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

Eetu Tulilahti

# APPLICABILITY OF JUS IN BELLO TO CYBER WARFARE

Bachelor's Thesis
Programme HAJB, Specialisation in European Union and International Law

Supervisor: Evhen Tsybulenko

Tallinn 2020

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 presented for grading.
The document length is 10,126 words from the Introduction to the end of Conclusions.

Eetu Tulilahti ……
(signature, date)
Student code: 177700HAJB
Student e-mail address: etulilahti@gmail.com

Supervisor: Evhen Tsybulenko, PhD:
The paper conforms to requirements in force

……
(signature, date)

Co-supervisor:
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

This thesis deals with the concepts of cyber warfare and cyber-attack, which are relatively new concepts of military action generated by technological development. The thesis provides an examination into means, methods and concepts of cyber warfare, major cyber incidents and assesses the position of cyber aspects in the light of international law with the aim of addressing cyber domain into the legal field. Under the magnifier is also the ethics of cyber warfare, which is closely related to the law of armed conflict. The outcome is an approach that is completely theoretical based on scientific texts from authors and experts around the world. Applicability of *jus in* bello, i.e. the law of armed conflict to cyber warfare is ambiguous and the issue has formed ethical and legal complexities. The research of this thesis demonstrates how the current international regulation is not up-to-date with contemporary means and methods of cyber warfare. It reviews the situation from the perspective of a legislator and proposes a new legal framework to be adopted to tackle the problem.



Keywords: cyber warfare, cyber attack, law of armed conflict, jus in bello, ihl

# LIST OF ABBREVIATIONS

| | |
|---|---|
| AP | Protocol Additional to the Geneva Conventions of 12 August 1949 |
| ATS | Antarctic Treaty System |
| CCDCOE | NATO Cooperative Cyber Defence Center of Excellence |
| CCW | UN Convention on Certain Conventional Weapons 1980 |
| DDoS | Distributed Denial of Service attack |
| ICJ | International Court of Justice |
| ICTY | International Criminal Tribunal for the former Yugoslavia |
| IHL | International Humanitarian Law |
| LOAC | Law of Armed Conflict |
| NATO | North Atlantic Treaty Organization |
| SCADA system | Supervisory Control and Data Acquisition system of a computer |
| Stuxnet | Computer 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 |
| WannaCry | Ransomware cryptoworm discovered in 2017 |

# INTRODUCTION

The use of information as a means of warfare is a centuries-old technique. The Internet, however, has provided more means for humans to continue their gruesome acts. Criminal, espionage, and warfare activities have a new battleground in the cyber domain due to technological development. Cyberspace is an entirely abstract domain, which makes it special and more difficult to regulate compared to physical domains. It is an international network that does not have national borders and thus has crossover effects affecting the interrelation of domestic and and international law. As more devices are connected and societies quickly become highly dependent upon cyber networks, the possibilities for causing harm grow in proportion.[1]

*Jus in bello*, as known as the law of armed conflict, regulates the use of force during armed conflict. Applying the customary rules and principles of *jus in bello* into the cyber domain raises more questions than answers. While contemporary weaponry is developing at a rate which has never been seen before, it is becoming constantly more difficult to apply the rules of *jus in bello* to cyber weapons to prohibit their use under international humanitarian law. International humanitarian law (IHL) is a set of purely humanitarian rules which regulate the conduct of war under *jus in bello* while seeking to limit the suffering caused by war.

*Jus in bello* will only apply to cyber warfare if the attack occurs during or triggers an armed conflict. It is questionable whether a cyber-attack can constitute an 'armed attack' for *jus in bello* to apply, and the attacks raise several issues regarding the interpretation of its applicability.[2] For example, only cyber-attacks that fulfill the criteria of armed attack as defined in the rules of IHL are subject to the prohibition against direct attacks at civilian objects and indiscriminate and disproportionate attacks.[3] In the light of rules of IHL, this leaves many potentially dangerous 'unqualified' cyber-attacks in a legal vacuum. Besides, the notion of cyber-attack has not been

[1] Springer, P. J. (Eds.) (2017). *Encyclopedia of Cyber Warfare*, ABC-CLIO, Preface.
[2] Krawczyk, L. (2019, Aug 09). How does cyber warfare fit in the framework of International Humanitarian Law? [Blog post] Leiden Law Blog. Retrieved from https://leidenlawblog.nl/articles/cyber-warfare-the-definition-challenge, 12 February 2020.
[3] *Cyber warfare: IHL provides an additional layer of protection (2019, Sept 10).* ICRC. Retrieved from https://www.icrc.org/en/document/cyber-warfare-ihl-provides-additional-layer-protection, 12 March 2020.

fully settled under international law.[4] There is a need for more adherent rules which encompass non-physical armed attacks to reflect the changing weaponry of the contemporary armed conflicts.[5]

The thesis will provide an examination into theories of cyber warfare, explain different cyber concepts, and examine if and how *jus in bello* applies to cyberspace and what are the focal points and main problems of its applicability. It will provide a comprehensive overview of the rules and principles of *jus in bello* and their applicability to cyber warfare. The research aims to examine that on what grounds the law of armed conflict applies to cyber-attacks, what are the main problems in its applicability, and how those problems could be solved by implementing new international regulation.

The main hypothesis of the thesis is that a cyber-attack can constitute an armed attack where the attack is a virtual or kinetic use of force of one state against another with the intent of altering its sovereignty or strategic capacity by disrupting its critical infrastructure. The research questions of the thesis are that what are the factors causing the obscure application of *jus in bello* to cyber warfare and what measures would facilitate cyber-attacks to reach the definition of an armed attack more properly.

The thesis uses qualitative research methods and the author analyses academic sources written by international and national experts around the world. The subject is appealing and there already exists conversation and debate about it, but still no further actions have been taken to fix the problem by new legislation or amendments to existing legislation.

The thesis' structure starts with introductory chapter to key cyber concepts and ethics of cyber warfare, following a review of most influential cyber-attacks. The third chapter presents the *jus in bello,* better known as international humanitarian law or law of armed conflict, its fundamental rules and principles, and analyses its applicability to cyber warfare. The final chapter reviews the situation in the form of current proposals and suggests a new theoretical solution to the problem.

[4] *Ibid.*
[5] Krawczyk, L. (2019, Aug 09) *supra nota* 1.

# 1. MEANS AND METHODS OF CYBER WARFARE

In a commonly perceived war, warfare is conducted on land, by sea, in the air, and across space. In contemporary world warfare is also conducted in a fifth battleground: cyberspace. Warfare which is conducted in cyberspace is called cyber warfare. Cyberspace is a special communication network with a distinct status, which is not dependent on any concrete state, legal system, or jurisdiction. Therefore, it is difficult to regulate. Cyberspace is used to store, exchange, and modify data via networked systems.[6] It is a virtual computer world connected to digital technology.

The definition of cyber warfare is not fully settled within the disciplines nor under international humanitarian law. The absence of a mutually shared definition has made the job difficult for analysts to develop coordinated policy recommendations.[7] Understanding the ensemble, a line must be drawn between other interrelated concepts such as cyber espionage or cybercrime. The concept of cyber warfare is different from cybercrime, since cybercrime is generally considered as financially motivated and cyber warfare politically motivated.[8] Cybercrime is a computer-oriented crime which is committed in cyberspace by a computer. If a non-state actor commits a cybercrime for a political or national reason, then it can be considered as cyber-attack. Cyber espionage, on the other hand, is a form of cyber-attack by which a nation steals classified or sensitive data from another nation. It is not prohibited under international humanitarian law. The term cyber warfare is also distinct from the term cyberwar. Cyber warfare does not imply scale, protraction, or violence which are generally understood in the sense of 'war'.[9] Isolated or small-scale acts of cyber aggression, which do not have direct kinetic effects but damage the infrastructure may also qualify as cyber warfare.[10] The terms cyber-attack and cyber operations are often used as synonyms to cyber warfare, and the same outline is adopted in this work.

[6] Valuch J., Hamulak O. (2018) *Cyber Operations During the Conflict in Ukraine and the Role of International Law*. In: Sayapin S., Tsybulenko E. (Eds.) *The Use of Force against Ukraine and International Law*. T.M.C. Asser Press/Springer, The Hague, p 217.
[7] 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, p 823.
[8] Mukherjee, S. (2019). Cyber Warfare and Implications. University of the Cumberlands, Literature review.
[9] Green, J. A. (Eds.) (2015). *Cyber Warfare: A Multidisciplinary Analysis: Introduction.* Oxon, Routledge, p 2.
[10] *Ibid.,* p 2.

Naturally, all of these above-mentioned cyber concepts are considered and qualify as cyber-attacks.

