Univerzita Karlova v Praze
Právnická fakulta

Eva Knopová

Nový MHP rámec pro kybernetickou válku

Diplomová práce

Vedoucí diplomové práce: JUDr. Martin Faix, Ph.D., MJI

Katedra mezinárodního práva

Datum vypracování práce (uzavření rukopisu): 1. říjen 2016

Charles University in Prague
Faculty of Law

Eva Knopová

New IHL Framework for Cyber Warfare

Master's Thesis

Thesis supervisor: JUDr. Martin Faix, Ph.D., MJI

Department of International Law

Date of completion (manuscript closure): 1 October 2016

Prohlašuji, že předloženou diplomovou práci jsem vypracoval samostatně a že všechny použité zdroje byly řádně uvedeny. Dále prohlašuji, že tato práce nebyla využita k získání jiného nebo stejného titulu.

Eva Knopová

I hereby declare that this Master's thesis is a result of my independent work and that all used sources have been quoted duly. I also declare that this Master's thesis has not been used in order to obtain any other or the same degree.

Eva Knopová

Poděkování

Tímto bych chtěla velice poděkovat vedoucímu své práce, JUDr. Martinu Faixovi, Ph.D., MJI za jeho trpělivost, vstřícnost, odborné rady, komentáře a zpětnou vazbu při psané této práce.

Dále bych chtěla poděkovat své sestře Martině a rodičům za trpělivost, podporu a pomoc při psaní této práce jakož po celou dobu mých studií.

Acknowledgement

I would like to express my deep gratitude to my supervisor, Dr. Martin Faix, for his patient guidance, kindness, expert advice, comments and feedback provided during my work on the thesis.

I also wish to thank my sister Martina and my parents for their patience, support and help during my work on the thesis as well as throughout my studies.

Motto: *“I don't know what kind of weapons will be used in the third world war, assuming there will be a third world war. But I can tell you what the fourth world war will be fought with -- stone clubs.”*

Albert Einstein

NEW IHL FRAMEWORK FOR CYBERWARFARE

Contents

SEZNAM ZKRATEK / LIST OF ABBREVIATIONS

CDCOE	NATO Cooperative Cyber Defense Center of Excellence
CERT	Computer Emergency Response Team
CNA	Computer Network Attacks
CNE	Computer Network Exploitation
DoS	Denial-of-Service
IAC	International Armed Conflict
ICC	International Criminal Court
ICJ	International Court of Justice
ICRC	International Committee of the Red Cross
IHL	International Humanitarian Law
ILA	International Law Association
NIAC	Non-International Armed Conflict
NATO	North Atlantic Treaty Organization
NSA	United States National Security Agency
PLC	Programmable Logic Controller
R2P	Responsibility to Protect
Swift	Society for Worldwide Interbank Financial Telecommunication
UN	United Nations

INTRODUCTION

Over the last twenty years, cyber space and its tools have entered all important spheres of human lives including armed conflicts and have reached there dimensions that were absolutely unimaginable when the current Laws of War in particular the International Humanitarian Law (IHL) were created. Yet, these rules designed for a kinetic cyber-free world are currently regulating them.

The purpose of this thesis is to highlight the legal vacuum governing the cyber warfare, cyber weapons and their use in an armed conflict and to advocate for a new IHL convention dedicated to cyber warfare and cyber weapons. It is done so using the qualitative method and legal analysis of the current legal framework including international treaties, customary law and work of the leading instances of international justice as well as writings of judicial scholars and legal and cyber experts.

Divided into five parts, the thesis firstly presents the main aspects of Laws of Wars, its three main regimes, their historical background as well as their theoretical development, and discuss the differences between them with a particular focus on one of them – the International Humanitarian Law.

Similarly, in its second part, the thesis highlights the topic of cyber warfare, divides its weapons into several groups, analyzes their effects and classifies them putting them into the context of relevant legal frameworks while using many practical examples of recent major cyber-attacks.

The third part of the thesis exposes major drawbacks of possible solutions of the legal vacuum related to cyber warfare other than a new treaty, featuring the method of interpretation.

The fourth part of the thesis exposes the key differences between the traditional kinetic warfare and weapons and cyber warfare and cyber weapons and thus provides the main evidence of inapplicability of the current Laws of War featuring International Humanitarian Law onto cyber warfare.

The last chapter provides suggestions of both formal and material aspects of a new IHL Convention on Cyber Warfare including the main issues related to cyber warfare in the context of IHL that will have to be addressed by the international community in the future.

1. KEY ASPECTS OF LAWS OF WAR AND INTERNATIONAL HUMANTIARIAN LAW

Laws of War, a term using a plural case, includes all branches of law related to the war – *jus ad bellum*, *jus in bello* and *jus post bellum*,[1] which all three originate from the just war theory, so called *bellum justum*. The first part of *bellum justum* is created by a set of "just" reasons for engaging in war, in other words *jus ad bellum*.

The *jus in bello*, which consists in law applicable during the time of war, stipulates that war and means of warfare must be regulated and some basic limitations to the conduct in war imposed. The *jus in bello* is the most developed branch of Laws of War, it can be identified today as International Humanitarian Law and will be described further on.

Finally, some scholars begun to include to Laws of War also a third set of war-related rules, so called *jus post bellum*, i.e. the law enforcement and instauration of justice, once the war is over.

1.1 Origins of Laws of War: Just War Theory

1.1.1 Historical Origins of Just War Theory

Essentially, all philosophies and religions consider the concept of war as wrong. On the other hand, under certain conditions, rulers and monarchs used to perceive war as a necessary component of keeping sovereignty over a certain territory. Nonetheless, given that secularized state is a modern concept, a certain consensus between the ruling class and religious authorities on the matters related to governance was needed in the past. Therefore, a theory justifying the act of entering an armed conflict or a certain type of behavior in war, so called "just war theory" was developed.

The origins of its today's form date back to Cicero's *De Officiis*, which appeared in 44 AC. It prescribed that "*war should be formally declared by the proper authority (the fetiales); only official soldiers can fight; there are limits in the conduct of warfare; everyone should respect and offer protection to surrendering enemy.*"[2] Yet, the just war theory has been traditionally associated rather with the Christian doctrine.

The first Christian scholar that developed the just war theory was Saint Augustine, who recognized the right to go to war to governments but not to individuals as such. Nine

[1] Ondřej, J., Šturma, P., Bílková, V., Jílek, D. a kol. *Mezinárodní humanitární právo*, Praha: C. H. Beck, 2010, p. 2

[2] Cicero, *De Officiis*, Cambridge: Harvard University Press, 1961, p. 37

centuries later, Thomas Aquinas, one of the most influential philosophers of scholasticism, deepened Saint Augustine's theory of just war and defined three principles of *jus in bello* as follows: *"Noncombatants must be given immunity; prisoners must be treated humanely; and international treaties and conventions must be honored."*[3]

1.1.2 Just War Theory Today

Today, the theory of just war includes six major principles.[4] First, it contains a just cause to enter war such as mostly a defensive, but in some cases also an offensive, action in the sense of defending a country's territory or population is necessary.

Second, the principle of proportionality prescribes that any undertaken attacks and their effects must be proportional to the scope of violence suffered during the attacks.

Third, right intention aiming to achieve final peace without hostilities and oppressions is needed.

Fourth, Proper authority is considered as legitimate to engage one's country in war and the governor must do so publicly.

Fifth, probability of success must be taken into account. In other words, if a victory is inevitably linked to mass atrocities on population, the country shall not pursue the conflict even if the other just war criteria are fulfilled.

Sixth, the last resort rule says that all possible non-military actions that might lead to a peaceful conflict's resolution must be undertaken before the war begins.

Currently, the just war theory is not codified in any internationally recognized document. The newest concept that is supposed to fill in for the weak states unable to take appropriate measures to protect their own population and territory even in a military manner, if needed, and consequently also aimed at the countries oppressing, threatening or simply not protecting their own citizens is called the Responsibility to Protect (R2P).

The concept is designed in the Outcome Document of the 2005 United Nations World Summit[5] and described in details in the Secretary General's 2009 Report (A/63/677) on Implementing the Responsibility to Protect[6]. It is based on the following three pillars:

---

[3] Burns, J. Patout, ed. *War and Its Discontents: Pacifism and Quietism in the Abrahamic Traditions.* Washington, DC: Georgetown. University Press, 1996, p. 112

[4] Charles, Guthrie, & Michael Q.: *Just War: The Just War Tradition: Ethics in Modern Warfare*, 2007, New York: Walker & Company, p. 17 – 30

[5] Outcome Document of the 2005 United Nations World Summit, p. 30, 24 October 2005

[6] Secretary General's 2009 Report (A/63/677) on Implementing the Responsibility to Protect, 12 January 2009

"*First, the State carries the primary responsibility for protecting populations from genocide, war crimes, crimes against humanity and ethnic cleansing, and their incitement; second, the international community has a responsibility to encourage and assist States in fulfilling this responsibility; and third, the international community has a responsibility to use appropriate diplomatic, humanitarian and other means to protect populations from these crimes. If a State is manifestly failing to protect its populations, the international community must be prepared to take collective action to protect populations, in accordance with the Charter of the United Nations*."

1.2 Definition of War

Having defined the three different legal regimes related to war, it is necessary to define the key element that differentiates them so that it is clear when one legal regime replaces the other, which is the notion of war, more precisely the notion of armed conflict in the contemporary language. Leading philosophers always attempted to provide a universal definition of war. Nonetheless, most definitions were too broad or not universal enough. In the Ancient Rome, Cicero used to define war as "*a contention by force*".[7]

Yet, already Grotius found discrepancies in Cicero's definition and stated the following: "*In treating of the law of war, we have to find out what is war, which is the subject under investigation; what the law, which is sought. Cicero called war a contention by force. Usage, however, holds that not the action, but the state, is indicated by the term 'war,' so that war is the condition of contention by force, as such.*"[8]

Evidently, some philosophical definitions of war appear to be too vague,[9] containing no notion about the most characteristic features of the conventional war from the legal point of view i.e. violence or hostilities, involvement of state (or simply structurally organized actors). On the other hand, generals and military theorists like Antoine-Henri Jomini or Carl Philipp Gottfried von Clausewitz, Prussian general, tried to provide a

[7] Wilson, G. G.: *Handbook of International Law*. St. Paul: West. Publishing Co., 1939, p. 241
[8] Idem, p. 242
[9] See Hobbes: "*A state of affairs, which may exist even while its operations are not continued*" in Hugo Grotius, *The Rights of War and Peace, including the Law of Nature and of Nations,* translated from the Original Latin of Grotius, with Notes and Illustrations from Political and Legal Writers, by Campbell, A.C. with an Introduction by Hill, D. J., New York: M. Walter Dunne, 1901, retrieved 14 September 2015. Or Jacques Rousseau – "*War is constituted by a relation between things, and not between persons […] War then is a relation, not between man and man, but between State and State […]"* in Rousseau, J.J.*: Social Contract & Discourses,* New York: E. P. Dutton & Co., 1913

single definition that would contain the necessary philosophical as well as military characteristics of war.

The most famous and recognized definition of war thus comes from Clausewitz's book definition On War, where he defined war as: *"an act of violence to compel our opponent to fulfil our will."*[10] Additionally, he is also the author of another famous theory on war, so called Clausewitz's trinity, according to which the existence of war depends on the three following features: *"Primordial violence, hatred, and enmity; the play of chance and probability; and the subordination to rational policy."*[11]

Additionally, Friedrich Martens, the representative of Russia at the Hague Peace Conferences 1899 and the author of the Martens clause "*whose writings represent a real dividing line between the period of so-called 'classical' international law and […] the period of ultimately monopolistic position of positivism*,"[12] defined war as: *"That state in which men constantly exercise acts of indeterminate violence against each other; [...] it is private or public; the first takes place between individuals in the state of nature, the second between men in society."*[13]

1.2.1 Currently Recognized Definition of War in IHL: Armed Conflict

However, despite numerous available definitions of the term *war*, none of them became a universal or widely recognized by the international community. In fact, the term itself became consequently replaced by the term "armed conflict", even though there is no official definition of an armed conflict in international law either. The experts of the International Committee of the Red Cross (ICRC) stipulated that an armed conflict arises when there is "*resort to armed force between two or more States*"[14] considering the duration and intensity of such a conflict as irrelevant,[15] which is based on the ICTY judgement in the Prosecutor vs. Dusko Tadic case.[16]

---

[10] Von Clausewitz, C., Howard, M. & Paret, P.: *On War*, Princeton: Princeton University Press, 1989, p. 1
[11] Idem, p.1
[12] Čepelka Č., Šturma, P., *Mezinárodní právo veřejné*, Praha: C.H.Beck, 2008, p. 6 - 7
[13] Martens, G. F. de & Cobbett, W.: *The law of nations: being the science of national law, covenants, power, &c*. London: W. Cobbett, 1829, p. 40
[14] ICRC, "*How is the Term "Armed Conflict" Defined in International Humanitarian Law?",* March 2008.
[15] ICRC, "*International Humanitarian Law and the challenges of contemporary armed conflicts*", October 2011, pp. 7 -8, retrieved 20 July 2016
[16] ICTY, Prosecutor vs. Dusko Tadic, Case No. IT-94-1-AR72; 35 ILM (1996) 32; Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, 2 October 1995

In May 2005, the international community started to question once again what *war*, i.e. *armed conflict*, actually means. The International Law Association (ILA) thus issued the Final Report on the Meaning of Armed Conflict in International Law during the 2010 Hague Conference: *"The Committee found that the term "*armed conflict*" had become especially significant with the adoption of the U.N. Charter in 1945 when the term "*war*" declined in importance. Nevertheless, neither the Charter nor any other important treaty currently defines armed conflict despite the fact that in many subfields of international law it is critical to determine whether or not a situation is one of armed conflict. […]; as a matter of customary international law a situation of armed conflict depends on the satisfaction of two essential minimum criteria, namely: a. the existence of organized armed groups [and] b. engaged in fighting of some intensity."*[17]

In addition, the Final Report confirmed the theory of the objective school on the existence of war or rather an armed conflict, which says that an armed conflict exists when specific criteria are fulfilled regardless any declarations of parties involved in the conflict. Unlike the ILA Final Report, the supporters of the subjective school on the existence of war ignore facts and qualify a state of affairs as an armed conflict or war only if one of the involved parties officially says so.

1.2.2 Different Types of Armed Conflict Triggering Different Legal Regimes

Bearing in mind that there are two decisive features that must be fulfilled in order to call an ongoing series of events war, or an armed conflict, i.e. presence of organized armed groups and fighting or rather hostilities of a certain intensity, today's international law defines four different types of conflicts. Firstly, it distinguishes internal tensions and disturbances described as "*riots, isolated and sporadic acts of violence and other acts of a similar nature.*"[18]

Secondly, once the conflict situation overpasses a certain level of disturbances violence appears but stays within borders of a single country, the situation is qualified as an Internal Armed Conflict, which is also called Non-International Armed Conflict (NIAC).[19] In practice, all the armed conflicts which do not enter any other recognized category (a conflict that surpasses the first category but cannot be qualified as the

[17] ILA: *Final Report on the Meaning of Armed Conflict in International Law*, The Hague Conference, Hague, 2010, p. 32
[18] Article 1(2) of Protocol II to the Geneva Conventions
[19] Article 1(1) of Protocol II to the Geneva Conventions

following two i.e. Wars of National Liberation and International Armed Conflict) are qualified as NIAC including civil wars.

Thirdly, contrary to the NIAC, International Armed Conflict (IAC) is described as "*all cases of declared war or of any other armed conflict 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.*"[20]

Finally, the forth category, so called Wars of National Liberation is defined as a situation when "*peoples are fighting against colonial domination and alien occupation and against racist regimes in the exercise of their right to self-determination."*[21]

However, during the 20th century when states started to interfere into other countries' conflicts by various means that were much more sophisticated than before, including different soft-power economic and diplomatic measures, the borders between NIAC and IAC became more and more blurred.

Nowadays, the disappearance of a clear distinction between NIAC and IAC causes many difficulties in determining if IHL rules apply to a specific conflict or not, since by definition, IHL in general does not apply to Non-International Armed Conflicts but it does contain rules for protection of civilians even during the NIACs (especially the Protocol II).

1.3 Definition of "Attack"

Once an armed conflict occurs, it is the IHL, which applies on the situation, regardless whether the armed conflict has arisen in conformity with jus ad bellum or not. The notion of attack naturally constitutes one of the key terms related to Laws of War in general, however, its legal definition is not the same in all laws-of-war regimes: "*An 'armed attack' is an action that gives States the right to a response rising to the level of a "use of force," as that term is understood in the jus ad bellum. By contrast, the term "attack" refers to a particular type of military operation during an armed conflict to which particular International Humanitarian Law norms apply."*[22]

In *jus ad bellum,* the meaning of the term "armed attack" is derived from the article 51 of the UN Charter: *"Nothing in the present Charter shall impair the inherent right of*

[20] Common Article 2 of the Geneva Conventions
[21] Article 1(4) of Protocol I to the Geneva Conventions
[22] Schmitt, M.N.: *"Attack" as a Term of Art in International Law: The Cyber Operations Context,* Tallinn: NATO CCD COE Publications, 2012, p. 286

collective or individual self-defence if an armed attack occurs against a member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security. Measures taken by members in exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security." This article thus constitutes one of the two lawful exceptions[23] to the ban of the use of force stipulated in the Article 2(4) of the Charter: "*All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations*".

Therefore, the exercise of the right to self-defence does not require a previous authorization by the Security Council and can be used either by the attacked state alone or in a form of a collective defense.

However, although every armed attack constitutes "use of force" not every "use of force" constitutes an armed attack, as stipulated by the International Court of Justice in the so called Nicaragua Case[24], which decided that only use of force of a certain degree, can constitute an armed attack. Nevertheless, the law of war theory still contains a certain gap between what type or amount of use of force already represents an armed attack and which kind and intensity of use of force does not.

Contrary to *jus ad bellum*, the term "attack" in jus in bello i.e. IHL is described as "*a particular category of military operations"*[25] and as such is not derived from the Article 51 of the Charter but from the Article 49 (I) of the Additional Protocol I: *"'Attacks' means acts of violence against the adversary, whether in offence or in defence."*[26] One of the leading IHL experts Michael Schmitt explains that IHL's "attack" *"is a neutral term in the sense that some attacks are lawful, whereas others are not, either because of the status of the object of the attack or how the attack is conducted. Neutral though it may be, "attack" is operatively a key threshold concept in International Humanitarian Law*

[23] The other one is the Collective Action authorized by the UN Security Council as stipulated in the articles 24 and 25, and Chapter VII of the Charter

[24] Nicaragua v. United States of America - Military and Paramilitary Activities in and against Nicaragua - Judgment of 27 June 1986 - Merits - Judgments [1986] ICJ 1 (27 June 1986).

[25] Schmitt, p. 285

[26] Article 49 (I) of the Additional Protocol I

because many of its core prohibitions and restrictions apply only to acts qualifying as such."[27]

In order to avoid any confusions on the following lines between the armed attack in the sense of the Article 51 of the Charter, i.e. the *jus ad bellum* regime, and the Article 49 (I) of the Additional Protocol I, i.e. IHL, the term "armed attack" in its entirety will be reserved for the *jus ad bellum* context, whereas the term "attack" will be used only in the IHL context.

Nonetheless, despite the different definitions of the term attack in *jus ad bellum* and IHL, the both notions face a similar problem when it comes to cyber warfare, which is whether the cyber-attacks can be qualified as "armed attacks" *in jus ad bellum* and/or "attacks" in IHL.

1.4 IHL: Conventions, Scope of Application and General Principles

Today, it is in particular the rules of IHL, which provide official binding definitions of many terms essential to the Laws of War. As a result, this work focuses on cyber warfare in the IHL context but without omitting the important parts of the other two branches of Laws of War, especially then of *jus ad bellum,* as they will be essential at the moment when an international convention on cyber warfare is negotiated. Therefore, it is necessary to further describe the cornerstone conventions that created International Humanitarian Law as well as its scope of application, key notions and principles.

1.4.1 Hague and Geneva Conventions

Concerning the practice of war, the parties involved in war used to agree upon the rules of war, *jus in bello* of their times, before the war itself or each of its battles. Alternatively, some rules of war used to be codified in bilateral treaties. However, most of the conduct in war used to follow the customary Laws of War.

The situation started to change in mid-19th century, catalyzed by two important events: the first organized medical help provided to the wounded on the battlefield regardless the affiliation coordinated by Henri Dunant during the Battle of Solferino in June 1859 and the first formation of a code containing rules of conduct on the battlefield by Francis Lieber called the Instructions for the Government of Armies of the United States in the Field and issued for the Union soldiers during the American Civil War in

[27] Schmitt, p. 285 -286

April 1863. The same year, Henry Dunant founded the Committee of the Five gathering representatives of five highly influential Geneva families to investigate the implementation of providing aid and relief to the wounded on the battlefields. The Committee was shortly after renamed to the International Committee for Relief to the Wounded. In 1876, the Committee was renamed again, this time to the International Committee of the Red Cross (ICRC).

