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

Emilia Rantala

APPLICABILITY OF RULES OF ARMED CONFLICT IN INTERNATIONAL CYBER-WARFARE

Bachelor's thesis

Programme Bachelor HAJB, specialisation European Union and International Law

Supervisor: Katrin Merike Nyman-Metcalf, PhD

Tallinn 2018

I declare that 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 8928 words from the introduction to the end of summary.

Emilia Rantala Emilia Rantala 21.12.2017
(signature, date)
Student code: 145427HAJB
Student e-mail address: emilia.rantala@netikka.fi

Supervisor: Katrin Nyman-Metcalf, PhD

The paper conforms to requirements in force

……
(signature, date)

Chairman of the Defence Committee: / to be added only for graduation theses /
Permitted to the defence
……
(name, signature, date)

TABLE OF CONTENTS

ABSTRACT

Author of the thesis presents a topic that has started to take shape in recent years: cyber-warfare. The research proposes particular cyber concepts and examines the impacts of defining these concepts in the legal field. The thesis aims to introduce the grounds of application of the law of armed conflict to cyberspace. This research is a theoretical approach based on scientific texts written by the legal professionals. Applying the principles of International Humanitarian Law to cyber-warfare is complex, and it raises more questions than it provides answers. The thesis reaches a conclusion where the law of armed conflict may be applied to cyber-warfare if it reaches the threshold of armed conflict, but if the threshold is not reached, then the law of armed conflict should not apply. As a result, the author finds that more attention should be paid to define the crucial concepts of the topic and provide guidelines on their application in legal context.

Keywords: cyber-warfare, cyber-attack, cyber law, international humanitarian law

LIST OF ABBREVIATIONS

CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
DDoS	Distributed Denial of service
DoS	Denial of service
ICTY	International Criminal Tribunal for the former Yugoslavia
IHL	International Humanitarian Law
SCO	Shanghai Cooperation Organisation
Stuxnet	A cyber worm discovered in 2010
Tallinn Manual	Tallinn Manual on the International Law Applicable to Cyber Warfare
Tallinn Manual 2.0	Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations
T-CY	The Cybercrime Convention Committee

INTRODUCTION

Nowadays, globally technology controls enormous part of our everyday life. Just to mention critical infrastructure, which may cause vast destruction, this includes electricity generation, water supplies, financial markets and communications.[1] Technology has now brought its difficulties to the legal field in the form of cyberspace. The whole international field of cyberlaw can be considered a bit blurry at the moment. While awareness of cybersecurity has become essential for policymakers, businesses and ordinary citizens, defending our computers is not enough by itself. Knowledge of cybersecurity protects better from cyber-crimes and online attacks. Greater preventive and deterrent measures should and have already been taken to guarantee that cyber-attacks would not cause damage to the critical infrastructure or cause a loss of life.[2]

The benefits cyberspace offers are significant, but in recent years state officials and scholars from different fields have awoken to the potentiality of cyberspace used as a military weapon in the combat. Information transforms through interconnected networks at an instant when put in cyberspace. Cyberspace is a virtual environment where actions do not physically take place, so it technically does not have geographically defined territories either. Anonymity is one of the reasons why the field has its challenges in legal regulation. Cyber-attacks for instance, often cannot be traced back to the operator because the attacker has used different networks. At stake has been the concerns whether the existing legal frameworks can apply to cyber activities or cyberspace at all. Whether the current legal framework applies or completely new one governing cyberspace is introduced, it is clear that application may be problematic at international level, since international law includes notions of territory conventionally.[3]

This thesis will view the topic that has just begun to take shape in recent years: cyber-warfare and its potential as a threat to national security. This thesis reflects the theories of cyber-warfare and whether laws of armed conflict could apply to cyberspace and on what grounds. Until state practice in the future indicates us the applicable law, this thesis is entirely hypothetical. Few years ago

[1] Ayalew, Y.E. (2015) Cyber Warfare: A New Hullaballoo under International Humanitarian Law – *Beijing Law Review*, Vol. 6, No. 4, 209-210
[2] Carr, J. (2012). *Inside Cyber Warfare*, 2nd Edition, Sebastopol: O'Reilly Media, Inc. 2
[3] *Research Handbook on International Law and Cyberspace.* (2015). / Eds. N. Tsagourias, R. Buchan. Cheltenham: Edward Elger Publishing Limited

cyber-warfare would have been considered as a fictive subject; however, today evidence from the occurred cyber-attacks show that cyber-weapons really exist.[4]

This thesis will give an overview of the basic principles of the law of armed conflict, how those principles would work in cyber-warfare and what might be the key issues arising from the application of those principles. The research aims to find out on what conditions the laws of armed conflict would apply to cyber-warfare and if other possible existing laws could govern the matter better.

The main hypothesis of the thesis is that, if the cyber-warfare fulfills the requirements of an armed conflict, then the laws of armed conflict should be applied. The research question of the thesis is: what type of cyber-warfare could fulfill the requirements of an armed conflict or should there be a distinction between different types of cyber-warfare? Besides the research question, the thesis aims to give some level of understanding about the cyber concepts and the differences between them. The thesis also provides an overview of some remarkable cyber-incidents that have happened in the 21st century and analyses the context of armed conflict through them.

The qualitative research method is used in this thesis, where the author analyses the existing documents that have been written by the professionals of these subjects since not much real life data yet exists about this particular topic, so this whole research is hypothetical on the part what law would apply to this kind of cases.

These areas of law are interesting and the subject of the thesis is new in the legal field, therefore researching the subject more deeply was intriguing. Compared to traditional armed conflict, in cyber-warfare, it may be more unclear whether an attack has occurred at all. The Internet offers the anonymity to cover the true identity of the attacker, which complicates determinating who started the attack in the first place. Variety of different actors can have access to this kind of cyber tools, also non-governmental actors, so this problem might be difficult to put under the certain existing category of law.

The first chapter introduces different cyber concepts, and in the second chapter, the thesis views serious cyber-attacks that have become publicly known. The third section gives an overview of the

[4] Mavropoulou, E. (2015). Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber-Attacks - *Journal of Law & Cyber Warfare,* Vol. 4, No. 2, 24

international humanitarian law, its basic principles and introduces the connection of these principles to the cyber environment. The applicability of humanitarian law to cyber-warfare is analyzed in the fourth chapter, and the final chapter attempts to assess the cyber-warfare that is possibly introduced in legal texts.

1. THE ERA OF CYBER TECHNOLOGIES

For most users, the Internet is a positive innovation, but the quickly changing global technical development also creates new possibilities for computer attacks and other cyber operations, which all people are not aware of.[5] Some of these cyber incidents are already common, and people are aware of them, but what is not always so clear, is the difference between cyber-crime, cyber-attack, and cyber warfare. Firstly it is crucial to try to explain the distinction between these concepts to enable to consider the thesis topic, although it is not simple to categorize these concepts because motivations committing different cyber actions can overlap, and there is a plenty of cyberspace targets.