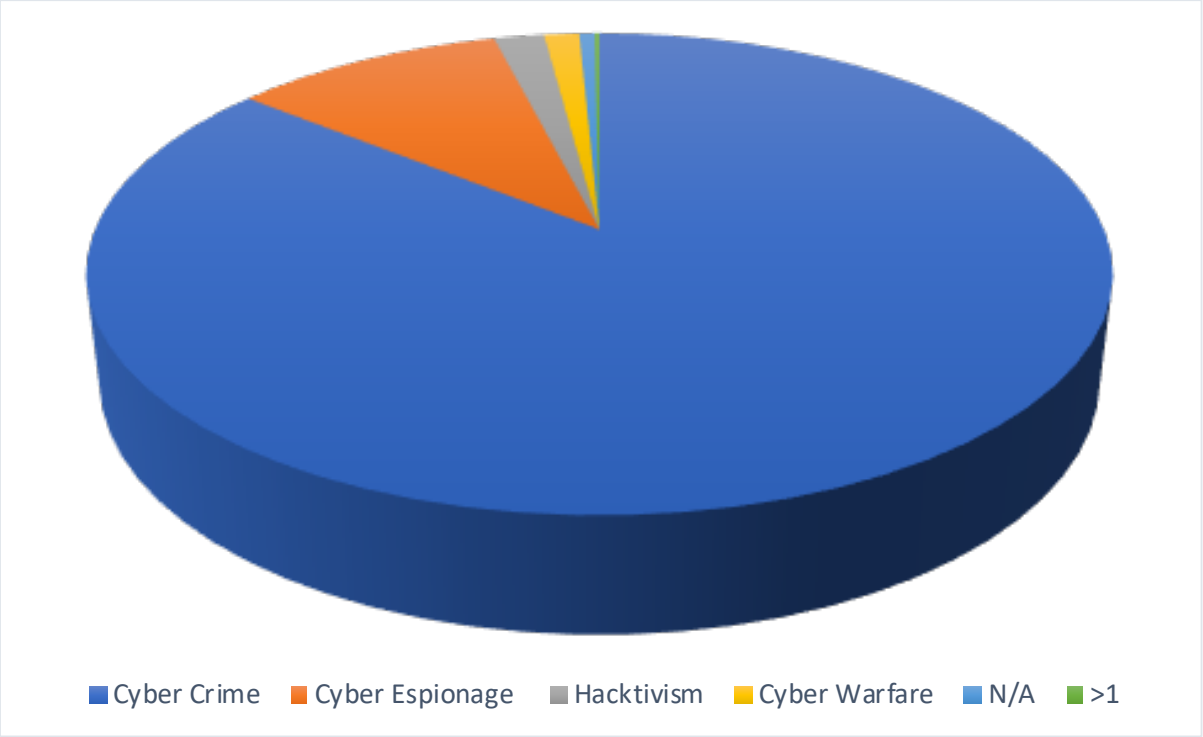


Figure 1. Statistical distribution of cyber-attacks for the first quarter of 2020 (520 total events) Source: Passeri, P. (2020, April 14). Q1 2020 Cyber Attacks Statistics [Blog post]. Retrieved from https://www.hackmageddon.com/2020/04/14/q1-2020-cyber-attacks-statistics/, 20 April 2020

The above chart shows the statistical distribution of motivations behind cyber-attacks in the first quarter of 2020. Cybercrime tops the chart due to ransomware campaigns related to the COVID-19 pandemic. The chart demonstrates the fact that cyber-attacks mostly amount to acts that fall into the criminalization of national legislation. Cyber warfare (yellow segment), on the other hand, is represented only in under two percent of the attacks. For the whole calendar year of 2019, cyber warfare was represented in circa one-point-five percent of the attacks.[11]

[11] Passeri, P. (2020, Mar 19). February 2020 Cyber Attacks Statistics. *Hackmageddon.* [Blog post]. Retrieved from https://www.hackmageddon.com/2020/04/14/q1-2020-cyber-attacks-statistics/, 22 February 2020.

*Jus in bello* applies only to international armed conflicts. Notable is that the whole body of law of armed conflict would, therefore, apply only to minimal amount of cyber-attacks that would be able to exceed the threshold of international armed conflict.

## 1.1 Cyber Warfare

The term cyber warfare adopted in this thesis follows a custom-built definition from various sources, including Clausewitz's definition of war, which is assembled by J.A. Green in the following structure:

"Cyber warfare is an extension of policy by actions taken in cyberspace by state actors (or by non-state actors with significant state direction or support) that constitute a serious threat to another state's security, or an action of the same nature taken in response to a serious threat to a state's security (actual or perceived)."[12]

Cyber warfare generally means the use of digital attacks, such as computer viruses or hacking, by one State to disrupt the central computer systems of another, with the aim of creating serious damage, death and destruction.[13] In the future, warfare will be more commonly conducted by conventional, physically fighting troops alongside supporting hackers who use computer codes to attack enemy infrastructure. Cyber warfare is an increasingly common and dangerous type of international conflict.

Whether an attack constitutes an act of cyber warfare depends on many different factors. These factors are the identity of the attacker, the nature of actions, the means they carry out and how much damage do they inflict. Cyber warfare is a conflict between states – not a conflict between individuals.[14] To qualify as cyber warfare, the attacks should be of significant scale and severity.[15] Attacks which are conducted merely by individual hackers or group of hackers and are not aided or directed by a state are not to be considered as cyber warfare. Crashing a company's website or

[12] Green, J. A. (2015) *supra nota* 1, p 2.
[9] Ranger, S. (2018, December 4). What is cyberwar? Everything you need to know about the frightening future of digital conflict. *ZDNet News.* Retrieved from https://www.zdnet.com/article/cyberwar-a-guide-to-the-frightening-future-of-online-conflict/, 19 February 2020 .
[14] Green, J. A. (2015) *supra nota* 2, p 2.
[15] *Ibid.*, p 2.

firing a missile at a data center do not qualify as acts of cyber warfare. On the other hand, disabling a missile defence system or digital attack on a computer system of a data center fulfil the definition.

Ethics of cyber warfare is closely related to the law of armed conflict. How should the states defend themselves in an occurrence of a cyber-attack? Can a state justify its actions when using force in response? These questions typically fall under *jus ad bellum* in a juridical sense, but with the assistance of just war theory it is possible to examine the military responses that could be morally permissible in the occurrence of a cyber-attack.[16] Just war theory deals with the justification of how and why wars are fought. Theoretically, it is concerned with ethically justifying the warfare and its various forms. International agreements such as Geneva and Hague Conventions regulate warfare in general, but ethics has the role of examining these institutional agreements for their philosophical coherence and inquiring whether aspects of the conventions ought to be changed.[17]

The lack of immediate physical destruction renders existing ethical theories less applicable than to those of more traditional forms of conflict.[18] Cyber-attacks, however, also inflict physical damage. In contrast to immediate effects, they usually inflict damage in the later stages. This mere fact makes them as lethal as conventional attacks. Second problem with applying cyber-attacks in the context of ethics is the difficulty to attribute the perpetrator or its origin. If the state cannot identify the aggressor, how it can equitably justify a counterstrike? In turn, the perpetrator of a conventional attack and his nationality or group affiliations can be identified normally. "According to the present legal and military norms, the epistemological bar for justified military retaliation is set at a level that may be appropriate for conventional attacks, but inappropriately high for cyber-attacks."[19] Cyber-attacks in this sense would require identifying the source computer and operator before any reactions. But due to indistinct nature of cyber-attacks, this fully reliable identification is almost impossible.

In this thesis, it is not suitable to discuss about the just response and identification of the aggressor in more detail. Whether a cyber-attack can be classified as an act of war is, however, is a very important question relating to the rules of the law of armed conflict. This classification complexity

[16] Dayem, L. (2018). The Ethics of Cyber Warfare. *The Illini Journal of International Security,* University of Chicago. Vol. 4, No. 1, p 4.
[17] Moseley, A. (2004). Just War Theory. *Internet Encyclopedia of Philosophy*, United Kingdom. Retrieved from https://www.iep.utm.edu/justwar/, 19 February 2020.
[18] Dayem, L. (2018) *supra nota* 1, p 3.
[19] *Ibid.,* p 4.

and lack of regulation in this sense has been tackled by philosophers and military ethicists in the form of three ethical standards.[20] Whether a cyber-attack can be classified as an act of war is not established in any Convention. For that reason, experts have developed certain standards for analysing whether a cyber-attack can be classified as an act of war. These standards are called means-based standard, target-based standard and effects-based standard.[21]

Cyber-attack will be classified as an act of war if the attack causes similar type of destruction that an existing conventional weapon is capable of causing. This is the so-called means based standard.[22] It brings already established military norms into the sphere of cyber warfare, and thus has a rather conservative nature. Target-based standard means that when a cyber-attack causes damage to vital national infrastructure, it constitutes an act of war. This infrastructure includes, but is not limited to electricity generation, telecommunication, the water supply, security services and financial services.[23] What particularly constitutes an unacceptable level of interference in electronic system, however, is a question tangled with ambiguity and could be open to different interpretations. The last proposed standard is effects-based standard, which categorises a cyber-attack as aggression if it causes physically violent or overall destructive consequence to its victim.[24] This standard is therefore in synthesis with the two former standards.