A few years later, in October 1863, the Committee convened the representatives of 16 states in Geneva and finally signed on 22 August 1864 the Convention for the Amelioration of the Condition of the Wounded in Armies in the Field, which became to be known as the First Geneva Convention: "*a set of ten articles that laid down rules designed to ensure that all soldiers wounded on the battlefield – whatever side they were on – were taken care of without distinction*."[28]

After the Russo-Japanesse war in 1906, the main provisions of the First Geneva Convention were adjusted to the conditions of wars at sea and issued as the Geneva Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea.[29]

Whereas by the end of the 19th century, the individual's protection was already covered by the first two Geneva Conventions, there was still no multilateral treaty on the means and methods of warfare. In 1899, the First Hague Peace Conference was in Hague[30] and resulted in the First Hague Convention concerning the laws and customs of war on Land. Its successful ratification process[31] led to the signature of the Second Hague Peace Conference in 1907 and consequently of the Second Hague Convention respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land, which eventually replaced the First Hague Convention between the state parties.

Even though the series of peace conferences was interrupted by the World War I, the states came back to the negotiation table in 1925 when, regarding the events of the World War I, they agreed upon and ratified the Protocol for the Prohibition of the Use in War of

[28] ICCR: *Development of modern International Humanitarian Law*, 13 May 2010
[29] Ondřej, J., Šturma, P., Bílková, V., Jílek, D. a kol. *Mezinárodní humanitární právo*. Praha: C. H. Beck, 2010, p. 96
[30] *idem* p. 97
[31] Ratified by 51 countries, whose list is available at: https://www.icrc.org/applic/ihl/ihl.nsf/States.xsp?xp_viewStates=XPages_NORMStatesParties&xp_treatySelected=150

Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare (so called First Geneva Protocol). In 1929, the Third Geneva Convention on the treatment of the prisoners of war, so called Convention (III) relative to the Treatment of Prisoners of War was issued. Eventually, all three Geneva Conventions were revised in 1949 at the occasion of the adoption of the Fourth Geneva Convention, i.e. Convention (IV) relative to the Protection of Civilian Persons in Time of War along with the Protocol I (1949) relating to the Protection of Victims of International Armed Conflicts.

The last big revision of all Geneva Conventions and the First Protocol took place in 1977 when the Common Article 2 relating to International Armed Conflict including the scope of application of the Geneva Conventions and the Common Article 3 relating to Non-International Armed Conflict, and the protection of the persons *"taking no active part in hostilities, including members of armed forces who have laid down their arms and those placed hors de combat by sickness, wounds, detention or any other cause, shall in all circumstances be treated humanely,"*[32] were adopted.

The most recent modification of Geneva documents dates back to 2005 when the Third Additional Protocol to the Geneva Conventions was adopted modifying thus the part on the Additional Distinctive Emblem in order to introduce a new more globally acceptable ICRC emblem – the red crystal.

1.4.2 Scope of Application

Concerning the scope of the IHL application, the IHL rules are applied: "*only under certain circumstances (the ratione materiae scope of application), during a certain period of time (ratione temporis), in certain territory (ratione loci) and on certain subjects (the ratione personae scope of application)."*[33]

Ratione materiae includes almost all already discussed types of conflicts but to a different extent, since different IHL rules may apply. IHL rules thus apply primarily to IACs. In addition, the Article 3 of the Convention I[34] and the Article 1 of the Additional Protocol II[35] both define the scope of application and applicable rules for NIACs. The

[32] Common Article 3; and Articles 10 – 16 of the of the Protocol I
[33] Ondřej, J., Šturma, P., Bílková, V., Jílek, D. a kol. p. 38
[34] Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Geneva, 12 August 1949
[35] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), Geneva, 8 June 1977

Article 3 of the Convention I covers also the conflict situations qualified as the Wars of National Liberation.

Regarding the *ratione personae* dimension of the IHL applicability, the IHL defines the category of protected persons, which includes a number of subcategories, and stipulates the rules for their protection. The category of protected persons thus includes the following groups: Wounded and sick in armed forces in the field[36]; Wounded, sick and shipwrecked members of armed forces at sea[37]; Medical and religious personnel attached to the armed forces[38]; Prisoners of war[39]; Wounded and sick civilians[40]; Civilian medical and religious personnel[41]; Civilian journalists[42]; Staff of civil defense organizations[43]; Emergency personnel[44]; Civilian population and civilians[45]; Civilians in the power of an adverse party because of the conflict or the occupation of a territory are also protected persons[46]; Detainees, detained or interned[47]; Population of an occupied territory[48]; Women and children[49]; and Foreigners, refugees and stateless persons in the territory of a party to the conflict[50].

However, persons not entering any of the protected person categories may still be protected based on the Common Article 3 and the Article 75 of the Protocol I. In case of the IACs, civilians that "*take a direct part in hostilities*"[51] of course lose their protection against attacks. Civilians in the NIACs are protected from direct attacks "*unless and for such time as they take a direct part in hostilities*."[52]

[36] Article 13 of the Geneva Convention I; and Articles 8 – 20 of the 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.
[37] Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea. Geneva, 12 August 1949.
[38] Articles 24 and 25 of the Geneva Convention I; and Articles 36 and 37 of the Geneva Convention II
[39] Article 4 of the Convention (III) relative to the Treatment of Prisoners of War. Geneva, 12 August 1949.; and Articles 43 – 47 of the Protocol II
[40] Common Article 3; and Articles 10 – 16 of the of the Protocol I
[41] Article 20 of the Convention (IV) relative to the Protection of Civilian Persons in Time of War. Geneva, 12 August 1949.; and Article 15 of the of the Protocol I
[42] Article 79 of the Protocol I
[43] Article 62 of the Protocol I
[44] Article 71 of the Protocol I
[45] Article 51 of the Protocol I
[46] Article 4 of the Geneva Convention IV
[47] Articles 41 - 42 and 79 – 135 of the Geneva Convention IV; and Article 75 of the of the Protocol I
[48] Articles 47 - 78 of the Geneva Convention IV; and Articles 63 and 69 of the of the Protocol I
[49] Articles 76 - 78 of the of the Protocol I
[50] Articles 35 - 46 of the Geneva Convention IV; and Article 73 of the of the Protocol I
[51] Article 51(3) of the Protocol I
[52] Article 13 (3) of the Protocol II

Besides, the protection of civilians was also a subject of the Convention on the Prevention and Punishment of the Crime of Genocide adopted in Paris in December 1948. Next to genocide-related crimes, the protection of civilians addresses also wounding and torturing; rape, sexual violence and sexual exploitation; forced and restricted movement; impoverishment; emotional suffering and post-war suffering. The punishment of the prohibited actions against the civilians are, nonetheless, subject of International Criminal Law and not IHL.

Next to the civilians, the IHL provides protection also to combatants - "*members of the armed forces of a Party to a conflict (other than medical personnel and chaplains covered by Article 33 of the Third Convention) are combatants, that is to say, they have the right to participate directly in hostilities.*"[53]

Moreover, as a group, combatants shall act according to IHL rules[54] and individually respect the obligation to distinguish themselves from the civilian population.[55] In such case, they are considered as privileged combatants and when captured, they shall be treated as a prisoner of war.[56] Combatants that cannot be considered as privileged ones include the combatants that would be qualified as privileged but have breached Laws of War, i.e. mercenaries, spies, child soldiers and *levée en masse*[57]. Even if a captive does not qualify as a privileged combatant, s/he can be still protected according to the Fourth Geneva Convention under certain circumstances.[58]

Additionally, even though not a part of the *ratione personae stricto sensu*, IHL protects also the environment: "*it is prohibited to employ methods or means of warfare which are intended, or may be expected, to cause widespread, long-term and severe damage to the natural environment*."[59] Finally, the Protocol I prescribes that "*Care shall be taken in warfare to protect the natural environment against widespread, long-term*

[53] Article 43(2) of the Protocol I
[54] Under the Protocol I, the combatants are openly carrying arms during the military engagements, which is visible to the enemy during the attack
[55] ibid
[56] Third Geneva Convention
[57] "*The population of a territory which has not been occupied who, on the enemy's approach, spontaneously take up arms to resist the invading troops without having time to organize themselves in accordance with Article 1, shall be regarded as belligerents, if they respect the laws and customs of war*." Article 2 of the Geneva Convention II
[58] Geneva Convention IV
[59] Article 35(3) of the Protocol I

and severe damage. […] Attacks against the natural environment by way of reprisals are prohibited."[60]

1.4.3 General Principles

The main goal of IHL is to avoid the absolute war, i.e. war without limits that could be fatal for humankind. IHL does so mostly by placing limits to the means and methods of warfare, which are stipulated in the IHL treaties as well as in the General Principles of IHL.

The General Principles are generally considered as a part of *jus cogens* and include two types of rules. Firstly, it is the General Principles that prohibit certain effects including the following four:[61] Unnecessary suffering, Military necessity, Proportionality and Indiscrimination.

Secondly, it is the principles that recommend a certain way of conduct featuring one major principle – the principle of precaution.

Along with the General Principles, the IHL theory includes also some specific rules regarding the means and methods of warfare. Firstly, there are IHL specific rules that prohibit certain means of warfare namely the denial of quarter, perfidy, pillage, terror, famine, reprisals against protected persons, capturing and holding hostages, forced recruitment of protected persons, forced movement of civilians and using people as human shields.

Secondly, concerning the methods of warfare, in particular the weaponry, it is divided into several categories according to the restrictions on its use. The first category contains weapons that are prohibited under all circumstances, which in practice concerns mostly chemical and biological weapons.[62] Even though chemical weapons were addressed already in the 1925 Protocol, their development did not progress till 70's and 80's when according to estimations,[63] 25 states were developing chemical weapons. "*Also problematic was the fact that many States that ratified the Protocol reserved the right to use prohibited weapons against States that were not party to the Protocol or as retaliation*

[60] Article 55 of the Protocol I
[61] Ondřej, J., Šturma, P., Bílková, V., Jílek, D. a kol., p. 139
[62] Nowadays, it is the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, adopted in March 1972, entering into force on 26 March 1975 and revised several times during the Review Conferences in 1986, 1991, 1996, 2001 and 2006
[63] UNODA: Chemical Weapons, www.un.org/disarment/WMD/Chemical/

in kind if chemical weapons were used against them." [64] In September 1992, the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction was finally negotiated, singed in 1993 and entered into force on 29 April 1997.

Another category of weapons prohibited in all circumstances is the category of anti-personnel mines covered by the Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction adopted in Ottawa in 1997 (so-called Ottawa Treaty). However, the Ottawa Treaty has not been signed by 34 countries including the biggest state players such as the United States, Russia, China or India.

Similarly, cluster bombs have been prohibited to use under any circumstances by the Convention on Cluster Munitions signed in Oslo in December 2008. Nevertheless, the most important actors on the world political scene like the United States, Russia, China and India as well as many North African and Latin American countries are not, once again, among the signatory state parties.

Moreover, there are some restrictions on the use of certain conventional weapons, too. The Convention on Certain Conventional Weapons restricts the use of certain weapons such as Mines, Booby Traps[65] and Other Devices[66]. The Protocol III of the Convention addresses incendiary weapons[67] and puts restrictions on its use.

Even though "*the first written codification of armament regulation ever was reached in the area of nuclear weapons in order to protect the environment against the harmful effects of nuclear tests*," [68] and despite numerous treaties on nuclear weapons and limitations of their spreading, the issue of nuclear weapons has not been solved yet, which was confirmed also by a very ambiguous final statement of the International Court of Justice from July 1996 and did not really provide any clear answer to the question on legality of the use of nuclear weapons. "*The ban of nuclear weapons as such is not in*

---

[64] ibid

[65] *"Any device or material which is designed, constructed or adapted to kill or injure, and which functions unexpectedly when a person disturbs or approaches an apparently harmless object or performs an apparently safe act."* Art. 2(2), Protocol II)

[66] *"Manually-emplaced munitions and devices including improvised explosive devices designed to kill, injure or damage and which are activated manually, by remote control or automatically after a lapse of time."* (Art. 2(5), Protocol II)

[67] *"Incendiary weapon" means any weapon or munition which is primarily designed to set fire to objects or to cause burn injury to persons through the action of flame, heat, or combination thereof, produced by a chemical reaction of a substance delivered on the target."* (Protocol III, Art. 1)

[68] Ondřej, J., Šturma, P., Bílková, V., Jílek, D. a kol., p. 721

sight and all reflections on a generally valid prohibition of those exist rather in the legis ferendae sphere."[69]

[69] Idem, p.726

2. CYBER WEAPONS, CYBER WARFARE AND IHL FRAMEWORK

In order to answer the ultimate question of this work, which is whether the current IHL framework can apply also on cyber-attacks and cyber warfare, it is necessary to determine the criteria according to which cyber tools can be considered as cyber weapons, name their main types, learn about the effects they can cause and eventually decide whether it is reasonably possible to apply onto them Laws of War, in particular the IHL framework.

2.1 Cyber Weaponry

To find a widely recognized definition of cyber warfare is probably even more difficult than finding a widely recognized definition of war. Despite the fact that cyberspace was recognized by U.S. Deputy Secretary of Defence as a new domain of warfare,[70] there is no official definition of cyber warfare on international level.

The main issue arises in particular when it comes to the relation or similarities between kinetic warfare in customary sense of widely recognized Clausewitz' definition of law and cyberwarfare, since many cyber experts argued that kinetic and cyber war have little in common.[71]

Nevertheless, most definitions of the term war including the Clausewitz' one do not contain any notion of which type of environment the war should be led in and how the war space can influence the existence of armed conflict per se.

In other words, no type of space has been excluded as impossible for war to take place in. However, the main reason for not questioning the type of space while defining war is the historical aspect of practically all widely recognized definitions of war, which disabled to take the cyber space into account. Therefore, the status of cyber space and its parallel to land, air or water constitutes a grey area of IHL as well as the extent of the parallel between kinetic warfare and cyber warfare.

One of the most well-known definitions of cyber warfare comes from a US cyber security expert, Richard A. Clarke, who defined cyber warfare as: "*actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing*

[70] Lynn, W. J.: *Defending a New Domain: The Pentagon's Cyberstrategy,* Foreign Affairs, September - October 2010, p. 101

[71] Schneier B.: *Threat of 'cyberwar' has been hugely hyped,* retrieved 7 July 2010

damage or disruption."[72] In conformity with Clarke's definition and for the purposes of the following lines, only the elements present solely in the cyber space and not in the physical space will be considered as relevant, i.e. drones and other similar devices lying on the border of cyber space and conventional weaponry will not be considered as cyber weapons and thus not an object of this work.

Regarding the cyber weaponry, it includes only the weapons that exist solely in cyber space, i.e. the computer network attacks (CNA),[73] which are: "*actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.*"[74]

The CNA are divided according to the action they cause into syntactic attacks and semantic attacks. The first category of attacks is caused by cyber weapons known as malware, in other words malicious software that aims to harm or destroy IT facilities including computer networks, their components or systems dependent on them.

On the other hand, semantic attacks do not attack computers directly but try to modify data available to users instead. In practice, the semantic attacks modify information published on an official website or in a computer network database. As a result, instead of causing harm to computers, IT networks or their users directly, the semantic attacks harm the end users of the information transmitted by computers. Both types of attacks are extremely dangerous, however, the syntactic attacks are considerably more developed, more popular and more differing in terms of forms, actions and possible consequences.

Therefore, the main types of syntactic attacks will be presented including examples of the ones that have been developed by state actors and recently used as cyber weapons plausibly as complements of conventional armed conflicts or as vanguards of new upcoming armed conflicts. CNA differ in several key features including the fear factor, which is the reaction provoked by a CNA that caused it, the spectacular factor, which depends on the level of actual damages caused by the CNA, and the vulnerability factor, which describes the ease to attack the aimed IT facility.

One of the most important terms regarding the CNA is the zero-day vulnerability, which stands for a defect in a software discovered by hackers by unknown or unfixed by its producers. Some hackers focus only on revealing the vulnerabilities and making them

[72] Clarke, R. A. et Knake, R. K.: *Cyber War: The Next Threat to National Security and What to Do about It*, New York: HarperCollins, 2010, p.32
[73] Dinniss, p. 4
[74] US Department of Defense, DOD Dictionary of Military Terms Online

public so that others including state actors can freely exploit them. The zero-day vulnerability thus constitutes an important element in the world of cyber warfare and quickly became one of the most favorite ways of hackers how to enter or attack computer networks.

Nonetheless, in order to be able to determine which types of cyber-attacks could be potentially qualified as armed conflicts, since some types of cyber-attacks can indeed effectively shut down electric grids, waterworks and power plants or IT systems navigating kinetic weapons or managing public facilities and systems in urban areas and the others that do not constitute the same risks despite their usefulness for espionage, it is necessary to describe the main categories of different malware and cyber-attacks including their effects.

First of all, there are two different categories of CNA – types of cyber-attacks and types of malware. First, there are nine different types of attacks; second, there are at least five major different types of malware, which constitute each a different type of cyber weapons, and each of these types launches a different kind of attack.

Regarding the types of attacks, the most well-known and well-spread CNA include:[75]

- Eavesdropping, which describes sniffing, snooping or simply monitoring one's unsecured, unencrypted IT traffic;
- Data Modification, a typical semantic attack;
- Identity Spoofing, in other words a falsely assigned or assumed IP address including thefts of IP addresses and their abuse for hacking purposes;
- Password Attacks, which are the cyber-attacks based on hacking password-protected user's accounts either via bypassing the password protection or gaining the valid password associated with the account thanks to phishing, additionally if the user has the position of administrator, the hacker can also abuse all the administrator's rights including access control, gaining information on other users, adding or deleting users or data, modifying server and network configurations etc.;
- Denial-of-Service (DoS) Attacks, which are on the borders of the syntactic and semantic CNA because DoS attacks eventually harm the end users by blocking certain functions or directly preventing their access to the targeted website for

[75] Monte, M.: *Network Attacks and Exploitation: A Framework*, Indianapolis: Wiley, 2015, p. 38

days or even weeks by sending too much invalid data to the website, its providers, the website's related services or applications;

- Man-in-the-Middle Attack, which is another level of eavesdropping, since the attacker does not only monitor or record the IT traffic but can also redirect its flows so that it passes through servers of the attacker before reaching its destination, or they can also directly overtake the communication pretending to be the initial sender or receiver;
- Compromised-Key Attacks, which are based on obtaining a secret key, i.e. code or information necessary for decrypting data, are misusing it;
- Sniffer Attacks, which focus on network packets and network data exchange including the ability to shut the network down;
- Application-Layer Attacks, which attack server's operating system resulting in gaining an access control to a network including administrator-type of rights to modify or even shut the network down.

Concerning the different types of malware, despite the fact that computer virus, self-injecting and self-reproducing malware, is probably the most well-known type of malware, it is used less and less. A typical virus replicates itself and deletes or modifies data and hard-drive boot sectors. It can also modify its digital footprint or get automatically attached to selected types of files.

Nonetheless, the most of today's computer "viruses" are actually so-called computer worms or Trojan horses. Worms can be transmitted even without being attached to another file, which increases the speed of their dissemination and as a consequence, also their vulnerability and fear factors.

Probably the most popular type of malware used by state actors is a Trojan horse. Trojan malware is installed by the victim that mistakenly takes it for a different (useful) software or an update of one of the programs already installed on their computer and thus can obtain an access to the affected computer, to related local area networks but also global ones. Normally, Trojan malware tries to hide from the user of the infected computer and sometimes can operate even when the computer is disconnected from the Internet or when powered off. Unlike the previous malware categories, Trojans usually do not replicate themselves, though.

Regarding the concealment, there is, in fact, a special type of malware, so-called rootkit, whose main purpose is to hide the malware from the user. Another type of malware, which has rather complementary effects and appears mostly along with other malware, is the backdoor. When it enters the IT system, it stays there in order to bypass further authentication procedures and provide an access to the system to its master or its other malware.[76]

2.2 Beginning of a New Era of Warfare: Cyber Attacks in Practice

Even though the theoretical types of cyber-attacks or malware might still seem as insufficient in order to be considered as an armed conflict in IHL, in order to decide whether cyber-attacks can constitute a separate category not only of weapons but of whole warfare and consequently need a special IHL treaty to regulate their use, one should examine above all the so-far cyber-attacks that have already appeared in practice and whose creators were most probably state actors. The evidences that some of the most serious past cyber-attacks were not of private but of a country's origin and aimed at another state entities are numerous.

First, the costs of developing a complex system not of one but of multiple malwares, which act in a complementary manner, suggest that their authors can be only entities with a large budget available for investing into development of cyber weapons, which are sovereign countries: "*Developing and operating such a professional malware campaign is extremely expensive and requires resources beyond those of everyday cybercriminals. The cost of developing and maintaining such a malicious framework is colossal: we estimate it to be around $50 million,"*[77] stated a Kaspersky Lab's cyber expert regarding the Duqu 2 malware.

Second, no matter who invest the large amounts of money into development of cyber weapons, the entity does not do it for financial purposes. Even though for instance the Trojan Gauss, a part of the Stuxnet family of malwares detected by Kaspersky Lab in August 2012, was collecting data about bank accounts and financial transactions for several months or even years in the Middle East but it was not used for hacking the accounts nor stealing the money from them.

[76] Idem, p. 39.
[77] Gilbert, D.: *Duqu 2: The most advanced cyber espionage tool ever discovered,* Kaspersky Lab, 10 June 2015

Third, some of the past cyber-attacks clearly constituted a response to actions of public state entities or private entities having a crucial role in functioning of the targeted country and came from the hackers of the same nationality. Therefore, it is reasonable to assume that their state authorities played a role at least in encouraging these cyber-attacks if not directly sponsoring or ordering them.

