Univerzita Palackého v Olomouci

Právnická fakulta

Filip Hloušek

Cyberspace: Ius ad bellum and Ius in bello

Diplomová práce

Olomouc 2015

I hereby declare that this thesis is the result of my independent scholarly work. No material other than correctly cited references acknowledging original authors has been used.

Prohlašuji, že jsem diplomovou práci na téma Cyberspace: Ius ad bellum and Ius in bello vypracoval samostatně a citoval jsem všechny použité zdroje.

In Olomouc 14.02.2016 ……..

Filip Hloušek

Acknowledgment:

I would like to sincerely thank to the supervisor of my master thesis, JUDr. Ondřej Svaček, Ph.D., LL.M., for his invaluable approach and professional guidance during creation of this thesis.

Poděkování:

Na tomto místě bych rád poděkoval vedoucímu diplomové práce, JUDr. Ondřeji Svačkovi, Ph.D., LL.M., za jeho neocenitelný přístup a jeho odborné vedení mé diplomové práce.

Contents

List of Abbreviations

AP I	Additional Protocol I
AP II	Additional Protocol II
CERT	Computer Emergency Response Team
CIA	Central Intelligence Agency
CSIRT	Computer Security Incident Response Team
DoS	Denial of Service
DDoS	Distributed denial of Service
EU	European Union
IAC	International Armed Conflict
ICC	International Criminal Court
ICJ	International Court of Justice
ICRC	International Committee of the Red Cross
ICTR	International Criminal Tribunal for Rwanda
ICTY	International Criminal Tribunal for Yugoslavia
LOAC	Law of the Armed Conflicts
NCI	National Critical Infrastructure
NIAC	Non-international Armed Conflict
NSA	National Security Agency
UN	United Nations
UN Charter	The Charter of the United Nations

1 Introduction

Stanley Kubrick famously depicted human evolution in opening sequence of 2001: Space Odyssey. The primal ape, after firstly using bone as weapon against his adversaries, throws it into air, for it to transform into spaceship in the next scene, symbolizing the evolution and progress of human race.

Progress of human race did not bypass any aspect of our lives. War has been an inherent part of the world since the dawn of human society and evolved with our progress as well, since methods of war are ultimately governed by social traditions like all our activities.[1] We constantly develop new means of warfare in order to gain upper hand over adversary. From the use of primitive tools to development of nuclear bomb people used their knowledge to wage war against each other. At the same time people were very well aware of the unnecessary suffering during fighting. Thus, even primitive cultures developed certain rules of combat in order to humanize them.[2] These rules developed through time, leading to state of international law, as we know it today.

Nowadays we live in world when technological process is faster than ever before. Modern society has become enormously reliant on computers. Almost every aspect of our lives is governed by computers and networks, what makes us vulnerable to their failure. As remarked by William Lynn "*in the 21st century, bits and bytes can be as threatening as bullets and bombs*"[3]

This is demonstrated by an increasing number of attacks against States, conducted through cyberspace. In 2007, Estonia experienced one of the first cyber incidents directed against whole State, when became subject of few weeks long DoS and DDoS attacks against its e-services and webpages.[4] In 2008 cyber operations were used against Georgia during military activities of Russia in South Ossetia.[5] Up to date, the biggest cyber incident occurred in 2010, when was Iranian uranium enrichment plant in Natanz infected with Stuxnet, computer program,

[1] REICHMANN, Felix. The Pennsylvania Rifle: A Social Interpretation of Changing Military Techniques. *The Pennsylvania Magazine of History and Biography*, 1945, Vol. 69, Issue 1, p. 3.
[2] Ondřej, Jan a kol. *Mezinárodní humanitární právo*. 1. vydání. Praha: C. H. Beck, 2010, p. 79 – 80.
[3] PELLERIN, Cheryl. DOD releases first Strategy for Operating in Cyberspace [online]. defense.gov, 14 July 2011 [cit. 26.01.2016]. Available at <http://archive.defense.gov/news/newsarticle.aspx?id=64686>.
[4] TIKK, Eneken, KASKA Kadri, VIHUL, Liis. *International Cyber Incidents: legal considerations*. Tallinn: Cooperative Cyber Defence of Excellence (CCD COE), 2010, p. 16.
[5] Ibid. p. 68.

commonly denoted to be first cyber weapon.[6] Stuxnet attacked Centrifuge Drive system, which operates a speed of rotors in enrichment plant.[7] It is suggested that plant had to be shut down twice due to Stuxnet and that it possibly set Iranian nuclear program years behind.[8] Furthermore, Ukraine experienced cyber operations which successfully caused extensive power outage[9] and some directed against Boryspil Airport.[10] It was recently disclosed that due to vulnerability in certain motor controlling drives, even a low-skill hacker can cause considerable physical damage to facilities using them.[11]

The above-mentioned incident show that cyber operations can cause considerable damage, comparable to damage caused by kinetic means. If we assume that certain cyber operation, which is sufficiently severe, can be attributed to a particular State (or other originator) the inevitable questions arise. Does international law governs cyber operations in relation to use of force and armed conflicts? If it is applicable how it must be interpreted in order to suit specific nature of cyberspace and cyber operations? What conditions must cyber operation meet to comply with law and whet it would be illegal under international law?

Goal of present thesis is answering these questions. Since they are quite broad they cannot be answered simultaneously. In order to answer these questions, each chapter of this thesis deal with partial questions. Thesis is divided into four main chapters.

Chapter 2 deals with issue of terminology. It is necessary to address terminology at the early stage of analysis, since various authors, States and organizations use different terms when addressing cyber warfare. Chapter provides comparative analysis of commonly used terms and sets terminological framework which will be used further in the thesis.

---

[6] ALVAREZ, Joshua. *Stuxnet: The world's first cyber weapon* [online]. stanford.edu, 3. February 2015 [cit. 26. January 2016]. Available at <http://cisac.fsi.stanford.edu/news/stuxnet>.

[7] LANGNER, Ralph. *To kill a centrifuge. A Technical Analysis of what Stuxnet's Creators Tried to Achieve*. The Langner Group, 2013, p. 12. Available at <http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf>.

[8] FLEMING, Ryan. *Bits before bombs: How Stuxnet crippled Iran's nuclear dreams* [online]. digitaltrends.com, 2. December 2010 [cit. 26. January 2016]. Available at <http://www.digitaltrends.com/computing/bits-before-bombs-how-stuxnet-crippled-irans-nuclear-dreams/>.

[9] PAGANINI, Pierluigi. *Hackers cause power outage with BlackEnergy malware in Ukraine. Is it an Information warfare act?* [online]. securityaffairs.co, 5. January 2016 [cit. 25. January 2016]. Available at <http://securityaffairs.co/wordpress/43321/hacking/ukraine-attack-caused-power-outage.html>.

[10] PAGANINI, Pierluigi. *Ukraine blames Russia of cyber attacks against Boryspil airport* [online]. securityaffairs.co, 18. January 2016 [cit. 25. January 2016].Available at <http://securityaffairs.co/wordpress/43703/hacking/cyber-attack-boryspil-airport.html>.

[11] ZETTER, Kim. *An Easy Way for Hackers to Remotely Burn Industrial Motors* [online]. wired.com, 12. January 2016 [cit. 25. January 2016]. Available at <http://www.wired.com/2016/01/an-easy-way-for-hackers-to-remotely-burn-industrial-motors/>.

Chapter 3 addresses applicability of international law on cyberspace and cyber operations. Relevant international treaties were adopted at the time when cyberspace did not exist. Customary international law did not have enough time to emerge specifically for cyber operations. Therefore it is necessary to analyse whether it is possible to make cyberspace subject of relevant legal provisions.

Chapter 4 provides brief overview on attribution of State responsibility. This is necessary because attribution of action in cyberspace will probable become the most challenging task when applying law to the cyber operation.

Chapter 5 is concerned with prohibition of the use of force in international law. It examines the concept of the prohibition in treaty and customary law. The focus is given on notion of force and on the questions whether cyber operations can be qualified as use of force. Subsequently, the most important exception from the rules is analysed, i.e. right to self-defence. The questions explored will answer the questions whether a cyber operation can trigger a reaction in self-defence and what are the conditions of lawful self-defence in cyberspace.

Chapter 6 focuses on cyber operations and *ius in bello*. It examines what situations are governed by law of armed conflict. The distinction is made between international and non-international armed conflict, examining what situations are considered as one of these types of armed conflict and whether they can be started and conducted purely via cyber means. Additionally, attention is shifted on issue of conduct of hostilities in armed conflict. This part of thesis examines rules which govern who, what and how can be attacked in armed conflict, with focus on cyber related issues, i.e. under what conditions can be cyber operation considered attack and how it must be employed to be considered as legal attack.

2 Terminology

At the very beginning of this thesis it seems appropriate to address issue of terminology used. This is necessary due to the fact that various national manuals and strategies use similar different terminology or assign different meanings to same terms. Similarly different authors use different terminology which evolved during last decade. Unfortunately, up to these days there is no widely consistent and accepted terminology.[12] This thesis will follow terminology used by Tallinn Manual, which seems to be the most consolidated and summarized.

Firstly, it is important to address the notion of cyberspace as limiting frame for further analysis. Tallinn Manual defines cyberspace as "*The environment formed by physical and non-physical components, characterized by the use of computers and the electromagnetic spectrum, to store, modify, and exchange data using computer methods*."[13] It is a broader term than internet, which is defined as "*a global system of interconnected computer networks that use a standard Internet protocol suite*"[14] as it includes all activities in cyber domain and additionally a physical components as well.

The majority of differences arises in relation to cyber-attack, which has become a universal term for any harmful activity in cyberspace, mainly due to its use by media and non-legal disciplines, which disregard the terminology of international law, and the use of term attack in *ius ad bellum* and *ius in bello*.[15]

The broadest and the most used term is cyber operation which means "*the employment of cyber capabilities with the primary purpose of achieving objectives in or by use of cyberspace.*"[16] What is clearly of utmost importance is effect of cyber operation, not its mechanics. Cyber operations "*can aim to do different things, for instance to infiltrate a system and collect, export, destroy, change, or encrypt data or to trigger, alter or otherwise manipulate processes*

[12] ROSCINI, Marco. *Cyber Operations and the Use of Force in International Law*. Oxford: Oxford University Press, 2014, p. 11.
[13] SCHMITT, Michael (ed.). *Tallinn manual on the international law applicable to cyber warfare: prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. Cambridge: Cambridge University Press, 2013, p. 258.
[14] Ibid.
[15] ZIOLKOWSKI, Katharina, Ius ad bellum in Cyberspace – Some Thoughts on the "Schmitt-Criteria" for Use of Force. In CZOSSECK, C., OTTIS, R., ZIOLKOWSKI, K. (ed). *4th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE Publications, 2012, p. 296.
[16] SCHMITT: *Tallinn Manual*…, p. 258.

controlled by the infiltrated computer system."[17] Therefore what distinguish types of cyber operations are its ultimate effects, which shall differentiate terminology as well.

As Roscini notes the main distinction is made between two groups. Firstly cyber exploitation, as unauthorized access to parts of cyberspace with intention to gain information, but without their altering.[18] Although it can be argued that they can be qualified as armed attack, due to importance of the data for national security[19] it goes against the traditional understanding of espionage which is not prohibited.[20] The most recent example would be hacking of Israeli drones conducted by NSA.[21] Although live video footage and photos from drones were acquired, there was no further damage made. Cyber exploitation thus falls outside scope of this thesis.

Secondly, cyber-attack (in broad, descriptive sense) are operations intended to disrupt the access to data in targeted parts of cyberspace, to cause external physical damage (thus as cyber-attack through cyberspace), or to serve as means of propaganda.[22] The main difference therefore appears to be the destructiveness of the operation.[23] States as well as some authors[24] have tendency to use term cyber network attack (CNA) describing offensive cyber operations, in connection to cyber network defence (CND). Such approach seems unnecessary in relation to present thesis. In accordance with Tallinn Manual, CNA will not be used and cyber-attack will be used only in connection to LOAC,[25] as "*a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction of objects.*"[26] It works with definition of attack as "*acts of violence against the adversary, whether*

---

[17] International Committee of the Red Cross. *International Humanitarian Law and the challenges of contemporary armed conflicts, 31st International Conference of the Red Cross and Red Crescent*. Doc 31IC/11/5.1.2, October 2011, p 36. Available at <http://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>.

[18] ROSCINI: *Cyber Operations*..., p. 17-18.

[19] JOYNER, Christopher, LOTRIONTE, Catherine. Information Warfare as International Coercion: Elements of a Legal Framework. *European Journal of International Law*, 2001, Vol. 12, No. 5, p. 855.

[20] WOLTAG, Johann-Christoph. Cyber Warfare. In WOLFRUM, Rüdiger (ed). *The Max Planck Encyclopedia of Public International Law – Vol. II.* New York: Oxford University Press, 2012, p. 989.

[21] KHANDELWAL, Swati. *How Spy Agencies Hacked into Israeli Military Drones to Collect Live Video Feeds* [online]. thehackernews.com, 31. January 2016 [cit. 5. February 2016]. Available at <http://thehackernews.com/2016/01/drones-hacking.html>.

[22] ROSCINI: *Cyber Operations*..., p. 18.

[23] LIN, S. Herbert. Offensive Cyber Operations and the Use of Force. *Journal of National Security Law & Policy*, 2010, Vol. 4, p. 64.

[24] WOLTAG, Johann-Christoph. Cyber Warfare. In WOLFRUM, Rüdiger (ed). *The Max Planck Encyclopedia of Public International Law – Vol. II.* New York: Oxford University Press, 2012, p. 989.

[25] SCHMITT: *Tallinn Manual*..., p. 106

[26] Ibid.

in offence or in defence"[27] This approach seems to be more suitable to legal discussion as term attack has different meanings in international law, such as armed attack in cases of self-defence and attack in cases of LOAC.

[27] Art. 49 (1), 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..

3 Applicability of international law in cyberspace

The first question which arises in relation to cyberspace and armed conflicts is whether certain rules of international law are applicable to cyberspace. As up to date there is no special international treaty which would govern *ius ad bellum* and *ius in bello* specifically in cyberspace. Although there were attempts to propose such instrument[28] these were unsuccessful, regardless their relevance or necessity. In this regard it shall be noted that there are still calls for new, comprehensive regulation of State conduct in cyberspace due to imperfect applicability of current legal rules to cyber operation.[29] This can be surpassed only by analogy, which leaves many legal questions unanswered and creates uncertainty among States.[30] Although such instrument would be undoubtedly a benefit for international community, the reality of current state of international relations suggest that adoption of such document is unrealistic in near future.

It is therefore essential, if possible, to apply traditional sources of international law. Two principle sources of international law are treaties and customs.[31] It seems that nowadays rules of *ius ad bellum* and *ius in bello* in treaties and customs overlap greatly. Still it shall be borne in mind that if rule contained in particular provision exists independently in realm of customary law, the conclusions regarding application of provision in cyberspace will be the same for customary rule. At this point it also shall be noted that there is possibility that new, independent customary law would arise specially in relation to cyberspace. Such predictions can be found between scholars,[32] however such rule could be hard to determine due to State practice and their *opinio iuris* is sparse and often not available to public.[33] On the other hand certain liberation from strict rules of State practice and *opinio iuris* can be observed in relation to

[28] Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, UN Doc. A/66/359, 14. September 2011. Available at <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N11/496/56/PDF/N1149656.pdf?OpenElement>.

[29] BROWN, Davis. A proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict. Harvard International Law Journal, 2006, Vol. 47, No. 1, p. 182.

[30] HOLLIS, B. Duncan. Why States Need an International Law for Information Operations. Lewis & Clark Law Review, 2007, Vol. 11, p. 1039.

[31] Article 38 of the Statute of International Court of Justice.

[32] D'AMATO, Anthony. International Law, Cybernetics and Cyberspace. *International Law Studies*, 2002, Vol. 76, p. 69.

[33] SCHMITT: *Tallinn Manual…*, p. 5.

creation of custom, it would be too farfetched to draw conclusions of already existing customary rules from now available cyber strategies, manuals and known cyber operations.[34]

The main package of treaty law governing *ius ad bellum* and *ius in bello* are the Charter of United Nations[35], the Hague Conventions of 1899 and 1907, and Geneva Conventions with their Additional Protocols.[36] Naturally none of these international instruments addresses cyberspace, since at the time of their conclusion the internet, as known today, was non-existent. This absence shall be bridged via interpretation. The international law dictates that any treaty concluded shall be interpreted within its context, what *inter alia* counts with subsequent practice in the application of treaty.[37] It is necessary for the treaty to be interpreted evolutionary, in the light of the current legal system.[38] At the same time in cases of long term treaties it is presumed that the general terms, as their meaning will possibly evolve over time, will be interpreted in line with this evolving interpretation in mind.[39] Therefore international law as such allows newly developed instruments to be subsumed under existing legal framework.

Firstly, regarding *ius ad bellum*, the UN Charter, containing general prohibition of the use of force and possible exceptions from this rule, shall be applied. Charter works with notion of force. It is irrelevant by what means or weapons this force is executed.[40] The use of force and the right to self-defence with relation to the cyberspace will be discussed in following chapter, however it is established that UN Chapter applies to cyber operations.