Even when the standards could interpret some non-physically threatening harm as aggression, it is not reasonable to start a war. Current international legal and moral norms do not give reason to begin a war just because a certain type of cyber-attack is considered as aggression. This type of retaliation would not meet the *jus ad bellum* proportionality and necessity requirements. Regardless of this, scholars and international policymakers acknowledge that cyber-attacks can and should be considered as acts of war. The ethical standards function as the basis for the theoretical application of the law of armed conflict to cyber warfare. Later in this thesis, these standards will be conceptualized as they are embodied in universal customary rules of International Humanitarian Law under *jus in bello.*

[20] *Ibid.,* p 4.
[21] *Ibid.,* p 3.
[22] *Ibid.,* p 3.
[23] *Ibid.,* p 11-12.
[24] *Ibid.,* p 12.

## 1.2 Cyber Weapon

The Tallinn Manual defines cyber weapons and cyber weapon systems as 'means of cyber warfare'. This definition allows for cyber warfare to encompass cyber devices, equipment, or software used, designed, or intended to be used to conduct a cyber-attack.[25] Subsequently, it defines cyber weapons as "cyber means of warfare that are used, designed, or intended to be used to cause injury to, or death of, persons or damage to, or destruction of, objects, that is, that result in the consequences required for qualification of a cyber operation as an attack".[26] The definition acknowledges that cyber weapons inflict harm. It also depicts the vast multitude of existing cyber weapons, which range from highly advanced weapons to 'basic' type of weapons. The difference between traditional weapons and cyber weapons is that the former usually causes immediate damage, while the latter inflicts damage or adverse effects at a later stage. The most well-known and controversial cyber weapon is the so-called Stuxnet worm, which was identified in 2010 during the cyber-attack on Iran.[27] According to famous data leaker Edward Snowden and widely accepted view, it was developed in collaboration by US and Israel Governments.[28] It was the first cyber-attack which was used to effect physical destruction. Stuxnet was unlike any other virus or worm. It did not only hijack computers or steal information from them, it escaped the digital realm to cause physical destruction on equipment the computer systems controlled. Stuxnet raised many legal, policy and practical issues including the issue of cyber weapons reviews under International Humanitarian Law. Stuxnet attack on Iran is further examined and analysed later in section 2.2 of this thesis.

The absence of mutual definition for cyber concepts is one of the most significant problems in current cyber discussion. International regulation should first focus on creating a definition for cyber-attack and cyber warfare before reaching some rough consensus on the definition of cyber weapon. The multitude of generic weapons are rather effortless to define, but the lack of definition

[25] Tallinn Manual referenced in Kittichaisaree, K. (2017). *Public International Law of Cyberspace.* Springer International Publishing, Switzerland, p 160.
[26] Tallinn Manual referenced in Krawczyk, L. (2019, Aug 09) *supra nota* 2.
[27] Wallace, D. (2018). Cyber Weapon Reviews under International Humanitarian Law: A Critical Analysis. *Nato Cooperative Cyber Defence Centre of Excellence,* p 5.
[28] Fruhlinger, J. (2017, August 22). What is Stuxnet, who created it and how does it work? *CSO, IDG Communications.* Retrieved from https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html, 18 February 2020.

for crucial concept of cyber weapon hampers the overall comprehension of cyberspace in international armed conflicts. The mutually recognized definition would cultivate the embryo for possible future regulation.

Prohibitions and limitations on particular weapons have existed for thousands of years. For example, in approximately 200 AD, the Hindu Code of Manu included a provision that prohibited poison arrows.[29] The current provisions of IHL concern first of all the legality of the weapons themselves. It raises a question whether the weapons and weapon systems are unlawful *per se.* Under IHL, most weapons are not illegal *per se,* but their use under some circumstances be unlawful.

Several international treaties such as Geneva Conventions and their Additional Protocols prohibit the use of certain types of weapons. Weapons that may cause unnecessary suffering or have indiscriminate effects are prohibited.[30] Under the provisions of IHL, indiscriminate weapons are those that cannot be directed at a military objective or whose effects cannot be limited.[31] The requirement to be directed at a specific military objective highlights the primary principle of IHL to respect the balance between humanitarian considerations and military necessity. Due to rapid technological development, an increasing amount of 'big stakeholder' states will be able to fulfill the requirement of directing the attack at a military objective. This might not be the case regarding the second requirement, the limitation on effects of the weapon. For example, a state-aided malware used during an armed conflict could unavoidably spread into unintended networks, such as civilian networks.

Whether a cyber weapon can be considered as indiscriminate is purely a matter of interpretation. If a malware can be directed at a specific military objective, it is not illegal. However, most malwares pose the ability to unintendedly spread into other networks. If the unintentional spread would occur, the effects of the malware could not be limited, and it would be considered as indiscriminate. The question and threshold regarding indiscriminate cyber weapons therefore lie within the concept of collateral damage. However, the damage must be harmful which amounts to injury or death to civilians or damage to civilian objects to violate the principle.

[29] Boothby, W. H. (2016). Weapons and the Law of Armed Conflict. Oxford, Oxford University Press, p 104.
[30] 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 35
[31] *Ibid*., Article 51(4)(b) and (c).

# 2. MAJOR CYBER ATTACKS

## 2.1 Distributed Denial of Service (DDoS) Attacks in Estonia and Georgia

The decision of the Estonian government to relocate a monument to Soviet troops from a busy city center into nearby military cemetery triggered the event for one of the most well-known cyber-attacks. The statue had recently become a point of tension between pro-Kremlin and Estonian nationalist movements. From peaceful protests to collisions with the police, the situation quickly escalated into cyber-attacks lasting in total of 22 days. The cyber-attack began in April 2007, when online distributed denial of service (DDoS) attacks started targeting Estonian government and private sector sites, including banking institutions and news sites.[32] DDoS attack refers to an attack in which multiple computer systems attack a server, website or other network resource and cause a denial of service for the users of the targeted source.[33] The attacks resulted in temporary degradation or loss of service on many commercial and government services.

Estonia has one of the highest broadband connectivities in Europe.[34] However, at the time of the attack, it lacked an IT security of similar status. The attacks resulted in total economic and political catastrophe in Estonia, also extending beyond its borders. They might also have indirectly caused loss of lives due to shutdown of the emergency phone service. It is believed that behind the actions was the small group of Russian activists associated with the pro-Kremlin youth group Nashi who later on claimed their responsibility.[35]

---

[32] Ottis. R (2008). Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. *Cooperative Cyber Defence Centre of Excellence,* Tallinn, Estonia, Abstract.
[33] Rouse, M. (Eds.) (2019 April). Definition of Distributed Denial of Service (DDoS) Attack. *SearchSecurity,* TechTarget. Retrieved from https://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack, 28 February 2020.
[34] Clarke & Knake, referenced in Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., Spiegel, J. (2012), *supra nota* 1, p 820.
[35] *A look at Estonia's Cyber Attack in 2007.* (2009, August 7). The Associated Press, NBCNews. Retrieved from http://www.nbcnews.com/id/31801246/ns/technology_and_science-security/t/look-estonias-cyber-attack/#.Xk19bi17HUo, 17 March 2020.

Since the attack, Estonia has been a frontrunner in developing offensive and defensive solutions to cybersecurity challenges. Estonian Cyber Defence League was created, which was aimed to protect Estonian cyberspace as part of the National Defence League.[36] As a consequence of the attacks, Estonia prompted NATO to enhance its cyber-war capabilities and to establish the alliance's cyber defence research center in Tallinn in 2008.[37] These fast reactions and establishments of Estonia have been vital for international cooperation in the cybersecurity domain. As a consequence, the blistering question concerning the application of international law in cyber domain was further examined and some important international guidelines were drawn in two academic, non-binding books, *Tallinn Manual on the International Law Applicable to Cyber Warfare* and *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* More detailed view of these manuals is discussed in section 4.1 of the thesis.

In July 2008, cyber-attacks against Georgian websites were reported. The attacks were similar DDoS attacks as in Estonia. Several weeks later, the amount of attacks increased while the Russian military simultaneously crossed the border into South Ossetia, a Georgian province. By August, the attacks had rendered most Georgian governmental websites inoperative.[38] At the time, government websites of Georgia were poorly protected and vulnerable to attacks. The attacks occurred in two phases: the first wave was focused attacking mainly on Georgian news and governmental websites while the second wave attacked financial institutions, businesses, educational institutions and Western media.[39] The attacks were conducted from the territory of Russia and were a mixture of professional acts and attacks performed by patriotic hackers similarly like in the case of Estonia. Russian government did not confess its involvement in the attack, although many experts proved that Russia was behind the attack.