The best example is the series of cyber-attacks, concretely DoS attacks aimed at important websites of official Estonian entities including websites of Estonian parliament, ministries, the largest banks, newspapers and other media in May 2007 from Russian hackers provoked by removal of a Soviet soldier's statue.[78]

Nonetheless, as under the jus ad bellum nor NATO framework were the cyber-attacks considered as an armed attack,[79] the organization could not launch its defensive mechanisms, which qualify as collective defense under the Article 5 of the North Atlantic Treaty, which is conform to the Article 51 of the UN Charter. The NATO stand has though changed in June 2016, when its Secretary General Jens Soltenberg stated that a cyber-attack could trigger the defensive mechanism of the organization.[80]

The 2007 cyber conflict in Estonia constituted also the first time in history when a state entity fully used the anonymity of cyberspace and declined its responsibility for officially recorded serious cyber-attacks, potentially able to be qualified as armed attacks, in another country.

In fact, the practice of denying a very existence of war or and armed conflict has become common since the 20th century: "*The state of war is a matter of states' judgement and as such states do not have to be recognize it. Since the Word War II, the practice of states shows in the vast majority of cases that the states prefer not to consider a common conflict as war. Nonetheless, even in these cases, the states that are the third parties to the conflict can recognize this de facto war for war in a legal sense.*"[81]

However, in a traditional armed conflict, even though the situation when an attacking country is denying the presence of its military forces in certain territory or use of airstrikes is not unprecedented, there is always a moment when the identity of attackers is revealed and the responsible country cannot deny its responsibility anymore. However, this is not

[78] Traynor, I.: *Russia accused of unleashing cyberwar to disable Estonia*, The Guardian, 17 May 2007
[79] Idem
[80] *Stoltenberg: Kybernetický útok na NATO bude důvod ke kolektivní obraně*, Lidové noviny, 14 June 2016
[81] Ondřej, J.: "*Právo ozbrojených konfliktů na přelomu tisíciletí,* Mezinárodní vztahy - Severní Amerika, 34, December 1999

the case in cyber warfare, where cyber-attacks may gain unprecedented measures and paralyze the targeted country for several days, weeks or even months but without any direct evidences how to convict the attacking state entity.

Last reason why there are clearly state entities behind the majority of the most serious cyber-attacks, which happened over the past years, and why the cyber-attacks can constitute a real armed-attacks *in jus ad bellum* and/or also the attacks in the sense of IHL and not only a tool for monitoring and espionage purposes, is their active role and the purpose to cause serious damages, which was characteristic to several complex malware systems.

The most well-known case is the Stuxnet malware that was officially disclosed in June 2010 as the malware that destroyed plausibly the whole or at least a considerable part of the nuclear program facilities operated on Siemens hardware.[82] However, its existence in Iranian nuclear facilities already in 2005 was proven later on. Even though most of the public learned about the revelation of Stuxnet, only a few of media completed the picture with the other malwares that were discovered either before or after Stuxnet but which clearly acted as its complements.

Despite their different characteristics and tasks, the disclosed malwares appeared to be interconnected, acting complementary with each other, all aiming at the Middle East and containing parallel source code characteristics.[83] Stuxnet itself was the first worm ever that acted without a need of any remote control or internet access thanks to a programmable logic controller rootkit (PLC). Spread mostly via USB flash drives and local networks and targeting the Microsoft Windows operational system through the man-in-the-middle type of attack, it targeted only controllers operating on Siemens hardware, which was known to be used in Iran. The worm was disclosed to the public in one of the Kaspersky Lab's reports, which underwent a severe DoS attack only a day before the publication of the report resulting in a part of the report being destroyed.[84]

[82] Langner, R.: *Stuxnet: Dissecting a Cyberwarfare Weapon,* IEEE Security & Privacy, 9(3), 2011, p. 49-51
[83] Collins, S. and McCombie, S.: *Stuxnet: the emergence of a new cyber weapon and its implications,* Centre for Policing, Intelligence and Counter Terrorism (PICT), Macquarie University, 21 March 2012
[84] Fidler, D. P.: *Was Stuxnet an Act of War? Decoding a Cyberattack*, IEEE Security & Privacy, 9(4), 2011, p. 56 - 59

Moreover, in spite of the fact that the Stuxnet's date of death, i.e. the day when a worm stops spreading, was recorded on 24 June 2012, another of its attacks was recorded again in Iranian power plants on 25 December 2012.[85]

But Stuxnet was not the only malware detected in Iran in 2000's. In September 2011, the Hungarian CrySyS (Laboratory of Cryptography and System Security) detected zero-day vulnerability spyware called Duqu, which collected information and stealing digital certificates especially in industrial control systems in the Middle East including Iran.[86] Its new version Duqu 2.0 was revealed in June 2015 by Kaspersky Lab. Although the authorship of Stuxnet family of malwares was attributed to the US and Israel, the speculated author of the Duqu 2.0 is solely Israel, since it was used for spying on Iranian authorities in the time of the negotiation of the nuclear deal with the USA: "*They [Kaspersky Lab] found out that the same virus had been used to infiltrate a series of other targets in the West and the Middle East, including, most notably, hotels where the Iranian delegates met with the P5+1 group to discuss Tehran nuclear ambitions*."[87]

Other malwares of the Stuxnet family included Gauss described above, Shamoon virus discovered also in the Middle East and similar to Gauss but targeting oil and energy sector facilities, which was described by Symantec in August 2012,[88] and finally Flame, disclosed in May 2012 by Kaspersky Lab, CrySyS and Iranian National Computer Emergency Response Team (CERT). The malware spread via LANs or USB disks and could not only monitor and record data but also take screenshots, record audio data through internal microphones of computers even when hibernating and actively collect data about other Bluetooth devices in the area.[89]

The Iranian CERT learned about the malware due to the cyber-attack in April 2012, which severely disrupted functioning of the Iranian oil terminals in the North-West of the country.[90] Eventually, the traces of Flame were discovered also in the French presidential office.[91]

---

[85] Collins, S. and McCombie, S., p.15
[86] Hossein, J.: *Iran says has detected Duqu computer virus,* Reuters, 13 November 2011
[87] Bacchi, U.: "*Israeli-linked malware Duqu 2.0 'used to spy on Iran nuclear talks venues",* International Business Times, 10 June 2015
[88] Symantec: *The Shamoon Attacks*, August 2012
[89] CRySyS Lab: *sKyWIper: A Complex Malware for Targeted Attacks,* Budapest University of Technology and Economics, 2012, 28 May 2012
[90] Hopkins, N.: *Computer worm that hit Iran oil terminals 'is most complex yet*, The Guardian, 28 May 2012
[91] *Flame: Israel rejects link to malware cyber-attack*, BBC News, 31 May 2012

2.3 Recognition of Cyber-Attacks by the International Community

Despite the demonstrated evidences that cyber-attacks constitute a serious threat for international security and possible extremely efficient means of warfare, the fact that they are being used more and more by states and against other state actors as well as the most recent development when they have been gaining both on frequency and intensity, the international community as whole has been successfully ignoring their actual importance and scale, refusing to appropriately reflect them in international law.

So far, when the international community has ever tackled any cyber-related question, it has been always in the context of international security[92] and jus ad bellum regime, but the question of cyber warfare in the IHL context is unfortunately remaining untouched on the ground of the United Nations, being discussed only on regional platforms, namely the NATO and its Tallinn Manual initiatives. Even international law experts and scholars have not been examining the topic of application of IHL onto cyber warfare too deeply, preferring to focus on the international security and jus ad bellum aspects.

For instance Michael N. Schmitt from the US Naval War College argues that the cyber-attack cannot qualify as an armed attack in the sense of article 51 of the UN Charter due to the lack of severe damages directly caused by the malware: "*A recurring question in the cyber context is whether the damage or destruction or manipulation of data that does not generate such consequences is capable of qualifying as an armed attack. Generally it does not, for so qualifying such action would dramatically lower the threshold at which States would enjoy a right to forcefully respond to actions directed at them."*[93]

He thus argues that the interpretation of the Article 51 of the Charter should stay very restrictive, since it is above all the Security Council and its power to authorize collective action that should be the first and main instance according an exception to the general ban of the use of force and that the Article 51 should serve rather as the "last resort" for the armed attacks, which according to him, clearly do not include the cyber-attacks, though.

[92] Within the UN system, the cyber domain is covered by the International Telecommunication Union and in the security and conflict-related context by the *United Nations Group of Governmental Experts (GGE)*, whose work is reflected in regular Reports of the Secretary General and significantly contributed also to the most recent General Assembly resolution related to cyber and international security context – resolution 70/237 entitled "*Developments in the field of information and telecommunications in the context of international security*" adopted on 23 December 2015

[93] Schmitt, M.N.: "Attack" as a Term of Art in International Law: The Cyber Operations Context, NATO CCD COE Publications, Tallinn, 2012

He goes even further and claims that conducting cyber-attacks on civilians is lawful as long as they do not qualify as armed attacks: *"The most important of these prohibit attacks on civilian objects and mandate various precautions that must be taken during an attack to avoid harming the civilian population and civilians. Simply put, the prohibition on directing military operations against civilians, civilian objects and other protected persons and objects must be understood as essentially a prohibition on attacking them. Conducting military operations that do not qualify as attacks against them is, in a general sense, lawful."*[94]

Schmitt defends his controversial position by arguing that cyber-attacks, which do not directly cause serious damages to the civilian population in terms of severe injuries and deaths are not considered as armed attacks and thus permitted: "*Cyber operations can be directed at civilian systems so long as the requisite type of harm is not triggered and no other specific International Humanitarian Law prohibition (such as those attending medical operations) applies."*[95]

However, some of the most relevant international organizations in the area – the International Court of Justice and the ICRC published statements directly or indirectly approving the possibility to qualify cyber-attacks as armed attacks. In its Nuclear Weapons advisory opinion, the ICJ stated that "*These provisions [i.e. those of the Charter] do not refer to specific weapons. They apply to any use of force, regardless of the weapons employed. The Charter neither expressly prohibits, nor permits, the use of any specific weapon, including nuclear weapons. A weapon that is already unlawful per se, whether by treaty or custom, does not become lawful by reason of its being used for a legitimate purpose under the Charter."*[96] Although issued for the purposes of nuclear weapons classification, the statement is clear and general enough to be legitimately applied also onto cyber weapons.

Therefore, the question what exactly the cyber-attacks are able to cause in practice arises. Besides the above described malwares and their actions, the standard malware operations feature especially the Remote Access tools consisting of monitoring the traffic of the networks the affected computer is connected to, overtaking the control over the affected computer (including its navigation tools such as a touchpad or mouse), capturing passwords, making audio and video records, all communication including social media

[94] Idem p. 289
[95] Idem p. 292
[96] *Legality of the Threat or Use of Nuclear Weapons,* I.C.J. Advisory Opinion, 1996, par.39, 8 July 1996

and e-calls, redirecting to command and control servers, recovering deleted files, self-reproduction and self-deletion.

A great example concentrating the most popular Remote Access features was the Red October, a Trojan revealed by Kaspersky Lab in October 2012 but active at least since 2007. Trojan written by Russian speakers was able to monitor and steal data from computers, network devices (Cisco), removable hard drives (counting also deleted files) and smartphones. The malware focused mostly on EU institutions, embassies, government bodies and governmental research institutes.[97]

Another highly important spying back-door malware, NetTraveler, revealed to the public in June 2013 but dating back to as early as 2004, affected over "*350 high profile victims in 40 countries."*[98] Kaspersky Lab indicates that the malware was written by Chinese speakers and targeted especially: "*Tibetan/Uyghur activists, oil industry companies, scientific research centers and institutes, universities, private companies, governments and governmental institutions, embassies and military contractors.*"[99]

Finally, in February 2015, Kaspersky Lab disclosed probably the most sophisticated group of cyber attackers called the Equation Group and assigned it to the US National Security Agency (NSA). The group had used two zero-day attacks identical to the ones launched by Stuxnet even before Stuxnet used them.[100] Kaspersky cites: "*thousands, or perhaps even tens of thousands of victims in more than 30 countries worldwide, covering the following sectors: Government and diplomatic institutions, Telecommunications, Aerospace, Energy, Nuclear research, Oil and Gas, Military, Nanotechnology, Islamic activists and scholars, Mass media, Transportation, Financial institutions and companies developing encryption technologies."*[101]

Moreover, today, the most sophisticated malwares do not target only computers running on Windows but contain versions also for Linux and iOS as well as versions for Android so that they can attack smartphones, too, like the Mask, a multiple back-doors malware disclosed in February 2014.[102]

---

[97] Securelist: *"Red October" Diplomatic Cyber Attacks Investigation*, 14 January 2013, p.3
[98] Kaspersky Lab: *NetTraveler Attacks,* Part 1, 4 June 2013
[99] Idem p. 3
[100] Kaspersky Lab: *Equation Group: The Crown Creator of Cyber-Espionage,* 16 February 2015
[101] Idem
[102] Kaspersky Lab: *Unvealing "Careto" – The Mask "APT",* February 2014, p.4

Nonetheless, there is a clear need to make a difference between espionage malware and malware constituting an armed attack, since a malware used only for espionage is clearly not setting off an electric grid or a power plant.

On the other hand, it is necessary to acknowledge the power that the cyber-attacks have and set up a clear international public law framework for international community defining when a cyber-attack does constitute an armed attack in conformity with the Article 51 of the Charter.

Regarding the IHL state of affairs, as it is being even less explored and discussed in relation to the cyber warfare than in the jus ad bellum regime, the discussion on qualification of a cyber-attack as an attack in IHL is practically nonexistent on the ground of the United Nations and very limited amongst scholars.

However, the most respected international organization in the field of IHL, the ICRC has recognized that a cyber-attack can be qualified as attack in IHL. In its publication at the occasion of the 37th International Conference of the Red Cross and Red Crescent Society in 2011, the ICRC issued an article including a stance on cyber-attacks and the possibility to qualify them as armed attacks: "*Cyber operations by means of viruses, worms, etc., that result in physical damage to persons, or damage to objects that goes beyond the computer program or data attacked could be qualified as 'acts of violence', i.e. as an attack in the sense of IHL. […However,] cyber operations do not fall within the definition of 'attack' as long as they do not result in physical destruction or when its effects are reversible."*[103]

The ICRC also underlined that "*the fact that a cyber-operation does not lead to the destruction of an attacked object is also irrelevant*."[104] Regarding the qualification of cyber-attacks as armed attacks according to the level of destruction or damages they cause, the IRCRC stated that: "*Pursuant to article 52 (2) of Additional Protocol I, […]the definition implies that it is immaterial whether an object is disabled through destruction or in any other way."*[105]

[103] ICRC: *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts,* Report 31IC/11/5.1.2, 31st International Conference of the Red Cross and Red Crescent, October 2011
[104] Idem p. 37
[105] Idem p. 37

3. DRAWBACKS OF APPLYING THE CURRENT LAWS OF WAR ON CYBER WARFARE

In regard to the new type of warfare, in particular its more and more developed forms and rising popularity, the international community, or at least some of its members, along with international law experts begun to look for options how to include cyber warfare into the Laws of War.

As a result, and possibly also the easiest solution, the current mainstream opinion on the legal rules applicable to cyber warfare is that the currently valid Laws of War, especially the IHL Conventions, apply to cyber warfare and cyber weapons accordingly.

Notwithstanding the lack of any agreement amongst the international community on such approach, let alone the lack of existence of any official document that would set rules which authority or according to which parameters the IHL Conventions should be interpreted when applied on cyber warfare, some interpretation efforts have already started on regional levels and amongst legal scholars.

The following chapter will therefore describe these efforts and point out their shortcomings and limits in the purpose to prove that a mere (re)interpretation of current IHL conventions cannot constitute an efficient solution to the implementation of cyber warfare into the IHL framework featuring the shortcomings of the main IHL principles when confronted with the nature of cyber-attacks, the insufficient level of legitimacy of the authorities interpreting the IHL and consequently a possible lack of respect and law enforcement of their outcomes by the international community as well as the severe discrepancies in the so-far efforts of legal scholars to apply the current Laws of War rules onto cyber-attacks.

3.1 General Drawbacks of Applying the Laws of War on Cyber Warfare by the Method of Judicial Interpretation

Regarding all the challenges of legal interpretation connected to the current IHL principles written for kinetic warfare, one could think of having them interpreted by the institutions dedicated to international justice. However, there are several main reasons why a judicial interpretation of IHL Conventions for the cases of cyber warfare would not be enough.

First of all, there is undeniable disproportion of the authority of legal scholars to the weight of an international convention that has been signed and ratified by a large number

of states, especially in the issues of a high importance, let alone Laws of War, which is definitely the case of cyber warfare.

In fact, all three branches of Laws of War heavily rely on consensus of the whole international community. First, in *jus ad bellum*, which includes the maintaining of peace and the right of self-defense featuring Article 2(4), Article 24 and 25, Chapter VII and Article 51, it is only either a Security-Council resolution or the consensus of Member States in the UN General Assembly, which dispose with the legitimacy of the international community, even though the latter does not even have a binding effect.

There is a parallel situation in *jus in bello*, i.e. IHL, where the legitimacy lies in the Conventions signed and ratified by the majority of countries. Lastly, in *jus post bellum* i.e. International Criminal Law, the legitimacy is very fragile and is effective only when established *ad hoc.* Thus, the International Criminal Tribunal for the Former Yugoslavia and the International Criminal Tribunal for Rwanda can be overall judged as bringing positive results in terms of interpreting the IHL and war crimes in particular.

Additionally, the concept of an obligatory globally universal jurisdiction itself is heavily contested up to nowadays and even in the matters of grave breaches of IHL instaured by the 1949 Geneva Conventions: "*Four Geneva Conventions of 1949 have not only defined grave breaches (Articles 50/I, 51/II, 130/III, 147/IV) and provided for their investigation and prosecution, but set up also the obligatory universal jurisdiction of States Parties with respect to the grave breaches (Articles 49/I, 50/II, 129/III, 146/IV). It is a kind of paradox that in 2009, after 60 years from the adoption of the Geneva Conventions, the universal jurisdiction is perceived, by a number of States, mostly developing States, as being problematic. As evidence, there is a recent proposal of the African Union leading to the adoption the adoption the UN General Assembly resolution on "The scope of application of the principle of universal jurisdiction."*[106]

Taking into account the character of cyber warfare, there are two possible situations when bodies of international justice could intervene and help establish new customary law related to cyber warfare. Firstly, shall the question of cyber warfare be treated a priori to a major cyber-attack causing massive atrocities, the International Court of Justice could issue an advisory opinion on cyber warfare upon obtaining related questions referred by

[106] Šturma, P.: *Universal Jurisdiction and Prosecution of Grave Breaches of The Geneva Conventions of 1949*, Acta Universitatis Carolinae Iuridica, 2009 (4), p.184

authorized United Nations organs and specialized agencies or theoretically also when judging a legal dispute submitted to it by the United Nations Member States.

Secondly, in certain *post bellum* cases related to cyber warfare – cases when cyber-attacks would cause major atrocities, it could be the International Criminal Court that would help create the international legal framework for cyber warfare, if applicable (i.e. prosecution of individuals for the international crimes of genocide, crimes against humanity, war crimes, and theoretically crimes of aggression, provided that the national jurisdiction cannot or does not have the will to do so).

However, the option that it would be one of the international justice institutions that would provide an interpretation of cyber-attacks for Laws of War including the IHL and international criminal law is highly improbable for three main reasons.

Firstly, the cyber-attack would have to be of a great measure and consequences, which would be publicly revealed. Secondly, the institutions of international justice, depending on their jurisdiction, can resolve disputes either between States or judge individuals but none of them can solve cases between a state and a non-state actor, which is, however, one of major potential author of offensive cyber-attacks. Thirdly, the author of the atrocities, in other words the accused parties, should be known, which is not that easy in the context of the cyber warfare.

Besides, there have been already some serious issues with recognizing legitimacy of some international justice bodies in the past. For instance, the USA withdrew from the ICJ's general jurisdiction and decided to obey it only on ad hoc basis after the Nicaragua vs. United States case in 1986. Moreover, the difficulties connected to enforcing judgements of international justice institutions are often embodied in the rules of the functioning of the international community.

For example, the ICJ cannot enforce its rulings but it is the Security Council that has the authorization to do so, which would not make future ICJ decisions issued in the context of cyber warfare extremely legitimate in the eyes of the members of international community that are not members of the Security Council regarding the fact that they have not even agreed to any underlining principles, which would govern the domain of cyber warfare.

Concerning the International Criminal Court (ICC) and the general legitimacy of its jurisdiction, it is equally questionable given the fact that the largest world powers including the United States, Russia China, India, Saudi Arabia and others have not ratified

or some of them not even signed the Rome Statue, which constitutes the ICC's founding document. What is more, both the ad hoc established international criminal courts and tribunals and the universal ICC with general jurisdiction have interpreted IHL rules in the context of crimes and weaponry the IHL Conventions were written for.

If the biggest powers of this world were not even able to recognize legitimacy of the ICC because of its general jurisdiction but with well-known and clearly defined scope of the type of situations and objects the rules should be applied to, it is highly doubtful that they would recognize legitimacy to interpret the currently binding IHL Conventions upon a completely new type of warfare to the ICC or a similar body of international justice.

