercial websites but because hostile external governmental involvement was never confirmed.

The cyber hostilities against Estonia in 2007 were the result of an escalation that occurred when the Estonian government planned to move a Soviet era monument. When it was decided to move the monument, Estonian websites in many industries were attacked.[68] The hostilities took place from April 27th to May 18th. The first phase of the attacks targeted Estonian e-services, some governmental institutions and news outlets. In the beginning phases of the attacks, the operations were not very coordinated, but seemed to express resistance towards the moving of the statue and were mostly DoS attacks. Starting from April 30th the attacks became more efficient and sophisticated, using DDoS and targeted internet service providers and seemed to be more organized and targeted more government communications, banks, and commercial websites. The offensive DDoS campaigns continued as a third and fourth wave on May 15th and 18th targeting banks and governmental websites.[69] The attacks targeted Estonian capabilities to contact anyone from outside about the events. The attacks escalated to a state where the entire internet in Estonia was nearly brought down.[70]

---

68 Shackelford, S. (2009). From Nuclear War to Net War: Analogizing Cyber Attacks in International Law. - Berkley Journal of International Law (BJIL), 25(3), 191-250, p 205.

69 Tikk, E. Kaska, K. Vihul, L. (2010). International Cyber Incidents, Legal Considerations, Cooperative Cyber Defense Center of Excellence, CCDCOE, 2010, 4-120, p 20.

70 Shackelford, S. (2009), *supra nota* 68, p 205.

5.3.1 Legal analysis of the situation

The nature of the situation was not legally speaking under the jurisdiction of IHL. The author has chosen to analyze the events from the perspective of IHL because it could be an example of the difficulty of identifying perpetrators in offensive cyber operations. The situation has also been selected because it was a visible example of an offensive cyber operation and therefore could resemble something that might occur in an actual conflict situation. The author argues that the involvement of international law can create extreme difficulty in analyzing offensive cyber operations since there is no confirmation as to who is responsible. Looking at specific hostile addresses was also extremely difficult since the attacks were conducted from a vast amount of different addresses which in essence would have been of very little benefit, since tracking one address alone would have had to go through a lot of bureaucracy in order to authorize obtaining the information.[71] If these hostilities had taken place in a situation that could be qualified as an armed conflict situation or an attack under the UN Charter, the legality of the investigation would have been more obvious and the data could have be collected.

5.3.2 What is the legal status of the attackers?

The attacks were shown to have been initiated from Russia, but it is difficult to show exactly from where. The attacks involved thousands of perpetrators known in the internet as "script kiddies" who were recruited from online chat rooms. Also involved was a youth organization called "Nashi su".[73] Making exact claims as to where the attacks came from is difficult, and many of the locations where the attacks were conducted from remain unknown. Even in the second wave of the operation no clear link to the attacks being government initiated could be established, but there are strong indications.[74] If the situation had developed into an armed conflict, in the aforementioned first wave of attacks the participants would have most likely been civilians participating in the hostilities with the addition that the attacks had an impact on military targets. The second more

71 Tikk, E. Kaska, K. Vihul, L. (2010), *supra nota* 69, p 26.

73 Shackelford, S. (2009), *supra nota* 68, p 205, 206.

74 Tikk, E. Kaska, K. Vihul, L. (2010), *supra nota* 69, p 23.

coordinated wave of attacks might imply a more organized approach in which the participants would seem to have been of a military nature.

5.4 Georgia

The attacks that Georgia faced in 2008 were initially DDoS against websites operated in the country. This was only the first phase of the attack, and three weeks later, the DDoS attacks were repeated on a larger scale. Analysis of the events showed that the DDoS attacks that ultimately attacked the Georgian government's communication tools seemingly at the same time as Russian troops were advancing on land.[76]

5.4.1 Legal analysis of the attack

The main legal question in the case, is whether the law of armed conflict is applicable? The link between the DDoS attacks and the advancement of the troops has been established, but due to the nature of cyberspace, the ability to remain hidden has granted the attackers anonymity at least in the sense of not being clearly identified. The legal problem of the attack is that since the operatives could not be identified during the attack, it is difficult to point the finger at the specific perpetrators. This marks as one of the first times that military action and a cyber operation have happened at the same time.[77]

The targeted functions were the ability of Georgia's government to inform its citizens of the situation.[78] This brings a civilian factor into the analysis since the population was a target of the attack in a causal connection between the attack and its results. During the attack, the attackers

76 Korns, S. Kastenberg, J. (2008). Georgia's Cyber Left Hook. - Parameters; Carlisle Barrack, Winter 2008/2009, 60-76, p 60.