Cyber-attack in Georgia was the first time in history when a cyber-attack was concurred with a kinetic one.[40] However, according to several sources, the cyber portion of the armed conflict in Georgia did not meet the common definition of an attack.[41] This depicts the problematic image of cyber-attacks and their high threshold of being recognized namely as 'cyber-attacks'. Despite this,

[36] *Estonian Defence League's Cyber Unit*. Kaitseliit. Estonian Defence League. Retrieved from https://www.kaitseliit.ee/en/cyber-unit, 14 March 2020.
[37] The Associated Press, NBCNews (2009), *supra nota* 1.
[38] Korns, S. W., Kastenberg, J. E. (2009). Georgia's Cyber Left Hook. *Army War College Carlisle Barracks PA Strategic Studies Institute,* Carlisle, Abstract.
[39] *Ibid.,* Abstract.
[40] Brown, G. D. (2011). Why Iran Didn't Admit Stuxnet Was an Attack. *Joint Force Quarterly,* Issue 63, 4th Quarter, p 71.
[41] *Ibid.,* p 71.

the incidents in Georgia indicated that the cyber-portion of an attack can evolve into attacks causing actual material damage.

## 2.2 Stuxnet Worm, Iran 2010

In 2010 a new, serious and far more complex computer virus had been discovered in Iran. Stuxnet, as the virus came to be known, was a complicated and powerful code capable of self-replicating its worm that targeted computers used to perform automated tasks in many industrial processes.[42] The Stuxnet code was discovered on computer systems around the world, but the numbers indicate that 60 percent of reported infections occurred on systems in Iran.[43] The specific target of Stuxnet was Iran's uranium enrichment facility at Natanz. It was programmed to target important central parts of the production of nuclear material. The nuclear centrifuges were destroyed effectively. Iran was at the time of the attack, and still is, a significant nuclear power country. Iran claimed that it was not as a consequence of cyber-attack.[44] According to scholars, however, it was a cyber-attack due to its intentional purpose of causing physical destruction to state-owned equipment.[45]

The incidents in Georgia and Iran presented the world that cyber-attacks are capable of causing physical damage. Stuxnet was a self-replicating worm, which did not contain enough control to prevent it from inserting itself into civilian computer systems and thus it violated the requirement of the provisions of IHL, in which indiscriminate weapons are described as those that cannot be directed at a military objective or whose effects cannot be limited. This is highly problematic in the light of current international regulation and cyber-attacks.

## 2.3 Global Ransomware Cyber-Attack

In May 2017, a massive ransomware cyber-attack infected computers in over 150 countries around the world, including the UK, Russia, China, Italy and the United States.[46] The attack is known as

[42] Reinikainen, M. (2019). Computer Viruses. *University of Eastern Finland,* Faculty of Science and Forestry, Kuopio, p 14-15.
[43] Gross, M. J. (2011). Stuxnet Worm: A Declaration of Cyber-War. *Vanity Fair,* Symantec referenced in *Ibid.,* p 71.
[44] Weinberger, S. (2011). Computer security: Is this the start of cyberwarfare? *Nature*, Nature Publishing Group, United Kingdom, p 142-145.
[45] *Ibid.,* p 142-145.
[46] Dayem, L. (2018) *supra nota 1*, p 7.

WannaCry cryptoworm, which presents a formidable threat to Internet users and has the potential to cause several types of disruptions.[47] It held Windows-operated computers as hostages by encrypting data that could only be disabled by paying ransom in the form of bitcoins.[48] It allegedly got started from a cache of cyber weapons stolen from the US National Security Administration (NSA), which is a government agency which collects cyber weapons and vulnerabilities in popular operating systems and software in order to engage in cyber warfare and espionage.[49] The attack had the most impact and adverse effects in England, where as a consequence England's National Health Services compelled some hospitals to divert its patients.[50] At least one-third of health trusts were disrupted and over 19,000 appointments cancelled, including surgeries, which consequently caused indirect death victims.[51]

The attacks against a country's national health services demonstrates how cyber-attacks can have consequences in deciding life and death. While placing the above-mentioned most infamous cyber-attacks chronologically in order, we can notice numerous notable issues. Firstly, the more recently the attack has occurred, the more it has spread. Future cyber-attacks could easily affect the whole world, with only minimal influence from its perpetrators. Means and methods of cyber warfare are constantly evolving in proportion with information technology and cyber-attacks are also constantly more difficult to trace.

## 2.3 The Rising Threat of Cyber Incidents

The current worry regarding warfare usually concerns nuclear tensions. The nuclear pacts, test-launchings and boasting of US, Russia, Iran and North Korea are giving rise to fears of a new nuclear arms race. Many people are inadvertently blinded by the fact that cyber-attack could cause as much damage as nuclear attack. While nuclear weapon would kill everyone within a half-mile radius as direct death victims, cyber-attack could kill people with slower pace while causing lack

[47] Reinikainen, M. (2019) *supra nota 1,* p 15.
[48] *Ibid*., p 7.
[49] Wong, J. C., Solon, O. (2017, May 2). Massive ransomware cyber-attack hits nearly 100 countries around the world. *The Guardian,* United Kingdom. Retrieved from https://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs, 20 March 2020
[50] *Biggest Cyber Attacks 2017: How They Happened.* (2017, November 30). *Calyptix Security.* Retrieved from https://www.calyptix.com/top-threats/biggest-cyber-attacks-2017-happened/, 18 February 2020.
[51] *Ibid.*

of food, power or gas and car crashes due to corrupted traffic light system.[52] A massively destructive cyber-attack conducted by a nation or terrorist organization could target electricity utilities, water treatment facilities or industrial plants. Being capable of shutting down nuclear centrifuges (Iran), air defence systems and electrical grids, cyber-attacks pose a severe threat to national security. To illustrate the genuine seriousness of cyber threats, consider that "as recently as 2007, malicious cyber activities did not register on the director of [the USA's] national intelligence's list of major threats to national security. In 2015 they ranked first."[53] The leading world militaries have acknowledged the potential for an expansion of cyber warfare.[54]

The rising threat of catastrophic cyber-attacks on critical infrastructure is hiding behind the curtains. Many cyber-attacks and incidents go unnoticed and thus unreported even though they occur in large frequency and intensity around the world. Cyber-attacks can be organized promptly from a distance without any disruptive hurdles. Attacks from distance are difficult to trace back with adequate precision. This makes the retaliation and punishment of perpetrators troublesome. Attacks happen already on a nationwide level, so it is not impossible to depict a situation where entire economies would be paralyzed by digital epidemic. The digital network is already today associated and tangled with every aspect of human life, which means that we are progressively more susceptible to cyber-attacks. In response to the rising threat of cyber-attacks, governments find theirselves in enhanced position regarding issues of cybersecurity and are the consolidation of the acceptance of various defensive measures such as technology, policy, and increasing international cooperation.[55]

[52] Straub, J. (2019, August 16). A Major Cyber Attack Could Be Just as Deadly as Nuclear Weapons, Says Scientist. *The Conversation.* Retrieved from https://theconversation.com/a-cyberattack-could-wreak-destruction-comparable-to-a-nuclear-weapon-112173, 14 April 2020.
[53] Clapper, J. R. (2016, February 9) referenced in Dayem, L. (2018) *supra nota 2*, p 2.
[54] Breene, K. referenced in Frankli, A. (2018). An International Cyber Warfare Treaty: Historical Analogies and Future Prospects. *Journal of Law & Cyber Warfare*, Vol. 7, Issue 1, Lexeprint, 149-163, p 4.
[55] Mukherjee, S. (2019) *supra nota* 1, Conclusions and Future Study.