Finally, there is also a belief that a new Convention on cyber warfare is not needed now because a new set of rules of cyber warfare should be created via establishing new customs of IHL a posteriori.

However, such a stance presumes that the world should wait for a series of cyber-attacks that would cause damages on the level of massive atrocities and then wait how those cyber-attacks would be solved by the international community in conformity with Marten's clause.

Nonetheless, it might be extremely dangerous to just wait while twiddling our thumbs and not considering the eventual aftermath and the price of such a waiting period, which would be extremely hazardous regarding all possible hostilities, damages, including major loss of human lives especially in parallel to the use of nuclear weapons at the end of the World War II when no international law regulations applied to them.

3.2 Drawbacks of the Method of Interpretation Specific to the IHL Conventions

There are several reasons why the method of interpreting the current IHL conventions will not be able to work in practice, namely because of the issue of applying the current underlying IHL principles including the classification of cyber weapons, as well as the obstacles in applying the principles of military necessity and proportionality onto cyber warfare.

Secondly, there is a rather technical issue related to cyber warfare that would be difficult to be judged by anybody else than the whole international community in the form of a new binding document, therefore a new IHL Convention, which is the question of how to classify cyber weapons.

Regarding their relative easiness to get out of control even in cases when they are precisely targeted and a possible chain reaction of unpredictable actions they could launch and which would be absolutely unanticipated by their producers, cyber weapons might be possibly qualified as blind weapons that are "*incapable of distinguishing between civilians and military targets*."[107]

As such, they could be de facto banned by the ICJ's Advisory Opinion on Nuclear Weapons: "*States must never make civilians the object of attack and must consequently never use weapons that are incapable of distinguishing between civilian and military targets*"[108] on the basis of one of the underlining rules of IHL, the protection of civilian population and civilian objects.

Unlike a kinetic attack, which can also cause unwanted damages or even life losses in case of a bad or imprecise targeting or just due to an extremely increased density or mixture of civilians and military objects, a cyber-attack targeted purely and precisely on military objects can have truly unthinkable consequences on civilian objects and lives due to the networks shared by civilians and armed forces.

For example, the US military communication passes in general via civil computer networks making them a possible target for cyber-attacks.[109]

But the principle of the protection of civilian population is not the only issue, which could not be solved only via interpretation by an international justice authority. There are also the principles of military necessity and proportionality, which pose serious IHL dilemma.

For instance, if cyber weapons were fully recognized as means of warfare, the situations where the principle of proportionality would require the use of kinetic weapons as a response to an attack by cyber weapons could occur.

However, the large scale of actions and effects that cyber-attacks can have and the constantly growing speed of their development would make any decision taken in this regard by any single authority and not the international community highly challengeable by all the disagreeing countries.

---

[107] Y. Dinstein: *The Principle of Distinction and Cyber War in International Armed Conflicts*, Journal of Conflict & Security Law, Vol. 17, No. 2, 2012, p. 262

[108] Legality of the Threat or Use of Nuclear Weapons, I.C.J. Advisory Opinion, par.78, July 8 1996

[109] Dinnis, H. Heather: *Cyber Warfare and the Laws of War*, Cambridge University Press, Cambridge 2012, p. 187

Moreover, in case of aggressive cyber-attacks, the principle of military necessity would become highly challengeable, too. States could indeed consider as necessary even a severe kinetic response to a "mere" cyber-attack, since they are evaluating the importance of their cyber networks much higher now than in the past, the US strategy of cyber security pointed out already in 2003: "*Cyberspace is their nervous system – the control system of our country*."[110]

Plus, the principles of proportionality and military necessity could be also challenged in the case of a cyber-attack's domino effect of an unattended scale. A good example of unwanted overreaching negative impacts on the civilian population could be the case of the attack on the Iraqi electric grid from the Gulf War in 1990 - 1991.

Even though it was a kinetic attack that caused a massive supply cut-off from electricity not only to the military controlled networks but also to the Iraqi civilians including electricity cuts in hospitals, power plants, and emergency systems, it is realistic to imagine a cyber-attack of the same nature causing the same or even more severe unintentional side-effects.[111]

A very similar case happened in spring 1999 during the war in Yugoslavia when NATO's forces during the Operation Allied Force hit Serbian electrical transformers, which resulted not only in damaging Serbian power facilities but also in cut-offs of many civilians from water supplies and in a shutdown of many gas stations.[112]

3.3 Shortcomings of the Tallinn Manual

The absence of a clear consensus of majority of the subjects of international law will always deeply undermine the respect of newly created rules of international law in the future, since despite the Article 38(1)(d) of the International Court of Justice Statute, which states that the "*teachings of the most highly qualified publicists of the various nations*" as one of the "*subsidiary means for the determination of the rules of law*" in international public law, it is the will of its authors, the states, that enjoys the highest respect of legal rules, since the states are subjects to their own rules.[113]

[110] *The US National Strategy to Secure Cyberspace*, The US Department of Homeland Security, 2003
[111] *The Weapon that Disabled Iraq's Power Grid,* Worldpress, 2010
[112] *NATO Denies Targeting Water Supplies*, BBC World Online Network, 1999
[113] ČEPELKA*, Č.,* ŠTURMA, P., *Mezinárodní právo veřejné*, Praha: C. H. Beck, 2008, p. 97

Currently, the sole document on the inclusion of cyber warfare into the IHL framework, which could be qualified as the teachings of the most highly qualified publicists of the various nations, is the Tallinn Manual on the International Law Applicable to Cyber Warfare.

Written in three years (2009 – 2012) and published in April 2013 by the Cambridge University Press, it constitutes an academic analysis of possible application of international public law, especially the Laws of War featuring IHL, onto cyber warfare and cyber armed conflicts. The Tallinn Manual, bearing the name of the city where the NATO Cooperative Cyber Defense Center of Excellence (CDCOE) is located, was written by a group of twenty independent legal scholars and practitioners in the field of cyber law that were convened by the CDCOE to give their qualified opinions on the issue of application of the Laws of War on cyber warfare.

Despite its NATO sponsorship, which will forever constitute an unsurmountable obstacle in becoming widely recognized by the most of international community, its academic contributions to the global debate on cyber warfare as well as to the laws-of-war theory are indeed undeniable. Above all, the Tallinn Manual constitutes the first effort of the kind, moreover gathering two main types of experts in the field – both legal scholars and practitioners, and as such constitutes an extremely important first step regarding cyber warfare and international law, which can be considered as the first preparatory work for a future convention on cyber warfare.

However, as it did not encourage any efforts to conclude a new international convention on cyber warfare, since it concluded with the stance that the current IHL Conventions and other internationally recognized provisions of Laws of War could be satisfyingly applied also on cyber weapons and warfare.

By pointing out its main detriments, it will be demonstrated that the Manual does not establish a sufficient legal tool, which could successfully cover the use of cyber warfare by the IHL and thus become generally respected IHL source for the matters of cyber warfare and as such enforced by the international community when appropriate.

First of all, since its creation, the Tallinn Manual was directly initiated and sponsored by NATO and as such can be always accused of being biased in favor of the USA and other members of the North-Atlantic Alliance and therefore never receive a full recognition or legitimacy from the international community.

Moreover, the opposing countries could also (successfully) argue that the establishment of the International Group of Experts and publication of the Manual was politically motivated and as such that their findings were, if not directly decided before the work of the IGE even started, then at least pre-defined beforehand.

Therefore, even though the main task of the International Group of Experts was to determine whether the current IHL rules could be applied also on the cyber-attacks, it was beforehand clear that the Group of Experts' answer would be "yes" – for the sakes of defending the political stability and interests of the main NATO Member States, which dispose of probably the most developed cyber weaponry in the world. Since, if the Tallinn Manual had concluded that it was not possible to apply the IHL rules on the cyber warfare, then there would have appeared a quasi-ultimate legal vacuum, in other words, the experts would have officially recognized the currently prevailing "complete chaos", which was not the aim of its sponsors.

3.3.1 Qualification of Cyber-Attacks in Tallinn Manual

Concerning the content, the Tallinn Manual deals primarily with the legal questions from both jus ad bellum and IHL regimes.

The first part of the Manual is dedicated to the questions of state sovereignty and its responsibility for its IT networks and other facilities. One of the most important conclusions of its first Chapter are rules 7 and 8 on acknowledging responsibility for a cyber-attack to a state: "*The mere fact that a cyber operation has been launched or otherwise originates from governmental cyber infrastructure is not sufficient evidence for attributing the operation to that State but is an indication that the State in question is associated with the operation. […] The fact that a cyber operation has been routed via the cyber infrastructure located in a State is not sufficient evidence for attributing the operation to that State;*"[114] and rule 9 recognizing that a cyber-attack can provoke and justify defensive countermeasures by the affected country: "*A State injured by an internationally wrongful act may resort to proportionate countermeasures, including cyber countermeasures, against the responsible State.*"[115]

It is also important to notice the use of the term "proportionality" in the rule 9, which is de facto a direct reference to IHL rules described in details in the commentaries of Rule

[114] Schmitt, N. Michael et col.: *Tallinn Manual on the International Law Applicable to Cyber Conflict,* Cambridge University Press, 2013, p. 39 - 40
[115] Idem, P. 41

14: "*A use of force involving cyber operations undertaken by a State in the exercise of its right of self-defense must be necessary and proportionate."*[116]

Regarding the purely jus ad bellum questions, firstly the one on the possibility to qualify cyber-attacks as a use of force, rule 10 says that it is possible: "*when its scale and effects are comparable to non-cyber operations rising to the level of a use of force*"[117] and provides a non-exhaustive list of criteria how to judge this level.

However, practically no real example of a CNA has been addressed with an exception of the DoS attack, which is questionably qualified as insufficient to be considered as a use of force: "*As an example, a highly invasive operation that causes only inconvenience such as temporary denial of service is unlikely to be classified as a use of force*."[118]

Yet, practical results of massive DoS attacks especially against a country with highly developed online government system but poor back-up system could be equal to a situation when the country's governmental buildings were bombed and thus unable to provide their services to its citizens for weeks.

Secondly, concerning the Article 51 of the Charter on the states' right to self-defense, the Manual provides the same answer as to the question of the use of force: "*Whether a cyber operation constitutes an armed attack depends on its scale and effects*,"[119] adding that if it does, the affected state can use its right to self-defense: "*A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence.*"[120]

The Rule 15 provides more details regarding the timing of self-defense operations: "*The right to use force in self-defence arises if a cyber armed attack occurs or is imminent. It is further subject to a requirement of immediacy."*[121] Additionally, the Rule 16 provides that the right of self-defense may be exercised collectively "*at the request of the victim-State and within the scope of the request*"[122].

Thirdly, on the Security Council, the Manual basically recognizes all of its current powers in relation to the cyber warfare. For instance, its Rule 18 states that the Security Council may authorize use of cyber operations and other cyber measures and that Security

[116] Idem p. 59
[117] P.45
[118] P. 52
[119] P. 53
[120] Idem, p.53
[121] Idem p.60
[122] Idem p.63

Council may also grant a mandate or an authorization to conduct cyber operations with international organizations, arrangements, agencies and other regional organizations.[123]

Finally, the conclusions of the Tallinn Manual on the application of the specific rules of IHL on cyber warfare will be mentioned further on along with their detailed discussion in the Chapter 4.

3.3.2 Lack of Answers to the Quintessential Issues

Although the Tallinn manual provides numerous answers, especially the answer to the question of whether current IHL can be applied to cyber-attacks, while careful reading, there are more additional answers asked than questions responded. For instance, the formulations of responses on some of the most important questions examined in the Manual are so vague that they in reality do not provide any clear answers.

A good example is the Rule 6 on Legal Responsibility of States for the cyber-attacks: "*A State bears international legal responsibility for a cyber operation attributable to it and which constitutes a breach of an international obligation*."[124] The term "attributable" is very vague as it in fact includes also the situation of mere speculations about the originator of the attack.

In some cases, it directly acknowledges that majority of the participating experts were not able to agree upon a unique position: "*The case of actions that do not result in injury, death, damage, or destruction, but which otherwise have extensive negative effects, is unsettled; […] the classic scenario illustrating this division of opinion is a cyber incident directed against the New York Stock Exchange that causes the market to crash*."[125]

Similarly, it did not provide a clear or firm opinion on the question of espionage, which thanks to the cyber weapons, reached an unprecedentedly different level in terms of danger threatening the affected country: "*For instance, consider the example of cyber espionage by State A against State B that unexpectedly results in significant damage to State B's cyber infrastructure. Some Experts were not willing to characterize the operation as an armed attack, although they acknowledged that measures could be taken to counteract the negative effects of the operation (especially in accordance with principle of necessity discussed in Commentary to Rule 9).*"[126]

[123] Idem, p. 67
[124] Idem, P.35
[125] P. 55
[126] P. 56

However, despite the numerous unclarified but crucial questions that remained open or only vaguely answered, the expert's panel unfortunately did not make a call for a new convention on cyber warfare, which might clear up the most fundamental questions with corresponding legitimacy for the future.

As the experts probably realize the main shortcomings of the Tallinn Manual, namely the fact that it responded to only very theoretical questions on cyber warfare but did not actually take into account the technical features that differentiate the cyber weapons and attacks from the kinetic ones, mainly. There is also a lack of legitimacy caused by leaving most of the countries out of the drafting process, NATO's CCDCOE convened another, this time even larger group of independent experts to prepare the Tallinn Manual 2.0.[127]

The new Tallinn Manual is expected to be published by the end of 2016, and should be larger in every possible sense.

First, led again by Professor Michael Schmitt from US Naval War College as its previous version, the team of authors of the Tallinn Manual 2.0 counted almost 50 international law and cyber experts.

Second, the version 2.0 will be consulted by 50 countries, so the process will be much more multilateral than before.

Third, it should focus more on the actual types of cyber-attacks that countries have been facing recently and provide their legal review even if the attacks' intensity and effects do not reach the necessary level so that they could be treated within the framework. As a result, the Tallinn Manual 2.0 should encompass particularly the position of cyber warfare in the context of human rights law, law of the sea, space law, international telecommunication law and diplomatic and consular law.

[127] CCDCOE: *Tallinn Manual 2.0 to Be Completed in 2016,* 9 October 2015

4. THE KEY INCOMPATIBILITIES OF CURRENT IHL RULES WITH CYBER WARFARE: ANONYMITY, TERRITORY & TIME

The unsurpassable difference which is making cyber warfare incompatible with the current IHL is based upon three main factual differences between cyber warfare and kinetic warfare regardless the type of space the kinetic attacks take place in (land, air, sea). The three crucial differences are the following: authorship, location, and speed. Therefore, these differences will be developed into a detailed perspective in order to demonstrate that some of the key legal provisions and principles created for kinetic warfare cannot be applied on cyber-attacks.

4.1 Anonymity of Authors of Cyber Attacks

In cyber warfare, anonymity becomes a different notion than during kinetic attacks. The issue of anonymity of cyber-attacks is in fact closely linked to the impossibility to trace down the original source of such an attack, since it is usually located in an absolutely different location than the one of its targets.

In addition, the route of a cyber-attack can take multiple detours only in order to cover its original source. The anonymity aspect is actually also one of the reasons why the attacks effectuated by modern war tools like drones are not considered as cyber-attacks – since even though a drone was operated from a very different place to the place of the attack, even from the other side of the world, its movements and its origin can be recorded and thus the drone can be easily traced down.

On the other hand, the real cyber-attacks can be launched from a distant place that may remain fully unknown for a very long period of time, using an unknown path in order to hit the target - a perfect example was the Stuxnet family of malware, whose origin countries have been revealed by never confirmed and recognized by its author – aggressor.

Therefore, in the kinetic warfare, keeping the anonymity of the aggressor was firstly impossible in the long term, secondly, even not desirable from the part of the aggressor. However, with the possibility to keep the identity of the author of cyber-attacks hidden even in a long run, sometimes even forever, possible cyber aggressors will probably prefer not to be revealed in order to minimize the probability of being attacked back. With cyber warfare, the world enters a completely new model of war, when the aggressors do not

need to claim their successful attacks but tend to be satisfied as long as the targeted device or a program has been destroyed.

Besides, once the location of the cyber aggressor is been revealed, it does not ensure revealing the identity of the author, since even though the attacker is a state entity, it can be made to look like the cyber-attacks were initiated purely by private entities or other states operating via their agents settled on the territory of the accused state. For instance, the series of Denial-of-Service attacks on Estonia in 2007 constitutes an exemplary situation when a state entity, the Russian Federation, denied its responsibility for the attacks and blamed it on a group of independent individuals.[128]

4.1.1 The Difference between Civilians and Combatants

One of the key areas where it would be impossible to apply the current IHL rules on cyber warfare in practice is the category of participants in an armed conflict, in particular combatants and civilians.

According to the Article 43(2) of Additional Protocol, combatants have a right to participate in hostilities, unlike civilians that are defined negatively by Article 50 of Additional Protocol as those who do not enter any of the categories enumerated in the Article 4 (a) of the Convention.

There are thus two categories of combatants: individuals that are "*members of the armed forces of a belligerent party (with the exception of medical and religious personnel), even if their specific tasks are not related to active hostilities; and second, any other person who takes an active part in the hostilities; this second group are unlawful combatants.*" [129] Hence, the civilians that become involved in hostilities but are not officially a part of belligerent party are qualified as unlawful combatants.

However, the characteristics of cyber warfare add numerous challenges to this clear distinction. What about civilians whose IT facilities serve for transmission of cyber-attacks? How can it be proved that they were not aware of the actions their computers and what networks were running? What about those that contribute to a cyber-attack by lawful actions but with harmful purposes like during a massive DoS attack where civilians can

[128] Richards, J.: *Denial-of-Service The Estonian Cyberwar and Its Implications for U.S. National Security*, International Affairs Review, The Elliot School of International Affairs at George Washington University
[129] Dinniss, p. 141

contribute even through a lawful consultation of a certain webpage or execution of other lawful actions but in an organized and coordinated manner?

The Tallinn Manual states that: *"Civilians are not prohibited from directly participating in cyber operations amounting to hostilities but forfeit their protection from attacks for such time as they so participate."*[130] However, this stance does not resolve the practical aspect of the issue when civilians get involved in transmission of a CNA, which can literally last a millisecond but can have vast impacts on targeted objects.

Additionally, the lawful combatants are supposed to fulfil four cumulative conditions prescribed by the Article 13 (2) of Geneva Conventions: "*(a) that of being commanded by a person responsible for his subordinates; (b) that of having a fixed distinctive sign recognizable at a distance; (c) that of carrying arms openly; (d) that of conducting their operations in accordance with the laws and customs of war."*[131] The requirements (b) and (c) seem for cyber attackers quite irrelevant, though.

However, for instance the Tallinn Manual, which argues that the IHL rules are applicable on cyber warfare, only cite those requirements without providing any explicative details about how to apply them on cyber combatants in practice.[132] There is indeed no means to fit the IHL rules onto the cyber "soldiers" by interpretation, which is one of the reasons why a new Convention on cyber warfare is needed.

Moreover, regarding the status of civilians and their rights, civilians generally protected under Article 13 of Additional Protocol, whose paragraph 2 also prohibits "*acts or threats of violence the primary purpose of which is to spread terror among the civilian population*"[133].

The current IHL provisions prescribe certain types of weapons as special precautions that are required to be taken when conducting an attack in order to spare the civilian population from hostilities.[134] They include selecting weapons and tactics "*with a view to avoiding, and in any event to minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects,*"[135] which could in many cases exclude the use of cyber weapons as their magnitude is always highly disputable.

---

[130] Rule 29, Tallinn Manual, p. 90
[131] Art. 13 (2) Geneva Conventions I and II
[132] Rule 26 on Members of Armed Forces, Tallinn Manual p. 85
[133] Art. 13 Additional Protocol
[134] Art 57 (1) 1925 Geneva Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare, June 17, 1925, 26 U.S.T. 571, T.I.A.S. No. 8061
[135] Article 57 (2) (a) (ii) of the Additional Protocol

As mentioned before, forcing an electric grid or a power plant out of order, or even only disabling access and functioning of government websites and online systems (including software operated by consulates and embassies where there is an actual risk of death in the case that they are inaccessible for multiple days or weeks), would constitute an act of violence among the civilian population. It would be difficult to argue that it was not with the primary purpose to spread terror amongst civilians.

4.2 Territorial Aspects of Cyber Armed Conflicts

Territorial aspect is equally one of the most differentiating features of cyber warfare. Even when operated from different place not identical to their own locations, kinetic weapons can always act only at one particular place at a time.

However, CNA do not contain a category titled 'virus' by coincidence: they can be precisely targeted but they can and more often do act rather like chemical or biological weapons – spreading uncontrollably at many places at once.

One of the main issues connected to cyber-attacks is the way they reach their targets, since it is mostly done through civilians' IT networks including those located in other countries, which can be also a targeted country.

In fact, cyber weapons can legally pass through another entity's networks or data clouds, since the current law of armed conflict does not contain any provision that would imply a general prohibition on passing the data. Thus passively legalizing a cyber-attack in the areas, where such an attack would be prohibited, if it was a location of a conventional armed conflict.