Secondly, regarding *ius in bello*, the treaty law applicable also counts with its application to newly developed instruments. It has been shown in the past that even old law is able to answer new questions, as the adaptability of LOAC, is one of its core characteristics.[41] The Martens Clause, codified in both Hague[42] and Geneva Conventions states in the latter version that *„in*

[34] ROSCINI: *Cyber Operations*..., p. 31.
[35] Particularly Article 2 (4) and Chapter VII.
[36] For precise list of relevant treaties see: ICRC. *Treaties and State Parties to such Treaties*. Available at <https://www.icrc.org/applic/ihl/ihl.nsf/vwTreatiesByTopics.xsp>.
[37] Art. 31(3)b) of Vienna Convention on the Law of Treaties.
[38] Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (1970), Advisory Opinion, I.C.J. Reports 1971, para. 53.
[39] Dispute regarding Navigational and Related Rights (Costa Rica v. Nicaragua), Judgment, I.C.J. Reports 2009, para. 66.
[40] ICJ: Nuclear Weapons..., para. 39.
[41] KODAR, Erki. Applying the law of Armed Conflict to Cyber Attacks: From the Martens Clause to Additional Protocol I, *ENDC Proceedings*, 2012, Vol 15, p. 107.
[42] Preamble of 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, in force 4 September 1900.

cases not covered by this Protocol or by any other international agreements, civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from principles of humanity and from the dictates of public consent."[43] Martens Clause thus works as safeguard prohibiting use of newly developed means of warfare which were not present at the time of conclusion of these treaties and would go against the main principles of international humanitarian law. It works as "*effective means of addressing the rapid evolution of military technology.*"[44]

Additionally States have obligation to determine whether newly developed weapon would be in accordance with international humanitarian law.[45] Contracting parties therefore accounted with fact that newly developed means of warfare will be subsumed under these treaties. Tallinn Manual reflects this in Rule 20 where states that "*cyber operations executed in the context of armed conflict are subject to the law of armed conflict*."[46] The experts working on manual did not manage to find consensus on the subject of nexus of cyber operation, whether all cyber operations during armed conflict are subjected to rules of armed conflict or only those which have been taken in furtherance of hostilities.[47] This question will be discussed further, however we see that cyberspace is not exempted from law of armed conflict. These conclusions are supported by ICRC which considers means of warfare related to cyber technology to be subject to international humanitarian law "*just as any new weapon or delivery system has been so far when used in armed conflicts…*"[48]

In conclusion, the legal framework set to maintain international peace and security, and to regulate conduct of hostilities during armed conflicts is designed flexibly enough to encompass cyber operations as well. Application of existing legal framework regarding cyberspace at *ius ad bellum* and *ius in bello* is acknowledged and accepted by states themselves[49] and international community as whole.[50]

---

[43] Art. 1(2) of the AP I.
[44] ICJ: Nuclear Weapons…, para. 78.
[45] Article 36 of AP I.
[46] SCHMITT: *Tallinn Manual*…, p. 75
[47] Ibid.
[48] ICRC: International Humanitarian Law..., p. 37.
[49] ROSCINI: *Cyber Operations*…, p. 22 – 23.
[50] Group of Governmental Experts on Developments in the Field of information and Telecommunications in the Context of International Security. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc A/68/98, 24. June 2013, p. 8. Available at <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N13/371/66/PDF/N1337166.pdf?OpenElement>.

4 Attribution of cyber operations

Before proceeding further to particular issues of *ius ad bellum* and *ius in bello*, the issue of attribution should be addressed. Attribution in cyberspace imposes great challenge as anonymity of cyberspace is a benefit, which is hard to beat by kinetic operation. Still, attribution of acts to States is rather a factual and proving problem than a legal one.[51] One approach to overcome this difficulty in cyberspace would be work with presumption that the State responsible is the one where cyber operation originated. This approach is unfortunately in conflict with current state of law. In addition it would impose unbearable burden on States, as it is practically impossible to have control over every cyber operation on its territory.[52]

Current legal frame of responsibility of States is set in Draft articles on Responsibility of States for Internationally Wrongful Acts.[53] Following this source of international law, cyber operation can be attributed to the States under various circumstances.

Firstly, according to Art. 4 State is responsible for actions of its organs, depending on its national law and regardless of their incorporation in State structure. Therefore not only actions of military units, but of any organ are attributable to State. For example certain departments of ministries or national agencies such as CIA or NSA would fall into this category.

Secondly, Article 5 imposes responsibility of, so called, de facto organs. These are entities different from State, which exercise certain element of governmental authority. This category would contain any entity on which State delegates authority over cyberspace. Most commonly it would consist of private CERTs[54] or in case of Czech Republic, the CSIRT.CZ on which certain responsibilities were delegated.[55]

Thirdly, Article 8 provides that acts of any entity can be attributed to State if they are carried out on instruction, under direction or control of the State. ICJ addressed this issue,

[51] ICJ: Nicaragua..., para 57.
[52] DROEGE, Cordula. Get off my Cloud: Cyber warfare, international humanitarian law, and the protection of civilians. *International Review of the Red Cross: Humanitarian Debate: Law, policy, action*, 2012, Vol. 94, No. 886, p. 542 – 543.
[53] Draft articles on Responsibility of States for Internationally Wrongful Acts with commentaries, Yearbook of the International Law Commission, Vol. II, Part Two, A/CN.4/SER.A/2001Add.1 (Part 2), 2001.
[54] SCHMITT, Michael. International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed. Harvard International Law Journal, 2012, Vol. 54, p. 35.
[55] Veřejnoprávní smlouva o zajištění činnosti Národního CERT a o spolupráci v oblasti kybernetické bezpečnosti mezi Českou Republikou – Národním bezpečnostním úřadem a CZ.NIC. z.s.p.o., 18. January 2015. Available at <https://www.csirt.cz/files/nic/doc/NBU-Smlouva-narodni-cert-201512.pdf>.

stating that State must have effective control[56] or that State has given the instructions in respect to every particular operation, not only generally to overall conduct of alleged entity.[57] Different approach was adopted by ICTY, which employed principle of overall control, when State "*has a role in organising, coordinating or planning the military actions of the military group, in addition to financing, training and equipping or providing operational support to that group*."[58] Regardless of this discrepancy, effective control shall be applied. Overall control test is limited in scope to organised and structured groups[59] not to individuals where effective control must be proven.[60] It was adopted for qualifications of armed conflicts and not for attribution of State responsibility, which is acknowledged by ICJ as well.[61]

Fourthly, Article 11 sets possibility of retrospective attribution of acts, which are acknowledged and adopted by State subsequently. It is hard to imagine a situation in which State would do so, since cyberspace offers great opportunity to carry out cyber operation which could never be linked back to the State.

The problems which arise in regard to attribution are factual rather than legal. In subsequent analysis the attribution of cyber operation to its actor will be presupposed. Still, it can be argued that proving that cyber operation shall be attributed to its alleged actor will represent biggest problem in application of international law.

[56] ICJ: Nicaragua..., para 115.
[57] Application of the Convention of the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, I.C.J. Reports 2007, para. 400.
[58] ICTY, Prosecutor v. Duško Tadić, Judgment of the Appeals Chamber, Case No. IT-94-1-A, 15. July 1999, para 137.
[59] Ibid. para 120.
[60] Ibid. para 118.
[61] ICJ: Genocide..., para. 404.

5 Cyberspace and *ius ad bellum*

One of the most important questions of cyber security and law is considering cyber operations in light of *ius ad bellum*. This refers to issues of permissibility of use of force in international law. The permissibility of force between States developed from understanding of war as continuation of politics by other means,[62] through first attempts of its prohibition by League of Nations,[63] which ended up unsuccessful and without much practical effect,[64] to limited prohibition by Kellogg-Briand Pact.[65] After World War II, world realized necessity of international peace and stability and nowadays, the prohibition of use of force[66] is to be a cornerstone of UN Charter.[67] As it is with every rule, even prohibition of the use of force has its exceptions. The most common and relevant for present study is the exception of right of self-defence.[68] This chapter will be thus focused on issue of prohibition of use of force and right of self-defence in relation to cyberspace and cyber operations.

5.1 Cyberspace and Use of Force

The general rule of prohibition of use of force states that "*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 Nation.*"[69] This provision was called a heart of the UN Charter[70] due to its importance in system of international security. Tallinn Manual is clearly based on this provision and states that "*cyber operation which constitutes a threat or use of force against the territorial integrity or political*

[62] CLAUSEWITZ, Carl von, translated by GRAHAM, J.J.. On War. Vol. I. London: Routledge, 2005, p. 23.
[63] Art. 10 of The Covenant of the League of Nations, 28 June 1919.
[64] DÖRR, Oliver. Use of Force, Prohibition of. In WOLFRUM, Rüdiger (ed). *The Max Planck Encyclopedia of Public International Law – Vol. X.* New York: Oxford University Press, 2012, p. 608.
[65] Art. 1 of General Treaty for the Renunciation of War as an Instrument of National Policy, 27 August 1928. LNTS Vol. XCIV, No. 2137, p. 58.
[66] Art. 2(4) of UN Charter.
[67] Armed Activities on the Territory of the Congo (Democratic Republic of Congo v. Uganda), Judgments, I.C.J. Reports 2005, para. 148.
[68] Article 51 of UN Charter.
[69] Art. 2(4) of UN Charter.
[70] HENKIN, Louis. The Reports of the Death of Article 2(4) Are Greatly Exaggerated. *The American Journal of International Law,* 1971, Vol. 65, No. 3, p. 544.

independence of any State, or that is in any other manner inconsistent with the purposes of the United Nation, is unlawful."[71]

Not only the UN Charter prohibits use of force, but this rule exists independently in customary law as well. ICJ found that the prohibition of use of force has its counterpart in customary law as well, although not exactly identical in content.[72] Unfortunately court did not examine the State practice regarding customary prohibition what was criticized due to lack of examination of State practice, which ignores the divergent interpretations of customary rule of States.[73] There is thus possibility that the customary rule of the prohibition of the use of force will develop differently in general, or particularly, in relation to cyberspace. As of today there is nothing that would support such conclusion.[74] But we can conclude that both rules of prohibition of the use of force are at least, generally uniform in content.[75]

Moreover prohibition of the use of force is considered to be a peremptory norm of international law. It has been addressed as a conspicuous example of *ius cogens*.[76] ICJ mentioned this conclusion,[77] however did not confirmed it. It seems to be a commonly used example of such norm.[78]

5.1.1 The notion of force in cyberspace

UN Charter uses the term "force" however its definition is absent. Even nowadays the precise content of the term is not definitely settled neither in theory nor state practice.[79] Force as such can comprise of various means to apply pressure on other states, e.g. political and economic means. This could be supported by argument that UN Charter uses term "armed

[71] SCHMITT: *Tallinn Manual…*, p. 42.
[72] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment, I.C.J. Reports 1986, para. 175 – 177.
[73] RANDELZHOFER, Albrecht. In SIMMA, Bruno (ed). *The Charter of the United Nations A Commentary*. Vol. I. 2. Edition. Oxford: Oxford University Press, 2010. p. 134 (Art. 2(4) UN Charter).
[74] SCHMITT, Michael, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law*, 1999, Vol. 37, p. 921 – 922.
[75] DÖRR, Oliver. Use of Force, Prohibition of. In WOLFRUM, Rüdiger (ed). *The Max Planck Encyclopedia of Public International Law – Vol. X.* New York: Oxford University Press, 2012, p. 609.
[76] Reports of the International Law Commission on the second part of its seventeenth session and on its eighteenth session, Document A/6309/Rev.l, in *Yearbook of the International Law Commision*, 1966, Vol. II, A/CN.4/SER.A/1966/Add.l, page 247.
[77] ICJ: Nicaragua…, para 190.
[78] KAHGAN, Carin. Jus Cogens and the Inherent Right to Self-Defense. *ILSA Journal of International & Comparative Law,* 1997, Vol. 3, p. 777 – 781.
[79] RANDELZHOFER: The Charter of United…, p. 117.

force" in other provisions[80] and thus by plain wording the Article 2(4) has broader scope.[81] Such argumentation has to be dismissed. The predominant view claims that Article 2(4) implicitly means armed force. The reason for this is that the teleological interpretation suggest that the goal of UN is to prevent war[82] not every coercive actions. This is supported by *travaux préparatoires*, when the proposal for inclusion of economic coercion was rejected. Finally this interpretation was confirmed by Friendly Relations Declaration.[83] By declaring that States may use economic or political means to coerce another States it confirms that Article 2(4) is restricted only to armed force.[84] Same conclusion can be made in relation to subsequently adopted Declaration on the Non-Use of Force.[85] Therefore cyber operations which would not arise to level of armed force but merely economically coerce another State cannot be considered as violation of Article 2(4). Some commentators argue that in age of cyber operations which can have devastating effect on economy, the scope of Art. 2(4) needs to be broaden to include economic force.[86] The approach still stands on the analogy of scale and effect test and basically comes to same conclusions as cyber operations disrupting National Critical Infrastructure.[87]

It also shall be noted that while Article 2(4) includes terms territorial integrity or political independence, it does not mean that solely these must be a target of use of force. These forms were introduced to emphasize the protection of territorial integrity and political independence.[88] The last segment of the provision provides a "catch–all phrase" in order to prevent every use of armed force.[89]

Relevant to the discussion on cyber operations is also, whether prohibition of the use of force also covers use of physical force of non-military nature, such releasing large amount of

[80] Article 41, 44, 46 of the UN Charter.
[81] KELSEN, Hans. *Collective Security under International Law*. New Jersey: The Lawbook Exchange, 1954, p. 55.
[82] Preamble of the UN Charter.
[83] Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations. General Assembly Resolution, Res. 2625(XXV), UN Doc. A/RES/25/2625, October 24 1970.
[84] RANDELZHOFER: The Charter of United…, p. 118.
[85] Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations, GA Res. 42/22, 18 November 1987.
[86] KILOVATY, Ido. Rethinking the Prohibition on the Use of Force in the Light of Economic Cyber Warfare: Towards a Broader Scope of Article 2 (4) of the UN Charter. *Journal of Law and Cyber Warfare*, 2015, Vol. 4, No. 3, p. 234.
[87] Disruption of NCI is addressed in part 5.1.3.
[88] RANDELZHOFER: The Charter of United…, p. 123.
[89] DÖRR, Oliver. Use of Force, Prohibition of. In WOLFRUM, Rüdiger (ed). *The Max Planck Encyclopedia of Public International Law – Vol. X.* New York: Oxford University Press, 2012, p. 610.

water or spreading fire. The prevalent opinion is that as it is with economic force, the final effect might be similar, but Article 2(4) only prevents use of armed force. Exception might be made in cases where this use of force arises to levels of armed attack in sense of Article 51 of UN Charter, which would permit State to act in self-defence. Still, some commentators argue that Article 2(4) covers also cases of non-military force.[90]

5.1.2 Indirect use of force and cyberspace

It is well established fact that prohibition of the use of force can be violated by State indirectly as well. ICJ has famously held that arming or training independent armed groups can be considered as use of force. However, the mere supply of funds to such groups does not amount to a use of force.[91] Therefore providing organized group with malware and the training for its use would qualify as use of force.[92] On the other hand simply affording sanctuary to non-state actor executing such cyber operation would not be considered as use of force. Only if coupled with substantial support or cyber defence, it could be qualified as use of force.[93] Present issue will need a careful consideration, since cyberspace seems as ideal space for use of non-state actors as a link between State and a non-state actor can be very loose. It will be crucial to carefully assess circumstances of the case to determine the substantiality of support given.

Similarly to that, a situation where a State would allow another State to use its infrastructure to employ certain cyber operation would be considered as use of force. This conclusion is based on the transposition of Article 3(f) of the Definition of Aggression. As aggression is clearly use of force,[94] one of categories of aggression is placing a part of its territory at disposal of another State, which commits the act of aggression.[95] Since States execute sovereignty over cyber infrastructure within its territory they have right to control this infrastructure. This sovereignty arises from their sovereignty over their territory.[96] States are

[90] RANDELZHOFER: The Charter of United…, p. 118-119.
[91] ICJ: Nicaragua…, para. 228.
[92] SCHMITT: *Tallinn Manual*…, p. 46.
[93] SCHMITT: *Tallinn Manual*…, p. 47.
[94] Article 1 of Definition of Aggression, United Nations General Assembly Resolution 3314 (XXIX), 14 December 1974.
[95] Article 3 (f) of Definition of Aggression, United Nations General Assembly Resolution 3314 (XXIX), 14 December 1974.
[96] SCHMITT: *Tallinn Manual*…, p. 16.

therefore analogically responsible for allowing use of its cyber infrastructure for purposes of cyber operation which would amount to act of aggression and thus to use of force.

5.1.3 Cyber operation as use of force

As was stated, prohibition of use of force applies regardless of weapons employed.[97] Therefore the core of the discussion lies within the question of whether one can analogically subsume cyber operation under notion of force.

In line with approach of ICJ, when applying rules of use of force to cyber operations their unique characteristics is an imperative for correct assessment.[98] The discussion whether and which cyber operations can be qualified as force ultimately depends on which analytical approach is adopted to equate cyber operations to kinetic force. In theory there are three main approaches, but there is no consensus regarding which approach shall be adopted.[99] These are instrument-based, target-based and effect-based approach.[100]

The instrument-based approach determines what qualifies as use of force by means employed. It is traditional approach to armed attack inquiry[101] which draws clear line in distinction between armed force and e.g. economic or diplomatic sanctions. On the other hand is hardly applicable to use of chemical and biological weapons and absolutely fails when considering cyber operations.[102] This would mean that since cyber operation lacks physical characteristics of traditional weapons,[103] cyber operation would never be considered as armed force,[104] even if it resulted in physical damage.[105]

This problem can be solved by approach adopted by Roscini, i.e. defining weapons by their effect. Thus it is an instrument-based approach, but the instrument itself is defined by its

[97] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996, para. 39.
[98] Ibid. para. 36.
[99] WAXMAN, Matthew. Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions. *International Law Studies*, 2013, Vol. 89, p. 111.
[100] ROSCINI: *Cyber Operations*…, p. 47.
[101] SCHMITT, Michael, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law*, 1999, Vol. 37, p. 909.
[102] WAXMAN, Matthew. Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions. *International Law Studies*, 2013, Vol. 89, p. 111.
[103] HOLLIS, B. Duncan. Why States Need an International Law for Information Operations. Lewis & Clark Law Review, 2007, Vol. 11, p. 1041.
[104] WAXMAN, Matthew. Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions. *International Law Studies*, 2013, Vol. 89, p. 111.
[105] ROSCINI: *Cyber Operations*…, p. 48.

violent effect. This view on the subject is innovative in sense that it allows application of instrument-based approach to cyber operations, however it combines instrument-based approach with effect-based approach.[106] It ultimately ends up on same subject matter as effect-based approach.