# 3. JUS IN BELLO AND ITS APPLICATION TO CYBER WARFARE

Law of armed conflict refers to law which governs conduct during wartime and provides different parameters for actions. These parameters include rules for actions of hostility and the protection of persons and objects.[56] Law of armed conflict encompasses *jus ad bellum,* which set the criteria for engaging in war and *jus in bello,* which set the rules during war. Law of armed conflict is also known as the law of war or international humanitarian law. International armed conflict occurs when one or more States uses armed forces against another State. Currently, the majority of cyber-attacks are carried out by non-state actors and thus fall outside what is considered to be traditional interstate armed conflict. It means that these aggressors do not principally adhere to the Geneva Conventions.[57] The concept of armed conflict is not defined in the Common Articles of the said Conventions.[58] However, the Appeals Chamber of the International Criminal Tribunal for the former Yugoslavia (ICTY) has defined the term in *Prosecutor v Tadić.* In the case, the tribunal held that an armed conflict exists when "there is a resort to armed force between States or protracted armed violence between governmental authorities and organized armed groups or between such groups within a State."[59] Therefore, any dispute which arises between two States and involves their armed forces is considered as armed conflict and thus triggers application of Common Article 2 and the body of IHL.[60]

The applicability of the rules of *jus in bello* in the context of cyberspace is obscure. In 2018, the UN Secretary-General Guterres stated that the concern "is not the use of cyberspace in war but rather the inadequacy of current IHL to address it".[61] At the time of drafting of current legal norms

[56] Ohlin, J. D., Govern, K., Finkelstein, C. (Eds.) (2015). *Cyberwar, Law and Ethics for Virtual Conflicts.* Oxford University Press, Oxford, United Kingdom, p 79.
[57] Sutherland, I., Xynos, K., Jones, A., Blyth, A. (2015). The Geneva Conventions and Cyber-Warfare. *The RUSI Journal*, Vol. 160, Issue 4, 30-39, p 31.
[58] Wallace, D. A., Jacobs, C. W. (2019). Conflict Classification and Cyber Operations: Gaps, Ambiguities and Fault Lines. *University of Pennsylvania Journal of International Law*, 643-693, p 661.
[59] Prosecutor v Tadić*,* IT-94-1, para 70 referenced in Ohlin, J. D., Govern, K., Finkelstein, C. (Eds.) (2015), *supra nota* 1, p 81.
[60] *Ibid*., p 81.
[61] Robertson, C. H. II. (2019). Different Problems Require Different Solutions: How Air Warfare Norms Should Inform IHL Targeting Law Reform & Cyber Warfare. *Michigan Journal of Law Reform,* Vol. 52, Issue 4. University of Michigan Law School, 985-1012, p 986.

and customary practice regulating warfare, there was merely any indication of the emergence of advanced cyber technology. The problem was not only the invention of cyber technology itself, but the very quick development. International legal treaties and conventions have been and still are several steps behind the armed development, which is rather problematic in the eyes of law of armed conflict. The classification of cyber-actions as an armed attack or conflict is really difficult. Sometimes it can be even difficult to determine when typical warlike actions trigger the law of armed conflict.

The main rules applicable in international armed conflict are all of the four Geneva Conventions, Additional Protocol I and Customary International Humanitarian Law. International Humanitarian Law is a tool of protecting people who do not take part in hostilities and to restrict means and methods of warfare.[62] It is comprised of international treaties and customary law. Customary law refers to universally recognized or general rules of law by which every State is bound. A major part of IHL is contained in the universally recognized four Geneva Conventions of 1949, which all of them apply to international armed conflicts. Geneva Conventions apply even though the attack was illegal, it takes place in the regime of a nation in state of war which is not recognized or if the attack occurs as unopposed occupation. The Conventions are over fifty years old and since then, most of the attacks have occurred more in the sense of 'armed conflict' than 'war'.

*Jus ad bellum* is founded on Article 2(4) and Chapter VII of the UN Charter.[63] As mentioned above, *jus ad bellum* governs the transition from peace to war. It sets out rules when states may lawfully use its armed forces against another state. *Jus in bello* governs the use of force during armed conflict. It sets forth the threshold that cyber-attack must cross to qualify as an act of war. Based on treaty provisions, the fundamental military necessity, principles of distinction and proportionality and the obligation to protect civilians, IHL creates certain obligations for the attacking party. These obligations, which must be obeyed at all times during an armed conflict, make warfare more 'justifiable'. The application of IHL rests on an objective analysis of certain situation and its facts to determine whether it meets the threshold for triggering IHL.[64]

[62] Allison, J. (Eds.) (2019, May 9). Research Guide for Program on International Law and Armed Conflict. *Harvard Law School Library.* Retrieved from https://guides.library.harvard.edu/c.php?g=310988&p=2079382, 11 April 2020.
[63] Bothe, M. (2013) (Eds.). *The Handbook of International Humanitarian Law.* Oxford University Press, Oxford, p 1.
[64] Ohlin, J. D., Govern, K., Finkelstein, C. (Eds.) (2015)., *supra nota* 2, p 42.

For the reminder, International Humanitarian Law applies only to armed conflicts. For instance, it does not cover isolated acts of violence or regulate whether a State may use force.[65] The use of armed force is prohibited under the Charter of the United Nations.[66] States may resort to armed force only in the exercise of individual or collective self-defence or as authorized by the Security Council.[67]

For IHL to apply or victim-state to respond with active defences, cyber-attack must qualify namely as an 'armed attack'. As presented above, the term armed attack is not defined by any international convention, which means that it has been left completely open to interpretation by states and scholars. Under Pictet's test, use of force is an armed attack when it is of sufficient scope, duration and intensity.[68] This view is generally accepted, and it fulfils the criteria of armed attack in a proper accuracy. If the actions do not reach the threshold of armed conflict, rules of IHL would not legally concern those actions.

Although it is high unlikely to occur, cyber acts alone should trigger or constitute an international armed conflict. If two states use cyber domain to engage in acts which amount to armed hostilities, an international armed conflict would exist, despite the fact if its duration and scope is limited. Cyber-attack should constitute an armed attack where the attack is a virtual or kinetic use of force of one state against another with the intent of altering its sovereignty or strategic capacity by disrupting its critical infrastructure. With this general rule, malicious and destructive cyber-attacks would reach the definition of armed attack properly, effortlessly and more precisely. It would catch attacks which current international regulation leaves outside the scope and rules of *jus in bello.*

In practice, the triggering of *jus in bello* would require cooperation between cyber operations and kinetic armed forces, as occurred in the Georgia case discussed in section 2.1. In this situation the law of armed conflict would apply for all attacks operated by any party to the conflict. This is problematic, since almost every cyber-attack stays merely in cyber domain without any contribution by kinetic forces.

[65] What is International Humanitarian Law? (2004). *Advisory Service on International Humanitarian Law*, ICRC. Retrieved from https://www.icrc.org/en/doc/assets/files/other/what_is_ihl.pdf, 11 March 2020.
[66] Charter of the United Nations*,* Article 2(4).
[67] *Ibid*., Articles 2(4), 51, 39-42.
[68] Wingfield referenced in Major Ching, A. B. (Eds.) (2009). *Military Law Review,* Vol. 201 Headquarters, Department of the Army, Washington D.C., p 51.

## 3.1 IHL Principles

International Humanitarian Law consists of rules aimed at improving the conditions of prisoners of war, medical and religious personnel who are positioned in battleground and improving the protection of civilians.[69] Humanitarian aspects have a fundamental role regarding the rules of civilian protection. This is embodied in the of law of targeting, a section of the *jus in bello* consisting of rules of distinction, proportionality and military necessity. The Geneva Conventions provide also certain humanitarian principles and rules of ethics which operate at the time of an armed conflict. All of these rules have a fundamental role of regulating armed attacks. Once an act is qualified as an armed attack, these principles must be followed at all times and by every party to the conflict.

Applying the well-known and widely accepted principles to cyber-attacks is a much more difficult task than applying them to conventional attacks. For most part, law of armed attack was developed in response to conventional wars between states.[70] The notion of attack is entangled in the concept of violence. The definition of violence has proven controversial in the battlefield of competing views which are attempting to challenge a conventional view, which is interprets it as a synonym of physical harm.[71] Acts not causing physical violence are not governed by the rules of distinction, proportionality and military necessity.[72] Notion of violence includes, however, also military harm. Military harm encompasses not only death, injury or destruction of military personnel or objects, "but essentially any consequence adversely affecting the military operations or military capacity of a party to a conflict."[73] Cyber-attacks are certainly capable of causing violent consequences. When the Stuxnet worm attacked Iran, it targeted the centrifuges of the nuclear facility in Natanz causing physical destruction. The same could be noted for the causation of military harm: a computer network attack can disrupt with the supervisory control and data acquisition system

[69] Biggio, G. (2017). Cyber Operations and the Humanization of International Humanitarian Law: Problems and Prospects, *Canadian Journal of Law and Technology,* Vol. 15, No. 1, p 42.
[70] Carr, J. (2012). *Inside Cyber Warfare, Second Edition.* O'Reilly Media, California, United States of America, p 45.
[71] Finlay, C. J. (2018). Just War, Cyber War, and the Concept of Violence. *Philosophy & Technology,* Vol. 31, Issue 3, 357-377, p 361.
[72] Biggio, G. (2017)., *supra nota* 1, p 43.
[73] Melzer referenced in *Ibid*., p 43.

(SCADA system) of a modern weapon system.[74] On the other hand, these attacks may cause no physical violence at all while still posing serious consequences.