77 Swanson, L. (2010), *supra nota* 56, p 304.

78 *Ibid*., p 303.

prevented communication between Georgian cyber actors in order to prevent them from creating any sort of counterattack against the attackers.[79]

At least from an international law point of view, analysis of the cyber operations that Georgia faced is not quite as simple as simply declaring them an attack on Georgia. The question would be whether the DDoS attacks constitute an attack that would justify the application of IHL. Within the Georgian population the use of the internet is quite low, so the attacks targeted on the governmental sector did not have a devastating effect on Georgia's citizens. Analysis of the DDoS and other malicious computer attacks, showed that these did not create suffering among the population. Taking into account the validity and clarity of the evidence of the case, did not create circumstances for the application of IHL.[80]

5.4.2 What is the legal status of the attackers?

The group conducting the cyber operation interrupted the government's network functions (CNA, DDoS attack), and there was a possible link between the forces on land and the group involved in the cyber operation. There was however, no evidence of this, the data collected on the DDoS attackers was not sufficient in order to claim that there was state involvement on the attacker's side.[81] The fact that the computer attacks did not create severe enough consequences in order for them to be analyzed under IHL, analyzing whether the attackers qualified for the status of combatants or directly participating civilians cannot be done on the case facts as they are.

The author will however analyze the events applying IHL, in order to analyze whether the participants would qualify for combatant status or direct participation in a situation where IHL is applicable. According to the Geneva Convention III Article 4, a combatant is defined according to the criteria of four characteristics which are subordinate structure, uniform or emblem, carrying arms openly, and conducting their operations in accordance with the law. Combatants fulfilling these criteria have the right to be prisoners of war. The difficulty is to determine whether someone

79 Hauptman, A. (2015). Direct Participation In Cyber Hostilities Proceedings of the 1st Interdisciplinary Cyber Research Workshop 2015, Tallinn University of Technology, 18th July 2015, Osula, A, Maennel, O. Tallinn University of Technology, 1-46, p 25.

80 Tikk, E. Kaska, K. Vihul, L. (2010), *supra nota* 69, p 90.

81 *Ibid.*, p 90.

engaging in a DDoS attack fulfills these criteria. In case it's assumed that the persons participating are not private contractors, they would probably fulfill the subordinate structure. However, the legislation seems redundant regarding their appearance or carrying arms openly. In case the program that conducts the DDoS is considered the weapon, then carrying it openly is not important according to the experts of the Tallinn Manual, as previously explained. In the hypothetical situation where such people would be captured during the attack, the interesting question would be whether carrying arms openly would be considered important. Carrying arms openly is a legal problem when considering the definition of a combatant since to be distinguished in person is not a similar necessity as it would be in the battlefield. This would be an important feature to define as part of IHL that is applied to cyber operations. The author argues that there still could be a relevant difference whether or not they were distinguishable from other civilians present since if the persons engaging in the attack were not wearing uniforms and their location could be determined, they could not be easily distinguished from those who are maintenance personnel or present for other reasons. Like the civilians who are allowed to assist armed forces while in combat, someone in charge of making the computers work should be distinguished from those who are engaging in cyber hostilities.

6 CONCLUSIONS

Traditionally IHL has set out clear criteria that combatants and civilians follow in order to be recognized correctly during a conflict and be eligible for prisoner of war status as combatant and protected as a civilian. The distinction between these two groups is as essential for the attacking forces as for the defensive forces. The distinction is based on clear rules in a traditional battlefield and the rules of governing distinction are not difficult to comprehend. A cause for concern is the internet, which has grown to dominate information and services growing to a degree previously unimaginable. It poses a viable threat in modern conflicts and provides completely novel methods for offensive and defensive actions. The previously made distinction in the battlefield is not as simple on the internet.