The target-based approach focuses on the object of the cyber operation. The argument is based on reliance of modern society on cyberspace and technologies increases the risk for national security. It takes into account problems with self-defence in cyberspace, particularly anticipatory self-defence. In order to overcome the impossibility to make legal evaluation necessary for self-defence in short period of time when cyber operation strikes it proposes presumptive solution. The penetration of NCI would be predetermined as case allowing anticipatory self-defence.[107] This shall be justified by the fact that until a cyber operation would be determined as armed attack, state would not have right for self-defence. The only possibility would therefore to apply a proportionate countermeasures with all requirements imposed by ICJ.[108] Since this approach does not suite instantaneous danger of cyber operations, the target-based approach shall be adopted.[109] It basically postulates that States should be allowed to "*use force in anticipatory self-defence against any identified state that demonstrates hostile intent by penetrating a computer system which is critical to their respective vital national interests*."[110]

It has been recognized that this approach is more or less incompatible with current state of international law.[111] It is more a proposal that the law should evolve in manner that it would permit state to act in self-defence in any case of cyber operation directed against national critical infrastructure, even if it would not meet threshold of armed attack.[112] This approach shall be disregarded. It indeed gives state a possibility to act in self-defence immediately however it seems over inclusive as any inconvenience would be considered as reason to resort to self-defence,[113] what opens door for increased use of force, since all operations against NCI would justify action in self-defence, destabilizing international peace and security, what goes

[106] ROSCINI: *Cyber Operations…*, p. 51.
[107] SHARP, Walter. *Cyberspace and the use of force*. Falls Church: Aegis Research Corp., 1999, p. 129 – 130.
[108] ICJ: Nicaragua..., para 249.
[109] JENSEN, Eric. Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense. *Stanford Journal of International Law*, 2002, Vol. 38, p. 221.
[110] SHARP: *Cyberspace and the use of force…*, p. 130.
[111] JENSEN: *Computer Attacks…,* p. 229.
[112] Ibid.
[113] ROSCINI: *Cyber Operations…*, p. 48.

against the core principles of UN Charter.[114] It also brings many practical challenges. As the determining factor is considered a target of cyber operation, the attacker itself seems irrelevant and thus state should be allowed to act in self–defence without attribution of attack which would be too "*time-consuming process, a luxury unavailable in cyber-attack era*."[115] Therefore if perpetrator redirects it attack through another state, a defending state could in theory execute attack in self-defence against this innocent state. This approach has indeed its value as shows the problems of imminence of cyber operations and possible lack of means of active defence, however in conclusion it is incompatible with current international law.

The approach which seems to be prevalently supported is effect-based approach.[116] This approach works with consequences of an attack in relation to a traditional armed force. If a cyber operation can cause analogical consequences as a traditional use of force, it would be qualified as use of force. According to Tallinn Manual *"a cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to level of use of force."*[117] It uses kinetic-equivalence doctrine[118] which settles for analogy with traditional means of armed force. It is based on position of ICJ that when considering act to be an armed attack, what depends is scale and effects.[119] This approach leaves opened the question when the cyber operation is qualified to be use of force. Argument can be made that there must be violent consequences as usually produced by bombs or bullets.[120] Therefore "*cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force.*"[121] This is commonly uncontested as it aligns with traditional approach to use of force.[122] It however ignores the development of world and dependence of modern society reliance on cyber infrastructure and connectivity.[123]

---

[114] Preamble of the UN Charter.
[115] JENSEN, Eric. Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense. *Stanford Journal of International Law*, 2002, Vol. 38, p. 232.
[116] ROSCINI: *Cyber Operations*…, p. 48.
[117] SCHMITT: *Tallinn Manual*…, p. 45.
[118] ROSCINI: *Cyber Operations*…, p. 103.
[119] ICJ: Nicaragua…, para. 195.
[120] DINSTEIN, Yoram. Computer Network Attacks and Self-Defense. In *International Law Studies*, 2002, Vol. 76, p. 103.
[121] KOH, Harold. *Remarks: USCYBERCOM Inter-Agency Legal Conference* [online]. state.gov, 18. September 2012 [cited 28.11.2015]. Available at <http://www.state.gov/s/l/releases/remarks/197924.htm>.
[122] ROSCINI: *Cyber Operations*…, p. 54.
[123] OWENS, William, KENNETH, Dam, LIN, Herbert. Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattacks Capabilities. Washington DC: National Academy Press, p. 253-254.

If one wants to define what non-kinetic action would constitute use of force and not only less grave form of coercion, finding of the threshold is problematic. Set of factors which are to be considered was created by Michael Schmitt.[124] These, also called "Schmitt Criteria" are deemed to be descriptive factors to consider, not legal criteria[125] and were subsequently adopted by Tallinn Manual. These criteria are severity, immediacy, directness, and invasiveness, measurability of effects, military character, state involvement and presumptive legality.[126] These criteria can be undoubtedly a benefit for states when assessing cyber operations. They are at same time subject to critique, as being unnecessary, since there is no need to focus on any other criteria apart from analogous effect of cyber operation.[127] The discussion in most cases thus goes down to question of severity.[128]

Different cyber operations can have very different effects when executed. It is therefore necessary to assess their qualification as force in smaller categories, as general assessment of whole group is impossible.

Firstly, we can isolate group of cyber operations causing physical damage to property, loss of life, or injury to persons. Clearly, cyber operation does not kill anyone directly, as it firstly affects only data. The alternation of data then has effect on physical property and after then, this physical effect on objects can injure persons.[129] This type of cyber operation will thus have the same effect as use of kinetic force. It is virtually undisputed that such cyber operation will fall under the scope prohibition of use of force. The main focus is thus placed on question of threshold of gravity. Wording of Article 2 (4) does not contain any indication that there should be a difference in gravity of force in order to its application. Similarly Tallinn Manual claims that such acts that injure or kill persons or damage property are unambiguously uses of force.[130] On the other hand, when applying Schmitt criteria, the severity is subject to *de minimis* rule.[131] Therefore cyber operations which cause only negligible consequences as destruction of one

[124] SCHMITT, Michael, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law*, 1999, Vol. 37, p. 914 - 915.
[125] SCHMITT: *Tallinn Manual…*, p. 48.
[126] Ibid. p. 48 – 51.
[127] ZIOLKOWSKI, Katharina, Ius ad bellum in Cyberspace – Some Thoughts on the "Schmitt-Criteria" for Use of Force. In CZOSSECK, C., OTTIS, R., ZIOLKOWSKI, K. (ed). *4th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE Publications, 2012, p. 308.
[128] SILVER, B. Daniel. Computer Network Attack as a Use of Force under Article 2(4). *International Law Studies*, 2002, Vol. 76, p. 91.
[129] ROSCINI: *Cyber Operations…*, p. 54.
[130] SCHMITT: *Tallinn Manual…*, p. 48.
[131] Ibid.

computer would not be considered as use of force. Of course this stands true if there are no further consequences directly linked to this destruction, nor is the computer of utmost importance. The assessment needs to be made on case by case basis, considering every special circumstances of the case.

Secondly there are cyber operations which could be qualified as subgroup of destruction of property. These are cyber operations which does not manifest in realm of physical world. The cyber operation in these case attacks data themselves. Whether destruction of data can have same consequences as destruction of physical property depends on whether data can be equated to physical property. According to Schmitt this can be a case only in situations of data which can be immediately converted to tangible objects.[132] It is hard to imagine in what situation such approach would be accepted.

Thirdly, there is group of cyber operations which does not damage the property but instead disrupts infrastructure. The infrastructure which is usually considered in relation to triggering rules of prohibition of use of force is NCI. As abovementioned, if one applies target-based approach every attack on NCI will be considered as use of force. There is no consensus on what exactly constitutes NCI. This is due to the fact that every state determines its own NCI.[133] According to UN this include "*those used for, inter alia, the generation, transmission and distribution of energy, air and maritime transport, banking and financial services, e-commerce, water supply, food distribution and public health – and the critical information infrastructures that increasingly interconnect and affect their operation*."[134]

Even if every state determines its own NCI, the common denominator seems to be that these are "*infrastructures vital for national security, including individual societal, and governmental security.*"[135] The most common sectors are banking, finance, government, communications, emergency and rescue services, energy, public health, transportation, food and water supply. It of course includes defence systems and networked weapons as well. The

[132] Michael N Schmitt. Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts. In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy.* Washington: The National Academies Press, 2010, p 164.
[133] Creation of a global culture of cybersecurity and the protection of critical information infrastructure, GA Resolution, A/RES/58/199, 30. January 2004.
[134] Ibid.
[135] ROSCINI: *Cyber Operations*…, p. 59.

dependence of society on this infrastructure causes that significant interference with functionality of the infrastructure would be considered as use of force.[136]

The main question regarding NCI is at when the disruption of its functionality amounts to use of force. This focus is necessary to successfully transpose the requirement of scale and effect from physical destruction to incapacitation. This is crucial due to the problem with this concept, which usually ends as too restrictive or expansive.[137] As example, we can consider attacks against NCI which would disable whole national power grid. If these types of cyber operation would not be considered use of force due to lack of kinetic force, the outcome seems to be disproportionate, as state cannot properly defend itself. The ultimate effect of the cyber operation would be disablement of the NCI. Indeed, kinetic attack would create additional damage on physical infrastructure. Such damage however would be probably of minor consideration. Let's assume that cyber operation renders electric grid of part of State dysfunctional. Imagine that the same outcome would be achieved by traditional military operation, for example cutting the electric lines on large area. Outcome of both operations is the same. Of course, in latter case the replacement of hardware is necessary, but the return of software to the state before the operation can be as difficult and costly as replacement of electric lines. It seems unreasonable to consider one operation a use of force meanwhile not to consider other to be use of force as well.

The important question is what remedies state has once a cyber operation amounting to use of force, but not armed attack, was executed. Basically there are three non-judicial options for state. These are acts of retorsion, resort to UN Security Council or application of countermeasures.[138] Taking in consideration the need for respond quickly and effectively to potential cyber operation, countermeasures and urgent countermeasures seem to be the most relevant option. Countermeasures are generally ignored in legal analysis, which focuses on self-defence. This is paradoxical considering that there is no cyber operation which would be consensually considered an armed attack.[139]

---

[136] OWENS, DAM, LIN: Technology, Policy, Law…, p.254.

[137] MELZER, Nils. *Cyberwarfare and International Law*. UNIDIR Resources, 2011, p. 14. Available at <http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf>.

[138] ROSCINI: *Cyber Operations…*, p. 105.

[139] SCHMITT, N Michael. "Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law. *Virginia Journal of International Law*, 2014 Vol. 54, p. 698.

According to ICJ in cases of use of force, which does not amount to armed attack, state cannot apply countermeasures involving use of force.[140] However injured state must comply with certain limits of application of countermeasures. Particularly countermeasures can be taken only against the responsible state and be, as far as possible, reversible.[141] At the same time an important consideration[142] is that whether they are proportionate.[143] This can be achieved by countermeasure in-kind, which are more likely to satisfy this requirement.[144] This however must be considered very cautiously as the dependence of states on cyber infrastructure may be different.[145] The general limit of countermeasures, which cannot be crossed in any case, prohibits acts which would violate prohibition of use of force, human rights, prohibition of reprisals and another peremptory norm.[146]

5.2 Cyberspace and self-defence

The right for self-defence is probably the most important exception from general prohibition of use of force.[147] It is provided by UN Charter which explicitly states that "*nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security."*[148]

Of course, the right of self-defence is not merely a treaty rule, but it is a part of customary law as well. This can be seen in reference to inherent right of self-defence in UN Charter, omission of conditions of execution of self-defence and the absence of definition of armed attack.[149] Since UN Charter does not contain definition of armed attack in its text, clearly the determination of the content of armed attack must be made through interpretation and

[140] ICJ: Nicaragua…, para. 249.
[141] Art. 49, Draft articles on Responsibility of States for Internationally Wrongful Acts with commentaries, Yearbook of the International Law Commission, Vol. II, Part Two, A/CN.4/SER.A/2001Add.1 (Part 2), 2001.
[142] Garabčíkovo-Nagymaros Project (Hungary/Slovakia), Judgment, I.C.J. Reports, 1997, para. 85.
[143] Art. 51, Draft articles on Responsibility of States for Internationally Wrongful Acts with commentaries.
[144] Draft articles on Responsibility of States for Internationally Wrongful Acts with commentaries, p. 129.
[145] ROSCINI: *Cyber Operations*…, p. 106.
[146] Art. 51, Draft articles on Responsibility of States for Internationally Wrongful Acts with commentaries, p. 131.
[147] Art. 2(4) of the UN Charter.
[148] Art. 51 of the UN Charter.
[149] ICJ: Nicaragua…, para. 176.

customary law.[150] The discussion thus comes down to the similar problem as with the use of force, i.e. what constitutes an armed attack. In addition to that the right of self-defence is subject to some limitations, which will be discussed. Moreover the two contemporary important questions shall be addressed, particularly when can be self-defence employed and against whom.

5.2.1 Cyber operation as armed attack

ICJ explicitly stated, that Article 51 does not refer to specific weapon, but applies to any form of force.[151] It therefore does not preclude its use in cases of cyber operations. As it was noted in relation to use of force, cyber operations must be considered as armed attacks as well, due to effect inflicted by them. Not the designation of device or its use, but its effect and intent of its use resulting in loss of life or destruction of property, including cyber operations make any attack an armed one.[152]

When it comes to basics an armed attacks are the gravest forms of the use of force.[153] In order to differentiate between mere frontier incidents and armed attack which triggers right for self-defence ICJ came with "scale and effect" test.[154] This approach was subsequently adopted by Tallinn Manual, which states that "*whether a cyber operation constitutes an armed attack depends on its scale and effects*."[155] This differentiation can be problematic since under certain circumstances even a relatively small attack, as mining of single military vessel can be sufficient.[156] The precise threshold is thus difficult to establish.[157]

Before further discussion on the issue of scale and effects it shall be noted that the right for self-defence can be triggered not necessarily only by one armed attack, but by accumulation of more incidents as well. This possibility was addressed by ICJ on several occasions, but due to cautious approach never definitely resolved. At first ICJ implied that such possibility exists in

[150] ZEMANEK, Karl. Armed Attack. In WOLFRUM, Rüdiger (ed). *The Max Planck Encyclopedia of Public International Law – Vol. I.* New York: Oxford University Press, 2012, p. 595.
[151] ICJ: Nuclear Weapons…, para. 39.
[152] ZEMANEK, Karl. Armed Attack. In WOLFRUM, Rüdiger (ed). *The Max Planck Encyclopedia of Public International Law – Vol. I.* New York: Oxford University Press, 2012, p. 599.
[153] ICJ: Nicaragua…, para. 191.
[154] Ibid. para. 195.
[155] SCHMITT: *Tallinn Manual*…, p. 54.
[156] Oil Platforms (Islamic Republic of Iran v. United States of America), Judgment, I.C.J. Reports 2003, para. 72.
[157] SCHMITT: *Tallinn Manual*…, p. 56.

Nicaragua case, but lacked sufficient information.[158] More recently ICJ considered the possibility of actions in self-defence as response to accumulation of attacks, failing to rule on the issue due to different reasons.[159] This means that cyber operation which alone does not reach scale and effect necessary, can be considered a "composite armed attack" in combination with other cyber operations.[160]

When considering whether force employed reaches the scale and effect necessary to be considered as armed attack one shall think of it as "*an act or the beginning of a series of acts of armed force of considerable magnitude and intensity (i.e. scale) which have as their consequence (i.e. effects) the infliction of substantial destruction upon important elements of the target State namely, upon its people, economic and security infrastructure, destruction of aspects of its governmental authority, i.e. its political independence, as well as damage to or deprivation of its physical element namely, its territory*" and "*the use of force which is aimed at a State's main industrial and economic resource and which results in the substantial impairment of its economy."*[161]

According to Tallinn Manual cyber operations which results in death or injury of persons or destruction or damage of property would undeniably be considered as armed attack.[162] Yet it seems unreasonable to claim that any damage on property or injury of persons shall be considered as armed attack, as it is not necessarily grave enough. As example, operations which would constitute armed attack could be considered disablement of electrical grid with harmful consequences, opening of water dams, crash of airplane or release of radioactive material from damaged core of nuclear plant.[163] Regarding last example the Stuxnet incident was deemed as armed attack by some experts,[164] others claim that scale and effects were not sufficient.[165]

The more complicated issue is, as with use of force in general, the qualification of cyber operation as armed attack in cases without physical effect, e.g. the attack on NCI, such as

[158] ICJ: Nicaragua…, para. 231.
[159] ICJ: Oil Platforms…, para. 64; ICJ: Armed Activities…, para. 146, Land and Maritime Boundary between Cameroon and Nigeria (Cameroon v. Nigeria: Equatorial Guinea Intervening), Judgment, I. C. J. Reports 2002, para.. 323–324.
[160] SCHMITT: *Tallinn Manual*…, p. 56.
[161] CONSTANTINOU, Avra. *The right of self-defence under customary international law and Art. 51 of the United Nations Charter*. Athens: Sakkoulas, 2000, p. 63 – 64.
[162] SCHMITT: *Tallinn Manual*…, p. 55.
[163] DINSTEIN, Yoram. Computer Network Attacks and Self-Defense. In *International Law Studies*, 2002, Vol. 76, p. 105.
[164] SCHMITT: *Tallinn Manual*…, p. 58.
[165] O`CONNEL, Mary Ellen. Cyber Security without Cyber War. *Journal of Conflict & Security Law,* 2012, Vol. 17, No. 2, p. 202.

electric grid. As was observed above the cyber operations disrupting NCI would be considered as use of force. Since armed attack is nothing more than severe use of force, the same applies to it as well. Many States has adopted position which is in line with this conclusion. The lack of State practice unfortunately precludes definitive answer.[166] It seems unsubstantiated to make difference between destruction of parts of grid and its disablement when the indirect consequences are the same and the only difference is in the physical damage on technology, which could be negligible. More problems arise in cases of attacks against financial sector. This issue divides scholars whether financial loss constitute damage and thus justifies self-defence or whether the catastrophic effect itself suffice to label such cyber operation as armed attack.[167] Regardless of scholar dispute most states would consider such cyber operation as armed attack and would engage in self-defence.[168]

5.2.2 Necessity, proportionality and immediacy of self-defence

Right for self-defence is subject to certain constraints. These apply either to self-defence in general, or are limited to Article 51. The conditions related only to application of Article 51, i.e. immediate report to Security Council of UN[169] will be omitted and focus will be directed on general requirements of proportionality, necessity and immediacy. As to necessity and proportionality, these are undeniably part of customary law.[170] The requirement of necessity and proportionality is included in Tallinn Manual as well.[171] Immediacy on the other hand is not listed by ICJ in its judgments, however is included in Tallinn Manual[172] and seems to be part of customary law.[173]

Principle of necessity requires that use of force which would be otherwise unlawful, is objectively necessary to repel an armed attack.[174] It relies on lack of alternative, non-forcible

---

[166] GILL, Terry, DUCHEINE, Paul. Anticipatory Self-Defence in the Cyber Context. *International Law Studies*, 2013, Vol. 89, No. 438, p. 444 – 445.
[167] SCHMITT: *Tallinn Manual…*, p. 57.
[168] ROSCINI: *Cyber Operations…*, p. 75.
[169] ICJ: Nuclear Weapons…, para. 44.
[170] ICJ: Nicaragua, para 176, 194; ICJ: Oil Platforms..., para. 43, 73, 76.
[171] SCHMITT: *Tallinn Manual…*, p. 61.
[172] SCHMITT: *Tallinn Manual…*, p. 63.
[173] DINSTEIN, Yoram. *War, Aggression and Self-Defence*, 5th edition. New York: Cambridge University Press, 2012, p. 230.
[174] MELZER, Nils. *Cyberwarfare and International Law*. UNIDIR Resources, 2011, p. 17. Available at <http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf>.

measures, which could be employed. If this passive defence is insufficient, the use of force is permissible.[175] It requires to find out the author of attack, verify whether the attack is not a mere accident and analyse intrusive means of response.[176] According to Melzer the above-mentioned forms a qualitative necessity, to which a quantitative necessity must be added. This requires "*kind and degree of force used in self-defence not exceed what is actually necessary to repel armed attack in question*."[177]

Proportionality limits the magnitude of force which might be employed. It can be balanced against scale and effect of armed attack or by how much force is necessary to repel armed attack.[178] Melzer claims that harm caused must be justified by gravity of armed attack, and that is legally justified if it remains in reasonable proportion.[179] According to Tallinn Manual the limit is given by what is necessary to end given situation, since the amount of force necessary might be higher given the circumstances.[180] The second approach seems to be more reasonable as gives states opportunity to effectively defend itself but prevents unnecessary escalation of conflict, as imposes limit only to force which is necessary to repel attack. This discrepancy is given due to the fact that Melzer divides principle of necessity into quantitative and qualitative part. Melzers system thus has two limits, one of force necessary to repel an attack and second to limit the force to maximum of original attack.