1.1. Cybercrime

The Internet offers the speed, convenience, and anonymity to commit a wide range of crimes that do not have borders. Many potential targets of cybercriminals even volunteerly offer their information without knowing the danger that is present. That is one of the reasons why cybercrimes continue to grow in number and sophistication. The widespread availability of Internet has created the suitable environment for cybercrimes. The concept of cyber-crime has no universally recognized definition, but it can be considered as a broad concept where a computer is either an object of the crime or used as a tool to commit a crime. Budapest Convention on Cybercrime[6] is first international treaty governing the subject of cybercrime entered into force in 2004. The convention includes definitions of some important terms like " 'Computer system' means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data".[7] The convention uses technology-neutral language to ensure the convention can also cover new technologies under the substantive criminal law. The Cybercrime Convention Committee (T-CY) agrees that the definition of "computer

[5] Ayalew, Y. E. (2015). *supra nota* 1, p 209.
[6] Council of Europe, *Convention on Cybercrime*, No. 185 of 23 November 2011, European Treaty Series, 08.11.2017
[7] *Ibid*. Article 1

system" also covers, for example, smartphones and tablets. Convention introduces criminal provisions that may apply to different crimes but it does not focus on specific techniques or technologies used, it can be considered as a tool to allow the states to criminalize different acts.[8] The convention is created to foster international cooperation in order to fight cybercrime more efficiently and also to make it possible to collect electronic evidence when the offense is committed relating to computer systems and data.[9]

Some scholars argue that a cyber-attack has a political or national security implication and that character is what distinguishes it from simple cyber-crime. For example, if a state actor takes aggressive action in the cyber domain, it is an implication that national security is at stake. Therefore this action is regarded as a cyber-attack if also other elements of the definition are satisfied. An act falls under the mere category of a cyber-crime and not under cyber-attack if it is committed by a non-state actor, for example, executed by an individual or a criminal group and the act falls under state or international criminal law. If a non-state actor hacks into the bank data by means of a computer network and successfully manage to do that with an economic gain on the mind, this would fall under a cyber-crime, but would not constitute a cyber-attack. On the other hand, if a non-state actor commits a cyber-crime for a political or national reason, then it can be considered as a cyber-attack.[10]

As said, the cyber-crime is a broad concept and cybercriminals may use the technology for example to these common crimes: to access private emails, operate wire frauds where money or property is obtained by false means, transmitting child pornography, harass or threaten people through communication channels, distributing drugs by means of Internet or infringe a copyright for a financial gain. These crimes are all criminalized under state or international law.[11] The fact that this sort of crimes is regularly committed and the impact these crimes can have on public or the economy are a very good reason to give more attention to regulating it.[12]

---

[8] Cybercrime Convention Committee (2017), *T-CY Guidance Notes*, Accessible: https://rm.coe.int/16806f9471, 8 November 2017.
[9] Clough, J. (2012), The Council of Europe Convention on Cybercrime: Defining 'Crime' in a digital world - *Criminal Law Forum*, No. 23, 363
[10] Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., Spiegel, J. (2012), The law of Cyber-Attack – *California Law Review*, Vol. 100, No. 817, 826-830
[11] INTERPOL, *The threats*. Accessible: https://www.interpol.int/Crime-areas/Cybercrime/The-threats, 8 November 2017.
[12] Lunn, B. (2014) Strengthened Director Duties of Care for Cybersecurity Oversight: Evolving Expectations of Existing Legal Doctrine – *Journal of Law & Cyber Warfare*, Vol. 4, 113.

1.2 Defining Cyber-Attack

The cyber-attack also lacks a common definition, but as some knowledge is necessary for legal analysis of this Thesis, describing different definitions of the cyber-attack will clarify things. The absence of the definition has also slowed down the legal analysts on developing coordinated policy recommendations and made it difficult for governments to engage in these actions.[13] There are two dominant approaches to the definitions, which are introduced below.

1.2.1 An Object-Based Definition of Cyber-Attack

A narrow definition is described according to "The Law of Cyber-Attack (2012)" as: " A cyber-attack consists of any action taken to undermine the functions of a computer network for a political or national security purpose."[14] A cyber-attack term requires the take of active measures whether it is governments offense or active defense. The act may be executed by any means, but for an act to fall under the cyber-attack its aim must undermine or disrupt the function of a computer network. In this definition the cyber-attack has the objective-based approach, which is followed by United States, and some people can see this approach as a superior to means-based approach.[15]

When the objective is to undermine the function of a computer network, it can be done in many different ways. Examples that include worms, viruses, and Trojan horses are considered as syntactic attacks to disrupt a computer's operating system, which causes the networks malfunction. Semantic attacks, however, compromise the accuracy of the information the operating system processes and reacts to, without harming the operating system and that is why it can seem to operate normally but the answers it will deliver will not match the reality. The objective-based approach outlines cyber-espionage and cyber-exploitation from the cyber-attack because even if those incidents compromise the security of the computer network, those do not affect on the computer networks current or future ability to function.[16]

It was mentioned before that some scholars argue that a political or national security purpose is the distinguishing factor between a cyber-attack and a cyber-crime. One of the most fundamental

[13] Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., Spiegel, J. (2012), *supra nota* 10, p 823
[14] *Ibid*. p 826.
[15] *Ibid.*
[16] *Ibid*. p 828-829.

interests of a political community, whether it is a country, state or nation, is freedom from invasion and domination; and to secure the resources that are vital for survival.[17]

Some scholars consider it crucial to exclude those crimes with a nonpolitical aim from the definition of a cyber-attack because those activities do not raise the same legal questions as the activities with a political aim what might cause the breach of the public international law. The more precise definition will also clarify the dividing the tasks of cyber-security inside the government departments. When the objective-based approach is used for a political or national security purposes, it does not limit the definition to only state actors. The exclusion is important because the cyber-attacks are appealing also for terrorists and other non-state actors due to the low cost and anonymity.[18]

The supporters of a means-based approach argue that this definition of "cyber-attack" is outmoded and misleading because it leaves room for broad interpretations of which types of actions could be included in targeting computers, assuming the traditional types of attacks which cause a physical destruction, can be used to destroy these computer facilities. According to them, no new legal framework is needed to address these traditional kinds of attacks since computers and computer networks hold no special legal status and therefore in such case, it would clearly raise a question of international law.[19]

1.2.2 A Means-Based Definition of Cyber-Attack

In means-based approach, the use of computers and networks are seen as instruments of attack and the supporters of this approach sees that it makes more sense to define "cyber-attack" by instrument.[20] This approach is followed for example by The Shanghai Cooperation Organization (SCO), which is a security cooperation group that covers China, Russia Iran, India, Pakistan and former Soviet Central Asian republics. This view enables the use of cyber operations as a weapon or form of the attack, where a particular objective can be executed. Some scholars view the risks posed by this an expansive vision of means-based approach includes that cyber-technology could

[17] *The Ethics of Information Warfare* (2014). /Eds. L. Floridi, M. Taddeo. Law, Governance and Technology Series, Springer International Publishing, 3-4
[18] Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., Spiegel, J. (2012), *supra nota* 10, p 831
[19] Nguven, R. (2013), Navigating Jus Ad Bellum in the Age of Cyber Warfare - *California Law Review*, Vol.101, 1087
[20] *Ibid*. p 1085.

be used to weaken political stability and some fear that this could to limit the Internet speech of censorship of political speech is justified by this vision.[21]

One proposed definition of cyber-attack is by Reese Nguven " a hostile act using a computer or related networks or systems to cause disruption or destruction for a political or national security objective."[22] This definition specifies the use of computers or their networks as the instrument for the attack but does not specify the disruption or damage it causes. This point of view agrees with the political or national objective, which is also a criterion in the objective-based approach because that objective is what distinguishes a cyber-attack under international law from a cybercrime that is governed by domestic law. This view also sees that it is important to include the attacks made against physical targets by using computers within the same legal work because the unclear line between cyber and physical is increasing, but none of the areas should be left ungoverned since it can cause difficulties in the future.[23]

1.3. Cyber-Warfare

Cyber-warfare is probably the most controversial topic in the field of armed conflict at the moment. The concept of utilizing information as means to conduct warfare has already existed for centuries.[24] All parties to the conflicts have accepted new technological inventions for their use over the years. At the present state of the world, there have not yet been any recognized cyber-attacks that would have reached the definition of armed attack. One of the questions has been if cyber-attacks are even capable of physical violence.[25]

These three mentioned cyber-categories are in connection with each other. A cyber-attack may overlap with a cyber-crime, but cyber-warfare has a distinctive character, and as a cyber-warfare occurs it also constitutes a cyber-attack, but not all cyber-attacks are considered as cyber-warfare.[26] This topic of cyber-warfare is difficult to assess since the scholars from different fields share such