### 3.1.1 Distinction

Principle of distinction requires combatants to direct their attacks against military objectives, and attacks against civilians are prohibited.[75] This relates to the requirement of military personnel to distinguish themselves from the civilian population, and the marking of cultural or civilian objectives with a distinctive emblem. The prohibition on directing attacks against civilian objectives is also recognized in the UN Amended Protocol II and Protocol III to the Convention on Certain Conventional Weapons (CCW).[76] Many States have adopted legislation to criminalize the attacking of civilian objects during an armed conflict, and high number of documents relating to the principle has been enacted all around the world. This highlights the importance of the principle in customary international law. The International Court of Justice has also approved its customary role in its *Nuclear Weapons* case, where it held that the principle of distinction was one of the "cardinal principles" of international humanitarian law and one of the "intransgressible principles of international customary law."[77] Principle of distinction offers protection for civilian population and is the cornerstone of humanitarian protection.

Using cyberspace as a battleground causes obscurity in the light of principle of distinction. Cyberspace can function in both civilian and military purposes. Some of the critical infrastructure of a state can be destroyed due to difficulties in distinguishing military and civilian infrastructure. An objective in cyberspace can function for both civilian and military purposes in a mixed assembly. Distinguishing the military personnel and civilians must also be given importance, since the number of civilians indirectly participating in cyber hostilities is constantly increasing. Civilians cannot be targeted unless they take direct part in hostilities. The classification issue is sometimes difficult to deal with during a conventional kinetic attack, but it gets an exponential effect in cyber-attacks.

[74] *Ibid.,* p 43.
[75] AP I, *supra nota* 1, Article 48.
[76] UN Amended Protocol II to the Convention on Certain Conventional Weapons, 3 May 1996, Article 3(7) and Protocol III to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may deemed to be Excessively Injurious or to have Indiscriminate Effects, 10 October 1980, Article 2(1).
[77] *Para 79* of Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 July 8, ICJ. Retrieved from https://www.icj-cij.org/files/case-related/95/7497.pdf, 13 March 2020.

### 3.1.2 Proportionality

The principle of proportionality also relates to the objectivity of a legitimate target. It generally prohibits indiscriminate attacks. Indiscriminate attack is an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.[78] The expression of 'military advantage' refers to the advantage achieved from the attacks as a whole, which has been confirmed by the ICJ.[79] Whether an attack is disproportionate is a question of comparison. The expectation of excessive civilian harm has to be compared to the concrete and direct military advantage anticipated. If the civilian harm is considered excessive in relation to direct military advantage, the attack may qualify as disproportionate and therefore constitute a war crime.

Military operations that do not cause violent consequences are not governed by the principle of proportionality. Proportionality is relevant in the context of cyber-attacks when the attack could have physical effects on civilian population. For example, destroying the data of a military objective which is also archiving sensitive medical data of certain civilian groups and the destruction is causing physical harm for them could be considered as disproportionate attack. The collateral damage in potentially disproportionate attacks is always measured against the achieved military advantage. Proportionality is not relevant in circumstances where the attack causes physical damage or loss of life to military objectives or personnel if it is not likely to cause those effects on the civilians. Emerging military technologies in cyberspace highlight the painful reality of the difficult assessment of this principle and creates challenges in its application, but may in turn also offer new perspectives on its more effective implementation.[80]

### 3.1.3 Military necessity

Military necessity is a restrictive doctrine which requires the attacking party to resort only in those acts which are necessary to accomplish a legitimate military objective.[81] This principle is

[78] AP I, *supra nota* 2, Article 51(5)(b).
[79] Rome Statute of the International Criminal Court*,* Article 8(2)(b)(iv).
[80] Beard, J. M. (2018). The Principle of Proportionality in an Era of High Technology. *Institute for Law and Land Warfare Book Series – Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare.* (Eds.) Ford, C. M., Williams, W. S. Oxford University Press, 1-23, p 3.
[81] Gill, T. D. (Eds.) (2014). *Yearbook of International Humanitarian Law.* T.M.C Asser Press, The Hague/Springer, p 344.

embodied in various parts of the Geneva Conventions and its Additional Protocols. It also requires that when a legitimate military objective is achieved, it must result in minimum loss of life and property. The likelihood number of civilian casualties or damage to civilian objects must be minimized. There is ongoing debate whether the principle is to be interpreted in a broad or restrictive sense.[82] In the broadest interpretation, this principle means that the armed forces can do whatever is necessary to achieve a legitimate military objective in the conduct of war, provided that is not unlawful under humanitarian law. More restrictive view of this principle requires that there must always exist limitations on military actions – no action should be taken unless it is actually necessary.

The principle of military necessity is connected to the aim of defeating the enemy. If the attack is not in connection with the military advantage it is considered as violation of international humanitarian law. Regarding cyber-attacks, this is quite problematic since targeting only to those objectives which could be capable of accomplishing a legitimate military objective are difficult to distinguish in cyberspace.

## 3.2 Cyber Weaponry in the Context of Jus In Bello

Cyberspace as a concept is similar to outer space: both of them are boundless and unregulated. There exists no prohibition on the use of outer space as a weapon, save when it involves the use of nuclear weapons. In this case it is prohibited by an international treaty.[83] However, there exists a void in between, which is unregulated. The problem in applying this analogy to cyber weapon relates to the difference in the threat it poses compared to nuclear weapon.[84] By common thinking, nuclear weapons pose much more devastating threat than cyber weapons, at least in the approximation of human casualties. Another problem is that only few states possess the means to wage war in outer space, whereas most states have the ability to wage war in cyberspace.[85] One example of banning a cyber weapon would be similar to Antarctic Treaty System (ATS), which bans all kind of weapons and military development in Antarctica.[86] The analogy in this sense would also be problematic due to difficulty in differentiating a ‘peaceful’ and ‘malicious’

[82] *Ibid.,* p 344.
[83] UN Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water, 10 October 1963.
[84] Carr, J. (2012) *supra nota 1*, p 33.
[85] *Ibid.,* p 33.
[86] *Ibid*., p 33.

computer code. Yet another problem is the absence of any boundaries in cyberspace and the difficulty to artificially create them. Analogy to ATS is therefore again not possible to implement.

Article 36 of the 1977 Additional Protocol I to the 1949 Geneva Conventions states as follows: "In the study, development, acquisition or adoption of a new weapon, means or method or warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party."[87] The Article demonstrates that it continues to apply while the instruments of warfare are evolving. However, something which is not explicitly prohibited by a treaty, such as a new type of weapon, is not *ipso facto* permitted under IHL. This so-called Martens Clause derives from the preamble to the 1899 Hague Convention and has been interpreted in multiple ways during the rapid evolution of military technology.[88]

Cyber weapons should be assessed with precision in relation to Article 36. Firstly, it must be assessed whether the weapon is of a nature to cause superfluous injury or unnecessary suffering. Secondly, it must be assessed whether the weapon is inherently indiscriminate. Under IHL, indiscriminate weapons are those that cannot be directed at a military objective or whose effects cannot be limited. Regarding cyber weapons, following these assessments gives rise to complex issues. First of all, it is noted by international experts that cyber weapons violate the prohibition of superfluous injury or unnecessary suffering only rarely.[89] Regarding the assessment of their indiscriminate nature, it must be stated that cyber weapons can be created in a way that the damage they cause is precisely delimited. Cyber-arms industry is so advanced that the weapon itself can be created, or the attack for which it is used to, can be executed so that no collateral damage is inflicted. Cyber weapon can be a stealthy malware that is causing significant amounts of damage to intended networks and systems, even protected ones, and inflict harm autonomously.[90] On the other hand, it can be a generic weapon which is influencing computer networks and systems from the outside without inflicting any direct harm.[91] The review and assessment of a cyber weapon under *jus in bello* must therefore be conducted by an objective analysis of its nature and potential to delimit its effects.

[87] AP I, Article 36, referenced in Ohlin, J. D., Govern, K., Finkelstein, C. (Eds.) (2015) *supra nota* 3, p 80.
[88] Ticehurst, R. (1997). International Review of the Red Cross, No. 317, ICRC. Retrieved from https://www.icrc.org/en/doc/resources/documents/article/other/57jnhy.htm, 15 April 2020.
[89] Wallace, D. (2018), *supra nota 1*, p 10.
[90] *Ibid.,* p 16.
[91] *Ibid.,* p 16.

# 4. CURRENT AND PROPOSED LEGAL SOLUTIONS

## 4.1 Tallinn Manuals

In the absence of a binding document, academic experts have had an important role in determining guidelines and making significant contributions to promoting and informing the debate concerning the application of international law to the cyber domain.[92] Among the few multinational organizations seeking solutions to the matter is the North Atlantic Treaty Organization (NATO) whose Cooperative Cyber Defence Center of Excellence (CCDCOE) is in Tallinn, Estonia. This multinational cooperation has been materialized in the form of two books: *Tallinn Manual on the International Law Applicable to Cyber Warfare* and *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* For linguistic purposes, these manuals are more commonly referred to as (original) Tallinn Manual and Tallinn Manual 2.0. Neither of the manuals is a legally binding document. However, their function is to act as a tool of advice for legal authorities in complex cyber-related issues.