Due to the current situation that is technologically possible to remain hidden and the current legal difficulty of a comprehensive application of IHL to cyberspace, the problems of cyberspace should be treated as a separate legal field. The aim should be towards legal instruments that are first legal interpretations of the present IHL legislation adapted to the cyber environment and later towards more precise legal instruments that give answers to the problems. The Tallinn Manual is an expanding effort towards the application of IHL to cyberspace.

International treaties and customary law are very clear that civilian objects are not permitted as targets of attacks. Therefore, the responsibility of those who engage in the conflict is to distinguish their combatants from their civilians. In cyberspace this of course creates trouble since attacks can be made from hidden locations and since clearly identifying who are civilians or combatants would require a closer view. Therefore, the author argues that there should be a different approach according to which civilian traffic could be distinguished from other traffic and thereby ensuring the protection of civilian traffic. This can be done for instance by developing technological capabilities for distinction. This would clarify what is civilian status in cyberspace and all other

traffic may be or may not be used for military purposes. This solution would secure the more important aspect of conflict legislation. This method would clarify situations where there is doubt as to a person' s status, and it would ensure that clearly civilian targets cannot be mistaken for combatant targets.

According to the present state of research, there are currently no sufficient legal instruments or technology to govern conflicts in cyberspace. Interpretations of legal authorities of treaties and treaties themselves may have to be separated into ones regarding weapons, conflict, situations, and persons in cyberspace. The legal and technological instruments regarding cyberspace and persons should be able to find a solution to the distinction between the persons taking part in the hostilities and those that are civilians. Some type of enforced measure to mark IP addresses is necessary that displays combatant and civilian traffic as separate. The current rules of IHL require that combatants distinguish themselves from civilians, but in cyberspace, the approach to the goal of successfully protecting civilians could be different. An unorthodox approach to protecting civilians would be to distinguish their location or traffic and thereby leave everything else as a potential battlefield setting, thus clarifying the area where combat is permitted. It would serve a similar purpose to the four criteria that are required in the battlefield. It would prevent cyber operatives from being completely masked and instead give a clear benchmark for how someone should be recognized in cyberspace.

Reference List

Books:

Schmitt, M. (2013). *Tallinn Manual on The International Law Applicable to Cyber Warfare*. Cambridge University Press

Schmitt, M. (2017). *Tallinn Manual 2.0 on The International Law Applicable to Cyber Warfare*. Cambridge University Press

Henckaerts, J. Doswald-Beck, L. (2005) *Customary International Law, International Committee of the Red Cross*, Vol 1, Cambridge University Press

Journal Articles

Brenner, S. Clarke, Leo. (2010). Civilians in Cyberwarfare: Conscripts. - *Vanderbilt Journal of Transnational Law*, October 2010, 1011-1076.

Cordula Droege, (2012). Get off my could: cyber warfare, international humanitarian law, and the Protection of Civilians. - *International Review of the Red Cross*, (New Technologies and Warfare), Issue 886, 94, June 2012, 533-578.

Crawford, E. (2013). Virtual Battlegrounds: Participation in Cyber Warfare. - *A Journal of Law and Policy for The Information Society*, 9 (1), 1-19.

Dinstein, Y. (2012). The Principle of Distinction and Cyber Warfare in International Armed Conflicts - *The Journal of Conflicts & Security Law*, Oxford University Press, 2012, 262-277.

Korns, S. Kastenberg, J. (2008). Georgia's Cyber Left Hook. - *Parameters; Carlisle Barrack*, Winter 2008/2009, 60-76.

Lilies, L. (2013). The Civilian Cyber Battlefield: Non-State Cyber Operators' Status Under the Law of Armed Conflict. - *The North Carolina Journal of International Law and Commercial Regulation*, Fall 2013, 39(1), 1092-1121.