[21] Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., Spiegel, J. (2012), *supra nota* 10, p 824-825
[22] Nguven, R. (2013), *supra nota* 19, p 1089.
[23] *Ibid*. p 1089-1090.
[24] *Encyclopedia of Cyber Warfare* (2017). / Eds. Paul J. Springer, ABC-CLIO, Introduction, xix
[25] *The Ethics of Information Warfare* (2014) *supra nota* 17, p 3.
[26] Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., Spiegel, J. (2012), *supra nota* 10, p 832-837

differing definitions. Some argue that no blood spill is required to defeat the opponent and therefore the cyber-warfare is a war without the fighting.[27] As a contrary, some view cyber-warfare as it satisfies the requirements of a cyber-attack but a cyber-warfare also have effects equivalent to an armed attack, or the activity occurred in the context of armed conflict.[28] Despite the definition, cyber-warfare can be considered to symbolize a state-sponsored use of cyber-weapons that have real-life destructive effects. The lack of universally recognized definition only complicates the application of international legal rules.[29]

1.3.1 The Concept of Cyber-Weapon

There are different views on which is considered as a cyber-weapon, and the distinction is usually made depending on which approach is taken to the definition of a cyber-attack. The subject is very challenging because of the existing uncertainties and disagreements of crucial and essential definitions such as the attacker's anonymity and traceability, and if a cyber-attack can be defined as an armed attack and on what grounds. The object-based approach views that the concept of cyber-weapon in the context of cyber-warfare is necessary to separate from the typical malware used in mere cyber-crimes because actions that are considered to rise to the level of cyber-warfare can be performed through malware or other information technology tools. Also, another crucial distinction is to separate cyber-weapons from malware or information technology tools used for the purpose of espionage.[30] Many nations have engaged in cyber espionage, and an example of this was already shown when the former NSA contractor Edward Snowden leaked top-secret documents on spying on American citizens.[31] Espionage often has a political or a national security goal to gain different advantages on enemies and allies either in war or peacetime, but this would not be considered as a cyber-weapon.[32] Espionage may be criminal, therefore punished according to domestic law but the activity is not prohibited under international law.[33] The separation is important because a situation where a cyber-weapon is used could lead to the beginning of a

[27] Carr, J. (2012). *supra nota* 2. Foreword
[28] Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., Spiegel, J. (2012), *supra nota* 10, p 832-837
[29] Raboin, B. (2011) Corresponding Evolution: International Law and the Emergence of Cyber Warfare – *Journal of the National Association of Administrative Law Judiciary*, Vol. 31, No. 2, 609.
[30] Mele, S. (2014). Legal Considerations on Cyber-Weapons and Their Definitions - *Journal of Law & Cyber* Warfare, Vol. 3, 56-57
[31] Shackelford, S. J. (2014), *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace*, Cambridge University Press, xxi
[32] Mele, S. (2014) *supra nota* 30, p 57.
[33] McGhee, J. (2014) Hack, Attack or Whack; The Politics of Imprecision in Cyber Law – *Journal of Law & Cyber* Warfare, Vol. 4, 16.

conflict.[34] If military forces are used in such situation, the facts of the case and how the event is defined effects crucially on the application of legal rules. Also, liability may come into question in cases where a cyber-attack is operated as an act of war, because in cyber-crimes the damages that occur outside the conflict may be covered by insurances and compensations can be claimed by the insurance company but the insurance rarely covers damages caused by acts of war.[35]

Information warfare systems are already being developed around the world at least in 120 countries for example in Croatia, United Arab Emirates, Vietnam and in Russia.[36] The information warfare system here means the developed networks to launch cyber-attacks via cyberspace to target financial, power, and utility infrastructures. China and North Korea have already developed the game and trained employers for cyber operations to their military gain.[37] Highlighting the current problem is crucial: the international regulations do not commonly define what a cyberspace, cyber-war or cyber-attack is, and it is likely that such definition will not appear in the near future. If these concepts are not defined, then the cyber-weapon cannot be defined either.[38] The missing definition complicates understanding of the cyber-attacks and their implications. Some discussion about the definitions and circumstances in which the cyber-weapon could be used would be beneficial. The use of weapons is usually governed by International Humanitarian Law (IHL), but at present state international regulations only provide the generic concept of weapon.[39]

[34] Mele, S. (2014) *supra nota* 30, p 57.
[35] McGhee, J. (2014) *supra nota* 33, pp 15-16.
[36] 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*, Vol. 32, No. 2, 306
[37] Solce, N. (2008) The Battlefield of Cyberspace: The Inevitable New Military Branch - The Cyber Force, *Albany Law Journal of Science & Technology*, Vol. 18, 297-298
[38] Ochmannova P., Thibault, A. (2013). Respoding to Change – Legal Challenges in the Future Security Environment: Report of the 2013 NATO Legal Conference on 24 -28 June 2013 in Tallinn - *Military Law and Law of War Review*, Vol. 52, 453
[39] Mele, S. (2014) *supra nota* 30, p 55.

2. OVERVIEW OF THE CYBER-ATTACKS

Although the cyber-attacks have never constituted an armed conflict before, cyber-attacks have been already used by governments to provoke the other party in the time of war.[40] Some people may think that cyber-warfare would not be as hideous as a normal armed conflict in domains that have been introduced already at the time of war: land, sea, and air, probably because so far there has not been human victims that resulted straight from the attack. The Internet's interconnectivity is what makes it different from other battlefields and why it is harder to assess in the legal sense.[41] At the moment cyber activities are considered as a support mechanism to assist other mentioned domains, rather than a tool to individually cause violence. However, the world has encountered several cyber-attacks that have drawn international attention and lead to consequences that have included injury, property damage, and death.[42] What is alarming that the devices people use for transportation or medical purposes can already be hacked, that has been shown by enterprising security researchers that have managed to hack insulin pumps, drones in flight and also cars on the road. These vulnerabilities create a new platform for cyber-attacks.[43]

2.1. Cyber-Attack in Estonia 2007

In 2007 Estonian government decided to move the statue of the Bronze Soldier, which was a statue of Russian soldier outside the city center of Tallinn, because the statue was held as a sign of foreign occupation. The decision gave a start to rioting and looting for several days which was resulted from the protests of Russian population living in Tallinn. These riotings were accompanied by cyber attacks.[44]

[40] Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., Spiegel, J. (2012), *supra nota* 10, p 831.
[41] Mavropoulou, E. (2015). *supra nota* 4, pp 25-26.
[42] Encyclopedia of Cyber Warfare (2017). *supra nota* 24, xix
[43] Cate, F. H., Kuner, C., Svantesson, D.J.B., Lynskey, O., Millard, C. (2017) The Rise of Cybersecurity and Its Impact on Data Protection - *International Data Privacy Law*, Vol. 7. No. 2, 73
[44] Buchan, R. (2012), Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? - *Journal of Conflict & Security Law*, Oxford University Press, Vol. 17, No. 2, 218

These cyber attacks in early 2007 were principally repeated denial-of-service attacks (DoS attacks), in which an Internet web page is under so many information requests that it causes the page to run extremely slow or it can even crash the page.[45] These attacks led to a temporary shutdown of a notable number of websites within Estonia, both private and governments held websites were attacked. The attack on the websites was catastrophic because Estonia is densely wired, e-government was freshly instituted in Estonia, and online covered many important government aspects, so it was obvious that Estonians felt confused. The DoS attacks often cause inconvenience for the targeted party, but this one could have caused a loss of lives because attacks also left the emergency phone number unavailable for an hour and that caused that ambulances and firemen were not able to reach the people in need.[46] The attacks resulted in riotings where about 150 people were injured, and one national of Russian Federation died.[47]

The IP addresses of the attack were traced back, and the Estonian Justice Minister found that those led to Kremlin and it was suggested already then, that the officials of Russian government were behind the attack. The Estonian government reached an official conclusion to declare it as an act of terrorism and not as a cyberwar which could have possibly be governed by the rules of armed conflict.[48] Nashi, which is a Kremlin political youth group receiving funding from the Russian State, was assumably being the operator of the attacks.[49] These kinds of organizations that include civilians have the advantage to execute cyber-attacks without people knowing about state's involvement in the action.