The original Tallinn Manual sets in its Rule 11 that "a cyber operation constitutes a use of force when its scale and effects comparable to non-cyber operations rising to the level of a use of force."[93] The explanation for what is considered as those scale and effects is left for sole interpretation. In its commentaries, actions which cause injury or death to person, or damage or destruction to object, are considered as use of force.[94] Cyber-attacks that cause such consequences should therefore constitute a use of force. While the original Tallinn Manual is limited to international law on the use of force and international humanitarian law, the Tallinn Manual 2.0 adds a legal analysis of more common cyber incidents that occur in a daily basis and that fall below the thresholds of the use of force or armed conflict. Tallinn Manual 2.0 is the most comprehensive book to analyze how the existing international law applies to cyberspace. Tallinn Manual 2.0 is

[92] Schmitt, M. N. (Eds.) (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge University Press. Cambridge, United Kingdom, Foreword.
[93] Schmitt, M. N. (Eds.) (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge University Press. Cambridge, United Kingdom, p 47.
[94] *Ibid.,* p 47.

intended as an objective restatement of the *lex lata,* ie. the law as it exists.[95] It covers a variety of international law principles which regulate occurrences in cyberspace, from peacetime acts to law of armed conflict.

In some parts, the Tallinn manuals lack consensus among the experts who drafted it. This clearly illustrates the disputability and constant obscurity in the application of international law to the cyber domain. The absence of their binding force is undisputed due to their solely advisory role. The rules, guidelines, and commentaries of both manuals could, however, be maximally utilized in the form of a binding, universal document like international cyber treaty or Geneva Convention. In this way the rules concerning cyber-operations would enjoy the binding force of international law. The manuals in turn could very well function as a starting point of discussion for further regulation.

## 4.2 New International Cyber Regulation

The digital era is challenging the rules of international law. The internet has achieved a leading role in modern international warfare. The incidents in Estonia, Georgia, and Iran demonstrate that these situations must be addressed more fundamentally. In 2017, technology-giant Microsoft called for a Digital Geneva Convention that would protect civilians from state-sponsored cyber-attacks.[96] Given the fact that the fundamental purpose of the Geneva Convention of 1949 is to protect civilians and non-combatants during warfare, this thesis recalls the proposal. The potential scale and scope of cyber-attacks is endangering the safety and security of the civilian society. Offering proper protection and reaching general consensus on cyber aspects would require the implementation of a new international framework, such as the Digital Geneva Convention or International Cyber Treaty.

First of all, the new legislation should define the terms relating to the cyber domain. As mentioned in the thesis, there are no common definitions for crucial cyber concepts. Without this first phase, it is not even possible to regulate other matters. Secondly, it should create new norms against

[95] Jensen, E. T. (2017). The Tallinn Manual 2.0: Highlights and Insights. *Georgetown Journal of International Law 48,* No. 3, p 738.
[96] Guay, J., Rudnick, L. (2017, June 25). What the Digital Geneva Convention means for the future of humanitarian action. *The Policy Lab.* Retrieved from https://www.unhcr.org/innovation/digital-geneva-convention-mean-future-humanitarian-action/, 14 April 2020.

targeting critical infrastructure. The law of targeting, which encompasses the principle of distinction and military necessity, is the most difficult to apply to the realm of the cyber domain. Cyberspace can function in both civilian and military purposes and targeting only to those objectives which could be capable of accomplishing a legitimate military objective are difficult to distinguish in cyberspace. In order for the law of targeting to catch cyber-attacks properly, it needs coherent and comprehensive updates in a completely new form. The general rule should be that cyber-attack will constitute an armed attack where the attack is a virtual or kinetic use of force of one state against another with the intent of altering its sovereignty or strategic capacity by disrupting its critical infrastructure. By implementing this rule, the most fundamental issues would be relieved. Thirdly, it should implement new rules concerning the non-proliferation of cyber weapons. Cyber weapons pose challenges for both public and private sectors. In a glimpse of an eye, the world could experience a cyber arms race. An international cyber treaty could deal with the most challenging features of cyber weapons, such as unpredictability, accountability, and attribution.[97]

Previous policy actions in the cyber domain have not reached a global consensus. They have rather projected basis for future multilateral initiatives. These policy actions include The United Nations Group of Governmental Experts (UNGGE), the European Union initiatives towards cybersecurity, the NATO public-private partnerships, the Shanghai Cooperation Organization proposal for an international code of conduct on information warfare, the confidence-building measures put in place by the Organization for Security and Co-operation in Europe (OSCE) and the Wassenaar Arrangement.[98] Despite these activities, the debate remains open and must be properly managed. A new international cyber regulation should address these important issues and finally interrupt the obscurity by creating binding rules for every contracting state. These rules would be stricter and more precise than the traditional rules of *jus in bello* and have binding force compared to advisory Tallinn Manuals.

[97] Barbieri, C., Darnis, J. P., Polito, C. (2018). Non-proliferation Regime for Cyber Weapons. A Tentative Study. *Instituto Affari Internazionali.* Issue 18/03, Roma.
[98] *Ibid.*

# CONCLUSIONS

The main purpose of the whole *jus in bello* is to regulate actions during war in a way that ensures protection for all people including, but not limited to belligerents, medical personnel, and civilian people. Its final aim is to restore peace and thus provide for the states to reorganize back to normal conditions as soon as possible. The rules and principles of *jus in bello* must be followed at all times during war and the minimum amount of collateral damage is achieved when the engaging parties conduct within these limits.

When it comes to cyber warfare, the universal customary rules are more difficult to follow. This is mostly due to the nature of the cyber environment. The cyber domain is mainly abstract, and technological development has occurred so quickly that the present norms are not in line with some of the modern features of warfare. Combatants are difficult to distinguish from civilians, illegal targets may be mixed with legal targets and new types of weapons can be indiscriminate either directly or indirectly. It is important for the states to recognize if they have a legal right for self-defense and what means they can carry out in cyber warfare. All of the issues in the field have resulted in a long-lasting debate about international law and its application to cyber warfare, which has eventually evolved into thoughts of renovations to law. This thesis is not an exception.

The hypothesis of the thesis is that a cyber-attack can constitute an armed attack where the attack is a virtual or kinetic use of force of one state against another with the intent of altering its sovereignty or strategic capacity by disrupting its critical infrastructure. Based on several academic sources, the hypothesis seems to get a seal of approval. Cyber-attacks need a separate, common rule for which to base their liability under *jus in bello*. It is important to note that not all cyber-attacks constitute an armed attack, even if similar-like rule is adopted. These acts fall outside the scope of *jus in bello*, into the jurisprudence of national or international criminal law.

The issues concerning attribution, accountability, and what constitutes an armed attack are the most fundamental ones within cyber warfare and international law. In theory, international law is

applicable to any military strategy, but practically the application is much more complicated.[99] It is against the odds that the present rules are able to regulate the issue properly in the future, when they have already faced troubles for years. In the near future, it remains to be seen if any practical policy action will be taken. States, institutions, and policy-makers should bear in mind that humanitarian protection is on the frontline. Wars are and will be fought every day.

The first crucial step for new international regulation would be establishing common definitions for cyber concepts and recognizing the fundamental issues concerning the application of *jus in bello* to cyber warfare. The latter should be conducted by examining the current regulation and analyzing its deficiencies with the aim of creating new, innovative solutions in collaboration with admitted international experts, lawyers, and scholars. Predicting and identifying potential future aspects and turning points which could influence the situation is also pivotal for the best possible outcome. All of this should be done while simultaneously respecting the role of ethics and keeping in mind that the fundamental purpose of *jus in bello*, the law in war, is the humanitarian protection of people.

[99] 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, p 640.

# LIST OF REFERENCES

## Scientific Books:


1. Bothe, M. (2013) (Eds.). *The Handbook of International Humanitarian Law.* Oxford University Press, Oxford.

2. Boothby, W. H. (2016). Weapons and the Law of Armed Conflict. Oxford University Press, Oxford.

3. Carr, J. (2012). *Inside Cyber Warfare, Second Edition.* O'Reilly Media, California, United States of America.

4. Gill, T. D. (Eds.) (2014). *Yearbook of International Humanitarian Law.* T.M.C Asser Press, The Hague/Springer.

5. Green, J. A. (2015). *Cyber Warfare: A Multidisciplinary Analysis.* Routledge, Oxon.

6. Kittichaisaree, K. (2017). *Public International Law of Cyberspace.* Springer International Publishing, Switzerland.

7. Major Ching, A. B. (Eds.) (2009). *Military Law Review,* Headquarters, Department of the Army, Washington D.C.

8. Ohlin, J. D., Govern, K., Finkelstein, C. (Eds.) (2015). *Cyberwar, Law and Ethics for Virtual Conflicts.* Oxford University Press, Oxford, United Kingdom.

9. Schmitt, M. N. (Eds.) (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge University Press. Cambridge, United Kingdom.