Proportionality in no way limits self-defence in relation to means employed, thus self-defence by kinetic means to cyber armed attack is naturally permitted.[181] The exact calculation of proportionality might be difficult given the specifics of cyberspace and problems to establish magnitude in short period of time.[182] Since in reality the cyber defence must rely on automated systems, the case by case analysis by personnel is difficult if not impossible, given the instantaneous nature of cyber operations.[183] In the end meeting the requirement of proportionality is basically a technical issue.[184]

---

[175] SCHMITT: *Tallinn Manual…*, p. 62.
[176] ROSCINI: *Cyber Operations…*, p. 90.
[177] MELZER: Cyberwarfare..., p. 17.
[178] ROSCINI: *Cyber Operations…*, p. 90.
[179] MELZER: Cyberwarfare..., p. 18.
[180] SCHMITT: *Tallinn Manual…*, p. 62.
[181] SCHMITT: *Tallinn Manual…*, p. 63
[182] HOISINGTON, Matthew. Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense. *Boston College International and Comparative Law Review*, Vol.32, Issue 2, p. 452.
[183] MELZER: Cyberwarfare..., p. 18.
[184] ROSCINI: *Cyber Operations…*, p. 90.

Requirement of immediacy is necessary to distinguish self-defence from retaliation. It includes temporal proximity, time which is necessary to prepare an answer and to establish factual basis for self-defence.[185] It does not necessarily means that the response must be instantaneous.[186] Melzer considers immediacy to be a temporal perspective of necessity, thus render self-defence illegal when is no longer necessary.[187]

5.2.3 Anticipatory self-defence

The literal wording of Article 51 suggest, that a state is entitled to self-defence only in cases where the attack already happened or is currently taking place. Such approach seems unreasonable, considering that any state would thus has to wait for attack to actually occur to defend itself. However some of the interpretations of Article 51 claim that this is indeed the case and that anticipatory self-defence is unlawful.[188] The more liberal approach allows to act in cases of interceptive self-defence where armed attack was already initiated, but has not yet invoked effect, so called interceptive self-defence.[189] On the other end of plethora of interpretations of self-defence is claim that State can act in self-defence even in cases of pre-emptive self-defence. These are cases when attack is not immediate but might happen, although time and place remain uncertain.[190]

The possibility of pre-emptive self-defence is however, generally considered as inconsistent with current state of international law.[191] The majority of scholars accepts, that objectively verifiable attacks which manifest as imminent, trigger right for self-defence.[192] This approach is adopted by Tallinn Manual as well, since it states that self-defence is permissible when "*cyber armed attack occurs or is imminent.*"[193] The requirement of imminence originates from Caroline affair, in which it was formulated that State must show " a *necessity of self-*

[185] SCHMITT: *Tallinn Manual…*, p. 66.
[186] ROSCINI: *Cyber Operations…*, p. 92.
[187] MELZER: Cyberwarfare..., p. 17.
[188] BROWNLIE, Ian. *International Law and the Use of Force by States*. Oxford: Claredon Press, 1963, p. 278.
[189] DINSTEIN, Yoram. *War, Aggression and Self-Defence*, 5th edition. New York: Cambridge University Press, 2012, p. 203 – 205.
[190] The national Security Strategy of the United States of America, September 2002, p. 15. Available at, >http://www.state.gov/documents/organization/63562.pdf>.
[191]GRAY, Christine. *International Law and the Use of Force*. 3. edition. New York: Oxford University Press, 2008, p. 213 – 216.
[192] ZEMANEK, Karl. Armed Attack. In WOLFRUM, Rüdiger (ed). *The Max Planck Encyclopedia of Public International Law – Vol. I.* New York: Oxford University Press, 2012, p. 595.
[193] SCHMITT: *Tallinn Manual…*, p. 63.

defence, instant, overwhelming, leaving no choice of means, and no moment for deliberation."[194] Although there is no definitive agreement in cases of anticipatory self-defence it seems that the international community is leaning towards its legality.[195]

The problem with anticipatory self-defence and cyberspace is in evaluation of incoming cyber armed attack. It is hard to assess whether cyber armed attack which is about to occur would rise to necessary level of scale and effect. Another problem could be assessment when the activity crosses the line. Tallinn Manual gives the example of insertion of a logic bomb, in cases when activation is likely to occur, which is analogous to placement of naval mines. On the other hand cases which would not be considered as armed attack are the emplacing remotely activating malware, which is basically acquisition of capability to launch attack.[196]

5.2.4 Self-defence against non-state actor

One of the most discussed questions regarding self-defence in current world is whether is self-defence permitted against a non-state actors as well. Article 51, in contrast to Article 2 (4) of UN Charter does not limit itself on actions between states, and only guarantees the right for self-defence to states. The question against whom self-defence is permissible is omitted. This is mainly due to the fact that when UN Charter was drafted, non-state actors did not have capabilities to attack on such scale. Thus this problem had remained omitted in Article 51. This omission serves as one of the arguments for possibility of self-defence against non-state actors.

A notion of non-State actor itself comprises of high number of subjects, from international organizations to transnational corporations. Due to the fact that the group includes practically all actors in international relations that are not states, there are no common sociological features to identify them.[197] In regard to issue of self-defence these actors would be most commonly terrorist or rebel groups. Cyberspace indeed seems to be ideal place for activities of terrorist groups as it provides high level of anonymity and offers high ration of

[194] Letter from Mr. Daniel Webster to Lord Ashburton, Washington, 27. July 1842, Enclosure 1 – Extract from note of April 24, 1841. Available at: <http://avalon.law.yale.edu/19th_century/br-1842d.asp#web1>.
[195] In Larger Freedom: Towards Development, Security and Human Rights for All, Report of the Secretary-General. UN Doc. A/59/2005, 21. March 2005, para. 124; A more secure world: our shared responsibility, Report of the High-Level Panel on Threats, Challenges and Change. UN Doc. A/59/565, 2. December 2004, para. 188.
[196] SCHMITT: *Tallinn Manual*..., p. 65.
[197] WAGNER, Markus. Armed Attack. In WOLFRUM, Rüdiger (ed). *The Max Planck Encyclopedia of Public International Law – Vol. VII.* New York: Oxford University Press, 2012, p. 742.

necessary input and potential effect. It is uncertain whether there needs to be a certain level of organization within the group. If not, then interestingly, it might be relatively possible, that an armed attack would be exercised by single individual.[198] If, as it is discussed below, states have right for self-defence against non-state actor, there is nothing what would preclude self-defence against individual if the attack amounts to sufficient scale and effect.[199] It is however questionable if requirement of necessity would be complied with.

The idea of self-defence against a non-state actor has become significant after attacks on World Trade Center in New York on 11 September 2001. The response against Al Qaeda, the terrorist organisation which was responsible for these attacks, was carried out as an execution of inherent right of self-defence.[200] In addition, the right for self-defence against non-state actor in this particular case was recognized by Security Council of United Nations.[201] Some commentators however claim that this was not a clear confirmation of wider understanding of Article 51.[202] Regardless, the current practice of states shows support for possibility of exercising self-defence against non-state actors.[203]

Unfortunately ICJ has not yet took explicit position on this issue. Some claim that the position of ICJ is that self-defence applies only to attacks attributable to the state.[204] Although the issue was recently touched upon on few instances, ICJ did not elaborate on the issue due to its irrelevance in the legal analysis of said cases.[205] ICJ thus did not explicitly exclude possibility of self-defence against non-state actor. It seems that in light of State practice and *opinio juris,* long lasted interpretation of self-defence must be reconsidered,[206] since it is

[198] SCHMITT: *Tallinn Manual…*, p. 59.
[199] ROSCINI: *Cyber Operations…*, p. 86.
[200] Letter dated 7 October 2001 from the Permanent Representative of the United States of America to the United Nations addressed to the President of the Security Council. UN Doc. S/2001/946, 7. October 2001. Available at <http://www.hamamoto.law.kyoto-u.ac.jp/kogi/2005kiko/s-2001-946e.pdf>.
[201] Resolution 1368 (2001) Adopted by Security Council at its 4370th meeting on 12 September 2001, UN Doc. S/RES/1368 (2001), 12. September 2001; Resolution 1373 (2001) Adopted by the Security Council at its 4385th meeting, on 28 September 2001, UN Doc. S/RES/1373 (2001), 28. September 2001.
[202] WAGNER, Markus. Armed Attack. In WOLFRUM, Rüdiger (ed). *The Max Planck Encyclopedia of Public International Law – Vol. VII.* New York: Oxford University Press, 2012, p. 742.
[203] ROSCINI: *Cyber Operations…*, p. 85.
[204] WAGNER, Markus. Armed Attack. In WOLFRUM, Rüdiger (ed). *The Max Planck Encyclopedia of Public International Law – Vol.VII.* New York: Oxford University Press, 2012, p. 742.
[205] Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, I.C.J. Reports 2004, para. 139; ICJ: Armed Activities…, para 147.
[206] Separate opinion of Judge Simma, Armed Activities on the Territory of the Congo (Democratic Republic of Congo v. Uganda), Judgments, I.C.J. Reports 2005, para 11.

unreasonable to deny right to self-defence to attacked State.[207] The analysis of State practice after 9/11 suggests that States in fact exercise self-defence against non-state actors, although with uncertainty to its exact scope.[208] Unfortunately ICJ "*does not seem to be prepared to adopt this approach*."[209]

Of course, the self-defence against non-state actor covers situations where armed attack of the group is not attributable to the State or it is not the case of indirect armed attack. Thus, since terrorist groups does not control particular territory, the crucial question is when and how it is permitted to take action. Firstly it is necessary to establish that states has obligation to "*not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely an unlawfully affect other States.*"[210] This is not a new obligation to international law, as it was, in general confirmed by ICJ.[211]

Therefore, in order not to violate the sovereignty of the State of origin of the attack, it is possible to act only in particular cases. First possibility is to operate with consent of the state. It is however doubtful that states will be willing to allow armed operation on its territory by another state. The main question is, when it is possible to act in non-consensual cases. Majority of authors of Tallinn Manual took position that such action is possible only in cases when state is unable, e.g. due to lack of technical capacity or unwilling to take effective action to stop cyber armed attack. Indeed, the unwilling or unable test is quite complicated as it is and it becomes even more complicated in cases within cyberspace.[212] Attacked State is obliged to primary demand territorial state to take necessary actions in order to stop ongoing armed attack. This is necessary to respect the sovereignty of territorial state and prevent premature attacks.[213]

Several States use the unwilling or unable test as correct standard for assessment of legality of self-defence considered. It was invoked during operations of Russia in Georgia

---

[207] Separate opinion of Judge Kooijmans, Armed Activities on the Territory of the Congo (Democratic Republic of Congo v. Uganda), Judgments, I.C.J. Reports 2005, para 30.
[208] REINOLD, Theresa. State Weakness, Irregular Warfare, and the Right to Self-Defense Post-9/11. *American Journal of International Law*, 2001, Vol. 105, No. 2, p. 62. Available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1939039>.
[209] SCHMITT: *Tallinn Manual*…, p. 59.
[210] SCHMITT: *Tallinn Manual*…, p. 26.
[211] Corfu Channel case, Judgment of April 9th 1949, I.C.J. Reports 1949, para. 22; United States Diplomatic and Consular Staff in Tehran, Judgment, I.C.J. Reports 1980, para 68.
[212] DEEKS, Ashley. The Geography of Cyber Conflict: Through a Glass Darkly. *International Law Studies,* 2013, Vol. 89, p. 3.
[213] SCHMITT: *Tallinn Manual*…, p. 61.

against Chechens, Turkey in Iraq against Kurdish Workers Party, Israel in Lebanon against Hezbollah and Palestine Liberation Organization, and by United States on several occasions.[214] In first two cases States specifically invoked this test, whilst third States tacitly condoned these actions, suggesting, that this approach is at least tolerated in current practice, even if not directly endorsed.[215] The unwilling or unable standard is one of due diligence as strict liability would create unacceptable high burden upon states.[216] Whole concept sprouts from principle of necessity, since territorial state does not put stop to cyber armed attack and attacked State needs to subsidiary defend itself.[217] Although State practice supporting this can be shown, the test itself is far from established in international law. It seems that in order to adapt to newly imposed threats by non-state actor, the concept of self-defence undergoes the period of interpretational transition.

[214] DEEKS, S. Ashley. „Unwilling or Unable": Toward a Normative Framework for Extraterritorial Self-Defense. *Virginia Journal of International Law*, 2012, Vol. 52, No. 3, p. 486 – 487.
[215] HAKIMI, Monica. Defensive Force against Non-State Actors: The State of Play. *International Law Studies*, 2015, Vol. 91, p. 14.
[216] ROSCINI: *Cyber Operations…*, p. 88.
[217] KREß, Claus. Some Reflection on the International Legal Framework Governing Transnational Armed Conflicts. *Journal of Conflict & Security Law*, 2010, Vol. 15, No. 2, p. 250.

6 Cyberspace and *ius in bello*

As discussed in previous chapter, international law is based on general prohibition of use of force with certain exceptions. Unfortunately, general prohibition of use of force has not come with absolute respect to this rule and States use the force up to this day. It is therefore unthinkable not to address issue of law of armed conflicts. The application of *ius in bello* and *ius ad bellum* is independent. Meanwhile *ius ad bellum* sets whether use of force is legal or illegal, *ius in bello* addresses legality of actions within armed conflict, regardless of legality of initial action.

The body of law which governs law of armed conflicts is quite wide. The LOAC consists mainly of Hague Conventions of 1899 and 1907 and four 1949 Geneva Conventions with their Additional Protocols, addressing means and methods of warfare, conduct of hostilities and protection of victims of war. Majority of rules set in these treaties are codification of customary law, particularly provisions of Additional Protocol I.[218]

This chapter will therefore address the issues of cyber operation in situations of armed conflicts. Firstly, as it is necessarily results from state of law of armed conflicts, the scope of applications of these sets of rules shall be discussed. Secondly the particular and crucial issues of conduct of hostilities will be addressed, in respect to cyberspace.

6.1 Application of the Law of Armed Conflict

The question of applicability of LOAC can be divided into four main categories. Firstly in what situations LOAC applies. Secondly in which period of time it applies. Thirdly in what territory it applies and fourthly on who it applies.

Firstly, *ratione materiae*, provides answer in which situations shall be LOAC applied. Since this covers a variety of situations which requires different conditions to be fulfilled, it will be addressed and discussed further.

Second point, i.e. *ratione temporae*, was clarified by ICTY when determined that "*international humanitarian law applies from the initiation of such armed conflicts and extends*

[218] SASSÒLI, Marco, BOUVIER, Antione, QUINTIN Anne. *How does law protect in war*? Chapter 2, Vol I. ed.3. ICRC, 2011, p. 24. Available at <https://www.icrc.org/eng/resources/documents/publication/p0739.htm>.

beyond the cessation of hostilities until a general conclusion of peace is reached; or, in the case of internal conflicts, a peaceful settlement is achieved."[219] The relevant exception in this rule applies to cases of occupation when LOAC stops to apply year after general close of military operation, with exception to certain provisions which apply even after the one year period.[220]

Third point, *ratione loci*, is not explicitly addressed in Geneva Conventions. Again, the clarification came thanks to work of international criminal tribunals. ICTY held that LOAC applies "*in the whole territory of the waring Stets or, in case of internal conflicts, the whole territory under the control of a party, whether or not actual combat takes place there*."[221] This was confirmed by ICTR[222] and further developed in a way that "*there is no necessary correlation between the area where the actual fighting is taking place and the geographical reach of the law of war*."[223] Although authors of Tallinn Manual naturally agree that cyber operations are subject to these limitations imposed by relevant LOAC, they point out that these limitation may be difficult to implement in cyber context, due to nature of technology which allows attack through cloud or routing data through servers in various countries.[224]

Fourthly, regarding *ratione personae*, LOAC applies primarily on States. But particular legal instruments bind non-state actors as well as States.[225]

6.1.1 International Armed Conflict

Tallinn Manual stipulates that "*international armed conflict exists whenever there are hostilities, which may include or be limited to cyber operations, occurring between two or more States.*"[226] This definition proves insufficient without analysis of IAC in general. Common Article 2 of Geneva Conventions, states that "*the present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting*

[219] ICTY, The Prosecutor v. Duško Tadić, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, Case No. IT-94-1-A, 2 October 1995, para 70.
[220] Art. 6 of the Geneva Convention IV.
[221] ICTY, The Prosecutor v. Duško Tadić, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, Case No. IT-94-1-A, 2 October 1995, para 70.
[222] ICTR, The Prosecutor v. Jean-Paul Akayesu, Judgment, Case No. ICTR-96-4, 2 September 1998, para 635.
[223] ICTY, The Prosecutor v. Dragoljub Kunacarac, Radomir Kovac and Zoran Vukovic, Judgment, IT-96-23 & IT-96-23/1-A, 12 June 2002, para 57.
[224] SCHMITT: *Tallinn Manual*…, p. 78.
[225] SIVAKUMARAN, Sandesh. *The Law of Non-International Armed Conflict*. 1. ed. Oxford: Oxford University Press, 2012, p. 236 – 237.
[226] SCHMITT: *Tallinn Manual*…, p. 79.