2.2. Distributed Denial of Service (DDoS) attacks in Georgia 2008

At the time and a few weeks before with the launch of ground and military air operations between Russia and Georgia in August 2008, the websites of the Georgian government were attacked, and the information provided on these sites were unavailable and replaced with pictures comparing similarities between the Georgian President Mikheil Saakashvili and Adolf Hitler. Those attacks

[45] *Ibid*. p 218.
[46] Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., Spiegel, J. (2012), *supra nota* 10, p 823.
[47] McGuinness, D. (2017) *How a cyber attack transformed Estonia*. Accessible: http://www.bbc.com/news/39655415, 6 December 2017.
[48] Fitz, C. (2017) ALL IS FAIR IN LOVE AND CYBERWAR: INTERNATIONAL LAW AND CYBER-ATTACKS - *Houston Journal of International Law*, Vol. 1, No. 1, 4
[49] Chayes, A. (2015) Rethinking Warfare: The Ambiguity of Cyber Attacks – Harvard National Security Journal, Vol. 6, No. 2, p 477.

and similar attacks on other important Georgian websites occurred at the time of those military operations. However, the Russian government did not confess their involvement and the actors behind the attacks were never decisively identified. Some people see that a new front of war was used by Russia in cyberspace because it would be too much of a coincidence if the attacks occurred inland and in cyberspace at the same time.[50]

This case is considered as one of the first instances where a conventional military conflict was supported by coordinated cyber attacks. Georgia was struggling to find its place after the Soviet Union collapsed, as it being part of the former republics of Soviet Union. When the attacks occurred, Georgia lacked many necessary tools to fight back the attacks: lack of knowledge, skills, and resources concerning Information and Communication Technology that would have secured the systems; policies and institutions. The case led to the point where Georgia reached for assistance abroad. [51]

The attacks were such of a nature that those did not attempt to cause chaos or injury but merely cause inconvenience and uncertainty to the civilian people who were under the bombing. Some considered that this is a political statement where the attackers show they are capable of targeting the critical infrastructures which could cause actual damage.[52]

2.3 Iran

The Iranian government maintains a nuclear plant to enrich uranium, the Iranian government has notified that the uranium is meant only for producing nuclear power, but not all of the international community agrees, because there is always a concern with any nuclear material, that it could be used as a source for mass destruction weapon.[53]

In June 2010 was discovered that a cyber worm called 'Stuxnet' had hit the nuclear facility in Natanz, Iran.[54] The worm succeeded in destroying centrifuges which were critical to Iran's nuclear

[50] Hollis, D. (2011) Cyberwar Case Study: Georgia 2008 - *Small Wars Journal*, Small Wars Foundation, 2
[51] Gamreklidze, E. (2014), Cyber security in developing countries, a digital divide issue - *The Journal of International Communication*. Vol. 20, No. 2, 201-202
[52] Hollis, D. (2011) *supra nota* 50, p 4
[53] Buchan, R. (2012) *supra nota* 44, p 219.
[54] Farwell, J. P., Rohozinski, R. (2011). Stuxnet and the Future of Cyber War, *Survival: Global Politics and Strategy*, Vol. 53, No.1, 23

weapons program.[55] The impacts of the 'Stuxnet' are still unclear since the Iranian government has not revealed the details.[56] What is clear, is that the attacks did not permanently damage the nuclear program and its rise again within a year. Stuxnet was considered as a first international computer attack known to cause actual physical damage.[57]

This case is important because it was proof that the cyber-attack is capable of physical destruction and if the point of view where the cyber-warfare must reach the level of armed attack is taken, then this case offers proof that there is potential for cyberwar to occur in the future. The case can be shown to be an indication of the growing trend to use cyber-attacks for the uncertainty of discovering the true origin of the attack.[58]

[55] Cate, F. H., Kuner, C., Svantesson, D.J.B., Lynskey, O., Millard, C. (2017) *supra nota* 43, p 73.
[56] Buchan, R. (2012) *supra nota* 44, p 219.
[57] Lindsay, J. R. (2013) Stuxnet and the Limits of Cyber Warfare - *Security Studies*, Vol. 22, No. 3, 366
[58] Raboin, B. (2011) *supra nota* 29, pp 623-624.

3. WHAT IS INTERNATIONAL ARMED CONFLICT?

International Humanitarian Law is attempting to protect people who take no part in hostilities and to restrict means and methods of warfare.[59]

The Geneva Convention enjoy the universal recognition, but some other major treaties in the field of humanitarian law lack this kind of asset. Therefore the are certain principles of customary humanitarian law that focus on protecting victims of war. Those principles are to apply everyone even though it would not be a party to the convention and these can be referred as "general" international law, where all parties to the conflict are bound by those laws without any formalities. The customary law also helps when interpreting the treaty law in good faith and taking into consideration all relevant rules of international law. Customary law is fundamental because treaty law is not always able to provide the whole picture of the state of law and the missing customary law would end in the parties not bound by the treaties to act as they wish.[60]

A general definition of international armed conflict that has been adopted by international bodies[61] was introduced in Tadic case by The International Criminal Tribunal for the former Yugoslavia (ICTY) "…we find that an armed conflict exists whenever there is a resort to armed force between States…"[62]

The Geneva Conventions of 1949 Common Article 2 provides an aspect where International Armed Conflicts are those which "…may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them." The conflict can occur when one or more states declare war or use armed force against the territory of another. According to this same provision, the IHL rules may be applicable even if there are no open hostilities and for

[59] *International Humanitarian law: Answers to your questions* (2005)/ ICRC, Accessible: https://shop.icrc.org/droit-international-humanitaire-reponses-a-vos-questions-2598.html (4 December 2017), 4
[60] Henckaerts, J-M., Doswald-Beck, L. (2005). *Customary International Humanitarian Law Volume I: Rules*, Cambridge University Press, xvi-xix
[61] *Ibid.*
[62] IT-94-1-AR72, para. 70

the rules to apply no formalities are required about the recognition of the situation. Such case may occur if one party does not recognize the government of the other party or in the case where the armed forces of states have intervened, but they deny the existence of armed conflict. The applicability of IHL rules depends on the facts of the incident as any other law as well, but for rules to apply the duration of the conflict or the number of the casualties makes no difference.[63]

All the Geneva Conventions apply to any international armed conflict. The Conventions also apply whether the state of war is recognised or not, as well as in the case of an unopposed occupation, those events may not be understood in the regular sense of war and that is why the term 'armed conflict' is rather used. As the most conflicts that have occurred after 1945 have been this sort of armed conflicts, which have not amount to war in the legal sense of the term war, it has been crucial to conventions to apply in all cases of armed conflict. When the armed conflict begins, the armed forces are abided by the law of armed conflict, despite the fact whether the conflict is legal or illegal.[64]

Some scholars view that an armed attack can occur besides kinetic attack also by virtual use of force if the attack inteded to alter the other country's powers by disrupting the country's fundamental infrastructure.[65]

As seen before definitions may be ambiguous, and sometimes it may be hard to detect the differences between the definitions (for example cyber-crime vs. cyber-attack). For the same reason, it was unclear what kind of actions can amount to armed attacks, and now it is even harder to determine what constitutes an armed conflict when individuals are capable of operating a cyber-attack from the place of their choosing. Normally, when international armed conflict is concerned, it can be hard to determine which State has violated the law and started to use force, in cyberspace determinating the violator is even harder.

[63] ICRC, *How is the Term "Armed Conflict" Defined in International Humanitarian Law? (2008)* Accessible: https://www.icrc.org/eng/assets/files/other/opinion-paper-armed-conflict.pdf, 8 November 2017.
[64] Green, L. C. (2000). *The contemporary law of armed conflict*, 2nd Edition, Manchester: Manchester University Press, p 44, p 70.
[65] Simmons, N. (2014) A Brave New World: Applying International Law of War to Cyber-Attacks – *Journal of Law & Cyber warfare*, Vol. 4, 42-43.