The Tallinn Manual also recognizes the difficulties connected with the territoriality issue and perceives it through cyber lenses: *"Restrictions based on geographical limitations may be particularly difficult to implement in the context of cyber warfare. For instance, consider a cyber-attack using cloud-computing techniques. Data used to prosecute the attack from one State may be replicated across servers in a number of other States, including neutral States, but only observably reflected on the systems where the attack is initiated and completed. As discussed in Rules 8 and 92, there is no general prohibition on the mere transit of data through areas where the conduct of cyber operations is otherwise prohibited during an armed conflict."*[136]

[136] Schmitt, N. Michael et col.: *Tallinn Manual,* p.78

Therefore, regarding the responsibility of a state for its networks, i.e. for "passing the data" that cause a cyber-attack, the Manual suggests to take off the responsibility from the transmitting countries as indicated in the above-mentioned Rule 7 and 8 of the Manual.

Nevertheless, taken into account possible impact of this decision, the stance of the International Group of Experts on the responsibility of transmitting countries should be equally confirmed (or declined) by the international community.

4.2.1 Law of Neutrality and the Globalized Cyber World

Nonetheless, the Tallinn Manual Group of Experts underlined that today's world of global cyber infrastructure does not correspond to the times when the IHL rules were created and as such were considering only "*situations in which entrance into or exit from a neutral State's territory is a physical act."*[137]

However, the experts basically applied the present law of neutrality, originating from Hague Conventions V and XIII and customary international law and currently applies currently only in IAC, onto cyber operations. As stated in the Chapter VII of the Manual: ''*neutral cyber infrastructure' means public or private cyber infrastructure that is located within neutral territory"*[138] and as such enjoys the protection of neutral territory: *"the exercise of belligerent rights by cyber means directed against neutral cyber infrastructure is prohibited."*[139]

Nevertheless, regarding the nature and the reality of cyber-attacks when a lack of transmission of data could sometimes constitute the only way to prevent the cyber-attack from happening and resulting in massive damages both to people's lives and physical objects including infrastructure and public goods, a decision whether to apply the concept of neutrality on cyber warfare in an unchanged form or whether to modify them accordingly needs to be made unconditionally by the Member States of the international community.

Since in the context of cyber warfare, where the state aggressor is not interested in recognizing its authorship and when the battlefield is practically all created by cyber space

[137] Schmitt, N. Michael et col.: *Tallinn Manual*, p. 203
[138] Schmitt, N. Michael et col.: *Tallinn Manual*, P. 202
[139] Schmitt, N. Michael et col.: *Tallinn Manual*, p. 203

but practically includes also physical IT servers and networks, it could be highly dangerous to apply un unrevised concept of neutrality also on cyber warfare.

The discrepancies between the application of the current principle of neutrality on kinetic and cyber warfare raised doubts also amongst the Group of Experts: "*The International Group of Experts struggled with the situation in which a cyber-attack against a military objective in belligerent territory has spill over effects in neutral territory. For example, a cyber-attack on a server in belligerent territory could significantly affect services in neutral territory. The Experts agreed that if such effects are not foreseeable, the attack does not violate the law of neutrality.*"[140] Again, the terminology used by the Tallinn Manual is quite fragile, as one of the main natural features of cyber-attacks is the non-foreseeability of their impacts.

4.2.2 Territoriality of Armed Conflict in the Cyber World and NIAC

So far, the Laws of War presume that an armed conflict is always taking place in a specific area, which can be traced on a map. In general, the territory of the armed conflict was defined in the contexts of provisions of spies, who in case of capture do not benefit from the status of war prisoner.

But under certain conditions and when in the territory controlled by their party, a member of armed forces of the respective party should not be considered as spies, which is plausibly the main reason the zone of an armed conflict as well as the place from where the members of armed forces operate, became a highly important issue for IHL. The Article 29 of the Hague Regulations uses the notion of *"zone of operations of a belligerent"*[141].

Moreover, the Article 46 (2) of the Additional Protocol I enlarges such a *zone to "territory controlled by an adverse Party."*[142] However, such a distinction becomes impossible to implement in practice in case of an armed conflict, which would also comprise cyber-attacks.

In fact, if an armed conflict with a cyber-attack component is similar in terms of territoriality to any current type of armed conflicts, it would be probably the NIAC, since it is especially the members of non-state organized armed groups such as terrorist groups,

[140] Idem, p. 204
[141] Annex to the Convention IV: Regulations Respecting the Laws and Customs of War on Land - Section II : Hostilities - Chapter II : Spies - Regulations: Art. 29
[142] Ibid

which tend to attack without respect to the territorial limits of conflict areas, and have been more and more proliferating: "*The development within the international community has, however, caused the increasing importance of other subjects and entities of international law and not only in the IHL context – movements of national liberation, insurgents, or even terrorists. Such evolution constitutes a real challenge for the legal framework of the IHL tailored to states as original and only actors of the international community.*"[143]

However, IHL currently does not sufficiently cover the territoriality issue in the context of NIAC: *"According to the traditional view of the law of armed conflict, military operations during a non-international armed conflict must be limited to the territory (including the territorial sea) and national airspace of the State in which the conflict is taking place. However, [...] today the exact geographical scope of non-international armed conflict raises a number of complex issues. Many States and commentators now take the view that a non- international armed conflict may extend to areas beyond the borders of the State in question, arguing that it is the status of the actors, not geography, which is the determinative factor in classification of conflict.*"[144]

The current blurred line for the determination of a NIAC could theoretically serve as a basis when searching for how to (re)define the rule of limiting the battlefield to the territory of armed conflict in case cyber weapons are used, too.

In theory, in the rule 23 of the Tallinn Manual, the International Group of Experts sets up the possibility of that a NIAC can be triggered solely by cyber-attacks thanks to the article 2 and 3 of the 1949 Geneva Conventions and on the case law.[145]

Nonetheless, conflicts of any nature can be qualified as NIAC if they reach a certain threshold of gravity, which was generally defined in the Tadic Decision of the International Criminal Tribunal for Former Yougoslavia by "*the gravity of attacks and their recurrence[146]; the temporal and territorial expansion of violence and the collective character of hostilities[147]; whether various parties were able to operate from a territory*

[143] Faix, M.: "*Operácie multinárodných síl a medzinárodné humanitárne právo*", Acta Universitatis Carolinae Iuridica, 2009(4), p. 25

[144] Schmitt, N. Michael et col.: *Tallinn Manual on the International Law Applicable to Cyber Conflict,* Cambridge University Press, 2013, p.79

[145] Tadic, Decision on the Defense Motion for Interlocutory Appeal, paras. 67, 70; U.K. MANUAL, para. 3.5 (as amended). See generally U.S. Commander's Handbook para. 5.1.2.2; Canadian Manual at GL-13; German Manual, paras. 20.1 -21.1

[146] Mrksic Judgment, para. 419; Hadzihasanovic Judgment, para. 22.; Limaj Judgment, paras. 135-167.

[147] Mrksic Judgment, paras. 39-40, 407-408

under their control[148]*; an increase in the number of government forces*[149]*; the mobilization of volunteers and the distribution and type of weapons among both parties to the conflict*[150]*; the fact that the conflict led to a large displacement of people*[151]*; and whether the conflict is the subject of any relevant scrutiny or action by the Security Council.*[152]"[153]

Therefore, the Tallinn Manual argues that a possibility of a cyber-attack triggering a conflict that would reach the necessary threshold of gravity that would enable its qualification as a non-international armed conflict, would be in reality practically almost impossible: "*cyber operations alone can trigger a non-international armed conflict in only rare cases.*"[154]

However, as for today, taking into account many terrorist organizations such as ISIS, such cases might not be that rare anymore.

Although, if the interpretation of today's IHL rules are being disputed in case of NIAC, which is a type of conflict that might theoretically arise even when the IHL rules were created, then it might be practically impossible to interpret the territorial aspects of the IHL rules in the context of cyber-attacks, which were not foreseeable even back then when the rules were created. Therefore, it seems inevitable to precisely define the relation of the IHL rules on territoriality onto armed conflicts consisting of cyber-attacks preferably in a new convention.

4.3 Time Issue and Speed of Cyber-Attacks

The third main aspect in which the cyber-attacks differ dramatically from the so far known kinetic attacks is time. The issue of cyber-attack speed causes problems both in *jus ad bellum* and IHL regime. In jus ad bellum, the issue particular arises in regarding

[148] Milosevic Decision, paras. 31
[149] Haradinaj Judgment, para. 49
[150] Mrksic Judgment, paras. 420-421
[151] *Tadic, Decision on the Defence Motion for Interlocutory Appeal*, para. 70. In *Abella, The Inter-American Commission on Human Rights characterized a 30-hour clash between dissident armed forces and the Argentinean military as non-international armed conflict.* Abella v. Argentina, Case 11.137, Inter-Am. C.H.R., Report No. 55/97, OEA\Ser.L\V\II.98, doc. 6 rev. (1998)
[152] In Limaj, the International Criminal Tribunal for the Former Yugoslavia concluded that the conflict in Kosovo in 1998 could be described as "*periodic armed clashes occurring virtually continuously at intervals averaging three to seven days over a widespread and expanding geographic area",* Limaj Judgment, paras. 168, 171-173
[153] Schmitt, N. Michael et col.: *Tallinn Manual,* p. 87
[154] Idem, p.87

the right to self-defense defined in the Article 51 of the UN Charter, which underlines the immediate character of response to an armed attack.

Nevertheless, the immediacy of self-defense can be relative in terms of cyber warfare. On the one hand, there are cyber-attacks with detectable causes immediately after their launch as in the case of DoS attacks in Estonia or during the war between Georgia and Russia in 2008. However, there are also cyber-attacks that can have much more severe character and yet, their impacts are not detected but several months or even years later after their launch.

Another issue in the *jus ad bellum* regime connected to time is the notion of preventive and preemptive attacks. For instance, the International Group of Experts rejected the idea of a "preventive self-defense" to a cyber-attack.

Moreover, they did not answer the pre-emptive self-defense in a persuasive manner either: "*the critical question is not the temporal proximity of the anticipatory defensive action to the perspective armed attack, but whether a failure to act at that moment would reasonably be expected to result in that State being unable to defend itself effectively when that attack actually starts."*[155]

Concerning the IHL regime, there are equally numerous reasons why its current rules cannot apply by interpretation to a cyber-attack due to the time issue.

Firstly, cyber-attacks can spread much faster and with much higher exponential dimension than kinetic attacks. Even in comparison with bombs, in terms of distance per unit of time, cyber-attacks would still be faster, in addition to their global scope.

Secondly, only some types of the most dangerous cyber-attacks are usually detected at the time they hit their target.

Despite the fact that in cases of cyber-attacks of a large scale, the immediately recognizable cyber-attacks would become more frequent. The espionage types of attacks that are used for preparing the battlefield as did for instance Duqu and Flame for Stuxnet are very difficult to discover at the time they are hitting the target, since the most complicated cyber-attacks are designed to act unnoticed and overcome anti-malware software.

In addition, the presence of some of them is often revealed rather by chance due to their (side) effects like slowing down the targeted operation system or causing blackouts

[155] Schmitt, N. Michael et col.: *Tallinn Manual*, p. 83

thanks to their commands, which they are programed to perform. Therefore, nowadays, the majority of cyber-attacks are not revealed until several weeks or months after the first infection of the IT facility.

Moreover, as the results of the fact that cyber-attacks are not always visible to the public, some of the affected entities prefer not to inform about themselves becoming a target of a cyber-attack, or at least not immediately. Therefore, the IHL rules where the notion of urgency is sometimes decisive should be reviewed.

Additionally, another important principle of IHL, which could be modified in order to reflect the time inconsistency of cyber-attacks is the principle of proportionality, which is codified in the Article 51 (5) (b) and repeated in the Article 57 of the Additional Protocol and which prohibits any excessive i.e. disproportionally large armed attacks.

It is also closely linked to the prohibition of indiscriminate attacks that are defined in the Article 51 (4) of the Additional Protocol as those: "*(a) which are not directed at a specific military objective; (b) which employ a method or means of combat which cannot be directed at a specific military objective; or (c) which employ a method or means of combat the effects of which cannot be limited as required by International Humanitarian Law; and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction."*[156]

The indiscriminate attacks are nonetheless different from the direct hostilities against civilians, since "*the attacker is not actually trying to harm the civilian population.*"[157] However, as cyber law expert Dinniss points out: "*Viruses and worms are two methods of computer network attack, which are particularly likely to fall into this category as their effects are often not limited by their creators.*"[158]

Since viruses and worms often contain self-reproducing and self-spreading commands, they can easily slip out of the targeted networks of computers or other IT facilities and spread freely and unstoppably around the world including civilian networks and computers. In fact, Trojans that usually need either an action for the part of the user, an unwanted click that launches their installation from an email or contaminated website, or an insertion of an affected USB stick, may be considered as indiscriminate attacks. Once again, the international community should make such an evaluation.

[156] Article 51 (4) of the Additional Protocol
[157] Dinstein, p. 127
[158] Dinniss, p. 203

5. NECESSARY COMPONENTS OF A NEW IHL CONVENTION ON CYBER WARFARE

Unlike the previous chapters, which aimed to provide critical review of current Laws of War in the context of cyber conflicts, or rather their incompatibility with cyber warfare, i.e. examine the measures *de lege lata*, the last chapter will completely adopt the *de lege ferenda* approach. The last chapter of the thesis therefore aims to suggest a very rough draft version of the key aspects that should comprise a new convention on cyber warfare including its parties and authors and mains aspects of warfare, which are different from traditional warship due to the cyber nature of an armed conflict.

5.1 Formal Attributes of the Convention

First of all, the term "Convention" should be understood as in the sense of an international treaty, i.e. "*an international agreement concluded between states in written form and governed by internationa*l *law*,"[159] as defined by the Vienna Convention on the law of treaties from 23 May 1969.

Secondly, concerning the contracting Parties, as usual for all international treaties, the contracting Parties shall be defined by the Vienna Formula[160], which contains a larger number of possible parties to a Convention and at the same time, is more precise than the All-State Formula.

The whole contracting process should be conducted within the framework of the United Nations and in line with the parts of the 1969 Vienna Convention on the Law of Treaties that are recognized as a part of customary law.

The scope of application concerning the addressed entities would be plausibly one of the most challenging issues. Nonetheless, regarding the current situation in the world, where the non-state actors are in the core of the largest and most severe armed conflicts, in order to ensure an effective and efficient implementation in practice, it would be quintessential to include also the non-state actors. However, the scope of included armed conflicts would most probably stay limited to International Armed Conflicts.

One of the most important aspects would be also the relation of the cyber treaty towards the law of Hague and Geneva Conventions. In order to eliminate any possible legal vacuum, it might be necessary to clearly stipulate that the relation between the two

[159] Article 2 (1) (a) Vienna Convention on the Law of Treaties 1969
[160] Idem, Article 81

would work as *lex specialis* towards *legi generali*, so that the validity of the current IHL customary law and the general principles in the field of cyber warfare would be officially recognized and all doubts regarding the relation between the two avoided.

Finally, concerning the possibility of reservations to the Cyber Convention, the final say should be left to the negotiation process, since reservations to a treaty are in general an unpopular but often necessary means how to make sure the treaty can benefit from a general acceptability and legitimacy. At the same time, the reservations should not overcome a bearable threshold, which divides respected treaties in practice to the extent that they later become a part of the customary law even with their reservations and those whose legitimacy is in practice threatened or prevented by too many substantive reservations.

5.2 Key Provisions

Nonetheless, the key aspects of the new Convention on Cyber Warfare should consist in rewriting the parts of IHL that would cause the most inconsistencies if applied on cyber warfare due to the specific nature of incomparable certain areas with the conventional warfare, weaponry and strategies.

5.2.1 Redefining the Notion of Attack in the Cyber Context

First, it should be clearly stated that a cyber-attack could be under certain conditions considered as an attack in the sense of the Article 49 (1) Additional Protocol I, where the notion of "violence" presenting the sine qua non element of the attack definition must be specified in cyber terms.

Therefore, the new cyber treaty needs to contain a new definition of an attack in cyber terms, so called cyber-attack, which would be the lex specialis for the current IHL definition of attack.

Cyber-attacks could thus be defined as the cyber operations, whether offensive or defensive, which, if exercised, have a serious direct impact onto persons or objects resulting in human injuries and deaths or in a serious damage or destruction of objects indispensable for a survival of a civilian population including public infrastructure and its networks. The wording "if exercised" would help include also those cyber-attacks, which would have caused the cited damages, but were stopped by the targeted country before doing so.

The Tallinn Manual for instance suggests defining the cyber-attacks as a "*cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destructions to objects."*[161]

Although the formulation develops the notion of a cyber-attack, the wording "reasonably expected" does not provide a clear definition of when a cyber-attack can be considered as an attack in IHL.

Similar formulation is used also in the rule 81 of the Tallinn Manual on Protection of Objects Indispensable to Survival, which presumes that "*Attacking, destroying, removing, or rendering useless objects indispensable to the survival of the civilian population by means of cyber operations is prohibited*,"[162] which is derived directly from the Article 54 (2) of the Additional Protocol I.

However, as the IHL interprets this rule concretely in relation to the starvation of the civilian population and its prohibition as a method of warfare in the Article 53 of the Additional Protocol I. It is questionable what exactly the survival of the civilian population stands for especially in the context of private goods and infrastructure indispensable for many of today's modern societies.

To the condition of survival, the International Group of Experts also added the situation when a population is forced to move, which if restated by the international community, could significantly enlarge the range of prohibited cyber operations: "*cyber operations may not be conducted against objects if those operations can be expected to so deprive the civilian population of food or water that it starves or is forced to move."*[163]

In addition, the notion of objects indispensable to the survival created one hundred years ago could actually be qualified as having a different meaning today. For instance, the Internet connection could be in twenty years considered as indispensable for survival in urban areas all over the world.

5.2.2 Principle of Distinction

The principle of distinction between the civilian population and combatants and between the objects and military objectives originates in the Articles 48 and 52 (2) of Additional Protocol I. In its Legality of the Threat or Use of Nuclear Weapons case, the

[161] Tallinn Manual, rule 30 p. 106
[162] Tallinn Manual, rule 81 p. 180
[163] Idem, Par. 7, comments on rule 81, p.186

International Court of Justice called the principle of distinction a "cardinal principle"[164] of IHL as well as one of the "*intransgressible principles of international customary law*".[165] The principle is also possible to be found in the Statue of the International Criminal Court, which stipulates that: "*intentionally directing attacks against civilian objects that is, objects which are not military objectives*"[166] represents a war crime in international armed conflicts.

There have been also several practical cases that provided a recognition of the principle such as the Tadic case, where the principle was actually broadened and applied onto NIACs,[167] and the conflict in the Middle East in October 1973, when the ICRC appealed to the state parties of the conflict to respect the distinction between civilian and military objectives, which was positively complied by the concerned countries i.e. the Syrian Arab Republic, Iraq, Egypt, and Israel.[168]

From the conceptual point of view, some legal scholars as well as military legal experts argue that it is not possible to respect the principle anymore. For instance, Charles Dunlap, former Deputy Judge Advocate General of the US Air Force, argues in favour of effect-based operations even for the price of targeting civilians' objects.

Since the effect-based theory of warfare is based on the combination of political and economic pressure and threats of severe attacks in exchange of a quick end to an armed conflict: "*We need a new paradigm when using force against societies with malevolent propensities. We must hold at risk the very way of life that sustains their depredations, and we must threaten to destroy their world as they know it if they persist. This means the air weapon should be unleashed against entire new categories of property that current conceptions of [Laws of Armed Conflict] put off-limits."*[169]

On the other side of the law of warfare theories, there are advocates of insurgents and anti-states dictatorship of rules such as Gabriel Swiney who argues that the principle of distinction can be easily adopted by the oppressing state regimes with all their institutional and military machineries, however, it also constitutes a significant obstacle for insurgents

[164] Nuclear Weapons case, I.C.J. Advisory Opinion, para. 179
[165] Ibid
[166] ICC Statute, Article 8(2)(b)(ii) (*ibid.*, para. 108)
[167] ICTY, Prosecutor vs. Dusko Tadic, Case No. IT-94-1-AR72; 35 ILM (1996) 32; Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, 2 October 1995
[168] ICRC: *The International Committee's Action in the Middle East*, International Review of the Red Cross, 13(152), 1973. para. 102
[169] Dunlap, C.:The *End of Innocence*: *Rethinking Noncombatancy in the Post-Kosovo Era*, 28 Strategic Review 9-17, Summer 2000, p. 14.

fighting against the regime or for their group's recognition especially but not only in NIAC.[170]

Nevertheless, the distinction in cyberwarfare is an extremely complex issue, since the cyber weaponry can either significantly simplify the situation thanks to precise targeting, which is characteristic for certain types of CNAs such was the case for Stuxnet, but also makes the situation extremely difficult due to side-effects of some CNA – for instance the DOS attacks but also Stuxnet-type of CNA, if not well targeted or when spreading gets out of control.

Yet, it seems crucial to preserve the principle of distinction in the context of cyber warfare too, since it is one of the few forms of protection the civilian population. Despite the fact that Swiney's argument seems to be reasonable and extremely pertinent especially in the first decade and half of the 21st century, which has been characterised by many NIAC and insurgent movements, it is extremely improbable that the states would recognise the most favourite current form of the insurgents' practices as lawful under IHL, as the attacks targeting civilian populations are also one of the characteristics of terrorist movements.