10. Schmitt, M. N. (Eds.) (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge University Press. Cambridge, United Kingdom.

11. Springer, P. J. (Eds.) (2017). *Encyclopedia of Cyber Warfare*. ABC-CLIO, California.

12. Sayapin S., Tsybulenko E. (Eds.) (2018). *The Use of Force Against Ukraine and International Law: Jus Ad Bellum, Jus In Bello, Jus Post Bellum*. T.M.C. Asser Press/Springer, The Hague.

13. Valuch J., Hamulak O. (2018) *Cyber Operations During the Conflict in Ukraine and the Role of International Law.* In: Sayapin S., Tsybulenko E. (Eds.) (2018). *The Use of Force against Ukraine and International Law*. T.M.C. Asser Press/Springer, The Hague.

## Scientific Articles:


14. Barbieri, C., Darnis, J. P., Polito, C. (2018). Non-proliferation Regime for Cyber Weapons. A Tentative Study. *Instituto Affari Internazionali.* Issue 18/03, Roma.

15. Beard, J. M. (2018). The Principle of Proportionality in an Era of High Technology. *Institute for Law and Land Warfare Book Series – Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare.* (Eds.) Ford, C. M., Williams, W. S. Oxford University Press, 1-23.

16. Biggio, G. (2017). Cyber Operations and the Humanization of International Humanitarian Law: Problems and Prospects, *Canadian Journal of Law and Technology,* Vol. 15, No. 1.

17. Brown, G. D. (2011). Why Iran Didn't Admit Stuxnet Was an Attack. *Joint Force Quarterly,* Issue 63, 4th Quarter.

18. Dayem, L. (2018). The Ethics of Cyber Warfare. *The Illini Journal of International Security,* Vol 4, No 1.

19. Finlay, C. J. (2018). Just War, Cyber War, and the Concept of Violence. *Philosophy & Technology,* Vol. 31, Issue 3, 357-377.

20. Frankli, A. (2018). An International Cyber Warfare Treaty: Historical Analogies and Future Prospects. *Journal of Law & Cyber Warfare*, Vol. 7, Issue 1, Lexeprint, 149-163.

21. 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.

22. Jensen, E. T. (2017). The Tallinn Manual 2.0: Highlights and Insights. *Georgetown Journal of International Law 48,* No. 3.

23. Korns, S. W., Kastenberg, J. E. (2009). Georgia's Cyber Left Hook. *Army War College Carlisle Barracks PA Strategic Studies Institute,* Carlisle.

24. Mukherjee, S. (2019). Cyber Warfare and Implications. *University of the Cumberlands.*

25. Ottis. R (2008). Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. *NATO Cooperative Cyber Defence Centre of Excellence,* Tallinn, Estonia.

26. 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

27. Reinikainen, M. (2019). Computer Viruses. *University of Eastern Finland,* Faculty of Science
and Forestry, Kuopio

28. Robertson, C. H. II. (2019). Different Problems Require Different Solutions: How Air Warfare Norms Should Inform IHL Targeting Law Reform & Cyber Warfare, *Michigan Journal of Law Reform*, Vol. 52, Issue 4. University of Michigan Law School, 985-1012.

29. Sutherland, I., Xynos, K., Jones, A., Blyth, A. (2015). The Geneva Conventions and Cyber-Warfare. *The RUSI Journal*, Vol. 160, Issue 4, 30-39.

30. Wallace, D. (2018). Cyber Weapon Reviews under International Humanitarian Law: A Critical Analysis. *NATO Cooperative Cyber Defence Centre of Excellence,* Tallinn, Estonia.

31. Wallace, D. A., Jacobs, C. W. (2019). Conflict Classification and Cyber Operations: Gaps, Ambiguities and Fault Lines. *University of Pennsylvania Journal of International Law*, 643-693.

32. Weinberger, S. (2011). Computer security: Is this the start of cyberwarfare? *Nature*, Nature Publishing Group, United Kingdom.

## EU and International Legislation

33. Charter of the United Nations, 26 June 1945

34. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 18 June 1977.

35. Rome Statute of the International Criminal Court, 17 July 1998

36. UN Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water, 10 October 1963

37. UN Amended Protocol II to the Convention on Certain Conventional Weapons, 3 May 1996

38. UN Protocol III to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may deemed to be Excessively Injurious or to have Indiscriminate Effects, 10 October 1980

## Other Sources:

39. *A look at Estonia's Cyber Attack in 2007*. (2009, August 7). The Associated Press, NBCNews.

Retrieved from http://www.nbcnews.com/id/31801246/ns/technology_and_science-security/t/look-estonias-cyber-attack/#.Xk19bi17HUo

40. Allison, J. (2019). Program on International Law and Armed Conflict. *Harvard Law School Library.*
Retrieved from https://guides.library.harvard.edu/c.php?g=310988&p=2079382

41. *Biggest Cyber Attacks 2017: How They* Happened (2017, November 30). Calyptix Security.
Retrieved from https://www.calyptix.com/top-threats/biggest-cyber-attacks-2017-happened/

42. *Cyber warfare: IHL provides an additional layer of protection* (2019, Sept 10). ICRC.
Retrieved from https://www.icrc.org/en/document/cyber-warfare-ihl-provides-additional-layer-protection

43. *Estonian Defence League's Cyber Unit.* Kaitseliit. Estonian Defence League.
Retrieved from https://www.kaitseliit.ee/en/cyber-unit

44. Fruhlinger, J. (2017, August 22). What is Stuxnet, who created it and how does it work? *CSO, IDG Communications.*
Retrieved from https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html

45. Guay, J., Rudnick, L. (2017, June 25). What the Digital Geneva Convention means for the future of humanitarian action. *The Policy Lab.*
Retrieved from https://www.unhcr.org/innovation/digital-geneva-convention-mean-future-humanitarian-action/

46. Krawczyk, L. (2019). How does cyber warfare fit in the framework of International Humanitarian Law? [Blog post].
Retrieved from https://leidenlawblog.nl/articles/cyber-warfare-the-definition-challenge

47. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion of 8 July 1996, ICJ
Retrieved from https://www.icj-cij.org/files/case-related/95/7497.pdf

48. Moseley, A. (2004). Just War Theory. *Internet Encyclopedia of Philosophy*.
Retrieved from https://www.iep.utm.edu/justwar/

49. Passeri, P. (2020, Mar 19). February 2020 Cyber Attacks Statistics. [Blog post]. Retrieved from https://www.hackmageddon.com/2020/04/14/q1-2020-cyber-attacks-statistics/

50. Ranger, S. (2018, December 4). What is cyberwar? Everything you need to know about the frightening future of digital conflict. *ZDNet News.*
Retrieved from https://www.zdnet.com/article/cyberwar-a-guide-to-the-frightening-future-of-online-conflict/

51. Rouse, M. (Eds.) (2019 April). Definition of Distributed Denial of Service (DDoS) Attack. *SearchSecurity,* TechTarget.
Retrieved from https://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack

52. Straub, J. (2019, August 16). A Major Cyber Attack Could Be Just as Deadly as Nuclear Weapons, Says Scientist. *The Conversation.* Retrieved from https://theconversation.com/a-cyberattack-could-wreak-destruction-comparable-to-a-nuclear-weapon-112173

53. Ticehurst, R. (1997). International Review of the Red Cross, No. 317, ICRC. Retrieved from: https://www.icrc.org/en/doc/resources/documents/article/other/57jnhy.htm

54. *What is International Humanitarian Law?* (2004). Advisory Service on International Humanitarian Law, ICRC. Retrieved from https://www.icrc.org/en/doc/assets/files/other/what_is_ihl.pdf

55. Wong, J. C., Solon, O. (2017, May 2). Massive ransomware cyber-attack hits nearly 100 countries around the world. *The Guardian.* Retrieved from https://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs

# APPENDICES

## Appendix 1. Non-exclusive licence

**Non-exclusive licence for reproduction and for granting public access to the graduation thesis[1]**

I Eetu Tulilahti (author's name)

1. Give Tallinn University of Technology a permission (non-exclusive licence) to use free of charge my creation

Applicability of Jus In Bello to Cyber Warfare

*(title of the graduation thesis)*

Evhen Tsybulenko, PhD.

supervised by *(supervisor's name)*

1.1. to reproduce with the purpose of keeping and publishing electronically, including for the purpose of supplementing the digital collection of TalTech library until the copyright expires;

1.2. to make available to the public through the web environment of Tallinn University of Technology, including through the digital collection of TalTech library until the copyright expires.

2. I am aware that the author also retains the rights provided in Section 1.

3. I confirm that by granting the non-exclusive licence no infringement is committed to the third persons' intellectual property rights or to the rights arising from the personal data protection act and other legislation.

[1] *The non-exclusive licence is not valid during the access restriction period with the exception of the right of the university to reproduce the graduation thesis only for the purposes of preservation.*