3.1 Basic rules of the law of armed conflict and legal challenges of these rules in the context of cyber-attacks

There are some basic rules and widely accepted principles of the law of armed conflict, which apply for cases on land, at sea, and in the air. These rules are the ones which always apply regardless of the legality of the conflict and also in the cases where the operations may be punitive or taken by police forces in the name of the United Nations (UN). These principles are introduced by Geneva Conventions and the Additional Protocol I to the Geneva Conventions.[66]

Applying these principles to cyber-context may be difficult because the law of the war was initially developed to apply wars between states. Compared to conventional war, the scope of the cyber-attack is harder to evaluate as is the identity of the attacker. Assessing the cyber-attacks is important also when determining self-defense. In the cyber-attacks that have occurred so far, states have not been eager to view these attacks as acts of war, and therefore states could not lawfully respond to these attacks in active defense because they were in fear of violating the law of war.[67]

A threat or use of force offending any state's territorial integrity or political independence is unlawful according to UN Charter, also by cyber means.[68] For analyzing how these rules would apply in cyberspace and what problems applying them would cause, let's assume that an armed conflict is now established by cyber means.

3.1.1. Military necessity

Balancing military necessity with humanitarian principles derives from the main purpose of the Hague and the Geneva law, which was introduced before.[69] The rule basically means that the force used in the conflict should not be greater than the necessities of what situation requires or directed towards any other than the legitimate military targets. Legal and moral rules limit the military necessity. Military and political considerations also have their effect on the limitation. When the laws of the war were written, the needs and the realities of armed conflict were taken into consideration. Therefore, such considerations are not permission to break the rules.[70]

[66] 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.
[67] Carr, J. (2012). *supra nota* 2. p 45-46.
[68] Tsagourias, N. (2013) Chapter 2: The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II- The Use of Force – *Yearbook of International Humanitarian* Law, Vol. 15, 20.
[69] Green, L. C. (2000) *supra nota* 64, p 17.
[70] Green, L. C. (2000) *supra nota* 64, p 348.

In the cyber-warfare context, the cyber-attacks which destroy property should also have a reasonable connection to the defeating of the enemy. The destruction that will not gain military advantage or is not in connection with gaining it are violations of the international law.[71] This may be a problem in cyber-attacks regarding the legitimate military targets, so far such cyber-attacks have effected on the civilian population as well and targeting civilians is not considered a way to gain military advantage.

However, cyber-warfare operations have the potential for being effective in armed conflict by its cost-efficiency and by causing less physical destruction. This military gain can be achieved with less risk to military personnel as well.[72]

3.1.2. Humanitarian principles

Some humanitarian principles, derived from the customs, operate at the time of the armed conflict so that wartime does not run alone on demands of military necessity.[73] The principles of ethics and humanity should be taken into consideration as well. Article 3 of the Four Geneva Conventions offers some basic and minimum conditions, which can be considered so fundamental that those have hardened into being customary law. The principles that Article 3 provides should be applied to people who are no longer taking part in hostilities with the principle of non-discrimination, where persons are not to be treated differently based on their race, color, religion or faith, sex, birth, or any other criteria equivalent. The Article prohibits the violation of life, health, or physical or mental well-being of a person by murdering, torturing, executing corporal punishment or executing mutilation. Also, humiliating and degrading treatment is prohibited.[74] The Article 3 may be hard to fulfill in cyber-warfare, because it may be demanding to distinguish who is taking direct part in hostilities. If cyber-attack is targeted for example towards the nuclear facility, the humanitarian principles are more laborious to fulfill since the impacts it may have on civilian health can be severe.

3.1.3. Distinction

[71] Dinstein, Y. (2016). *The Conduct of Hostilities under the Law of International Armed Conflict*, 3rd Edition, Cambridge: Cambridge University Press, 11.
[72] Schaap, A. (2009) Cyber Warfare Operations: Development and Use under International Law -*Air Force Law Review*, Vol. 64, No. 1, 158.
[73] Dinstein, Y. (2016). *supra nota* 71, p 9.
[74] Green, L. C. (2000) *supra nota* 64. p 348.

The distinction should be made between civilian and military personnel and objects. Acts of armed conflict must be limited only towards military objects and objectives, which by their nature, location, purpose or use make an effective contribution to military action and in that current moment offers a military advantage. Therefore the military personnel must distinguish themselves from the civil population and also distinctive emblem signs must be marked on places which are considered as a civilian in character or are protected as cultural property. This principle offers more protection for civilians as they are exempt from being the object of attack. However, the law of the armed conflict does not provide a provision for a violation if a civilian suffered incidental injury when the attack was made towards a legitimate military objective. Such attacks failing to fulfill the principle of distinction are forbidden and indiscriminate.[75]

If cyberspace is used as a battlefield, the obstacle may come across in principle of distinction. Obviously, the civilian and military infrastructure is connected closely because the cyberspace as a use of an object can serve both civilian and military purposes.[76] Modern society is depended on the critical infrastructures, and some of these are operated by private actors like electricity and telecommunication companies and states do not have complete control over these actors even if the companies were under the influence of the state.[77] Therefore the classification of objects may be problematic. Also distinguishing between the military personnel and civilians can cause problems when taking into account the number of civilians participating in cyber hostilities and the increasing civilization of the military.[78]

Determining who is participating directly in hostilities is difficult already in conventional situations of conflicts, but adding the equation of cyber is complicating the matter even more. Who can be considered to take a direct part in cyber hostilities? The cyber hostilities offer many unclear situations in that sense, for example, is the person who executed the code taking a direct part in hostilities? How about the person who wrote the code but did not execute it? Or the person who has given these orders?[79] These notions are linked to the rule of distinction since civilians cannot

[75] Green, L. C. (2000) *supra nota* 64, p 350.
[76] Mavropoulou, E. (2015). *supra nota* 4, p 24.
[77] Kessler, O., Werner, W. (2013) Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare – *Leiden Journal of International Law,* Vol. 26, 798.
[78] Mavropoulou, E. (2015). *supra nota* 4, p 26.
[79] Crawford, E. (2013) Virtual Backgrounds: Direct Participation in Cyber Warfare – *I/S: A Journal of Law and Policy for the Information Society*, Vol. 9, No. 1, 2.

be targeted unless they have directly taken part in hostilities. The direct participation is an exemption from the civilian immunity.[80]

3.1.4. Proportionality

The principle of proportionality becomes important in a situation where the legitimacy of the target has to be decided. This principle can be found in the customary law of armed conflict, and it must be respected because although being customary law, it can be measured and held excessive in a subsequent war crimes trial. Under the principle, the actions must be limited to what is necessary to achieve the aim that is pursued. In military actions, the interests of specific action are compared against the consequences of that action, for example, the effect it has on civilians or civilian objects. When deciding whether the principle has been respected, there must have been an acceptable relation between the effects on legitimate targets and the effects on undesirable collateral.[81] Additional Protocol I to the Geneva Conventions[82] mentions that the effect upon civilians shall not be 'excessive,' but the protocol does not offer a definition what can be considered as 'excessive,' therefore reasonable military assessments and expectations have to be considered when deciding on the action.[83]

In the context of the law of armed conflict, attacks are "… acts which result in (or are intended to result in) the direct or reasonably foreseeable causation of physical damage, destruction, injury or death…".[84] Military operations that do not have reach this threshold of attack is not governed by proportionality, for example, cyber intelligence. If Estonian cyber-attack in 2007 was a military operation, it could have been considered as a case that might not be governed by proportionality. Even if the civilians were affected, the cyber-attacks caused mere inconvenience and the physical damage it caused, was probably not foreseeable to the attackers. Even if serious inconvenience occurred, it is still not likely to qualify as attacks in the context of the law of armed conflict. If in such operations important data would be destroyed or lost, it is still probable that those operations would not fall under the category of attacks because data is not considered as a physical property itself. There are claims that if the operation to destroy the data is severe enough, it would be considered as an act of violence, but at the moment there is no law governing that matter.

[80] *Ibid.* p 3.
[81] Green, L. C. (2000), *supra nota* 64, p 350.
[82] 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 51 (5)(b)
[83] Green, L. C. (2000), *supra nota* 64, p 351.
[84] Research Handbook on International Law and Cyberspace. (2015). *supra nota* 3, p 374.