Parties, even if the state of war is not recognized by one of them. *The Convention shall also apply to all cases of partial or total occupation of the territory of a High Contracting Party, even if the said occupation meets with no armed resistance."*[227] It probably shall be noted that nowadays the Conventions would apply virtually in every case, since almost every state is a contracting party. Even if non-contracting party is concerned, key rules are applied via customary law.[228] As can be seen from common Article 2, we can apply LOAC in international conflict in three cases. Firstly, it is case of declared war, secondly the case of occupation of territory and lastly in case of any other armed conflict.

It is thus conclusive that LOAC would apply to cyber operations in cases, when cyber operation follows the declaration of war, occupation of territory, when occurs in already existing international armed conflict or when cyber operations themselves amount to armed conflict, independently on traditional means of attack.[229] The last situation, where cyber operation is the first or only hostility, is the most difficult one, as far as its relation to LOAC goes[230] and therefore will be addressed in the greatest extent.

It seems unnecessary to excessively address the cyber operations in cases of declared war and occupation of territory of state. Firstly, declaration of war seems to be an outdated concept, since current state of LOAC concentrates on concept of armed conflict.[231] Still, parties to the Convention (III) relative to the Opening of Hostilities[232] are bound by its Article 1 not to start any hostilities without previous explicit warning, e.g. declaration of war. The important element of declaration of war is the manifestation of state to turn peaceful state to the state of war, i.e. *animus bellandi*.[233] It is irrelevant whether after declaration of war actual hostilities take place, as the declaration itself triggers application of LOAC. Every relevant cyber operation after such declaration would be covered by LOAC. On the other hand, interestingly, there is no prescribed method of declaration of war. It is therefore possible, that state would declare war through cyberspace, for example by email. Indeed it seems improbable, however there is no legal obstacle for such approach.

---

[227] Common Art. 2 of Geneva Conventions.
[228] CLAPHAM, Andrew. In CLAPHAM, Andrew, GAETA, Paola, SASSÒLI, Marco (eds). The 1949 Geneva Conventions: A Commentary 1. ed. Oxford: Oxford University Press, 2015, p. 8.
[229] ROSCINI: *Cyber Operations…*, p. 121.
[230] DÖRMANN, Knut. *Applicability of the Additional Protocols to Computer Network Attacks.* ICRC, 200 4, p. 6. Available at <https://www.icrc.org/eng/resources/documents/misc/68lg92.htm>.
[231] ROSCINI: *Cyber Operations…*, p. 123.
[232] Art. 1 of Convention (III) relative to the Opening of Hostilities, Hague, 18. October 1907.
[233] WRIGHT, Quincy When Does War exist? American Journal of International law 26 1932, p. 363.

The issue of cyber operations in regard to partial or total occupation seems to be of little relevance as well. "*The territory is considered occupied when it is actually placed under authority of the hostile army*."[234] To comply with this, belligerent State must exercise effective control over said territory. The concept of effective control was elaborated by legal doctrine, whilst several indications of effective control over territory were developed.[235] This however would be impossible without actual physical presence of foreign forces, what constitute one element of "effective control test."[236] Therefore territory of a State cannot be occupied via cyber operations as well as there is no notion of occupation of cyberspace.[237] However once occupation takes place, relevant cyber issues would be subject to LOAC.[238]

Probably the most intriguing question of LOAC in relation to cyber operation is whether an armed conflict, in this case of international character, can start and consist only of cyber operations. The abovementioned definition from Tallinn Manual suggests so, however it seems necessary to discuss individual elements which constitute IAC. Of course the issue is not definitively resolved and brings many problems. The definite answers will be probably provided only by future state practice. [239]

As mentioned above, the current LOAC stands on concept of armed conflict. As one might expect, there is no indication what constitutes armed conflict. The departure from concept of war and absence of definition of armed conflict was intentional, for expansion of application of LOAC and its dependence on factual analysis rather that legal assessment.[240] Subsequently, international armed conflict was described as *"any difference arising between two States and leading to the intervention of members of the armed forces*."[241] This was altered in favour of factual existence of armed force rather than involvement of armed forces to nowadays widely accepted approach that "*an armed conflict exists whenever there is a resort*

[234] Article 42 of the Convention (VI) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land, Hague, 18. October 1907.
[235] ICTY, Prosecutor v. Mladen Naletilic, aka "TUTA" and Vinko Martinovic, aka "Štela", Trial Judgment, Case No. IT-98-34-T, 31. March 2003, para 217.
[236] FERRARO, Tristan. Determining the beginning and the end of an occupation under international humanitarian law. *International Review of the Red Cross*, 2012 Vol.94, No. 885, p. 142.
[237] SCHMITT: *Tallinn Manual…*, p. 239.
[238] SCHMITT: *Tallinn Manual…*, p. 239 – 247.
[239] ICRC: International Humanitarian Law..., p. 37.
[240] PICTET, Jean (ed). *The Geneva Conventions of 12 August 1949 Commentary - Vol. IV.* Geneva: International Committee of Red Cross, 1958, p. 20 (Art. 2).
[241] Ibid.

to armed force between States."[242] Thus two condition must be fulfilled, i.e. firstly there must be a resort to armed force and secondly it must happen between States.

Therefore, the question is what constitutes resort to armed force and whether it can be achieved by cyber operation. The "resort to armed force" must be distinguished from use of force in sense of Article 2(4) of UN Charter, since use of force does not automatically triggers use of LOAC.[243] This distinction arises from wide understanding of use of force by ICJ. The indirect use of force, i.e. arming or training of armed groups is not sufficient to be considered as resort to armed force.[244]

With this in mind, Tallinn Manual claims that IAC exists whenever there are hostilities occurring between two states.[245] The concept of hostilities, which according to authors, is clearly requirement of notion armed conflict, may solely consist of cyber operations and "*presupposes collective application of means and methods of warfare*."[246] Therefore not the use of force but occurrence of hostilities is necessary to start IAC.[247] Hostilities themselves refers to the collective resort to methods and means of injuring enemy.[248] Therefore, and there is practically no dispute, cyber operations which have analogical effects as traditional kinetic hostilities, i.e. death, injury or destruction, can start IAC on their own.[249] More problematic is the situation of cyber operations which does not directly cause injury or destruction, but rather incapacitate their target.

Could a disablement of NCI, for example a power grid alone, start an IAC? Up to now state practice shows high level of tolerance against cyber-attacks, suggesting necessary level of severity of such attack to be considered cyber-attack.[250] It seems reasonable to assume that State, who's NCI would be severely disrupted by cyber operation, would consider such operation as hostility. Imagine a coordinated cyber operation against State which would disrupt banking sector, power grid, water supply, health and emergency sector. This would cause huge

[242] ICTY, The Prosecutor v. Duško Tadić, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, Case No. IT-94-1-A, 2 October 1995, para 70.
[243] ICJ: Nicaragua…, para. 216.
[244] ICTY, Prosecutor v. Duško Tadić, Judgment of the Appeals Chamber, Case No. IT-94-1-A, 15. July 1999, para 137.
[245] SCHMITT: *Tallinn Manual*…, p. 79.
[246] SCHMITT: *Tallinn Manual*…, p. 82.
[247] MELZER: Cyberwarfare..., p. 24.
[248] MELZER, Nils. *Interpretative Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*. ICRC, 2009, p. 43.
[249] MELZER: Cyberwarfare..., p. 24
[250] ARIMATSU, Louise, Classifyng cyber warfare. In TSAGOURIAS, Nicholas, BUCHAN, Rusell. *Research Handbook on International Law and Cyberspace*. Northampton: Edward Elgar Publishing, 2015, p. 332.

economic loss, chaos and presumably even damage and injury. Nevertheless damage or injury would not be necessarily directly caused by cyber operation, rather than their indirect cause. Therefore if State loses its capacity to carry out its essential functions due to severe cyber operations it would be probably considered a start of IAC.[251]

Additionally there is controversy regarding the threshold of required violence. It seems that the majority of international community agrees that there is no threshold.[252] Art. 2 of Geneva Conventions does not require any threshold. Armed conflict exists between Parties regardless of intensity existence of armed force is sufficient.[253] Contrary approach claims that certain level of intensity is necessary and so isolated border clashes would not be covered by LOAC.[254] This approach creates a dangerous legal vacuum, in which no protection is given to persons engaged.[255] If threshold was necessary, Parties of conflict would have opportunity to deny that hostilities reached this threshold and LOAC would depend on intention of Party, what would bring same problems as older concept of war.[256] Although States may avoid addressing incidental violence as armed conflict, the LOAC shall apply regardless of their opinion.

Above-mentioned is indeed true as far as cyber operations with analogous effects as kinetic hostilities go. On the other hand, cases of cyber operations with disruptive effects must be significantly harmful to qualify as resort to armed force. This does not mean that there exists threshold regarding this kind of operations, but only severely disruptive operations can be equated to those traditional and destructive.[257]

Second requirement of IAC is that it must happen between States. This is of extreme importance as it determines whether an armed conflict will be defined as international or non-

[251] Advisory Council on International Affairs, Advisory Committee on Issues of Public International Law. *Cyber Warfare*. No. 77, AIV/No. 22, CAVV, 2011, p. 24. Available at: <http://aiv-advies.nl/download/da5c7827-87f5-451a-a7fe-0aacb8d302c3.pdf>.
[252] ICRC: International Humanitarian Law…, p. 7
[253] ICTY, Prosecutor v. Zejnil Delalić, Zdravko Mucić also known as "Pavo", Hazim Delić, Esad Ladžo also known as "Zenga", Judgment of Trial Chamber, Case No. IT-96-21-T, 16. November 1998, para 184
[254] SCHMITT, N. Michael. Wired Warfare: Computer network attack and jus in bello. *International Review of the Red Cross,* 2002, Vol. 84, No. 846, p. 372.
[255] KLEFFNER, K Jann. Scope of Application of International Humanitarian Law. In FLECK, Dieter. *The Handbook of International Humanitarian Law*. Oxford: Oxford University Press, 2013, p. 45.
[256] DOSWALD-BECK, Louise. Some Thoughts on Computer Network Attack and the International Law of Armed Conflict. *International Law Studies*, 2002, Vol. 76, p. 164.
[257] ROSCINI: *Cyber Operations*…, p. 136.

international and therefore which set of rules will be applied.[258] This is however the question of attribution of action to States, which was already addressed above.

Lastly it is important to address which cyber operations would be subjected to LOAC, when they are employed in already existing international armed conflict. It seems logical that as Tallinn Manual states "*cyber operations executed in the context of an armed conflict are subject to the law of armed conflict*."[259] The wording is compromise since there was no consensus on nexus between cyber operation and armed conflict. One approach subjects all cyber operations of one party against its opponent to LOAC. On the other hand, in view of some, only those cyber operations which are undertaken in order to contribute to originator's military effort are subject of LOAC.[260] Generally speaking not every act that affects military operation is to be considered as participation in hostilities, but it must reach necessary belligerent nexus. The mere objective likelihood of harm is insufficient and the act (in this case cyber operation) must be "*specifically designed to directly cause the required threshold of harm in support of a party to the conflict and to the detriment of another*."[261] Therefore only those cyber operations which are used against opposing party and capable of generating sufficient harm upon it would be subject to LOAC once international armed conflict is established.

6.1.2 Non-International Armed Conflict

Tallinn Manual states that NIAC "*exists whenever there is protracted armed violence, which may include or be limited to cyber operations, occurring between governmental armed forces and the forces of one or more armed groups, or between such groups. The confrontation must reach a minimum level of intensity and the parties involved in the conflict must show a minimum degree of organization*."[262] One can only agree with such definition as it encompasses all necessary elements which have been developed so far.

Common Article 3 of the 1949 Geneva Conventions is a foundation for a NIAC but does not provide any definition of what constitutes NIAC. There were several indicators what

[258] DROEGE, Cordula. Get off my Cloud: Cyber warfare, international humanitarian law, and the protection of civilians. *International Review of the Red Cross: Humanitarian Debate: Law, policy, action*, 2012, Vol. 94, No. 886, p. 543.
[259] SCHMITT: *Tallinn Manual*…, p. 75.
[260] SCHMITT: *Tallinn Manual*…, p. 76.
[261] MELZER: Interpretative Guidance…, p. 58.
[262] SCHMITT: *Tallinn Manual*…, p. 84.

constitutes NIAC, however nowadays most authoritative and accepted approach is one adopted by ICTY which stated that non-international armed conflict exists when there is "*protracted armed violence between governmental authorities and organized armed groups or between such groups within a State."*[263]

Firstly, NIAC can occur only if and organized armed group is a Party to the conflict. In relation to cyber operations, a group is to be considered as armed when it has capacity to conduct cyber-attack.[264] When considering the requirement of organization ICTY proposed several factors which shall be considered, i.e. *„existence of a command structure and disciplinary rules and mechanisms within the group; the existence of a headquarters; the fact that the group controls a certain territory; the ability of the group to gain access to weapons, other military equipment, recruits and military training; its ability to plan, coordinate and carry out military operations, including troop movements and logistics; its ability to define a unified military strategy and use military tactics; and its ability to speak with one voice and negotiate and conclude agreements such as cease-fire or peace accords.*"[265] It is irrelevant whether members of organization violate, even regularly international law, as long as organizational ability to comply with LOAC is present.[266]

It is typical for cyberspace that groups that never met can execute a cyber operation, which can have devastating consequences. The absence of physical meeting is not a problem, however it is necessary that the group would have a kind of leadership and organizational structure to coordinate and plan its operations.[267] Problems can arise with requirement of ability to implement LOAC through organizational structure. Mere online meeting would be probably too vague to qualify group as organized, not to mention the problem to identify person operating behind the computer and determine its membership in group. It is indeed possible, however it seems unrealistic.[268]

---

[263] ICTY, The Prosecutor v. Duško Tadić, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, Case No. IT-94-1-A, 2 October 1995, para 70.
[264] SCHMITT: *Tallinn Manual…*, p. 88.
[265] ICTY, Prosecutor v. Ramush Haradinaj et al., Judgment, Trial Chamber I, Case No. IT-04-84-T, 3. April 2008, para. 60.
[266] ICTY, Prosecutor v. Ljune Boškoski, Johan Tarčulovski, Judgment, Trial Chamber II, Case No. IT-04-82-T, 10. July 2008, para 205.
[267] SCHMITT: *Tallinn Manual…*, p. 89.
[268] GEISS, Robin. Cyber Warfare: Implications for Non-international Armed Conflicts. *International Law Studies*, 2013, Vol. 89, p. 636.

Additionally, protracted armed violence must take place. This is not dependent on particular weapon and therefore can be achieved by cyber operation. Given the conditions required, it will hardly do so on its own.[269] The question is what constitutes protracted violence. ICTY examined this questions on many occasions after setting this requirement in Tadić case, focusing on the intensity of conflict rather that other elements.[270] In order to establish whether the intensity is grave enough, ICTY considers among other possible factors "*number, duration and intensity of individual confrontations; the type of weapons and other military equipment used; the number and calibre of munitions fired; the number of persons and type of forces partaking in the fighting; the number of casualties; the extent of material destruction; and the number of civilians fleeing combat zone*."[271] Cyber operations therefore must be considered on case by case basis, whether their consequences reach necessary intensity.

In relation to non-destructive cyber operation, the answer is unclear. Tallinn Manual avoids analysis due to absence of consensus on the issue.[272] Roscini is of the opinion that "*only multiple coordinated cyber operations seriously disrupting the functioning of several or all critical infrastructures of heavily digitally reliant state for a prolonged time may potentially be considered by states to reach the intensity requirement needed for the application of the law of non-international armed conflict in the absence of associated kinetic hostilities*."[273] Even if States will consider these as protracted armed violence of sufficient intensity to start NIAC, it is unlikely that such cyber operations will take place on its own in foreseeable future.

It shall be also noted that the fact that the operation takes place outside the territory of given State does not render conflict international. The scenario of spill over is possible, however does not render conflict international. This is relevant to the cyber operations, since

[269] SCHMITT: Tallinn Manual…, p. 85

[270] ICTY: Mucić et al…, para. 190; Milošević Rule 98 bis Decis ICTY, Prosecutor v. Slobodan Milosević, Decision on Prosecution's Motion under Rule 73 (A) for a Ruling on the competence of the Amici Curiae to present a Motion for Judgment of Acquittal under Rule 98 bis, Trial Chamber, Case No. IT-02-54-T, 5. February 2004, para. 17; ICTY, Prosecutor v. Dario Korcić and Mario Čerkez, Judgment, Appeals Chamber, Case No. IT-95-14/2-A, 17. December 2004, para. 341; ICTY, Prosecutor v. Sefer Halilović, Judgement, Trial Chamber I, Case No. IT-01-48-T, 16. November 2005, para. 173; ICTY, Prosecutor v. Limaj et al., Judgment, Trial Chamber I, Case No. IT-03-66-T, 30. November 2005, para. 93; ICTY, Prosecutor v. Enver Hadžihasanović and Akmir Kubura, Judgment, Trial Chamber, Case No. IT-01-47-T, 15. March 2006, para. 20; ICTY, Prosecutor v. Milan Martić, Judgment, Trial Chamber I, Case No. IT-95-11-T, 12. June 2007, para 347; ICTY, Prosecutor v. Mile Mrkšić et al., Judgment, Trial Chamber II, Case No. IT-95-13/1-T, 27. September 2007, para. 140.

[271] ICTY, Prosecutor v. Ramush Haradinaj et al., Judgment, Trial Chamber I, Case No. IT-04-84-T, 3. April 2008, para. 49.

[272] SCHMITT: *Tallinn Manual*…, p. 88.