5.2.3 Lawfully Targeted Individuals

According to IHL, there are three categories of individuals who can be lawfully subjected to targeting during an armed conflict: "*Combatants, civilians directly participating in hostilities, and civilians acting in a continuous combat function. Civilians lose their right not to be targeted to the extent that they 'take a direct part in hostilities. Furthermore, under customary international law affirmed by the International Committee of the Red Cross, civilians who adopt a continuous combat function may also be targeted.*[171]"[172]

However, as evoked earlier, it can be practically impossible to distinguish a combatant or another lawfully targeted individual from a civilian for two main reasons.

First, it may be very difficult, if not impossible, to determine whether a civilian is aware of their computer network device participating in a cyber-attack.

---

[170] Swiney, G.: *Saving Lives*: *The Principle of Distinction and the Realities of Modern War*, 39 INT'L L. 733, 733, 2005

[171] ICRC: *Interpretive Guidance On The Notion Of Direct Participation In Hostilities Under International Humanitarian Law* 16, 2009

[172] Hathaway, O.A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue W., & Spiegel, J.: *The Law of Cyber Attack*, California Law Review, 2012

Secondly, the civilian engineers and other designers of weaponry were not considered as lawfully targeted individuals because their role was indeed minor in comparison to military leaders including military engineers and generals.

Nonetheless, the role of civilian software engineers is apparently significantly more important in the context of cyberwarfare, especially because once the CNA is launched, often no more actions are needed, since its route and actions have been automatically programmed by its creators. This feature of cyberwarfare can be easily abused by official state authorities, which can deny any connection to a civilian group that openly claims responsibility for an attack as it probably happened during the cyber-attacks against Estonia in 2007, when the pro-Kremlin youth group Nashi claimed responsibility for the attacks.[173]

Therefore, it is possible that the new cyber treaty would contain provisions, which would consider all civilians actively and knowingly participating on cyber-attacks including their preparation and organization as lawfully targeted individuals.

On the other hand, individuals, whose computer network devices are contributing to cyber-attacks without their owner's knowledge, cannot become subjects to lawful targeting. Similarly, it does not seem possible that the state, through whose computer networks a cyber-attack is conducted, could be held (partly) accountable for attacks; unless it is proven that it was done so with its leaders being aware of it.

5.2.4 Lawfully Targeted Objects

A cyber-attack on private entities could be in theory considered as an armed-attack only if it had serious health-threatening impacts on a country's citizens. It is rather unrealistic to expect that the international community would agree that an attack on a stock exchange software is considered as an armed attack despite the wide range of possible serious damages that it could cause including major loss of jobs and consequent threats to survival of many civilians.

However, even the International Group of Experts was divided over this issue: "*Some of the Experts were unprepared to label it* [attack against the New York Stock Exchange] *as an armed attack because they were not satisfied that mere financial loss constitutes damage for this purpose. Others emphasized the catastrophic effects such a crash would occasion and therefore regards them as sufficient to characterize the cyber operation as*

[173] Noah Shachtman: *Kremlin Kids: We Launched the Estonian Cyber War*, Wired, 3 November 2009

an armed attack"[174]. Thus, a clear statement with the legitimacy of international community is needed.

5.2.5 Principle of Neutrality

The principle of neutrality is closely related to the assumption that it is possible to delimitate the geographical area the armed conflict is taking place in. Consequently, it was set up to protect especially civilians and their property as well as other state entities and their population situated in proximity but not directly in the zone of the armed conflict.

However, this presumption does not very well correspond to the reality of cyber warfare, in which the delimitation of the zone of an armed conflict is not possible. Regardless of this impossibility, the Tallinn Manual still overtakes the current principle of neutrality and applies it to cyber-attacks. In its Rule 91 and 92 on Protection of Neutral Cyber Infrastructure respectively Cyber Operations in Neutral Territory, it says that the neutrality principle prohibits the belligerents in use of cyber weaponry against neutral cyber infrastructure and in neutral territory.[175]

The Group of Experts took such a stance being perfectly aware of the geographical issue with cyber weapons: "*the fact that the law of neutrality developed based on situations in which entrance into or exit from a neutral State's territory is a physical act,"*[176] which is not very consistent with the Rules 91 and 92, though, and might create many issues in practice, if ever stipulated in the Cyber Convention in the same way.

Therefore, Convention should instead reformulate the principle of neutrality based on the specific nature of cyber weapons and provide concrete provisions on which territory and cyber infrastructure are considered as neutral. Would it be all those officially labelled as civilian or indispensable for civilians even if they are being simultaneously used for military purposes?

Even though it may seem only logical to ban all belligerent cyber operations towards neutral infrastructure and in neutral territory, as it would evoke the right to self-defense, it should be confirmed by the international community.

[174] Tallinn Manual, p. 55
[175] Tallinn Manual, p. 203 - 204
[176] Tallinn Manual, p. 203

Nonetheless, regarding such a prohibition, the real concern consists in the extent of states whose IT infrastructure or territory are used for transmitting cyber-attacks should be held accountable.

The Rule 93 of the Tallinn Manual suggests that *"a neutral State may not knowingly allow the exercise of belligerent rights by the parties to the conflict from cyber infrastructure located in its territory or under its exclusive control."*[177] However, proving to the government authorities that they permitted a cyber-attack launched from their territory knowingly will be an extremely difficult if not even impossible task.

5.2.6 Principle of Proportionality

The principle of proportionality in IHL is based in the Article 51 (5) (b), which requires to anticipate incidental loss of civilian lives, injuries and damages to civilian objects and make sure that those will not exceed the concrete and direct military advantage brought by the attack. In the opposite case, the attack is by the IHL rules prohibited as indiscriminate.

Obviously, it is already rather difficult to follow whether the principle of proportionality is respected in the current armed conflicts, since the concrete and direct military advantage would not be probably evaluated the same by the offensive party and by an impartial judge, let alone the defensive party. Therefore, it is not the bordering cases where the author's party could be prosecuted for breach of the proportionality principle but rather the obvious cases where the defense actions as a reaction to an attack would be extremely disproportionate.

However, such an evaluation requires a thorough analysis of anticipated incidental casualties and/or damages to civilian objects, which in cyber warfare, are usually not easy to determine, since the targeted objects may be a part of a vast civilian systems or may share civilian networks.

5.2.7 Permitted Defense

The last major reason why it is in the very own interest of states as members of the international community to have a new international treaty is not only to give legal permission to use kinetic weapons in self-defense against cyber-attacks, but also to give legal permission to use cyber weapons as a means of defense against cyber and kinetic

[177] Idem Rule 93, p. 205

armed attacks. As countries around the world do not have the same level of dependency on cyber infrastructure and services, they do not have the same level of vulnerability against cyber-attacks either.

Moreover, despite the high price, the costs of cyber-attacks can be still much lower than the costs of kinetic attacks. Besides, the present status is not sure whether cyber-attacks can be officially considered as armed attacks according to international public law. This may act as an encouraging factor for using cyber weapons especially for countries on the edge of the international community.

For instance, North Korea seems to be developing a strong cyber war program[178] as a less-costly but very efficient alternative to kinetic weapons in case of a new conflict with South Korea, a country extremely dependent on its IT infrastructure, with the highest internet connection speed in the world.[179]

There have been already several cyber-attacks detected between the two countries featuring numerous attacks by the Lazarus Group against banks, media stations and manufacturing entities including some cases of military espionage as well as the attack against the Sony Pictures Entertainment on 24 November 2014, which followed Sony's controversial satirical movie on North-Korean political authorities.[180]

In addition, one of the latest cases recorded by the South Korean officials was a case of hacking mobile devices of 40 South Korean national security officers publicized on 13 March 2016.[181]

North Korean attacks were not oriented only towards South Korea. On 30 May 2016, the Society for Worldwide Interbank Financial Telecommunication (Swift), an internet provider of secured financial messaging services, reported that numerous banks claimed to have suffered a certain type of cyber-attack, whose origins were traced to North Korea.[182]

However, categorized according to targets, the most serious cyber-attack hailing apparently from North Korea happened on South Korean nuclear plants in December

[178] Park, J.-M.: *Keyboard warriors: South Korea trains new frontline in decades-old war with North*, The Reuters, 21 June 2016
[179] *Akamai's State of the Internet*, Q4 2015 Executive Review, Akamai, 2015,
[180] Kochetkova, K.: *What is known about the Lazarus Group: Sony hack, military espionage, attacks on Korean banks and other crimes,* Kaspersky Lab, 24 February 2016
[181] *North Korea denies cyber-attacks on South Korea officials,* The Reuters, 13 March 2016
[182] Riley, D.: *Finger pointed at North Korea as Swift malware attacks hit 12 banks*, Silicon Angle, 30 May 2016

2014.[183] Even though no actual serious damages were recorded, the hackers tempted to affect the functioning of atomic reactors, which could cause serious damages, if the attack had succeeded.

The issue of a possible legal use of cyber weapons as a means of not only self-defense but also as an action in the sense of the Article 41 and 42 of the UN Charter becomes even more pertinent in the context of the Resolution 2270 of the UN Security Council issued on 2 March 2016, which imposed new sanctions on North Korea as a response to their nuclear test conducted on 6 January 2016.[184]

Once clearly formulated in the Cyber Convention, which would be created within the framework of the UN Charter, the UN Security Council could even decide on direct cyber operations against countries illegally running their own nuclear programs.

Nonetheless, unlike nowadays, publicity of such measures would have to be restricted, which could also be regulated by the new Cyber Convention. This would allow to the UN Security Council not to publicize resolutions adopted in unanimity, which would imply taking cyber actions against countries' nuclear-weapon programs that would constitute threats to the peace in conformity with the Chapter VII of the UN Charter.

5.2.8 Cyber Espionage

In the context of cyber weapons, which can have vast consequences even when utilized in a form of an espionage malware or a system of related malwares and can constitute an irreplaceable part of a multidimensional-armed attack, should be reconsidered. Currently, according to the Article 46 of Additional Protocol I and the Articles 29 and 31 of the Hague Regulations, espionage is not considered as a violation of international law. However, the practice of cyber espionage could violate some of the current IHL rules like the Article 37 of the Additional Protocol I.

Additionally, it is again the deformed notion of armed conflict and its zone that is as divergent as it could only be in case of cyber warfare. Already, the definition of espionage in the Article 29 of the Hague Regulations counts on existence of a precisely demarcated zone of operations: "*A person can only be considered a spy when, acting clandestinely or*

[183] *South Korea Accuses North of Cyber-attacks on Nuclear Plants*, Security Week, 17 March 2015,
[184] *Security Council Imposes Fresh Sanctions on Democratic People's Republic of Korea, Unanimously Adopting Resolution 2270 (2016)*, SC/12267, 7638th Meeting, Security Council Press Release, 2 March 2016

on false pretences, he obtains or endeavours to obtain information in the zone of operations of a belligerent, with the intention of communicating it to the hostile party. Thus, soldiers not wearing a disguise who have penetrated into the zone of operations of the hostile army, for the purpose of obtaining information, are not considered spies."[185]

However, in the cyber world, the whole world or at least whole countries and their IT infrastructure could become the zone of operations. Now, most cyber operations, which could not be classified as armed attacks, would not be perceived as espionage but as "*the employment of measures necessary for obtaining information about the enemy are considered permissible*"[186] as says the Article 26 of the Hague Regulations.

Similarly, the International Group of Experts, being aware of the current legal status of CNA as well as of the diverging character of cyber espionage in comparison to the conventional espionage techniques, followed the current doctrine and made a distinction between espionage taking place in the territory of the affected state: "*Cyber espionage and other forms of information gathering directed at an adversary during an armed conflict do not violate the law of armed conflict"*[187]; and outside of its territory: "*Cyber espionage must be distinguished from computer network exploitation (CNE), which is a doctrinal, as distinct from an international law, concept. CNE often occurs from beyond enemy territory, using remote access operations. Cyber operators sometimes also use the term 'cyber reconnaissance'. The term refers to the use of cyberspace capabilities to obtain information about enemy activities, information resources, or system capabilities. CNE and cyber reconnaissance are not cyber espionage when conducted from outside enemy controlled territory."*[188]

Nevertheless, the Group concluded that neither of the two violate the current Laws of War. Given the unparalleled character of cyber warfare and the lack of "zone of operations" in the cyber world, the definition and the *per se* legality of espionage should be confirmed or restated for the case of cyber warfare.

All in all, members of international community need to be provided with a clear stance on the cyber espionage, which currently remains one of the greyest areas of Laws of War applied on cyber warfare.

---

[185] Schindler, D. & Toman, J.: *The Laws of Armed Conflicts*, Geneva: Martinus Nihjoff Publisher, 1988, p.72.
[186] Idem, Article 26
[187] Tallinn Manual, p.158
[188] Idem, p. 159

CONCLUSION

In its five chapters, this thesis provided a set of arguments proving the necessity of drafting a new international Convention on cyber warfare and cyber weapons.

Firstly, to assure that all key terms and understood in a unique sense, the thesis focused on the essential terminology of Laws of Wars, especially IHL and its theory including the necessary philosophical and historical background, which constituted a key element in its development.

Secondly, the thesis provided as well a detailed description of cyber warfare and cyber weapons, since their main characteristics, actions and consequently effects constitute a new object which does not have to be familiar to legal experts, but which is necessary in order to understand the whole scope and the power of cyber warfare.

Thirdly, a set of the most important reasons was introduced in order to prove that a mere interpretation of the current Laws of War and more specifically the IHL rules cannot serve as a sufficient and reliable source of binding rules applicable on cyber warfare.

The fourth chapter developed the previous one by pointing out the main differences between the kinetic weapons, for which the current treaties were written, and the cyber ones, thus trying to highlight the major aspects of incompatibilities between the two.

Finally, the last chapter tried to provide a draft of both the main formal, and substantive aspects, of the new Cyber Warfare Convention, and thus reinforcing the arguments of the major issues arising when it comes to the application of Laws of War and IHL in particular to cyber warfare. Arguing this cannot be resolved in any other way but by a consensus of international community embodied in a new international Convention on Cyber Warfare.

SEZNAM POUŽITÉ LITERATURY A DALŠÍCH ZDROJŮ / BIBLIOGRAPHY

Legal documents:

- Charter of the United Nations
- Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Geneva, 12 August 1949
- Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Geneva, 12 August 1949
- Convention (III) relative to the Treatment of Prisoners of War, Geneva, 12 August 1949
- Convention (IV) relative to the Protection of Civilian Persons in Time of War, Geneva, 12 August 1949
- Convention (II) with Respect to the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 29 July 1899
- 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
- Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977
- Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the Adoption of an Additional Distinctive Emblem (Protocol III), 8 December 2005
- Rome Statute of the International Criminal Court
- Vienna Convention on the Law of Treaties 1969

Cases & Advisory Opinions:

- Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, International Court of Justice (ICJ), 1996, 8 July 1996
- Prosecutor v. Limaj et al. (Trial Judgment), IT-03-66-T, International Criminal Tribunal for the former Yugoslavia (ICTY), 30 November 2005
- Nicaragua v. United States of America - Military and Paramilitary Activities in and against Nicaragua, Merits – Judgments - 1986, International Court of Justice (ICJ), 27 June 1986
- Prosecutor v. Haradinaj et al. (Trial Judgment), IT-04-84-T, International Criminal Tribunal for the former Yugoslavia (ICTY), 3 April 2008
- Prosecutor v. Milosevic, Decision on Assigned Counsel Request for Provisional Release, IT-02-54, International Criminal Tribunal for the former Yugoslavia (ICTY), February 23, 2006

- Prosecutor v. Mrksic et al. (Trial Judgment), IT-95-13/1-T, International Criminal Tribunal for the former Yugoslavia (ICTY), 27 September 2007
- Prosecutor vs. Tadic, Case No. IT-94-1-AR72; 35 ILM (1996) 32; Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, International Criminal Tribunal for the former Yugoslavia (ICTY), 2 October 1995
- Abella v. Argentina, Case 11.137, Inter- Am. C.H.R., Report No. 55/97, OEA\Ser.L\V\II.98, doc. 6 rev., 1998

United Nations Official Documents:

- Secretary General's 2009 Report (A/63/677) on Implementing the Responsibility to Protect, 12 January 2009
- General Assembly's Resolution (A/RES/60/1) 2005 World Summit Outcome, p. 30, 24 October 2005
- General Assembly's Resolution (A/RES/70/237) Developments in the field of information and telecommunications in the context of international security, 23 December 2015

Books:

- Boyer, Stuart A.: *SCADA Supervisory Control and Data Acquisition,* ISA – International Society of Automation, 2010, pp. 350
- Burns, J. Patout, ed. *War and Its Discontents: Pacifism and Quietism in the Abrahamic Traditions.* Washington, DC: Georgetown. University Press, 1996, pp. 240
- Carr Jeffrey: *Inside Cyber Warfare*: *Mapping the Cyber Underworld*, *2nd edition*. O'Reilly Media. Sebastopol, CA, 2011, pp. 316
- Cicero, *De Officiis*, Cambridge: Harvard University Press, 1961
- Clarke, Richard A. et Knake, Robert K. *Cyber War: The Next Threat to National Security and What to Do about It.* New York: HarperCollins. New York. 2010. pp. 292
- Clausewitz, C. Von, Howard, M. & Paret, P.: *On War*, Princeton: Princeton University Press, 1989, pp. 732
- Čepelka Č., Šturma, P., *Mezinárodní právo veřejné*, Praha: C.H.Beck, 2008, pp. 896
- Dinniss H. Heather: *Cyber Warfare and the Laws of War*, Cambridge University Press, Cambridge, 2012, pp.331
- Grotius, H.: "*The Rights of War and Peace, including the Law of Nature and of Nations" translated from the Original Latin of Grotius, with Notes and*

Illustrations from Political and Legal Writers, by A.C. Campbell, New York: M. Walter Dunne, 1901, pp. 315

- Guthrie, C. & Michael Q.: *Just War: The Just War Tradition: Ethics in Modern Warfare*, 2007, New York: Walker & Company, pp. 64

- Martens, G. F. de & Cobbett, W.: *The law of nations: being the science of national law, covenants, power, &c*. London: W. Cobbett, 1829, pp. 454

- Monte, M.: *Network Attacks and Exploitation: A Framework*, Indianapolis: Wiley, 2015, pp. 198

- Ondřej, J., Šturma, P., Bílková, V., Jílek, D. a kol. *Mezinárodní humanitární právo*, C. H. Beck, Praha, 2010, pp. 837

- Roscini, M.: *Cyber Operations and the Use of Force in International Law*, Oxford University Press, New York City, 2014, pp. 469

- Rousseau, J.J.*: Social Contract & Discourses*, New York: E. P. Dutton & Co., 1913

- Schmitt, N. Michael et col.: *Tallinn Manual on the International Law Applicable to Cyber Conflict*, Cambridge University Press, 2013, pp. 304

- Schindler, D. & Toman, J.: *The Laws of Armed Conflicts*, Geneva: Martinus Nihjoff Publisher, 1988, pp. 358

Academic Articles:

- Collins, S. et McCombie, S.: *Stuxnet: the emergence of a new cyber weapon and its implications*, Centre for Policing, Intelligence and Counter Terrorism (PICT), Macquarie University, 21 March 2012, pp. 80 – 91

- Dinstein, Y: *The Principle of Distinction and Cyber War in International Armed Conflicts*, Journal of Conflict & Security Law, Vol. 17, No. 2, 2012, pp. 262

- Dervan, L.: *Information Warfare and Civilian Populations: How the Law of War Addresses a Fear of the Unknown*, Goettingen Journal of International Law 3, 2011.

- Dunlap, C.:The *End of Innocence*: *Rethinking Noncombatancy in the Post-Kosovo Era*, 28 Strategic Review 9-17, Summer 2000, pp. 14

- Faix, M.: *Operácie multinárodných síl a medzinárodné humanitárne právo*, Acta Universitatis Carolinae Iuridica, 4/2009, pp.25-39

- Fidler, D. P.: *Was Stuxnet an Act of War? Decoding a Cyber Attack*. Security & Privacy, IEEE , vol.9, no.4, July-Aug. 2011, pp. 56 - 59

- Hathaway, O. A. et col.: *The Law of Cyber-Attack*, California Law Review, HeinOnline, 2012

- ICRC: *The International Committee's Action in the Middle East*, International Review of the Red Cross, 13(152), 1973

- ILA: *Final Report on the Meaning of Armed Conflict in International Law*, The Hague Conference, Hague, 2010, pp. 33

- Langner, R.: *Stuxnet: Dissecting a Cyberwarfare Weapon*, IEEE Security & Privacy, 9(3), 2011, p. 49-51

- Lynn, W. J.: Defending a New Domain: The Pentagon's Cyberstrategy. Foreign Affairs. Sept/Oct. 2010. pp. 97–108.