Proportionality could be relevant if the destroyed data could likely have physical effects, for example, medical records in the hospital were destroyed when the attack was made towards a military target and the civilians suffering from it were a side effect of the attack. If this were the case, the collateral damage would be measured against the military advantage to determine whether the attack was proportional.[85]

Proportionality is not relevant even if it causes damage or death to the military objectives or personnel, as long as the attack is not likely to cause such effects on the civilian population. For example in an Israeli attack on Syrian air defense system in 2007, the proportionality would not have been relevant since such systems are usually well protected from civilians, and therefore the collateral damage is not considered. Similarly, if the attack was operated towards a military target, but the potential collateral damage was neglected when it was foreseen, the question of proportionality rises. Stuxnet case is a good example of such, although not used in the context of armed conflict, as the virus was intended to affect only the Iranian nuclear programme but affected civilian computers as well.[86]

If such cyber-attacks were carried out beside the traditional kinetic attacks, the principle would apply to the whole attack and not to a single act alone. When a mere cyber-attack is concerned, the proportionality can be applied to the extent where a military object was targeted, and it was likely to result in foreseeable civilian physical effects. Regarding proportionality, the conduct of such acts is lawful to the extent where the rules relating to the conduct are obeyed.[87]

[85] *Ibid.* p 376.
[86] *Ibid.*
[87] *Ibid.* p 377.

4. APPLICABILITY OF HUMANITARIAN LAW TO CYBER-WARFARE

When current legal norms both customary and treaty-based norms emerged, the arrival of cyber technologies could not be predicted at the time. The development of technologies is a reason why the agreed understanding to legal regime governing the cyber practice may be outdated quickly. It has been common that legal treaties are a one step behind from the development, especially in the field of war. IHL Treaties have usually been one war behind, and the horrors have already occurred before those actions are prohibited, for example, The Convention on the Treatment of Prisoners of War from 1929 resulted from the World War I where mass killings of prisoners occurred.[88]

According to the law, the law of armed conflict can only apply if the conditions of the situation are such of a nature that existence of armed conflict is reached.[89] The cyber-warfare definition must then match the situation where the status of armed conflict can be reached as introduced in chapter 3.1. One consideration is the improbability of stand-alone cyber-attack at the time of the armed conflict. Some scholars see that if such circumstances have arisen, it would not be logical only to use one weapon to conduct hostilities because it would be more efficient to use all means of warfare to defeat the opponent. This point of view originates from the thought that cyber vulnerabilities are exaggerated, and cyber means alone could not provide permanent destruction or effective damage. The most likely scenario would be that cyber actions are operated together with traditional kinetic attacks, and therefore the law of armed conflict may be applied for all attacks operated by any party to the armed conflict. In such case, parties to such a conflict are equally obligated to follow the rules and principles of International Humanitarian Law, despite the means and methods of warfare.[90]

[88] Ayalew, Y.E. (2015), *supra nota* 1, p 210.
[89] Research Handbook on International Law and Cyberspace. (2015). *supra nota* 3, p 367.
[90] *Ibid.*

4.1 Circumstances when humanitarian law would or would not apply to cyber-warfare

As stated before, the law of armed conflict can only apply if there is, in fact, an armed conflict. However, it can be unclear, whether all the rules of IHL apply in the inconsequential incidents where armed forces of two States encounter. As a rule, any armed clash between two or more States, irrespective of the extent or volume of the incident, creates the existence of international armed conflict and therefore the rules of IHL apply to all the parties. The actions that result in below the threshold of armed conflict, are not legally governed by IHL, but parties may decide to apply some rules of IHL as a policy matter.[91]

The geographical scope can become a matter of importance because, in international armed conflict, IHL rules are applicable to the territory of all parties to the conflict and also the territory of the third state can be used if it has failed in its duties as a neutral state and military operations are conducted from that state.[92] However, the cyberspace offers the anonymity, and it can be problematic to figure out the real operator of the act as have been already noticed in cyber-attack in Estonia 2007 and other publicly known cyber-attacks. Therefore the geographical scope can be harder to apply if the operator of the attack cannot be traced. From the international perspective, tracing back to a state may cause difficulties since nonstate hackers are more common in engaging in cyber-attacks.[93]

Surveillance, espionage, another kind of information operations and sabotage can be operated by cyber means, but in a factual or legal sense, those actions do not fall under the threshold of armed conflict. For example, Stuxnet was considered as sabotage, where the nuclear centrifuge systems were targeted, but the actions did not meet the criteria for an armed attack.[94]

At the present circumstances, the IHL rules would apply to cyber means and methods of warfare most likely when the cyber technologies would be used together with kinetic armed force. There are already two cases known to occur where this kind of combined attack is used. One was the Georgia and Russia case in 2008, which was mentioned in chapter 2.2. Cyber operations that the

[91] *Ibid.* p 368.
[92] *Ibid.* p 368.
[93] Carr, J., (2012). *supra nota* 2, p 3.
[94] Research Handbook on International Law and Cyberspace. (2015). *supra nota* 3, p 370.

Russian hackers conducted did not constitute an armed attack, but if cyber actions had supported the military operations by affecting the weapons and military communications systems, it probably would have been part of an armed attack at large.[95] Other cyber-attack that presumably could have been a part of armed conflict occurred in September 2007 when the Israeli airstrike hit the Syrian nuclear reactor. Apparently, along with the airstrike, cyber technologies were used to neutralize Syrian air defense systems temporarily for the time that airstrike managed to destroy the facilities. Combining kinetic and cyber-attacks create effective means and methods of warfare, which might give a military leverage for the party using such means. Some countries have already started to integrate the cyber technologies into military operations, and it is likely that it will be the future trend.[96]

[95] Gill, T.D., Ducheine, P.A.L. (2013). Anticipatory Self-Defence in the Cyber Context – *International Law Studies (Naval War Collage)*, Vol. 89, 461
[96] *Ibid.* p 462.

5. ADDRESSING CYBER WARFARE IN LEGAL CONTEXT

The cyber-warfare concept raises more questions than it offers solutions. Overall states have started to pay attention to problems deriving from cyberspace, but for now there has not been a solution regarding the cyber-warfare. The Convention on Cybercrime that was introduced does not apply to cyber-warfare.[97] In recent years groups of experts, in conflict and security law, have tried to offer solutions how the international law should deal with these irregular forms of warfare. The task of these experts as a part of committees in conflict and security law is not actually make new laws but rather introduce the law that already exists that could apply in those special circumstances. The aim of these committees is to produce legal content in the context of cyber-warfare within existing legal frames so that the uncertainty around the matter could be absorbed. International legal experts are important when international law is facing some new challenges, but using these experts can also harden these uncertainties or even create new ones.[98]

5.1 Offered legal solutions

Academics have proposed that the legal analogies could possibly cover the legality of the cyber-warfare. It has been suggested that adequate models which could govern the matter are introduced in the Nuclear Nonproliferation Treaty by Charter of the UN or in Antarctic Treaty System. These analogies would provide certain principles to govern the potential cyber-warfare. It is however argued, that these models would not work in reality because the cyber warfare can be used as a mean to force states with the greater military capacity to take part in asymmetric warfare and also because critical infrastructure can be attacked by cyber means to prevent the counter state's military action.[99]

Also, existing international analogies governing outer space, air, land, and sea have been compared to cyber warfare, but it has been decided that those would not apply to cyber-warfare since

[97] Raboin, B. (2011) *supra nota* 29, p 633.
[98] Kessler, O., Werner, W. (2013) *supra nota* 77, pp 793-795.
[99] Preciado, M. (2012) If You Wish Cyber Peace, Prepare for Cyber War: The Need for the Federal Government to Protect Critical Infrastructure from Cyber Warfare – *Journal of Law & Cyber Warfare*, Vol. 1, No. 1, 102.

cyberspace in its nature is not limited to physical world only as it is in other domains. Outer space is regarded the closest physical analogy to cyberspace, but the physical factor is not a nature of cyberspace. The use of outer space is limited by international law. The limitation concerns military purposes, where mass destruction weapons are placed in celestial orbit. These laws are enforceable because states have means and methods to monitor the compliance of the rules on limitation. Consequently, it is held that international means are not sufficient to properly regulate the cyber-warfare because the nature of the domain is not taken into account.[100]