[273] ROSCINI: *Cyber Operations*…, p. 154.

they can be executed practically from around the globe. However if cyber-attack is made from another State, it does not automatically makes it an international conflict.[274]

The abovementioned applies to common Article 3 of Geneva Conventions. Certain NIAC are covered by provisions of AP II. These are those and *„which take place in the territory of a High Contracting Party between its armed forces and dissident armed forces or other organized armed groups which, under responsible command, exercise such control over a part of its territory as to enable them to carry out sustained and concerted military operations and to implement this Protocol."*[275] Clearly it is practically impossible to apply this Convention to purely cyber NIAC, as control of part of territory inevitably requires physical presence. On the other hand it can be argued that, at least in view of ICRC, the difference is irrelevant as most if not all the rules of AP II apply to situations of Common Article 3 through customary law.[276]

However, it shall be still taken into account that *"situations of internal disturbances and tensions, such as riots, isolated and sporadic acts of violence, and other acts of similar nature"*[277] Therefore sporadic cyber incidents which even may cause damage or injury do not qualify as NIAC in the sense of AP II.[278]

6.2 Conduct of hostilities in cyberspace

As was mentioned, as far as treaty law goes, different treaties apply to IAC and NIAC. IAC is governed by 1899 and 1907 Hague Conventions, 1949 Geneva Conventions and their AP I. NIAC on the other hand is governed by Common Article 3 to Geneva Conventions which was subsequently supplemented by AP II. The difference in substantive provisions substance is even more striking, as for example AP I contains 3 times more articles as AP II. The question which shall be asked is why the rules of fighting shall be different in IAC and NIAC. It seems that the situation changed from the times when affected treaties were drafted. Nowadays many rules apply to both, IAC and NIAC through customary law.[279] Of course these rules cannot be copied

[274] SCHMITT: *Tallinn Manual…*, p. 85.
[275] Article 1 (1) of AP II.
[276] MILANOVIC, Marko and HADZI-VIDANOVIC, Vidan. A Taxonomy of Armed Conflict. In WHITE, Nigel, HENDERSON, Christian (ed). *Research handbook on international conflict and security law.* Northapton: Edward Elgar Publishing, 2013. p. 28.
[277] Article 1(2) of AP II.
[278] SCHMITT: *Tallinn Manual…*, p. 86.
[279] HENCKAERTS, Jean-Marie, DOSWALD-Beck, Lousie. *Customary International Humanitarian Law – Vol. I: Rules*. Cambridge: Cambridge University Press, 2005.

from IAC to NIAC mechanically, rather their general essence shall be applied.[280] It therefore follows that analysis presented applies to both IAC and NIAC, with respect to certain different issues.

Tallinn Manual approaches LOAC with intent to transpose relevant rules of LOAC to cyber operations. It is necessary and meritorious approach. Taking into account the broad spectrum of rules developed by Tallinn Manual it seems out of range of this thesis to elaborate on every one of them. The focus will thus lie on main principles and their representation in form of rules which govern LOAC.

6.2.1 Are cyber operations legal means and methods of warfare?

As a starting point it seems appropriate to address that certain means and methods of warfare are prohibited in any situation regardless enemy or conflict, as the right to choose method or mean of warfare is not unlimited.[281] What constitutes means and methods of warfare is not defined by treaty law. Tallinn Manual provides its own definition of both terms in regard to cyber warfare.

Methods of cyber warfare are described as "*cyber tactics, techniques, and procedures by which hostilities are conducted.*"[282] This term is broader that notion of cyber-attack (which will be addressed further bellow), and includes other kinds of cyber operations as well, such as interference of enemy's communication.[283]

Means of cyber warfare are defined by Tallinn Manual as „*cyber weapons and their associated cyber systems.*"[284] This includes means that are designed, used or intended to cause injury or death of persons, damage or destruction of objects, i.e. any devices, mechanism, equipment or software which can be used to execute cyber-attack.[285] This definition unfortunately does not include the effect of disruption of NCI. It seems reasonable to expect that disruptive attacks on NCI will be considered as means of warfare, as rendering NCI useless has same effects as its destruction.

[280] ICTY, The Prosecutor v. Duško Tadić, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, Case No. IT-94-1-A, 2 October 1995, para 126.
[281] Art. 35 (1) of AP I.
[282] SCHMITT: *Tallinn Manual*…, p. 141.
[283] Ibid. p. 142.
[284] Ibid. p. 141.
[285] Ibid. p. 142.

Means and methods of warfare which are prohibited regardless of other circumstances are, in regard to cyberspace addressed from rule 41 to 48 of Tallinn Manual and are derived from various provisions of AP I. Primarily it is prohibited to employ weapons which cause superfluous injury or unnecessary suffering.[286] What constitutes unnecessary suffering is a question of debate, ICJ defined it as *"a harm greater than that unavoidable to achieve legitimate military objectives."*[287] It means that that it is necessary to balance the military necessity and excessive injury or suffering. Also the availability of alternative means shall be considered as well as inevitability of death or permanent injury.[288] Obviously cyber operations *per se* are not of such nature, however in very rare, theoretical cases even cyber operations can be unlawful. Tallinn Manual sets an example of stopping and restarting internet accessible built-in defibrillator, causing unnecessary suffering.[289]

Moreover the methods or means which may cause widespread, long-term and severe damage to natural environment are prohibited[290] as well as those which may cause damage to natural environment and thus endanger health or survival of population.[291] The threshold is seems to be high, e.g. long-term is to be interpreted as decades.[292] Tallinn Manual does not even reflects on these provisions. It is understandable, since it is hard to imagine that a cyber-attack would achieve such high threshold when conventional attacks, e.g. bombing, was unable to do so.[293] The conceivable examples are release of chemicals from production facility, rupture of oil pipeline or meltdown of nuclear reactor and release of radioactivity.[294]

Another important prohibition bans means and methods which cannot be directed at specific military objective,[295] which effect cannot be limited as required[296] and are therefore considered to be indiscriminate. This is reflected by Tallinn Manual as well. In this case, what shall be noted is, that although this provision has its roots in principle of distinction, it does not deal with targeting, but with fact whether a weapon is inherently incapable of distinction between civilians and military objectives or behave unpredictably. This would be for example

[286] Art. 35 (2) of AP I.
[287] ICJ: Nuclear Weapons…, para. 78.
[288] HENCKAERTS: Customary International…, p. 241.
[289] SCHMITT: *Tallinn Manual*…, p. 144.
[290] Art. 55 of AP I.
[291] Art. 35 (3) of AP I.
[292] HENCKAERTS: Customary International…, p. 157
[293] Ibid.
[294] SCHMITT: Wired Warfare..., p. 386.
[295] Art. 51 (4) b) of AP I.
[296] Art. 51 (4) c) of AP I.

case of contagious biological weapons (leaving aside their prohibition in treaty law).[297] It is more likely that weapon is used in indiscriminate way than it is *per se* inherently indiscriminate.[298] In cyberspace malware might be great example. Even if delivered into military network, it eventually start spreading uncontrollably. Still, it would have to reach certain level of intensity, presumably causing damage, destruction or injury, as mere inconvenience is irrelevant.[299] It is unlikely that such situation will occur in foreseeable future, since program capable of such effect must be very specialized and would require additional support.

Another interesting and highly relevant example is the prohibition of booby traps. Tallinn Manual derives the rule from treaty law and states that "*it is forbidden to employ cyber booby traps associated with certain objects specified in the law of armed conflict.*"[300] The booby trap is defined "*any device or material which is designed, constructed or adapted to kill or injure and which functions unexpectedly when person disturbs or approaches an apparently harmless object or performs an apparently safe act.*"[301] The booby trap must be attached to or associated with particular types of objects or signs.[302] An example of possible cyber booby trap is a mail attachment sent to technician of water plant, under the identity of for example, Red Cross. This attachment would after opening, release a code which would contaminate water.[303] Other examples can be disabling electricity needed for life supporting facilities or triggering an explosion which would lead to injury, possibly death. It seems as a necessary rule, since human factor is still the most vulnerable element of any cyber defence. On the other hand it is questionable how these provisions will be interpreted in practice for example whether software can be subsumed under notion of device.

It is clear that some kinds of cyber operations can be considered as prohibited means and methods of warfare. Due to diversity of cyber operations, their legality cannot be assessed generally, but in relation to every cyber operation on case by case basis.[304] This however does not excuse States from doing so. The general obligation of States to review its weapons. This

---

[297] *HPCR commentary on the HPCR manual on international law applicable to air and missile warfare*. Cambridge: Program on Humanitarian Policy and Conflict Research at Harvard University, 2010, p. 64. Available at <http://www.ihlresearch.org/amw/manual/>.

[298] DINSTEIN, Yoram, Warfare, Methods and Means. In WOLFRUM, Rüdiger (ed). *The Max Planck Encyclopedia of Public International Law – Vol. X*. New York: Oxford University Press, 2012, p. 771 – 772.

[299] SCHMITT: *Tallinn Manual…*, p. 146.

[300] Ibid.

[301] Art. 2 (2) of Protocol (II) on Prohibition or Restrictions on the Use of Mines, Booby-Traps and Other Devices.

[302] Ibid. Art. 6.

[303] SCHMITT: *Tallinn Manual…*, p. 148.

[304] ROSCINI: *Cyber Operations…*, p. 177.

evaluation must be made before the employment of particular weapon.[305] This obligation is relevant for cyber weapons as well as for any other means or methods of warfare.[306]

6.2.2 Cyber operation as attack

As has been seen, certain cyber operations might be considered as unlawful means or methods of warfare. Those which would be considered legal can be employed in armed conflict, but they must comply with particular provisions of conduct of hostilities. The conduct of hostilities is based on several principles, namely principle of distinction, necessity, proportionality, humanity and neutrality. This section will address certain issues of cyber-attacks.

Before further assessment, it is necessary to address notion of cyber-attack. This necessity arise from the fact that limitations regarding distinction, necessity and proportionality, apply to the attacks conducted in armed conflict and not every military operation.[307] This is based on the wording of Art. 51(2) and (5) of AP I. Although AP I uses in Article 51(1) term of operations, it is to be interpreted as referring military operations, during which violence is used.[308] The same applies to existence of principle in customary law, i.e. attacks cannot be directed against civilians.[309] Attack is defined as "*means of violence against the adversary, whether in offence or in defence.*"[310] Therefore the main defining element is violence. Nevertheless cyber operations are not violent per se, as their primary effect only affects data. This does not disqualify cyber operations from being attack. The purpose of relevant provisions is to protect particular persons and objects. Therefore the notion of violence depends on consequences and not acts.[311] It is the effect of attack that is violent not the way of attack. Therefore, Tallinn Manual adopts definition of cyber-attack which is "*a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or destruction to objects*."[312] This

[305] Article 36 of AP I.
[306] SCHMITT: *Tallinn Manual*…, p. 154.
[307] SCHMITT: Wired Warfare..., p. 376.
[308] PILLOUD, Claude, SANDOZ, Yves, SWINARSKI, Christophe, ZIMMERMANN, Bruno (ed). *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*. Norwell: Kluwer Academic Publishers, 1987, para. 1875.
[309] HENCKAERTS: Customary International…, p. 3.
[310] Article 49 (1) of the AP I.
[311] SCHMITT: Wired Warfare..., p. 377.
[312] SCHMITT: *Tallinn Manual*…, p. 106.

means that the cyber operation has to cause injury, death, damage or destruction to be qualified as cyber-attack.

As always with cyber warfare, the problem with this approach lies within realm of non-physical effects. Tallinn Manual states that majority of its authors agrees that interference with functionality is a cyber-attack, if it requires replacement of physical component.[313] On the other hand many commentators come to different conclusion, although by different approaches. We can find the claim that these principles apply to every cyber hostility, therefore what is attack seems irrelevant.[314] Schmitt argues that mental suffering shall be considered as injury and therefore cyber operation against banking system causing widespread mental anguish would be an attack.[315] Roscini proposes broadening the notion of violence to include incapacitation of infrastructure due to dependence of modern society on these technologies.[316] Dörmann claims that Article 52(2) works with notion of neutralization and is irrelevant whether the disablement is achieved by destruction or not.[317] Schmitt recently amended his position, shifting from "injury, death, damage or destruction" to functionality test, for it makes no difference how is the object disabled, since it does not work. What matters is that the object is no longer able to serve its purpose.[318]

For example a recent power outage in Ukraine left more than 80 000 people without electricity for about three hours. This outage was achieved purely by cyber operation, what makes it a first case of successful case of cyber operation which achieved disruption of electric grid. Letting aside technical details of operation, the repair have been made by physical closing of remotely opened circuit breakers. So far there are no reports of damage or injury caused by this operation. Speculations suggest that this cyber operation can be attributed to Russia as retaliation for energy outages in Crimea.[319] But if we presumed that this cyber operation could be attributed to Russia, would it constitute cyber-attack? As seen above, there is no consensus

[313] SCHMITT: *Tallinn Manual…*, p. 109.
[314] MELZER, Nils. *Cyberwarfare and International Law*. UNIDIR Resources, 2011, p. 27. Available at <http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf>.
[315] SCHMITT: Wired Warfare…, p. 377.
[316] ROSCINI: *Cyber Operations…*, p. 182.
[317] DÖRMANN, Knut. *Applicability of the Additional Protocols to Computer Network Attacks.* ICRC, 200 4, p. 6. Available at <https://www.icrc.org/eng/resources/documents/misc/68lg92.htm>.
[318] SCHMITT, Michael. Rewired warfare: rethinking the law of cyber attack. *International Review of the Red Cross: Scope of the law in armed conflict*, 2014, Vo. 96, No. 893, p. 202 – 203.
[319] ZETTER, Kim. *Everything we know about Ukraine's power plant hack* [online]. wired.com, 20. January 2016 [cit. 4. February 2016]. Available at <http://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/>.

among scholars on this issue. The assessment is hard to make since there was no follow up to this operation, the power outage was considerably short, without any additional damage or injury reported. If considered as stand-alone cyber operation, one would probably argue that it should be considered as inconvenience as it did not achieve sufficient severity to be equated to kinetic attack. Contrary to that, imagine that circuit breakers would be damaged by explosives, causing same power outage. Such scenario would be undeniably considered as an attack. Should the negligible damage caused on breakers be the decisive point in determination of what is attack? It therefore seems appropriate for operation with such big-scale effect to be considered a cyber-attack.

6.2.3 Cyber-attacks against persons

There is no debate on the subject that principle of distinction applies to cyber-attacks. The practical application of principle is twofold. Firstly civilian population or civilians individually cannot be object of the attack[320] and secondly, that civilian objects cannot be object of attack as well.[321] Both situation must be addressed separately, as the conditions what can and cannot be attacked are different.

Firstly we should address what individuals can be targeted in armed conflict. As was stated it is prohibited to attack civilians. Civilians are defined negatively, as persons who does not belong to certain group of persons.[322] Of course civilians can directly participate in cyber hostilities, but with the consequence of losing their protection from attacks.[323] The issues of combatant status and status of prisoner of war will not be addressed as they are not directly affected under prism of cyber warfare. What shall be addressed are persons which can be directly targeted by cyber-attack.

Tallinn Manual consolidates list of persons against which cyber-attack can be employed. These persons are members of armed forces of State, members of organized armed groups, civilians taking direct part in hostilities and participants in *levée en masse* (in cases of IAC).[324] The detailed analysis of every aspect and condition of every particular group goes beyond the

[320] Art. 51 (2) of AP I; Art. 13 (2) of AP II.
[321] Art. 52 (1) of AP I.
[322] Art. 50 (1) of AP I.
[323] SCHMITT: *Tallinn Manual*…, p. 104.
[324] SCHMITT: *Tallinn Manual*…, p. 115.

scope and extent of present work. Only the main principles and issues which are cyber related will be addressed.

Members of armed forces of party of conflict are members of "*all organized armed forces, groups and units, which are under a command responsible to that party for the conduct of its subordinates.*"[325] Therefore the members of cyber military units are combatants and lawful target of attack and as military objective can be attacked at any time of armed conflict.[326] This is of course subject to exceptions of medical personnel, clerics[327] and *hors de combat*.[328]

Members of organized armed groups are lawful target as well. The controversy remains when person qualifies as member of group. Tallinn Manual does not provide answer due to the lack of consensus among authors.[329] One opinion claims that members of such groups can be attacked at any time[330] however more compelling argumentation is provided by ICRC which distinguishes between different types of groups. In cases of groups where is no act of integration, the membership is determined by continuous combat function. That means that a particular individual must continuously carry out cyber-attacks with likelihood to cause injury, damage or destruction of property to be targeted. Cyber recruiters, trainers or propagandists would not qualify and would remain civilians.[331]

Third group, civilians taking direct part in hostilities, represents one of the most rapidly developing group in cyber warfare. It only takes computer, software and connection to internet to conduct cyber operations.[332] The direct participation of civilians is quite complicated itself. It shall be noted that three elements must be fulfilled. Threshold of harm, direct causation and belligerent nexus. In order to reach said threshold, the act is "*likely to adversely affect the military operations or military capacity of a party to an armed conflict or, alternatively, to inflict death, injury, or destruction on persons and objects protected against direct attack*."[333] Therefore a cyber operation which affects enemy reaches threshold when has effect on it military performance. Otherwise a physical consequence is necessary.

---

[325] Art. 43(1) of AP I.
[326] PILLOUD: Commentary on the Additional Protocols…, para. 2017.
[327] Art. 43(2) of AP I.
[328] Art. 41(1) of AP I.
[329] SCHMITT: *Tallinn Manual*…, p. 117.
[330] PILLOUD: Commentary on the Additional Protocols…, para. 4789.
[331] MELZER: Interpretative Guidance…, p. 33-35.
[332] BARNETT, W Rodger. A different Kettle of Fish: Computer Network Attack. *International Law Studies*, 2002, Vol. 76, p. 22.
[333] MELZER: Interpretative Guidance…, p. 46.

Last case is the case of *levée en masse* what can be described as "*mass networked mobilization that emerges from cyber-space with a direct impact on physical reality*."[334] The participants are an object of attack as long as they participate in it.