- Ondřej, J.: "*Právo ozbrojených konfliktů na přelomu tisíciletí,* Mezinárodní vztahy - Severní Amerika, 34, December 1999

- Schmitt, M. N.: *International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed*, Harvard International Law Journal, Vol. 54, 2012

- Schmitt, M.N.: *"Attack" as a Term of Art in International Law: The Cyber Operations Context*, Tallinn: NATO CCD COE Publications, 2012, pp. 286

- Swiney, G.: *Saving Lives*: *The Principle of Distinction and the Realities of Modern War*, International Law 39 (733), 2005

- Šturma, P.: *Universal Jurisdiction and Prosecution of Grave Breaches of The Geneva Conventions of 1949,* Acta Universitatis Carolinae Iuridica, 2009(4), pp. 175 – 184

Articles:

- Bacchi, U.: *Israeli-linked malware Duqu 2.0 'used to spy on Iran nuclear talks venues*, International Business Times, 10 June 2015. Retrieved 24 August 2016. http://www.ibtimes.co.uk/israeli-linked-malware-duqu-2-0-used-spy-iran-nuclear-talks-venues-1505427

- Falliere, N., O Murchu, Liam et Chien, Eric: *W32.Stuxnet DoSsier.* Symantec Report, February 2011. Retrieved 24 August 2016. http://www.wired.com/images_blogs/threatlevel/2011/02/Symantec-Stuxnet-Update-Feb-2011.pdf

- Hopkins, N.: *Computer worm that hit Iran oil terminals 'is most complex yet*, The Guardian, 28 May 2012. Retrieved 24 August 2016.

https://www.theguardian.com/world/2012/may/28/computer-worm-iran-oil-w32flamer

- Hossein, J.: *Iran says has detected Duqu computer virus,* Reuters, 13 November 2011. Retrieved 24 August 2016. http://www.reuters.com/article/us-iran-computer-duqu-idUSTRE7AC0YP20111113

- ICRC: *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts,* Report 31IC/11/5.1.2, 31st International Conference of the Red Cross and Red Crescent, October 2011. Retrieved 24 August 2016. https://app.icrc.org/e-briefing/new-tech-modern-battlefield/media/documents/4-international-humanitarian-law-and-the-challenges-of-contemporary-armed-conflicts.pdf

- Kochetkova, K.: *What is known about the Lazarus Group: Sony hack, military espionage, attacks on Korean banks and other crimes,* Kaspersky Lab, 24 February 2016, Retrieved 20 July 2016. https://blog.kaspersky.com/operation-blockbuster/11407/

- Langner, R.: *Stuxnet: Dissecting a Cyber warfare Weapon*. Security & Privacy, IEEE, vol.9, no.3, pp. 51, May-June 2011. Retrieved 24 August 2016. http://www.mediafire.com/download_repair.php?dkey=7z3101x31rx&qkey=k86sevhvvzklgek

- Park, J.-M.: *Keyboard warriors: South Korea trains new frontline in decades-old war with North,* The Reuters, 21 June 2016. Retrieved 20 July 2016. http://uk.reuters.com/article/us-northkorea-southkorea-cyber-idUKKCN0Z50Y0

- Nguyen, Nam K.: *The International Humanitarian Law Implications of the 'Tallinn Manual'*, 2014. Retrieved 24 August 2016. http://www.e-ir.info/2014/02/12/the-international-humanitarian-law-implications-of-thetallinn-manual/

- Ondřej, J.: *Právo ozbrojených konfliktů na přelomu tisíciletí*, Mezinárodní vztahy, Severní Amerika, 34, December 1999. Retrieved 24 August 2016. https://mv.iir.cz/article/view/1228

- Richards, J.: *Denial-of-Service The Estonian Cyberwar and Its Implications for U.S. National Security*, International Affairs Review, The Elliot School of International Affairs at George Washington University. Retrieved 24 August 2016. http://www.iar-gwu.org/node/65

- Riley, D.: *Finger pointed at North Korea as Swift malware attacks hit 12 banks*, Silicon Angle, 30 May 2016. Retrieved 24 August 2016. http://siliconangle.com/blog/2016/05/30/finger-pointed-at-north-korea-as-swift-malware-attacks-hit-12-banks/

- Silverstein, R.: *Flame: Israel's New Contribution to Middle East Cyber war*. 29 May 2012. Retrieved 24 August 2016.

http://www.richardsilverstein.com/2012/05/28/flame-israels-new-contribution-to-middle-east-cyberwar/

- Schwartz, M. J.: *Flame 2.0: Gauss Malware Targets Banking Credentials.* 9 August 2012. Retrieved 24 August 2016. http://www.darkreading.com/attacks-and-breaches/flame-20-gauss-malware-targets-banking-credentials/d/d-id/1105727?

- Schneier, B.: *Threat of 'cyberwar' has been hugely hyped,* 7 July 2010. Retrieved 24 August 2016. http://edition.cnn.com/2010/OPINION/07/07/schneier.cyberwar.hyped/index.html

- Shachtman, N.: *Kremlin Kids: We Launched the Estonian Cyber War*, Wired, 3 November 2009. Retrieved 24 August 2016. https://www.wired.com/2009/03/pro-kremlin-gro/

- Traynor, I.: *"Russia accused of unleashing cyberwar to disable Estonia",* The Guardian, 17 May 2007. Retrieved 24 August 2016. https://www.theguardian.com/world/2007/may/17/topstories3.russia

- Zetter, K: *Meet 'Flame,' The Massive Spy Malware Infiltrating Iranian Computers*, Wired, 29 May 2012. Retrieved 24 August 2016. http://mashable.com/2012/06/04/flame-malware/

Websites:

- *Akamai's State of the Internet*, Q4 2015 Executive Review, Akamai, 2015. Retrieved 20 July 2016. https://www.stateoftheinternet.com/downloads/pdfs/Q4-2015-SOTI-Connectivity-Executive-Summary.pdf

- Arms Control Association: *The UN Takes a Big Step Forward on Cyber Security.* Retrieved 20 July 2016. http://ccdcoe.org/united-nations-group-governmental-experts-long-awaited-reportmaintaining-peace-and-stability-ict.html

- BBC News: *Flame: Israel rejects link to malware cyber-attack*, May 31 2012. Retrieved 24 August 2016. http://www.bbc.com/news/technology-18277555

- BBC News: *US 'launched Flame cyber attack on Sarkozy's office*, 21 November 2012. Retrieved 24 August 2016. http://bbc.in/T4mbzx

- BBC News: *Iran 'fends off new Stuxnet cyber attack'*. 25 December 2012. Retrieved 24 August 2016. http://bbc.in/TmriwM

- BBC World Online Network: *NATO Denies Targeting Water Supplies*, 1999. Retrieved 24 August 2016. http://www.news.bbc.co.uk/hi/english/world/europe/newsid_351000/351780.stm

- CCDCOE: Tallinn Manual 2.0 to Be Completed in 2016, 9 October 2015. Retrieved 25 July 2016. https://ccdcoe.org/over-50-states-consult-tallinn-manual-20.html

- CRySyS Lab*: sKyWIper: A Complex Malware for Targeted Attacks*, Budapest University of Technology and Economics, 28 May 2012. Retrieved 20 July 2016. http://www.crysys.hu/skywiper/skywiper.pdf

- Cyberarms: *The Weapon that Disabled Iraq's Power Grid,* 2010. Retrieved 20 July 2016.https://cyberarms.wordpress.com/2010/04/28/the-weapon-that-disabled-iraqs-power-grid/

- ICRC: *International Humanitarian Law and the challenges of contemporary armed conflicts*", October 2011, pp. 8. Retrieved 20 July 2016. https://www.icrc.org/eng/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-en.pdf

- ICRC: *Interpretive Guidance On The Notion Of Direct Participation In Hostilities Under International Humanitarian Law*, 2009. Retrieved 20 July 2016. http://www.icrc.org/eng/assets/files/other/icrc_002 0990.pdf

- ICRC: *Development of modern International Humanitarian Law*, 13 May 2010. Retrieved 20 July 2016. https://www.icrc.org/eng/who-we-are/history/since-1945/history-ihl/overview-development-modern-international-humanitarian-law.htm

- ICRC: *How is the Term "Armed Conflict" Defined in International Humanitarian Law?*, March 2008. Retrieved 20 July 2016. https://www.icrc.org/eng/assets/files/other/opinion-paper-armed-conflict.pdf

- Kaspersky Lab in Gilbert, D.: *Duqu 2: The most advanced cyber-espionage tool ever discovered*", 10 June 2015. Retrieved 20 July 2016. http://www.ibtimes.co.uk/duqu-2-most-advanced-cyber-espionage-tool-ever-discovered-1505439

- Kaspersky Lab: *NetTraveler Attacks*, Part 1, 4 June 2013. Retrieved 20 July 2016. https://cdn.securelist.com/files/2014/07/kaspersky-the-net-traveler-part1-final.pdf

- Kaspersky Lab: *Equation Group: The Crown Creator of Cyber-Espionage*, 16 February 2015. Retrieved 20 July 2016. http://www.kaspersky.com/about/news/virus/2015/equation-group-the-crown-creator-of-cyber-espionage

- Kaspersky Lab: *Unvealing "Careto" – The Mask "APT",* February 2014. Retrieved 20 July 2016. http://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/unveilingthemask_v1.0.pdf

- *Resource 207: Kaspersky Lab Research Proves that Stuxnet and Flame Developers are Connected*. Kaspersky Lab. 11 June 2012. Retrieved 24 August 2016. https://www.kaspersky.com/about/news/virus/2012/Resource_207_Kaspersky_Lab_Research_Proves_that_Stuxnet_and_Flame_Developers_are_Connected

- Reuters: *North Korea denies cyber-attacks on South Korea officials*, 13 March 2016. Retrieved 24 August 2016. http://www.reuters.com/article/us-northkorea-korea-cyber-idUSKCN0WF05V

- Securelist: *"Red October" Diplomatic Cyber Attacks Investigation*, 14 January 2013, p.3. Retrieved 20 July 2016. https://securelist.com/analysis/publications/36740/red-october-diplomatic-cyber-attacks-investigation/#7

- *Security Council Imposes Fresh Sanctions on Democratic People's Republic of Korea, Unanimously Adopting Resolution 2270 (2016)*, SC/12267, 7638th Meeting, Security Council Press Release, 2 March 2016. Retrieved 20 June 2016. http://www.un.org/press/en/2016/sc12267.doc.htmv

- *South Korea Accuses North of Cyber-attacks on Nuclear Plants*, Security Week, 17 March 2015. Retrieved 24 August 2016. http://www.securityweek.com/south-korea-accuses-north-cyber-attacks-nuclear-plants

- *Stoltenberg: Kybernetický útok na NATO bude důvod ke kolektivní obraně,* Lidové noviny, 14 June 2016. Retrieved 20 July 2016. http://www.lidovky.cz/stoltenberg-nato-oznaci-kyberprostor-za-bezne-operacni-prostredi-1d0-/zpravy-svet.aspx?c=A160614_201214_ln_zahranici_ELE

- Symantec: *Flamer: Highly Sophisticated and Discreet Threat Targets the Middle East.* 30 May 2012. Retrieved 20 July 2016. https://www.symantec.com/connect/blogs/flamer-highly-sophisticated-and-discreet-threat-targets-middle-east

- Symantec: *The Shamoon Attacks.* 12 August 2012. Retrieved 20 July 2016. https://www.symantec.com/connect/blogs/shamoon-attacks

- UNODA: *Developments in the field of information and telecommunications in the context of international security.* Retrieved 20 July 2016. http://www.un.org/disarmament/topics/informationsecurity/

- UNODA: *Chemical Weapons.* Retrieved 20 July 2016. www.un.org/disarment/WMD/Chemical/

- US Department of Defense, DOD Dictionary of Military Terms. Retrieved 20 July 2016 http://www.dtic.mil/doctrine/dod_dictionary/data/c/10082.html

- US Department of Homeland Security: *The US National Strategy to Secure Cyberspace*, 2003. Retrieved 20 July 2016. http://georgewbush-whitehouse.archives.gov/pcipb/

TEZE DIPLOMOVÉ PRÁCE V ČESKÉM JAZYCE (SUMMARY IN CZECH LANGUAGE)

1. Základní východiska válečného a mezinárodního humanitárního práva

Během posledních dvaceti let, kybernetický prostor zahrnující počítačové sítě a jejich zařízení prostoupil významnou měrou všechny důležité sféry lidského života, a to včetně ozbrojených konfliktů. V jejich oblasti pak kybernetické sféra dosáhla rozměrů naprosto nevídaných a jen těžce představitelných v době vytvoření právního rámce určeného pro regulaci použití této sféry a jejích nástrojů ve válečném stavu na mezinárodní úrovni, a sice válečného a mezinárodního humanitárního práva (MHP).

Přesto tato pravidla určená pro regulaci ozbrojených kinetických konfliktů v současnosti regulují i mezinárodní konflikty kybernetické, a nadto pouze teoreticky, neboť v praxi v této oblasti panuje mezinárodně právní vakuum. Jelikož, i když je stávající teze taková, že se na mezinárodní kybernetické konflikty dosahující úrovně ozbrojených konfliktů kinetických aplikuje MPV v plném rozsahu, tato teze je nejenže v praxi kvůli naprosto odlišnému charakteru kybernetických zbraní a útoků zřídka kdy proveditelná, nicméně navíc ani není potvrzená žádným oficiálním konsensem na mezinárodní úrovni.

Proto si tato práce klade za cíl v prvé řadě osvětlit problematiku kybernetických útoků, jejich charakter a klasifikaci; představit ty oblasti a nástroje kybernetické války, jež jsou prakticky nepokryté současnou MHP úpravou; poukázat na hlavní oblasti inkompatibility kybernetických konfliktů se stávajícím MHP rámcem určeným pro kinetické konflikty spočívající především v odlišnostech co do autorství, času a teritoria; a konečně představit návrh řešení současného stavu, a sice návrh nové mezinárodní úmluvy o kybernetické válce a klíčové prvky, které by měla obsahovat.

Válečné právo („*laws of war*“) má svůj původ v teorii spravedlivé války, která se objevuje již u Cicera v jeho De Officiis roku 44 př.n.l. V té době teorie spravedlivé války obsahovala pravidla nejen pro vedení války, ale také pro její začátek, a tak v sobě spojovala dva původní režimy válečného práva, a sice *jus ad bellum,* tj. právní úpravu vztahující se na období před vstupem do ozbrojeného konfliktu vymezující legitimní vstup země do války, a *jus in bello,* které je dnes známo jako mezinárodní humanitární právo, tj. pravidla pro vedení ozbrojeného konfliktu jako takového, bez ohledu na to, zda ke vstupu do něj došlo v souladu s *jus ad bellum.* Později byl k těmto dvěma režimům

spravedlivé války přidán i třetí, a sice *jus post bellum,* jež se vztahuje na časové období po ukončení válečného konfliktu, a v současnosti se dá prakticky ztotožnit s mezinárodním právem trestním.

Práce se soustředí na režim MHP, nicméně v některých částech pojednává také o *jus ad bellum* a méně často pak i *jus post bellum,* neboť zaprvé bylo mnohdy nutné vymezit rozdíl v pojetí literárně totožných pojmů v těchto režimech, poněvadž se význam dotyčných pojmů v závislosti na tom či onom režimu markantně liší; zadruhé se v mnoha odborných pramenech zabývajících se otázkou vztahu MHP a kybernetické války tato prolíná s otázkou vztahu kybernetické války a *jus ad bella*, takže při analýze těchto pramenů bylo zmínění příbuzných právních rámců vztahujících se na ostatní dva válečné režimy nevyhnutelné.

V současnosti se teorie spravedlivé války i nadále vyvíjí, a ovlivňuje tak i mezinárodněprávně politický vývoj. Nejnovější koncept, podle kterého suverenita státu zahrnuje také jeho odpovědnost za ochranu vlastních obyvatel a jejich lidských práv, se nazývá Odpovědnost za ochranu („*Responsibility to Protect", R2P*). Koncept ustanovený ve Výstupní dokumentu Světového summitu Spojených národů v roce 2005 stanoví, že v případě selhání suverénního státu v povinnosti dostát své odpovědnosti za ochranu svého obyvatelstva, je zajištěním této ochrany povinováno mezinárodní společenství na základě rozhodnutích Rady bezpečnosti.

Navzdory mnoha pokusům předních právních expertů, filozofů a vojevůdců definovat termín války, žádný se neujal tak, jako Clausewitzova definice války: „*Aktu násilí za účelem donucení našeho oponenta naplnit naši vůli,*"[189] a to navzdory faktu, že oficiální definice neexistuje. Jelikož kodifikace MHP však znamenala, že po oficiálním vstupu do války musela být dodržována dotyčná pravidla MHP režimu, vyhlašování války přestalo být dodržováno, a důsledkem toho ztratilo na významu.

V současnosti je tak pojem válka nahrazován pojmem ozbrojený konflikt, i když ani jeho oficiální definici nikde nenajdeme. Nicméně Mezinárodní výbor červeného kříže („*International Committee of the Red Cross*", ICRC) jej definuje jako: „*Uchýlení se k ozbrojeným silám jedním nebo vice státy*". [190] Mezinárodní právní asociace v roce 2005 prohlásila, že existence ozbrojeného konfliktu závisí na naplnění minimálních kritérií, a

[189] Von Clausewitz, C., Howard, M. & Paret, P.: *On War*, Princeton: Princeton University Press, 1989, p. 1
[190] ICRC: *How is the Term "Armed Conflict" Defined in International Humanitarian Law?,* March 2008.

sice: „*Existence ozbrojených organizovaných skupin zapojených do bojů určité intenzity.*"[191]

Konečně je také nutno rozlišit mezi ne-mezinárodním ozbrojeným konfliktem („Non-International Armed Conflict" NIAC)[192], na které se MHP až na explicitní výjimky prakticky nevztahuje, a mezinárodním ozbrojeným konfliktem („International Armed Conflict", IAC)[193] pro které bylo MHP vytvořeno především. Ačkoli kvůli nedávnému vývoji zahrnujícímu jak rozšíření teroristických útoků, tak použití kybernetických zbraní, dochází poměrně často ke stírání hranice mezi NIAC a IAC.

Nadto je třeba rozlišit pojem ozbrojeného útoku v *jus ad bellum*, kde je tento: „*Akcí, která dává státům právo na odpověď dosahující úrovně předcházejícího užití síly protivníka*" a pojmu útok v MHP, kde je tento definován jako: „*Jistá kategorie vojenských operací,*"[194] a dále také jako: „*Akt násilí proti protivníkovi, ať už v ofenzivě či v defenzivě.*"[195] Práce tedy používá termínu „ozbrojený útok" v kontextu *jus ad bello* a termínu „útok" v kontextu MHP. Nicméně v obou právních režimech se klade otázka, zda lze kybernetický útok považovat ať už za ozbrojený útok v *jus ad bello* či útok v MHP.

Počátek MHP se datuje do druhé poloviny 19. století, kdy byla založena mezinárodní instituce dnes známá jako Mezinárodní výbor červeného kříže, která v roce 1864 přivedla 16 zemí k podpisu První ženevské úmluvy o zlepšení osudu raněných a nemocných příslušníků ozbrojených sil v poli. Po Rusko-japonské válce v roce 1906 následovala Druhá ženevská úmluva vztahující se na členy námořních ozbrojených sil, v roce 1929 byla podepsána Třetí ženevská úmluva o zacházení s válečnými zajatci, a konečně v roce 1949 Čtvrtá ženevská úmluva vztahující se na civilisty, přičemž zároveň došlo také k významné revizi úmluv předcházejících. Součást Ženevských konvencí tvoří také tři Dodatkové protokoly a tři Společné články, které definovaly pole působnosti úmluv, tzv. ženevského práva, které se věnuje především ochraně osob v průběhu ozbrojených konfliktů. Pravidla vedení ozbrojených konfliktů, způsobů a prostředků v nich použitých upravuje tzv. haagské právo, jehož původním a hlavním pramenem je První a Druhá Haagská úmluva z roku 1899, respektive 1907.

[191] ILA: *Final Report on the Meaning of Armed Conflict in International Law*, The Hague Conference, Hague, 2010, p. 32
[192] Article 1(1) of Protocol II to the Geneva Conventions
[193] Common Article 2 of the Geneva Conventions
[194] Schmitt, p. 285
[195] Article 49 (I) of the Additional Protocol I

Obecné zásady MHP vycházejí z úsilí zamezit tzv. absolutní válce, jež by mohla být pro lidstvo fatální, a jsou tak považovány za součást *jus cogens.* Obecné zásady se tak dělí do kategorie zakazující určité dopady útoků, a sice zákaz zbytečného utrpení, zásada vojenské nezbytnosti, proporcionality a nediskriminace, a kategorie, která stanovuje určité chování jako například zásada předběžné opatrnosti. Dále existují specifické zásady MHP týkající se konkrétních typů zbraní či způsobu vedení konfliktu.

2. Kybernetické zbraně, kybernetická válka a MHP rámec

Aby bylo možno zodpovědět otázku, zda je možné kybernetický útok považovat za útok a kybernetickou válku za ozbrojený konflikt, je v prvé řadě nutné pochopit fungování kybernetických zbraní.