5.2 Tallinn Manual

A group of international experts (international law scholars and practitioners) were gathered by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in 2009 to Tallinn to examine the international law that might govern the cyber warfare. Also, three organizations took part in the process: the International Committee of the Red Cross, NATO's Allied Command Transformation, and the United States Cyber Command. In the process, the Tallinn Manual on the International Law Applicable to Cyber Warfare was born.[101]

The Tallinn Manual is an academic analysis on how existing international law applies to cyberspace actions. To emphasize the Tallinn Manual is not legally binding or official document, but rather a resource tool when legal advisers are dealing with complex legal issues around cyber operations.[102] The original Tallinn Manual from 2013 focused on the most severe cyber operations where jus ad bellum and jus in bello could possibly be applied to the war in cyberspace.[103] Tallinn Manual also provides Rule 11, in which cyber operation reaches the level of use of force if the scale and effects are equal to non-cyber operation reaching the threshold of use of force. The Rule does not provide an explanation of what is considered the scale and effects in non-cyber operation to reach the threshold of use of force, so that is left under interpretation.[104] However, in the commentery of the rules is noted that actions, which cause the injury or the death of person are

[100] Raboin, B. (2011) *supra nota* 29, pp 625-626.
[101] Heintschel von Heinegg, W. (2014) Chapter 1 The Tallinn Manual and International Cyber Security Law - *Yearbook of International Humanitarian Law*, Vol. 15, 3-4
[102] Eichensehr, K. (2014) Review of *The Tallinn Manual on the International Law Applicable to Cyber Warfare* (Eds. Michael N. Schmitt, Recent Books on International Law, 585
[103] Boer, L. (2013) 'Restating the Law "As It Is"': On the Tallinn Manual and the Use of Force in Cyberspace - *Amsterdam Law Forum*, Vol. 5, No. 3, 5
[104] Roscini, M. (2014) *Cyber Operations and the Use of Force in International Law*, Oxford: Oxford University Press, p 45.

considered to be use of force, as well as the damage or destruction caused to objects. If cyber-attacks have comparable consequences to those, it is likely to be regarded as a use of force.[105]

The original Manual was criticized for not systemically covering legal problems of cybersecurity outside of the context of armed conflict and this was a problem as the biggest cyber operations so far have been outside of the scope of armed conflict, although it has not been excluded that such incident might arise in future.[106] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations was published in February 2017, and it is updated and expanded edition of the 2013 Tallinn Manual. Tallinn Manual 2.0 offers a legal analysis of more common cyber incidents that states encounter daily and which do not reach the level of armed conflict. The new version takes into account the legal regimes that may cover the cyber operations in the peacetime and also in the time of war. The analysis includes general international law principles and also specialized legal regimes of international law within the context of cyber operations.[107]

[105] Haataja, S. (2017) *The 2007 cyber attacks against Estonia and international law on the use of force: an informational approach* – Law, Innovation and Technology, Vol. 9, No. 2, 166
[106] Fleck, D. (2013) Searching for International Rules Applicable to Cyber Warfare – A Critical First Assessment of the New Tallinn Manual - *Journal of Conflict & Security Law*, Vol. 18 No. 2, Oxford University Press, 331-332
[107] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. CCDCOE, Accessible: https://ccdcoe.org/sites/default/files/documents/CCDCOE_Tallinn_Manual_Onepager_web.pdf, 25 October 2017.

CONCLUSIONS

The ideal case of IHL is when rules of IHL are followed during armed conflict. Following the rules is important for maintaining some level of protection for all people, especially for people not taking part in hostilities such as civilians, hors de combat, medical personnel and employees of humanitarian organizations. Compliance with IHL rules shows good governance from the state when means and methods of warfare are followed according to law, and this is a vital factor for the re-establishment and maintenance of peace. Compliance also sets a good example, that could be in the case of rebel groups of non-state actors which often lack guidance and incentive to follow such rules. However, if the party follows the rules, it discourages belligerents to act unlawfully in the case where the other party to the conflict is not maintaining the same laws. In other words, the military discipline is easier to maintain when combatants focus on the legitimate enemy targets and disabling enemy's resources. The quicker the enemy is incapacitated, the peace can be regained also faster. In peacetime, human rights can be protected even better.[108]

In cyber-warfare, certain aspects of international law are hard to fulfill. Belligerents have rules they must follow to be considered as a lawful combatant such as, carry arms openly, wear either a uniform or some other recognizable sign, be part of armed forces of a state or belong to the organization which has a clear hierarchy and the members of that group are obeying the law of armed conflict. If these rules are not fulfilled, then the belligerent is probably not considered as a lawful combatant, and it loses its protection under the law of armed conflict.[109] In cyber-warfare, it may be challenging to determine who is a combatant. The requirements of lawful combatant might not be fulfilled in many cases because the combatant who launches the attacks is often invisible so the combatant cannot be recognized from a distance. If in cyber-warfare a lawful combatant does not exist, then basically the law of the armed conflict does not protect such person. When civilians are concerned, they must keep clear of the conflict if they want to be protected by the law of armed conflict. So to say civilians are not allowed to operate cyber-attacks as a part of

[108] Changeta, T. (2016) Measuring Autonomous Weapon Systems against International Humanitarian Rules. – *Journal of Law and Cyber Warfare,* Vol. 5, No. 1, 75
[109] Springer, P. (2015) *Cyber warfare : a reference handbook.* California: ABC-CLIO, LLC, p 52.

military actions and then return to normal their normal life because then these persons would be taking a direct part in the hostilities.[110]

To conclude the earlier and coming to the hypothesis, the law of armed conflict may apply if the cyber-attack reaches the threshold of armed conflict, so the hypothesis is indicated to be true based on the writings of legal scholars. Of course, most of the cyber-attacks do not reach the threshold of armed attack or use of force, therefore the IHL framework does not fit the purpose of such attacks. The attacks that do not reach the threshold are criminal acts, but should probably be governed by some new law, because the present legislation of IHL is not applicable to attacks that do not reach that threshold, regardless how the cyber-warfare is defined.

States should bear in mind when developing new weapons and designing methods of warfare, that they comply with IHL rules, even if it would cause short-term disadvantages. The interest of own state should not be the only thing to consider, but also the people affected by the chose of weapons in the area of conflict.[111] Even if the law of armed attack would cover the cyber-attack, it is still unsettled whether the law of armed attack would apply if a real-life situation occurred.[112]

At present state, the international law dealing with cyber-warfare has three fundamental legal issues it fails to respond: attribution, jurisdiction and what is regarded as a use of force. These key issues were introduced earlier in this thesis. In theory, international law is applicable to any military strategy, but the reality of the application is more complicated than that.[113] So it remains unsettled, whether rules existing at the moment would be enough to respond the new challenges that cyber activities are to bring in the future. Regarding the new challenges, it raises questions if the existing laws should be interpreted more evolutionarily or if adopting new rules would be the solution for these questions.[114]

A good start point for new international regulation would be universally recognized definitions for crucial cyber concepts and understanding the main legal issues the cyber warfare raises. New and effective legal solutions can be only formulated if the flaws of current law are identified.[115] As a

[110] *Ibid.* p 53.
[111] *Ibid*. p 76.
[112] Gervais, M. (2012) Cyber Attacks and the Laws of War – Journal of Law & Cyber Warfare, Vol. 1, No. 8, 10.
[113] Raboin, B. (2011) *supra nota* 29, p 640
[114] Bannelier-Christakis, K. (2016) Marco Roscini, Cyber Operations and the Use of Force in International Law – *Journal of Conflict and Security Law*, Vol. 21, No. 2, 367.
[115] Raboin, B. (2011) *supra nota* 29, p 640.

result from this research, it is noticeble that more attention need to paid to these issues mentioned in the thesis. When new means and methods of warfare are developed, it requires thorough analysis of how legal framework applies to military actions operated by those means. Even if cyber-warfare has not yet occurred, serious cyber-attacks have. Therefore governing the matter is important for countries that encounter cyber-attacks, so these countries would be aware of the acts they can legally take in self-defense.