In addition to abovementioned manifestation of principle of distinction, when conducting cyber-attack, an attacker must comply with principle of proportionality. Principle of proportionality manifests itself through Article 51 (5) (b) which states that indiscriminate attacks are prohibited. These are those that "*may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.* "[335] The attacker must make an assessment of proportionality of attack before the attack itself. This is no easy task, which is even more complicated in context of cyber operations, since flaws of final evaluation "*are significantly greater than those usually associated with kinetic attacks in the sense that there may not be analytic or experiential basis for estimating uncertainties at all*."[336]

The requirement of principle of proportionality itself seems clear. Incidental loss cannot be excessive to anticipated military advantage. Incidental loss includes direct effect as well as indirect effect[337] while includes loss of functionality without destruction as well.[338] On the other hand the military advantage must be concrete and direct. It means that the benefit of attack must be real and quantifiable[339] not hardly perceptible or uncertain in future.[340] It shall be understood as consequence which *"directly enhances friendly military operations or hinders those of enemy*"[341] Both element must be considered in their mutual effect. The incidental damage must not be excessive. That means that even huge damage is permissible if compensated with huge military advantage. The assessment should be question of common sense and good faith[342] and it is objective test which takes into account *"whether a reasonably well-informed person in the circumstances of the actual perpetrator, making reasonable use of the information available to him or her, could have expected excessive civilian casualties to*

[334] CRONIN, Audrey Kurth. Cyber -Mobilization: The New Levée en Masse, *Parameters*, 2006, Vol. 36, No. 2, p. 77.
[335] Art. 51 (5) b) of AP I.
[336] OWENS, DAM, LIN: Technology, Policy, Law…, p. 262.
[337] SCHMITT: Tallinn Manual…, p. 160.
[338] ROSCINI: *Cyber Operations*…, p. 223
[339] SCHMITT: *Tallinn Manual*…, p. 161.
[340] PILLOUD: Commentary on the Additional Protocols…, para. 2209.
[341] *HPCR commentary on the HPCR manual on international law applicable to air and missile warfare*. Cambridge: Program on Humanitarian Policy and Conflict Research at Harvard University, 2010, p. 36. Available at <http://www.ihlresearch.org/amw/manual/>.
[342] PILLOUD: Commentary on the Additional Protocols…, para. 2208.

result from the attack."[343] Therefore the less information one has when assessing the proportionality, the higher probability of unproportioned attack exists.

Moreover it is prohibited to use perfidy in order to kill or injure an adversary.[344] Not every action which conceals identity of attacker is perfidious. Camouflage, decoys or misinformation are lawful ruses of war.[345] Therefore anonymization of IP address, honeynets containing false information are allowed. Perfidy is special in a sense that the deception is insufficient and the cyber-attack must invite the confidence that person is entitled to receive protection under the law. This can be achieved through feigning a status of civilians, civilian objects, UN personnel, medical personnel or persons who are hors de combat.[346] For example if one sends an email appearing to be from UN, while containing a code which would result in injury or death, such conduct would constitute perfidy.[347]

6.2.4 Cyber-attacks against objects

Next is the issue of cyber-attacks against objects. As was stated it is forbidden to attack civilian objects. The civilian objects are defined negatively as those which are not military objectives.[348] Generally speaking, "*military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage*."[349] Apart of objects which are traditionally military objectives and might be attacked by cyber means, these might consist of computers, networks or cyber infrastructure.[350] Additionally authors of Tallinn Manual did not found consensus whether data per se can be military objective. Since object is considered to be something visible and tangible, majority of them agreed that data cannot be considered as object. However they agreed that an operation targeting data can be considered an attack if it affects the

[343] ICTY, Prosecutor v. Stanislav Galić, Judgement and Opinion, Trial Chamber I, Case No. IT-98-29-T, 5. December 2003, para. 58.
[344] Art. 37(1) of AP I.
[345] Art. 37 (2) of AP I.
[346] SCHMITT: *Tallinn Manual*…, p. 182.
[347] ROSCINI: *Cyber Operations*…, p. 218.
[348] Art. 52(1) of AP I.
[349] Art. 52(2) of AP I.
[350] SCHMITT: *Tallinn Manual*…, p. 125.

functionality of particular system.[351] Then however the object is not the data, but the system itself. On the other hand minority considered even data as an object, and majority accepted it as *de lege ferenda* position.[352] Accepting this, it seems that data are not considered as an object and therefore cyber operation which affects data without manifestation in physical realm or without manipulation of software, are not subject of principle of distinction. Considering the reliance of modern societies on data, its importance and potential menacing effect of its lost, this approach is unlikely withstand in increasingly cyber-dependent States.[353]

The term of military objective has legal character. The first necessary element is that the object must make effective contribution to military action by its nature, location, use or purpose. Nature refers to inherent character to the object, designed to be directly used by armed forces,[354] for example special military software. As to the criterion of location, military objective would be a reservoir from which water is released via cyber-attack, into area where military operations are expected.[355] The criterion of purpose is used in cases when object is not in use but it is clear that the purpose of the object is to contribute to military action.

The constitution of object to be a military objective by its use will be very common in cyberspace. Virtually all technology and infrastructure is used by civilian population as well as by military, forming so called dual-use objects.[356] Military codes would therefore travel through dual-use cyber infrastructure, such as servers, routers, cables, satellites and software, contributing to military action and making them military objective.[357] These objects could beh can be attacked for the period of time of their use by military.[358] What must be considered in such cases, is principle of proportionality. The principle of proportionality of course applies to attacks against objects as well. The analysis is however identical as was presented above and therefore it seems unnecessary to restate it again. The abovementioned objects must make an effective contribution to military action for the party attacked.

[351] SCHMITT: *Tallinn Manual…*, p. 127.
[352] Ibid.
[353] SCHMITT, Michael. Rewired warfare: rethinking the law of cyber attack. *International Review of the Red Cross: Scope of the law in armed conflict*, 2014, Vo. 96, No. 893, p. 204.
[354] PILLOUD: Commentary on the Additional Protocols…, para. 2020.
[355] SCHMITT: *Tallinn Manual…*, p. 128.
[356] ROSCINI: *Cyber Operations…*, p. 186.
[357] GEISS, Robin, LAHMAN, Henning. Cyber warfare: applying the principle of distinction in an interconnected space. *Israel Law Review*, 2012, Vol. 45, No. 3, p. 386.
[358] PILLOUD: Commentary on the Additional Protocols…, para. 2023.

Moreover the destruction, capture or neutralization of the object must provide definite military advantage. The wording includes neutralization is very suitable for cyber operations which only incapacitate particular object, denying its use.[359] The military advantage must be definite, what means that attacks with hypothetical, potential, indeterminate advantages are prohibited and sufficient information must be available to make an assessment.[360] Also the military advantage must exist in the circumstances at the time, what implies that the qualification of object as military objective changes trough time and therefore the military advantage cannot be determined in a way, that it will provide military advantage in undetermined future.

The problem with assessment of military objective in cyberspace and potential military advantage provided is huge. Virtually every cyber infrastructure could be considered a military objective, even if the use by military would be minimal. Calculating military advantage and proportionality in cyberspace seems more like a gamble than a proper analysis. With huge civilian reliance on these dual-use objects, the most appropriate solution would be exclusion of certain objects which neutralization would "*result in significant civilian impact that would outweigh the military benefits*."[361] The protection of this infrastructure with "essential civilian functions" which would stem from existing protection of certain objects excluded from attacks, would necessarily require adoption of new treaty or new additional protocol to Geneva Conventions.[362]

Lastly certain objects are excluded from possibility of attack at all. This prohibition applies to cyber-attacks as well and protects variety of objects, such as cultural objects and places of worship,[363] objects indispensable to the survival of population,[364] works and installations containing dangerous forces,[365] non-defended localities,[366] and demilitarized zones.[367]

---

[359] ROSCINI: *Cyber Operations*…, p. 188.
[360] PILLOUD: Commentary on the Additional Protocols…, para. 2024
[361] GEISS, Robin, LAHMAN, Henning. Cyber warfare: applying the principle of distinction in an interconnected space. *Israel Law Review*, 2012, Vol. 45, No. 3, p. 391.
[362] SCHMITT, Michael. Rewired warfare: rethinking the law of cyber attack. *International Review of the Red Cross: Scope of the law in armed conflict*, 2014, Vo. 96, No. 893, p. 205.
[363] Art. 53 of AP I.
[364] Art. 54 of AP I.
[365] Art. 56 of AP I.
[366] Art. 59 of AP I.
[367] Art. 60 of AP I.

7 Conclusion

The goal of the thesis was to observe, analyse, and describe the use of *ius ad bellum* and *ius in bello* in cyberspace, or better said, to certain cyber operations. The thesis followed structure laid out in introduction. It seems appropriate to follow said structure in conclusion as well.

The first issue which needed to be established was the applicability of relevant legal provisions to cyberspace. As was shown there is no relevant legal instrument which specifically addresses cyber operations. Therefore is necessary to interpret law, if possible, in a way that subsumes cyber operations. UN Charter works with notion of force and armed attack, both flexible enough to include cyber operations under its normative effect. Law of armed conflict is applicable as well. Thanks to Martens Clause, which works as safeguard for newly developed weapons, cyber operations must obey law of armed conflicts. If is cyber operation used as weapon, there is no reason not to treat it as one.

Secondly, the focus was shifted to *ius ad bellum* and cyber operations. The core issue of this part is the notion of armed force. The prohibition does not preclude any kind of force, e.g. economic or political means of force, but only armed force. It is also matter of fact that is irrelevant what weapons are used to execute armed force. It was shown that the approach, which is most commonly used and most suitable is effect based approach. It follows that cyber operation must be considered by its effects. If the effect is of a nature, which would render traditional means as use of force, cyber operation must be by analogy consider equally. It is therefore concluded that cyber operations with severe physical effect that results in injury, damage or destruction is use of force. On the other hand there is no definitive agreement on cyber operations that disrupt functionality of national critical infrastructure. However it seems that most States consider cyber operation against its critical infrastructure to be use of force and legal analysis suggest, that considering the dependency of modern society on these networks and the effect of their disruption, cyber operations severely disrupting NCI shall be considered as use of force.

It was also established that possibility of indirect force, when State is adequately involved with armed groups exists. Therefore a State which provides substantial support to a group, which uses cyber force would be responsible for this violation of UN Charter.

Next issue regarding *ius ad bellum* was right to self-defence, which represent inherent right of States and forms the most important exemption from prohibition of use of force. Self-defence can be carried out only in cases of armed attack. Armed attack is a form of use of force, which achieved sufficient effect and scale. This can be accomplished by accumulation of smaller incidents as well. It is hard to establish the threshold of severity as there are no criteria other that effects and scale. Every cyber operation would have to be considered on case by case basis. Moreover, it was shown that international law allows anticipatory self-defence but forbids pre-emptive self-defence. In cases of imminent verifiable cyber-attacks a State can act self-defensively before actual cyber-attack takes place. The action in self-defence must comply with requirement of necessity, proportionality and immediacy. It is not necessary that a reaction would be conducted via cyberspace as well. There is no imperative on same means of self-defence. Lastly it was observed that self-defence can be conducted against a non-state actor. It was established that unwilling or unable test is accepted approach. Therefore State can act in self-defence against non-state actor if state where this actor resides cannot or does not want to stop an armed force against a victim State.

Thirdly, after evaluation of *ius ad bellum*, focus was shifted to cyber operations *and ius in bello.* In the beginning of analysis, the observation was made in what cases law of armed conflict applies. The biggest difference consist in qualification of armed conflict as international or non-international. The LOAC applies to cyber operations when they are executed in already existing IAC. It was concluded that only operations directed against opposite party and with sufficient severity are subjected to LOAC. The question of whether cyber operation can start on its own IAC was answered positively. IAC occurs when there are hostilities between States. Therefore cyber operation with kinetic effect between states would start an IAC. Similar conclusion was made in relation to non-kinetic attacks against NCI. There seems to be no threshold in question of start of IAC. On the other hand, States have tendency not to consider occasional incidents with minimal force as hostilities.

The cases of NIAC governed by Common Article 3 require protracted armed violence, with organized armed group involved. Organizational requirement would be hardly fulfilled in cases of network groups that never meet physically, don’t have rigid chain of command and often do not know identities of other members. Armed group is defined by its capability to conduct cyber-attack. Requirement of protracted violence sets threshold which must be reached for LOAC to govern the situation. Threshold is set relatively high and seems unlikely

that will be achieved only by cyber-operation. There is no consensus on issue of non-kinetic attacks, however it is submitted that even these can be considered as protracted violence if they are very severe and take long time. The situations covered by AP II cannot be triggered solely by cyber operations, as control over territory is a condition for application.

Lastly the conduct of hostilities regarding cyber operations was addressed. Focus was given to legality of cyber operations in armed conflict. As conclusion, cyber operations form very wide and diverse group of means and methods of warfare. Some can be definitely be considered as illegal and some not. There is no general rule which would define the legality of whole group. Conclusions must be therefore made on case by case basis.

Subsequently issue of conduct of hostilities, particularly of cyber-attacks was addressed. Cyber-attacks were defined as operations which are capable to cause death, injury, damage, or destruction. In regard to non-physical attacks, it was shown that scholars attempt to conform interpretation of violence to include these types of attack, either through concept of neutralization or referring to dependency on technologies. Absolute confirmation cannot be made as State practice is practically non-existent. Furthermore attack against persons and objects were addressed. Principles of necessity and proportionality were examined. They were set to context of cyber-attacks. The particular groups of people which may be attacked by cyber-attack were defined and described, as well as cases in which even civilians can be subject of attack. In relation to attacks against objects the concept of military objective was studied.

Cyber-attacks can attack only military objectives as any other attack. It has been established that majority of opinions does not consider data to be objects and therefore their destruction would not be considered as attack. Since most of cyber infrastructure is dual-use, virtually every attack would have to be subjected to evaluation of military advantage and incidental loss. Only if loss is not disproportionate to military advantage cyber-attack can be conducted. Moreover cyber-attacks are prohibited against certain objects under any circumstances. In order to sufficiently guarantee protection of civilians laid by LOAC, it seems appropriate, *de lege ferenda*, to broaden this prohibition to certain infrastructure, essential for civilian population.

8 Bibliography

Articles

1) BARNETT, W Rodger. A different Kettle of Fish: Computer Network Attack. International Law Studies, 2002, Vol. 76, p. 21 – 33.
2) BROWN, Davis. A proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict. Harvard International Law Journal, 2006, Vol. 47, No. 1, p. 182 – 221.
3) CRONIN, Audrey Kurth. Cyber -Mobilization: The New Levée en Masse, Parameters, 2006, Vol. 36, No. 2, p. 77 – 87.
4) D'AMATO, Anthony. International Law, Cybernetics and Cyberspace. International Law Studies, 2002, Vol. 76, p. 59 – 71.
5) DEEKS, Ashley. The Geography of Cyber Conflict: Through a Glass Darkly. International Law Studies, 2013, Vol. 89, p. 1 – 20.
6) DEEKS, S. Ashley. „Unwilling or Unable": Toward a Normative Framework for Extraterritorial Self-Defense. Virginia Journal of International Law, 2012, Vol. 52, No. 3, p. 483 – 550.
7) DINSTEIN, Yoram. Computer Network Attacks and Self-Defense. International Law Studies, 2002, Vol. 76, p. 99 – 119.
8) DOSWALD-BECK, Louise. Some Thoughts on Computer Network Attack and the International Law of Armed Conflict. International Law Studies, 2002, Vol. 76, p. 163 – 185.
9) DROEGE, Cordula. Get off my Cloud: Cyber warfare, international humanitarian law, and the protection of civilians. *International Review of the Red Cross: Humanitarian Debate: Law, policy, action*, 2012, Vol. 94, No. 886, p. 533 – 578.
10) DÖRMANN, Knut. Applicability of the Additional Protocols to Computer Network Attacks. ICRC, 2004, 12 p. Available at <https://www.icrc.org/eng/resources/documents/misc/68lg92.htm>.
11) FERRARO, Tristan. Determining the beginning and the end of an occupation under international humanitarian law. International Review of the Red Cross, 2012 Vol.94, No. 885, p. 133 – 163.

12) GEISS, Robin, LAHMAN, Henning. Cyber warfare: applying the principle of distinction in an interconnected space. *Israel Law Review*, 2012, Vol. 45, No. 3, p. 381 – 399.
13) GEISS, Robin. Cyber Warfare: Implications for Non-international Armed Conflicts. International Law Studies, 2013, Vol. 89, p. 627 – 645.
14) GILL, Terry, DUCHEINE, Paul. Anticipatory Self-Defence in the Cyber Context. *International Law Studies*, 2013, Vol. 89, No. 438, p. 438 – 471.
15) HAKIMI, Monica. Defensive Force against Non-State Actors: The State of Play. *International Law Studies*, 2015, Vol. 91, p. 1 – 31.
16) HENKIN, Louis. The Reports of the Death of Article 2(4) Are Greatly Exaggerated. The American Journal of International Law, 1971, Vol. 65, Issue 3, p. 544 – 548
17) HOISINGTON, Matthew. Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense. Boston College International and Comparative Law Review, Vol.32, Issue 2, p. 439 – 454.
18) HOLLIS, B. Duncan. Why States Need an International Law for Information Operations. Lewis & Clark Law Review, 2007, Vol. 11, p. 1023 – 1061
19) JENSEN, Eric. Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense. Stanford Journal of International Law, 2002, Vol. 38, p. 207 – 240.
20) JOYNER, Christopher, LOTRIONTE, Catherine. Information Warfare as International Coercion: Elements of a Legal Framework. European Journal of International Law, 2001, Vol. 12, No. 5, p. 825 – 865.
21) KAHGAN, Carin. Jus Cogens and the Inherent Right to Self-Defense. ILSA Journal of International & Comparative Law, 1997, Vol. 3, p. 767–827.
22) KILOVATY, Ido. Rethinking the Prohibition on the Use of Force in the Light of Economic Cyber Warfare: Towards a Broader Scope of Article 2 (4) of the UN Charter. *Journal of Law and Cyber Warfare*, 2015, Vol. 4, No. 3, p. 210 – 244.
23) KODAR, Erki. Applying the law of Armed Conflict to Cyber Attacks: From the Martens Clause to Additional Protocol I. ENDC Proceedings, 2012, Vol 15, p. 107 – 132.
24) KREß, Claus. Some Reflection on the International Legal Framework Governing Transnational Armed Conflicts. Journal of Conflict & Security Law, 2010, Vol. 15, No. 2, p. 245 – 274.
25) LIN, S. Herbert. Offensive Cyber Operations and the Use of Force. Journal of National Security Law & Policy, 2010, Vol. 4, p. 63 – 86.