Ačkoliv opět chybí oficiálně přijatá definice kybernetické války, tato práce vychází z definice Richarda A. Clarke, kybernetického expera z USA: „*Akce podniknuté národem-státem za účelem proniknutí do státních počítačů či sítí za účelem způsobení škody nebo přerušení procesů*,"[196] a dále zužuje Clarkovu definici na útočné akce uskutečněné po počítačových sítí („computer network attacks", CNA),197 za což jsou považovány: „*Akce podniknuté za použití počítačových sítí za účelem porušení, poškození, znehodnocení nebo zničení informací uchovávaných na počítačích a počítačových sítí či počítačích a sítích zvlášť."*[198]

CNA se tak dělí na syntaktické útoky, známé také jako malware, jež cílí na IT zařízení a sítě jako takové, a sémantické útoky, které cílí uživatele dat, a snaží se proto zabránit uživateli v přístupu k datům zprostředkovaných prostřednictvím napadnutých IT zařízení. CNA se mohou dělit podle typu útoku, který způsobují, nebo podle druhu malwaru, do kterého spadají.[199]

Pro účely práce nejdůležitějšími útoky jsou DoS útoky („Denial-of-Service", DoS), které se nacházejí na rozhraní syntaktických a sémantických útoků, podle toho, zda usilují také o poškození či zničení informace, nebo pouze o její znepřístupnění po určitou dobu; dále pak trojští koni, kteří se typicky vydávají za jiný program na počítačovém zařízení, přičemž zároveň monitorují uživatelovu aktivitu, či do ní dokonce zasahují; a

[196] Clarke, R. A. et Knake, R. K.: *Cyber War: The Next Threat to National Security and What to Do about It*, New York: HarperCollins, 2010, p.32
[197] Dinniss, p. 4
[198] US Department of Defense, DOD Dictionary of Military Terms Online
[199] Monte, M.: *Network Attacks and Exploitation: A Framework*, Indianapolis: Wiley, 2015, p. 38

v neposlední řadě také tzv. backdoor malwary, které umožňují obejít běžné autentizační metody spočívající v zadávání kódů a hesel a zanechat napadené zařízení „otevřené“ pro původce malwaru.

Mezi nejznámější akce, které poodhalily sílu CNA útoků jakož i možnou cestu národní obrany, kterou se státní entity v současnosti vydávají, bezesporu patřil útok provedený malwarem Stuxnet oficiálně odhalený v červnu 2010, jež působil na Blízkém východě a dokázal zničit či minimálně odstavit část íránského vládního programu; a série DoS útoků ruských hackerů na oficiální webové stránky mnoha předních estonských jak vládních, tak soukromých aktérů, včetně největších estonských bank a mediálních společností, provedených v květnu 2007.

Dále během několika méně známých útoků, které pravděpodobně pocházely od státních entit a byly mířené na oficiální entity jiného státu, došlo k hromadným odposlechům nejen aktivit provozovaných na daných sítích či počítačích, ale také fyzických aktivit v bezprostřední blízkosti daných zařízení, získání přístupů do bankovních účtů, interních počítačových sítí a softwarů ovládajících provoz inženýrských sítí včetně elektráren, elektrických rozvodů a přehrad, jakož i interních systémů vládních úřadů, ministerstev a zastupitelských úřadů v zahraničí.

Navzdory těmto nebezpečím, mezinárodní společenství stejně jako mnoho významných expertů na MHP se buďto ke vztahu MHP a kybernetické války nevyjadřuje nebo se k ní staví skepticky. Nicméně ICRC již v roce 2011 vydal prohlášení, ve kterém uvádí, že CNA by mohly být kvalifikovány jako útoky ve smyslu MHP[200] a že: „*Fakt, že nevedou k fyzické destrukci napadeného objektu je irelevantní.*“[201]

[200] ICRC: *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts,* Report 31IC/11/5.1.2, 31st International Conference of the Red Cross and Red Crescent, October 2011
[201] Idem p. 37

3. Nevýhody aplikace současných právních rámců válečného práva na kybernetickou válku

Vzhledem k tomu, že současný MHP rámec je poměrně dobře rozvinutý, tak je logické, že se v případě, kdy se vyskytne nová sféra, která spadá do MHP, aplikace metodou interpretace nabízí asi jako vůbec první možné řešení problému právní úpravy této nové sféry. Nicméně tato kapitola si klade za cíl osvětlit, proč metoda interpretace není nejefektivnějším řešením, a to zaprvé poukázáním na její obecné nedostatky, a za druhé na její konkrétní nedostatky v konfrontaci s kybernetickým prostorem.

Prvním závažným obecným nedostatkem metody interpretace je nedostatečná úroveň legitimity subjektů, které by měly interpretaci provádět, a s tím spojený následný nedostatek respektu a dodržování nově ustanovených pravidel vyplývajících ze závěrů interpretačních subjektů. Tento nedostatek představuje již dnes reálný problém předních mezinárodních soudních institucí, jelikož mnohé státy dlouhodobě oponují ideji globálně univerzální jurisdikce, a to i v případech závažných porušení MHP.[202] Například co se týče mezinárodních sporů řešenými Mezinárodním soudním dvorem (MSD), Spojené státy americké se stáhly z obecné jurisdikce této instituce v roce 1986, a sice v reakci na vydání rozsudku ve věci Nikaragua vs. Spojené státy americké. Nicméně i v případech, kdy státy obecnou jurisdikci Mezinárodního soudního dvora respektují, je vynutitelnost rozsudků MSD velmi zdlouhavá a obtížná, neboť Dvůr sám vynucovací pravomoc nemá a je odkázán na Radu bezpečnosti OSN.

Co se týče Mezinárodního trestního soudu (MTS) ustanoveného Romským statutem, jeho jurisdikce je velice omezená, neboť mnohé státy včetně předních mocností jako USA, Rusko, Čína, Indie či Saudská Arábie tento zakládající dokument ani neratifikovaly. Pokud největší mocnosti odmítly uznat rozhodovací pravomoc mezinárodní soudní instituce v případě, kdy je právní rámec definující její působnost dobře znám a předem konsensuálně dohodnut, je spíše nerealistické předpokládat, že by podobné mezinárodní instituci byla udělena nejen rozhodovací pravomoc, ale také pravomoc interpretační tak silná, že by se překrývala s pravomocí tvořit právní normy nové, což by byla realita v případě, že by jí byla svěřena pravomoc interpretovat MHP normy v kontextu kybernetické války a zbraně.

[202] Šturma, P.: *Universal Jurisdiction and Prosecution of Grave Breaches of The Geneva Conventions of 1949*, Acta Universitatis Carolinae Iuridica, 2009 (4), p.184

V tomto případě je tedy ještě nereálnější se domnívat, že by interpretaci mohly provádět instituce disponující ještě menší kolektivní mezinárodní legitimitou jako například právní experti a vědci, což dosvědčuje příklad Tallinnského manuálu. Ten, jakožto produkt skupiny expertů svolané Severoatlantickou aliancí (NATO), bohužel postrádá celosvětovou legitimitu, neboť nečlenské státy NATO mohou a budou jeho závěry vždycky napadat jako politicky motivované. Nadto Tallinnský manuál při pečlivém čtení přináší spíše více otázek než odpovědí, čehož si je vědom i iniciátor jeho vzniku – NATO, které již připravuje s obdobnou skupinou expertů Tallinnský manuál 2.0.

Další problém metody interpretace spočívá více v jeho technickém rázu – jedná se o samotnou klasifikaci kybernetických zbraní. Jelikož vojenské objekty využívají pro komunikaci civilní počítačové sítě, kybernetické zbraně by tak teoreticky mohly být považovány za tzv. slepé zbraně, které jsou „*neschopny rozlišovat mezi civilisty a vojenskými objekty*,“[203] a jako takové být de facto zakázány podobně jako jaderné zbraně.[204] S tím souvisí také potřeba vyřešit otázky související s principem proporcionality, a sice za jakých podmínek je možné na kybernetické zbraně odpovědět kinetickými útoky a naopak. I tady je nepravděpodobné, že by zodpovězení těchto otázek bylo svěřeno komukoliv jinému než mezinárodnímu společenství jako celku.

4. Základní nekompatibilita mezi současnou úpravou MHP a kybernetickou válkou a zbraněmi: anonymita, teritorialita a čas

Hlavní překážka aplikovatelnosti současné úpravy MHP na kybernetickou válku a zbraně spočívá ve třech fakticky naprosto odlišných pojetí základních dimenzí ozbrojeného konfliktu – původu, teritoriality a času. Tato odlišná pojetí spočívají konkrétně v nežádoucímu autorství respektive anonymitě útoků, pojetí lokace a teritoria ozbrojeného konfliktu, a konečně rychlosti útoku v kontextu kybernetického konfliktu a ozbrojeného konfliktu kinetického, ať už se tento odehrává na souši, ve vzduchu či na moři.

Co se týče autorství útoků, respektive anonymity jejich autorů, tu je v případě kinetických útoků velice obtížné si zachovat, a to především v dlouhodobém hledisku. Nicméně v případě útoků kybernetickými zbraněmi může být anonymita útočníků

[203] Y. Dinstein: *The Principle of Distinction and Cyber War in International Armed Conflicts*, Journal of Conflict & Security Law, Vol. 17, No. 2, 2012, p. 262
[204] Legality of the Threat or Use of Nuclear Weapons, I.C.J. Advisory Opinion, par.78, July 8 1996

zachována i při opakovaných útocích téměř navěky, jelikož je v praxi jen velice obtížné zjistit odkud přesně byl útok zahájen. Navíc, i když je odhaleno zapojení konkrétních útočníků či útočníků konkrétní národnosti do kybernetického útoku, je velmi těžké těmto dokázat, že útoky provedli na objednávku či v přímém nasazení pro státní aktéry, a nikoliv v jejich soukromém zájmu, popřípadě v rámci nestátní organizované zločinecké skupiny, jako tomu bylo například při kybernetických útocích v Estonsku.

S anonymitou útočníků souvisí také zásada ochrany civilistů v MHP, která je ve své aktuální podobě na kybernetické útočníky prakticky neaplikovatelná, neboť pokud by již lokace útočníků byla přesně odhalena (původce nakažených USB disků, lokace skutečné IP adresy), což je už i tak v praxi téměř nemožné, útočník používající kybernetických zbraní se může vždycky vydávat za civilistu, jehož počítač byl k útokům zneužit prostřednictvím backdoor malwarů. Navíc kybernetické útoky mohou být na dálku řízeny i z počítačů opravdových civilistů, a tím je tak ohrozit.

Co se týče teritoriálního aspektu kybernetických útoků, ten je také naprosto nesrovnatelný s pojetím teritoria a lokalizace při kinetických útocích. Zaprvé, v případě kybernetických útoků je takřka nemožné teritorium ozbrojeného konfliktu jakkoli fyzicky vymezit či omezit, neboť způsob šíření kybernetických zbraní je srovnatelný s šířením zbraní chemických či biologických, ale na ještě větším rozsahu, navíc opět s takřka nevystopovatelným epicentrem útoku. Vedle toho kybernetické zbraně dosahují svých cílů mnohdy za užití civilních počítačových sítí, ale mohou jich dosahovat také prostřednictvím kybernetických útoků mířených či postihujících civilisty, jako v případě zasažení elektrické sítě či v případě DoS útoků.

Dalším problémem spojeným s teritorialitou útoků je, jestli má stát, jehož sítěmi útok pouze prochází, právo či povinnost takovému kybernetickému útoku zamezit, a pokud ano, tak jestli i v případě, že by tomu tak bylo na úkor domácích uživatelů dané sítě.

Nadto, dokonce i v případě kybernetických útoků lze občas lokalizovat data, jelikož datová úložiště jsou ve skutečnosti přece jen relativně snadno lokalizovatelné materiální objekty, což je případ především hromadných datových úložišť, které mohou teoreticky sloužit jako skladiště kybernetických zbraní. I v tomto případě se nabízí otázka, zda má stát, na jehož území se dané úložiště nachází, právo anebo dokonce povinnost toto úložiště jakkoliv sledovat, zasahovat do něj či jej dokonce fakticky modifikovat, a současně opět také otázka proporcionality takovéhoto eventuálního práva v porovnání s právy běžných uživatelů.

Hledisko teritoriality se tak v mnohém podobá také NIACu v kontextu teroristických útoků, jejichž cíl jakož i směr šíření jsou opět nepředvídatelné.

Konečně, co se týče otázky pojetí času, to úzce souvisí s dvěma předcházejícím body: díky rychlosti útoků je schopnost zasáhnout obrovské teritorium maximalizována, a zároveň schopnost útočníka zachovat si anonymitu je významně zesílena faktem, že ačkoliv kybernetický útok může působit takřka okamžitě, o jeho existenci se napadený nemusí dozvědět hned v době útoku, ale až daleko později, jelikož ty nejvíce sofistikované CNA jsou navrženy tak, aby nebyly hostitelem či obětí zaznamenány a obsahují i velmi rozvinuté způsoby maskování se jako neškodný software.

Nadto, absence povědomí o proběhlém útoku znemožňuje dalším entitám, které by mohly představovat potencionální cíl dalších útoků tyto efektivně předvídat. Například, pokud je napadena elektrárna soukromé společnosti, ta ve skutečnosti ne vždycky své souputníky či vládní entity o proběhlém útoku informuje, a to z důvodu obavy o svoji pověst nebo postavení na trhu. Tím pádem jsou ty normy MHP, kde hraje pojem nezbytné nutnosti či neodkladnosti důležitou roli, ohroženy na významu. S tím také souvisí zákaz nepřiměřeně závažného útoku ustanoveného v čl. 51 (5) (b) a čl. 57 Dodatkového protokolu I, jakož i zákaz neurčitých útoků stanového v čl. 51 (4) Dodatkového protokolu I, do jejichž rámců by CNA mohly snadno spadat.

5. Nezbytné části nové úmluvy o kybernetické válce

Na rozdíl od předchozích kapitol, které analyzovaly a kriticky hodnotily současnou MHP úpravu, poslední pátá kapitola práce zaujímá hledisko *de lege ferenda* a snaží se navrhnout základní body, které by nová úmluva o kybernetické válce, jejíž nezbytnost dosvědčily předcházející kapitoly, měla obsahovat.

Co se týče formální stránky, nová úmluva by se řídila standardně Vídeňskou úmluvou o smluvním právu z roku 1969. Strany úmluvy by byly definovány tzv. Vídeňskou formulí a celý smluvní proces by byl koordinován OSN.

Co do obsahu nové úmluvy, ten by měl zcela jistě zahrnovat novou definici pojmu útok v kontextu kybernetické války a zbraní včetně specifikace pojmu „násilí“, jež má podle čl. 49 (1) Dodatkového protokolu I pro definici útoku ve stávající MHP úpravě postavení *sine qua non* prvku. Kybernetické útoky by tak mohly být definovány jako *kybernetické operace, ať ofenzivní či defenzivní povahy, které, pokud provedeny, mají závažný dopad na osoby či objekty, jež zároveň vede k lidským ztrátám na životech či*

zraněním a nebo k vážné škodě nebo zničení předmětů nezbytných pro přežití civilního obyvatelstva včetně veřejné infrastruktury a jejích sítí.

Dále by pak měly být specifikovány hlavní zásady MHP v kybernetickém kontextu, pozornost by se samozřejmě měla soustředit na ty, které by v daném případě vzbuzovaly nejvíc nejasností. Například zásada rozlišování by měla být v novém kontextu zcela redefinována, nicméně by měla zůstat zachována, a to i navzdory právním expertům volajícím po upuštění od této zásady[205].

Podobně by mělo dojít k přehodnocení zásady zákazu cílení civilistů, a sice ve smyslu její konkretizace nejen vzhledem ke kybernetickým útočníkům, ale především k civilním počítačovým sítím a jejím uživatelům. Úmluva by tak mohla považovat všechny civilisty, kteří aktivně a vědomě participují na kybernetických útocích za jedince, které je možno legitimně považovat za cíl.

Zároveň by také měla být zodpovězena otázka, zda soukromé entity, jejichž existence či činnost jsou nezbytné pro řádný chod země, mohly profitovat ze zvláštního ochranného statusu podobně jako entity spravující základní infrastrukturu, či nikoliv.

Dále by měla být adresována také zásada neutrality, která má v kybernetickém kontextu obzvlášť komplexní povahu, a to zejména s ohledem na země, na jejichž území se nacházejí či jež spravují datové sítě.

Vedle toho by měla být specifikována rovněž i zásada proporcionality, jež vyžaduje, anticipovat dopady útoků vzhledem k možným zraněním a ztrátě na životech a škodách na civilních objektech tak, aby tyto nepřesáhly očekávané a přímé vojenské zisky vyvolané útokem. V opačném případě se totiž jedná o neurčité útoky, jejichž výkon současný MHP rámec nedovoluje.

Konečně by úmluva měla redefinovat pojem špionáže v kybernetickém kontextu, neboť techniky, které jsou podle aktuální pravidel hodnoceny nikoliv jako útok, nýbrž jako špionáž, by v nevídaně vysokém měřítku a frekvenci, jež jsou umožněny právě kybernetickými zbraněmi, teoreticky mohly být hodnoceny jako útok ve smyslu MHP.

Celkově by se tak členové mezinárodního společenství měli dohodnout na konkrétním společném pojetí útoků, ozbrojených konfliktů a pojetí zbraní a násilí platném v případě kybernetické války, jež v současnosti představuje jednu z nejdynamičtěji se rozvíjejících oblastí právního vakua panujícího v mezinárodním humanitárním právu, a

[205] Dunlap, C.:The *End of Innocence*: *Rethinking Noncombatancy in the Post-Kosovo Era*, 28 Strategic Review 9-17, Summer 2000, p. 14.

to raději dříve, než se tak bude muset stát *a posteriori* – po proběhnutí kybernetických útoků či kybernetického konfliktu nevídaných rozměrů.

ABSTRAKT / ABSTRACT

ABSTRAKT

Inspirována rostoucím počtem odhalených kybernetických útoků mířených na veřejné a vládní zařízení a instituce, tato diplomová práce si klade za cíl poodhalit stěžejní význam kybernetické války a kybernetických zbraní, poukázat na kritické právní vakuum, které v současnosti panuje v oblasti aktuálně platné úpravy mezinárodního humanitárního práva, a navrhnout doplnění tohoto rámce o MHP úmluvě, jež by regulovala použití kybernetických zbraní v mezinárodních ozbrojených konfliktech.

Aby práce mohla poskytnout dobře strukturované a relevantní argumenty na podporu své hlavní teze, využívá metod kvalitativní analýzy současného MHP rámce, včetně mezinárodních smluv, zvykového práva a výstupních materiálů hlavních institucí věnovaných mezinárodní spravedlnosti spolu s prací předních autorů a odborníků v oblastech MHP a kybernetické bezpečnosti.

Práce se skládá z pěti hlavních kapitol. První kapitola představuje základní principy válečného práva, včetně jeho historie, teorie a rozvoje, a zaměřuje se na jeden z jeho tří hlavních režimů - mezinárodní humanitární právo.

Druhá část je věnována problematice kybernetické války a zbraní, definuje je jako počítačové útoky, vysvětluje jejich klasifikační systém, analyzuje jejich účinky a uvádí skutečné příklady takovýchto útoků z praxe.

Třetí kapitola je zaměřena na problematiku současného právního vakua MHP ve vztahu ke kybernetické válce a přináší kritickou analýzu hlavních nevýhod současně dostupných možných řešení tohoto vakua na základě současného MHP rámce.

Čtvrtá část představuje kritické rozdíly mezi tradiční kinetickou válkou a zbraněmi a válkou kybernetickou a jejími nástroji a zbraněmi a snaží se vysvětlit, proč současný MHP rámec skutečně není možno efektivně aplikovat na kybernetickou válku v praxi.

Poslední část práce navrhuje řešení otázky neslučitelnosti stávající MHP úpravy s kybernetickou válkou v podobě nové MHP úmluvy pro kybernetickou válku a poskytuje návrh jejích hlavních bodů tak, aby budoucí kybernetické konflikty mohly být vyhodnoceny a posuzovány podle aktualizovaného MHP rámce korespondujícího současné době.

ABSTRACT

Regarding the increasing number of revealed cyber-attacks aimed at public facilities including the governmental ones by who seems to be other state actors, this thesis aims to reveal the major importance of cyber warfare, point out the fatal vacuum regarding the IHL framework currently in force and suggests its completion by a new IHL convention, which would regulate cyberwarfare in International Armed Conflicts.

In order to provide a well-structured and pertinent arguments to support its main points, the thesis uses methods of qualitative analysis of the current IHL sources including international treaties, customary law and work of the main institutions of international justice along with work of judicial scholars and cyber experts.

The work contains five main chapters. The first chapter presents the underlining principles of Laws of Wars, including its theory, history and development; and focuses on one of its three main regimes – the International Humanitarian Law.

The second part is dedicated to the topic of cyber warfare, defines its scope as computer network attacks, explains their classification system, analyses their effects and provides examples of such attacks.

The third chapter focuses on the issue of the current legal vacuum in relation to cyber warfare and delivers a critical analysis of the most severe drawbacks to possible solutions of the vacuum.

The fourth part presents the insurmountable differences between the traditional kinetic warfare and cyber warfare and explains why these differences make the current IHL framework truly incompatible with cyber warfare in practice.

The last part of the thesis suggests a solution to the issue of incompatibility of the current IHL provisions and cyber warfare in a form of a new IHL treaty dedicated to cyber warfare and provides a draft of its main points so that future cyber conflicts can be evaluated and judged according to the updated IHL framework, which would correspond to its era.

KLÍČOVÁ SLOVA / KEY WORDS

Klíčová slova:

Kyberprostor

Kybernetická válka

Kybernetická úmluva

Úmluva o kybernetické válce

Kybernetický útok

Počítačový útok

Ozbrojený konflikt

Mezinárodní humanitární právo

Key words:

Cyberspace

Cyber Warfare

Cyber War

Cyber Treaty

Cyber Warfare Convention

Cyber Attack

Computer Network Attack

Armed Conflict

International Humanitarian Law