Lessig, L. (1996). The Zones of Cyberspace. - *Stanford Law Review* 48, 1403-1411.

Lobel, H. (2012). Cyber Warfare Inc.: The Law of War Implications of the Private Sector's Role in Cyber Conflict. - *Texas International Law Journal*, Summer 2012 47(3), 618-640.

Ophardt, J. (2010). Cyberwarfare and the Crime of Aggression: The need for Individual Accountability for Tomorrows Battlefield. - *Duke Law & Technology Review*, 1-28.

Richardson, J. (2011). Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield. - *The John Marshall Journal of Computer & International Law an International Journal on Information Technology*, Fall 2011, 29(1), 1-27.

Rid, T. McBurney, P. (2012). Cyber-Weapons. - *The Rusi Journal*, 6-13.

Schaap, M. (2009). Cyberwafare Operations: Development and Use Under International Law. - *Air Force Law Review*, (64), 121-174.

Shackelford, S. (2009). From Nuclear War to Net War: Analogizing Cyber Attacks in International Law. - *Berkeley Journal of International Law* (BJIL), 25(3), 191-250.

Schmitt, M. (2005). Humanitarian Law and Direct Participation in Hostilities by Private Contractors or Civilian Employees. - *Chicago Journal of International Law*, Volume 5 No. 2, Winter 2005,511-546.

Schmitt, M. (2011). Cyber Operations and the Jus ad Bellum Revisited. - *Villanova Law Review*, Vol 56, December 2011, 569-606.

Schmitt, M. (2012). Classification of Cyber Conflict. - *Journal of Conflict and Security Law*, Summer 2012, 17(2), 245-260.

Swanson, L. (2010). The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict. - *Loyola of Los Angeles International and Comparative Law Review*, Winter 2010 Volume 32 (1), 303-333.

Conference and seminar material

Hauptman, A. (2015). Direct Participation In Cyber Hostilities, *Proceedings of the 1st Interdisciplinary Cyber Research Workshop 2015*, Tallinn University of Technology, 18th July 2015, Osula, A, Maennel, O. Tallinn University of Technology, 1-46.

Liles, S. Dietz, J. Rogers, M. (2012). Applying Traditional Military Principles to Cyber Warfare. - 4th *International Conference on Cyber Conflict*, 5-8 June, Tallinn. (Ed.) C. Czosseck, R. Ottis, K. Ziolkowski, Estonia: NATO CCD COE Publications, 169-180.

Mirkovic, J. Prier, G. Reiher P. (2002). Attacking DDoS at the source, *10th IEEE International Conference on Network Protocols 2002*, 12-15 November 2002, Paris. (Ed.) Werner, B. The Printing House in The United States, The Institute of Electrical and Electronics Engineers, 312-321.

Prescott, J. (2012). Direct Participation in Cyber Hostilities: Terms of Reference for Like-Minded States. - 4th *International Conference on Cyber Conflict*, 5-8 June, Tallinn. (Ed.) C. Czosseck, R. Ottis, K. Ziolkowski, Estonia: NATO CCD COE Publications, 251-266.

Electronic sources

Melzer, N. (2009). ICRC Interpretive Guidance on the Notion of Direct Participation in Hostilities. Accessible: https://www.icrc.org/eng/assets/files/other/icrc-002-0990.pdf, 23 April 2018

Treaties, conventions, customary law and reports

ETS. 185 Budapest Convention on Cybercrime, Accessible : https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

Geneva Convention III, Accessible: https://ihl-databases.icrc.org/ihl/INTRO/375

Geneva Convention IV, Accessible: https://ihl-databases.icrc.org/ihl/INTRO/380

ICRC Customary International Humanitarian Law, Accessible: https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul

United Nations Governmental Experts on Information Security, Accessible: http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

Tikk, E. Kaska, K. Vihul, L. (2010). International Cyber Incidents, Legal Considerations, Cooperative Cyber Defense Center of Excellence, CCDCOE, p 1-132. Accessible: https://ccdcoe.org/publications/books/legalconsiderations.pdf, 13th May 2018.