LIST OF REFERENCES

Scientific books:

1. Carr, J. (2012). *Inside Cyber Warfare*, 2nd Edition, Sebastopol: O'Reilly Media, Inc.

2. *Encyclopedia of Cyber Warfare* (2017). / Eds. Paul J. Springer, ABC-CLIO

3. Green, L. (2000). *The contemporary law of armed conflict*, 2nd Edition, Manchester: Manchester University Press

4. Henckaerts, J-M., Doswald-Beck, L. (2005). *Customary International Humanitarian Law Volume I: Rules*, Cambridge University Press

5. *International Humanitarian law: Answers to your questions* (2005)/ ICRC. Accessible: https://shop.icrc.org/droit-international-humanitaire-reponses-a-vos-questions-2598.html (4 December 2017)

6. *Research Handbook on International Law and Cyberspace.* (2015). / Eds. N. Tsagourias, R. Buchan. Cheltenham: Edward Elger Publishing Limited

7. Roscini, M. (2014) *Cyber Operations and the Use of Force in International Law*, Oxford: Oxford University Press, p 45.

8. Shackelford, S. J. (2014). *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace*, Cambridge University Press

9. *The Ethics of Information Warfare* (2014). /Eds. L. Floridi, M. Taddeo. Law, Governance and Technology Series, Springer International Publishing

Scientific articles:

10. Ayalew, Y.E. (2015) Cyber Warfare: A New Hullaballoo under International Humanitarian Law – *Beijing Law Review*, Vol. 6, No. 4, 209-210

11. Bannelier-Christakis, K. (2016) Marco Roscini, Cyber Operations and the Use of Force in International Law – *Journal of Conflict and Security Law*, Vol. 21, No. 2, 367.

12. Boer, L. (2013) 'Restating the Law "As It Is"': On the Tallinn Manual and the Use of Force in Cyberspace - *Amsterdam Law Forum*, Vol. 5, No. 3, 5

13. Buchan, R. (2012) Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? - *Journal of Conflict & Security Law*, Oxford University Press, Vol. 17, No. 2, 218-219

14. Cate, F. H., Kuner, C., Svantesson, D.J.B., Lynskey, O., Millard, C. (2017) The Rise of Cybersecurity and Its Impact on Data Protection - *International Data Privacy Law*, Vol. 7. No. 2, 73

15. Changeta, T. (2016)., Measuring Autonomous Weapon Systems against International Humanitarian Rules. – *Journal of Law and Cyber Warfare,* Vol. 5, No. 1, 75

16. Clough, J. (2012), The Council of Europe Convention on Cybercrime: Defining 'Crime' in a digital world - *Criminal Law Forum*, No. 23, 363

17. Crawford, E. (2013) Virtual Backgrounds: Direct Participation in Cyber Warfare – *I/S: A Journal of Law and Policy for the Information Society*, Vol. 9, No. 1, 2-3

18. Farwell, J. P., Rohozinski, R. (2011). Stuxnet and the Future of Cyber War, *Survival: Global Politics and Strategy*, Vol. 53, No.1, 23

19. Fitz, C. (2017), ALL IS FAIR IN LOVE AND CYBERWAR: INTERNATIONAL LAW AND CYBER-ATTACKS - *Houston Journal of International Law,* Vol. 1, No. 1, 4

20. Fleck, D. (2013) Searching for International Rules Applicable to Cyber Warfare – A Critical First Assessment of the New Tallinn Manual - *Journal of Conflict & Security Law*, Vol. 18 No. 2, Oxford University Press, 331-332

21. Gamreklidze, E. (2014), Cyber security in developing countries, a digital divide issue - *The Journal of International Communication*. Vol. 20, No. 2, 201-202

22. Gervais, M. (2012) Cyber Attacks and the Laws of War – *Journal of Law & Cyber Warfare*, Vol. 1, No. 8, 10.

23. Gill, T.D., Ducheine, P.A.L. (2013). Anticipatory Self-Defence in the Cyber Context – *International Law Studies (Naval War Collage)*, Vol. 89, 461-462.

24. Haataja, S. (2017) *The 2007 cyber attacks against Estonia and international law on the use of force: an informational approach* – Law, Innovation and Technology, Vol. 9, No. 2, 166

25. Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., Spiegel, J. (2012), The law of Cyber-Attack – *California Law Review*, Vol. 100, No. 817-837.

26. Heintschel von Heinegg, W. (2014) Chapter 1 The Tallinn Manual and International Cyber Security Law - Yearbook of International Humanitarian Law, Vol. 15, 3-4

27. Hollis, D. (2011) Cyberwar Case Study: Georgia 2008 - *Small Wars Journal*, Small Wars Foundation, 2-4.

28. Kessler, O., Werner, W. (2013) Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare – *Leiden Journal of International Law*, Vol. 26, pp 793-798.

29. Lindsay, J. R. (2013) Stuxnet and the Limits of Cyber Warfare - *Security Studies*, Vol. 22, No. 3, 366.

30. Lunn, B. (2014) Strengthened Director Duties of Care for Cybersecurity Oversight: Evolving Expectations of Existing Legal Doctrine – *Journal of Law & Cyber Warfare*, Vol. 4, 113.

31. Mavropoulou, E. (2015). Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber-Attacks - *Journal of Law & Cyber Warfare*, Vol. 4, No. 2, 24-26.

32. McGhee, J. (2014) Hack, Attack or Whack; The Politics of Imprecision in Cyber Law – *Journal of Law & Cyber* Warfare, Vol. 4, 15-16.

33. Mele, S. (2014). Legal Considerations on Cyber-Weapons and Their Definitions - *Journal of Law & Cyber Warfare*, Vol. 3, 56-57

34. Nguven, R. (2013) Navigating Jus Ad Bellum in the Age of Cyber Warfare - *California Law Review*, Vol.101, 1087-1091.

35. Ochmannova P., Thibault, A. (2013). Respoding to Change – Legal Challenges in the Future Security Environment: Report of the 2013 NATO Legal Conference on 24 -28 June 2013 in Tallinn - *Military Law and Law of War Review*, Vol. 52, 453

36. Preciado, M. (2012) If You Wish Cyber Peace, Prepare for Cyber War: The Need for the Federal Government to Protect Critical Infrastructure from Cyber Warfare – *Journal of Law & Cyber Warfare*, Vol. 1, No. 1, 102.

37. Raboin, B. (2011) Corresponding Evolution: International Law and the Emergence of Cyber Warfare – *Journal of the National Association of Administrative Law Judiciary*, Vol. 31, No. 2, 609-640.

38. Schaap, A. (2009) Cyber Warfare Operations: Development and Use under International Law -*Air Force Law Review*, Vol. 64, No. 1, 158.

39. Simmons, N. (2014) A Brave New World: Applying International Law of War to Cyber-Attacks – *Journal of Law & Cyber warfare*, Vol. 4, 42-43.

40. Solce, N. (2008) The Battlefield of Cyberspace: The Inevitable New Military Branch - The Cyber Force, *Albany Law Journal of Science & Technology*, Vol. 18, 297-298

41. 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*, Vol. 32, No. 2, 306

42. Tsagourias, N. (2013) Chapter 2: The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II- The Use of Force – *Yearbook of International Humanitarian Law*, Vol. 15, 20.

Websites and other material:

43. Council of Europe, *Convention on Cybercrime*, No. 185 of 23 November 2011, European Treaty Series, 08.11.2017

44. Cybercrime Convention Committee (2017), *T-CY Guidance Notes*, Accessible: https://rm.coe.int/16806f9471, 8 November 2017.

45. ICRC (2008), *How is the Term "Armed Conflict" Defined in International Humanitarian Law?*, Accessible: https://www.icrc.org/eng/assets/files/other/opinion-paper-armed-conflict.pdf, 8 November 2017.

46. INTERPOL, The threats. Accessible: https://www.interpol.int/Crime-areas/Cybercrime/The-threats, 8 November 2017.

47. McGuinness, D. (2017) *How a cyber attack transformed Estonia*. Accessible: http://www.bbc.com/news/39655415, 6 December 2017

48. 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.

49. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. CCDCOE, Accessible: https://ccdcoe.org/sites/default/files/documents/CCDCOE_Tallinn_Manual_Onepager_web.pdf, 25 October 2017.

Cases:

50. IT-94-1-AR72