26) O`CONNEL, Mary Ellen. Cyber Security without Cyber War. Journal of Conflict & Security Law, 2012, Vol. 17, No. 2, p. 187 – 209.
27) REICHMANN, Felix. The Pennsylvania Rifle: A Social Interpretation of Changing Military Techniques. The Pennsylvania Magazine of History and Biography, 1945, Vol. 69, Issue 1, p. 3 – 14.
28) REINOLD, Theresa. State Weakness, Irregular Warfare, and the Right to Self-Defense Post-9/11. *American Journal of International Law*, 2001, Vol. 105, No. 2, p. 244 – 286.
29) SCHMITT, N Michael. "Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law. Virginia Journal of International Law, 2014 Vol. 54, p. 698-732.
30) SCHMITT, Michael, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. Columbia Journal of Transnational Law, 1999, Vol. 37, p. 885–937.
31) SCHMITT, Michael. International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed. Harvard International Law Journal, 2012, Vol. 54, p. 13 – 37.
32) SCHMITT, N. Michael. Wired Warfare: Computer network attack and jus in bello. International Review of the Red Cross, 2002, Vol. 84, No. 846, p. 365 – 399.
33) SCHMITT, Michael. Rewired warfare: rethinking the law of cyber attack. *International Review of the Red Cross: Scope of the law in armed conflict*, 2014, Vo. 96, No. 893, p. 189 – 206.
34) SILVER, B. Daniel. Computer Network Attack as a Use of Force under Article 2(4). International Law Studies, 2002, Vol. 76, p.73 – 97.
35) WAXMAN, Matthew. Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions. International Law Studies, 2013, Vol. 89, p. 109 – 122.

Books

36) BROWNLIE, Ian. *International Law and the Use of Force by States*. Oxford: Claredon Press, 1963. 532 p.
37) CLAUSEWITZ, Carl von, translated by GRAHAM, J.J.. On War. Vol. I. London: Routledge, 2005. 319 p.

38) CONSTANTINOU, Avra. *The right of self-defence under customary international law and Art. 51 of the United Nations Charter*. Athens: Sakkoulas, 2000. 225 p.

39) DINSTEIN, Yoram. *War, Aggression and Self-Defence*, 5. edition. New York: Cambridge University Press, 2012. 375 p.

40) GRAY, Christine. International Law and the Use of Force. 3. edition. New York: Oxford University Press, 2008. 455 p.

41) KELSEN, Hans. Collective security under international law. New Jersey: The Lawbook Exchange, 2001. 275 p.

42) LANGNER, Ralph. To kill a centrifuge. A Technical Analysis of what Stuxnet's Creators Tried to Achieve. The Langner Group, 2013. 36 p. Available at < http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf>.

43) MELZER, Nils. Interpretative Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law. ICRC, 2009. 85 p.

44) MELZER, Nils. Cyberwarfare and International Law. UNIDIR Resources, 2011, 37 p. Available at <http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf>.

45) ONDŘEJ, Jan a kol. Mezinárodní humanitární právo. 1. vydání. Praha: C. H. Beck, 2010. 559 p.

46) OWENS, William, KENNETH, Dam, LIN, Herbert. Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattacks Capabilities. Washington DC: National Academy Press. 367 p.

47) ROSCINI, Marco. Cyber Operations and the Use of Force in International Law. Oxford: Oxford University Press, 2014. 307 p.

48) SASSÒLI, Marco, BOUVIER, Antione, QUINTIN Anne. *How does law protect in war*? Vol I. 3. ed. ICRC, 2011. 400 p. Available at: <https://www.icrc.org/eng/assets/files/publications/icrc-0739-part-i.pdf>.

49) SHARP, Walter. Cyberspace and the use of force. Falls Church: Aegis Research Corp., 1999. 234 p.

50) SCHMITT, Michael (ed). Tallinn manual on the international law applicable to cyber warfare: prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence. Cambridge: Cambridge University Press, 2013. 282 p.

51) SIVAKUMARAN, Sandesh. *The Law of Non-International Armed Conflict*. 1. ed. Oxford: Oxford University Press, 2012. 657 p.

52) TIKK, Eneken, KASKA Kadri, VIHUL, Liis. International Cyber Incidents: legal considerations. Tallinn: Cooperative Cyber Defence of Excellence (CCD COE), 2010. 130 p.

Commentaries

53) CLAPHAM, Andrew, GAETA, Paola, SASSÒLI, Marco (eds). The 1949 Geneva Conventions: A Commentary 1. ed. Oxford: Oxford University Press, 2015. 1651 p.

54) HENCKAERTS, Jean-Marie, DOSWALD-Beck, Lousie. Customary International Humanitarian Law – Vol. I: Rules. Cambridge: Cambridge University Press, 2005. 623 p.

55) HPCR commentary on the HPCR manual on international law applicable to air and missile warfare. Cambridge: Program on Humanitarian Policy and Conflict Research at Harvard University, 2010. 348 p. Available at <http://www.ihlresearch.org/amw/manual/>.

56) PILLOUD, Claude, SANDOZ, Yves, SWINARSKI, Christophe, ZIMMERMANN, Bruno (ed). Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949. Norwell: Kluwer Academic Publishers, 1987. 1625 p.

57) PICTET, Jean (ed). The Geneva Conventions of 12 August 1949 Commentary - Vol. IV. Geneva: International Committee of Red Cross, 1958, 660 p.

58) SIMMA, Bruno (ed). The Charter of the United Nations A Commentary - Vol. I. 2. edition. Oxford: Oxford University Press, 2010. 895 p.

Collaborative papers

59) ARIMATSU, Louise, Classifying cyber warfare. In TSAGOURIAS, Nicholas, BUCHAN, Rusell (ed). In *Research Handbook on International Law and Cyberspace*. Northampton: Edward Elgar Publishing, 2015, p. 326 – 342.

60) DÖRR, Oliver. Use of Force, Prohibition of. In WOLFRUM, Rüdiger (ed). *The Max Planck Encyclopedia of Public International Law – Vol. X.* New York: Oxford University Press, 2012, p. 608 – 620.

61) KLEFFNER, K Jann. Scope of Application of International Humanitarian Law. In FLECK, Dieter. The Handbook of International Humanitarian Law. Oxford: Oxford University Press, 2013, p. 45 – 78.

62) MILANOVIC, Marko and HADZI-VIDANOVIC, Vidan. A Taxonomy of Armed Conflict. In WHITE, Nigel, HENDERSON, Christian (ed). *Research handbook on international conflict and security law*. Northapton: Edward Elgar Publishing, 2013. p. 256 – 314. Available at: <http://ssrn.com/abstract=1988915>.

63) SCHMITT, Michael. Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts. In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*. Washington: The National Academies Press, 2010, p. 151 – 177.

64) WAGNER, Markus. Armed Attack. In WOLFRUM, Rüdiger (ed). *The Max Planck Encyclopedia of Public International Law – Vol. VII*. New York: Oxford University Press, 2012, p.741 – 749.

65) WOLTAG, Johann-Christoph. Cyber Warfare. In WOLFRUM, Rüdiger (ed). *The Max Planck Encyclopedia of Public International Law – Vol. II*. New York: Oxford University Press, 2012, p. 988 – 994.

66) ZEMANEK, Karl. Armed Attack. In WOLFRUM, Rüdiger (ed). *The Max Planck Encyclopedia of Public International Law – Vol. I*. New York: Oxford University Press, 2012, p. 595 – 606.

67) ZIOLKOWSKI, Katharina, Ius ad bellum in Cyberspace – Some Thoughts on the "Schmitt-Criteria" for Use of Force. In CZOSSECK, C., OTTIS, R., ZIOLKOWSKI, K. (ed). *4th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE Publications, 2012, p. 295 – 317.

International Treaties

68) Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, 12 August 1949.

69) Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, 12 August 1949.

70) Convention (III) relative to the Treatment of Prisoners of War, 12 August 1949.

71) Convention (IV) relative to the Protection of Civilian Persons in Time of War, 12 August 1949.

72) 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.

73) 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.

74) 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.
75) 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, 29 July 1899.
76) Convention (III) relative to the Opening of Hostilities, 18 October 1907.
77) Convention (VI) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land, 18 October 1907.
78) Convention in the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction, 13 January 1993.
79) Protocol (II) on Prohibition or Restrictions on the Use of Mines, Booby-Traps and Other Devices, 10 October 1980.
80) General Treaty for the Renunciation of War as an Instrument of National Policy, 27 August 1928. LNTS Vol. XCIV, No. 2137.
81) The Charter of the United Nations
82) The Covenant of the League of Nations, 28 June 1919.
83) Vienna Convention on the Law of Treaties, 23 May 1969.

Judicial decisions

International Court of Justice

84) Application of the Convention of the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, I.C.J. Reports 2007.
85) Armed Activities on the Territory of the Congo (Democratic Republic of Congo v. Uganda), Judgment, I.C.J. Reports 2005.
86) Corfu Channel case, Judgment of April 9th 1949, I.C.J. Reports 1949.
87) Dispute regarding Navigational and Related Rights (Costa Rica v. Nicaragua), Judgment, I.C.J. Reports 2009.
88) Gabčíkovo-Nagymaros Project (Hungary/Slovakia), Judgment, I.C.J. Reports, 1997.
89) Land and Maritime Boundary between Cameroon and Nigeria (Cameroon v. Nigeria: Equatorial Guinea Intervening), Judgment, I. C. J. Reports 2002.

90) Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, I.C.J. Reports 2004.
91) Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (1970), Advisory Opinion, I.C.J. Reports 1971.
92) Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996.
93) Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), Merits, I.C.J. Reports 1986.
94) Oil Platforms (Islamic Republic of Iran v. United States of America), Judgment, I.C.J. Reports 2003.
95) Separate opinion of Judge Simma, Armed Activities on the Territory of the Congo (Democratic Republic of Congo v. Uganda), Judgments, I.C.J. Reports 2005.
96) Separate opinion of Judge Kooijmans, Armed Activities on the Territory of the Congo (Democratic Republic of Congo v. Uganda), Judgments, I.C.J. Reports 2005
97) United States Diplomatic and Consular Staff in Tehran, Judgment, I.C.J. Reports 1980.

International Criminal Tribunal for Rwanda

98) ICTR, The Prosecutor v. Jean-Paul Akayesu, Judgment, Case No. ICTR-96-4, 2 September 1998

International Criminal Tribunal for Yugoslavia

99) ICTY, Prosecutor v. Ljune Boškoski, Johan Tarčulovski, Judgment, Trial Chamber II, Case No. IT-04-82-T, 10. July 2008.
100) ICTY, Prosecutor v. Zejnil Delalić, Zdravko Mucić also known as “Pavo”, Hazim Delić, Esad Ladžo also known as “Zenga”, Judgment of Trial Chamber, Case No. IT-96-21-T, 16. November 1998.
101) ICTY, Prosecutor v. Stanislav Galić, Judgement and Opinion, Trial Chamber I, Case No. IT-98-29-T, 5. December 2003.
102) ICTY, Prosecutor v. Ramush Haradinaj et al., Judgment, Trial Chamber I, Case No. IT-04-84-T, 3. April 2008.

103) ICTY, Prosecutor v. Sefer Halilović, Judgement, Trial Chamber I, Case No. IT-01-48-T, 16. November 2005.

104) ICTY, Prosecutor v. Enver Hadžihasanović and Akmir Kubura, Judgment, Trial Chamber, Case No. IT-01-47-T, 15. March 2006.

105) ICTY, Prosecutor v. Dario Korcić and Mario Čerkez, Judgment, Appeals Chamber, Case No. IT-95-14/2-A, 17. December 2004.

106) ICTY, The Prosecutor v. Dragoljub Kunacarac, Radomir Kovac and Zoran Vukovic, Judgment, IT-96-23 & IT-96-23/1-A, 12 June 2002.

107) ICTY, Prosecutor v. Limaj et al., Judgment, Trial Chamber I, Case No. IT-03-66-T, 30. November 2005.

108) ICTY, Prosecutor v. Milan Martić, Judgment, Trial Chamber I, Case No. IT-95-11-T, 12. June 2007.

109) ICTY, Prosecutor v. Slobodan Milosević, Decision on Prosecution's Motion under Rule 73 (A) for a Ruling on the competence of the Amici Curiae to present a Motion for Judgment of Acquittal under Rule 98 bis, Trial Chamber, Case No. IT-02-54-T, 5. February 2004.

110) ICTY, Prosecutor v. Mile Mrkšić et al., Judgment, Trial Chamber II, Case No. IT-95-13/1-T, 27. September 2007.

111) ICTY, Prosecutor v. Mladen Naletilic, aka "TUTA" and Vinko Martinovic, aka "Štela", Trial Judgment, Case No. IT-98-34-T, 31. March 2003.

112) ICTY, The Prosecutor v. Duško Tadić, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, IT-94-1-A, 2 October 1995.

113) ICTY, Prosecutor v. Duško Tadić, Judgment of the Appeals Chamber, Case No. IT-94-1-A, 15. July 1999.

Miscellaneous

114) A more secure world: our shared responsibility, Report of the High-Level Panel on Threats, Challenges and Change. UN Doc. A/59/565, 2. December 2004.

115) Advisory Council on International Affairs, Advisory Committee on Issues of Public International Law. *Cyber Warfare*. No. 77, AIV/No. 22, CAVV, 2011, 38 p. Available at: <http://aiv-advies.nl/download/da5c7827-87f5-451a-a7fe-0aacb8d302c3.pdf>.

116) Creation of a global culture of cybersecurity and the protection of critical information infrastructure, GA Resolution, A/RES/58/199, 30. January 2004.

117) Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations. General Assembly Resolution, Res. 2625(XXV), UN Doc. A/RES/25/2625, October 24 1970.

118) Draft articles on Responsibility of States for Internationally Wrongful Acts with commentaries, Yearbook of the International Law Commission, Vol. II, Part Two, A/CN.4/SER.A/2001Add.1 (Part 2), 2001.

119) Group of Governmental Experts on Developments in the Field of information and Telecommunications in the Context of International Security. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc A/68/98, 24. June 2013, 13 p. Available at <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N13/371/66/PDF/N1337166.pdf?OpenElement>.

120) ICRC. Treaties and State Parties to such Treaties. Available at <https://www.icrc.org/applic/ihl/ihl.nsf/vwTreatiesByTopics.xsp>.

121) In Larger Freedom: Towards Development, Security and Human Rights for All, Report of the Secretary-General. UN Doc. A/59/2005, 21. March 2005.

122) International Committee of the Red Cross. International Humanitarian Law and the challenges of contemporary armed conflicts, 31st International Conference of the Red Cross and Red Crescent. Doc 31IC/11/5.1.2, October 2011, 53 p. Available at <http://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>.

123) Letter dated 7 October 2001 from the Permanent Representative of the United States of America to the United Nations addressed to the President of the Security Council. UN Doc. S/2001/946, 7. October 2001. Available at <http://www.hamamoto.law.kyoto-u.ac.jp/kogi/2005kiko/s-2001-946e.pdf>.

124) Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, UN Doc. A/66/359, 14. September 2011. Available at <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N11/496/56/PDF/N1149656.pdf?OpenElement>.

125) Letter from Mr. Daniel Webster to Lord Ashburton, Washington, 27. July 1842, Enclosure 1 – Extract from note of April 24, 1841. Available at: <http://avalon.law.yale.edu/19th_century/br-1842d.asp#web1>.

126) The National Security Strategy of the United States of America, September 2002, 31 p. Available at, >http://www.state.gov/documents/organization/63562.pdf>.

127) Reports of the International Law Commission on the second part of its seventeenth session and on its eighteenth session, Document A/6309/Rev.l, in Yearbook of the International Law Commission, 1966, Vol. II, A/CN.4/SER.A/1966/Add.l.

128) Resolution 1368 (2001) Adopted by Security Council at its 4370th meeting on 12 September 2001, UN Doc. S/RES/1368 (2001), 12. September 2001.

129) Resolution 1373 (2001) Adopted by the Security Council at its 4385th meeting, on 28 September 2001, UN Doc. S/RES/1373 (2001), 28. September 2001.

130) Veřejnoprávní smlouva o zajištění činnosti Národního CERT a o spolupráci v oblasti kybernetické bezpečnosti mezi Českou Republikou – Národním bezpečnostním úřadem a CZ.NIC. z.s.p.o., 18. January 2015. Available at <https://www.csirt.cz/files/nic/doc/NBU-Smlouva-narodni-cert-201512.pdf>.

Website articles

131) ALVAREZ, Joshua. Stuxnet: The world's first cyber weapon [online]. stanford.edu, 3. February 2015 [cit. 26. January 2016]. Available at <http://cisac.fsi.stanford.edu/news/stuxnet>.

132) FLEMING, Ryan. Bits before bombs: How Stuxnet crippled Iran's nuclear dreams [online]. digitaltrends.com, 2. December 2010 [cit. 26. January 2016]. Available at <http://www.digitaltrends.com/computing/bits-before-bombs-how-stuxnet-crippled-irans-nuclear-dreams/>.

133) KHANDELWAL, Swati. *How Spy Agencies Hacked into Israeli Military Drones to Collect Live Video Feeds* [online]. thehackernews.com, 31. January 2016 [cit. 5. February 2016]. Available at <http://thehackernews.com/2016/01/drones-hacking.html>.

134) KOH, Harold. Remarks: USCYBERCOM Inter-Agency Legal Conference [online]. state.gov, 18. September 2012 [cited 28.11.2015]. Available at <http://www.state.gov/s/l/releases/remarks/197924.htm>.

135) PAGANINI, Pierluigi. Hackers cause power outage with BlackEnergy malware in Ukraine. Is it an Information warfare act? [online]. securityaffairs.co, 5. January 2016 [cit. 25. January 2016]. Available at <http://securityaffairs.co/wordpress/43321/hacking/ukraine-attack-caused-power-outage.html>.

136) PAGANINI, Pierluigi. Ukraine blames Russia of cyber attacks against Boryspil airport [online]. securityaffairs.co, 18. January 2016 [cit. 25. January 2016].Available at <http://securityaffairs.co/wordpress/43703/hacking/cyber-attack-boryspil-airport.html>.

137) PELLERIN, Cheryl. DOD releases first Strategy for Operating in Cyberspace [online]. defense.gov, 14 July 2011 [cit. 26.01.2016]. Available at <http://archive.defense.gov/news/newsarticle.aspx?id=64686>.

138) ZETTER, Kim. An Easy Way for Hackers to Remotely Burn Industrial Motors [online]. wired.com, 12. January 2016 [cit. 25. January 2016]. Available at <http://www.wired.com/2016/01/an-easy-way-for-hackers-to-remotely-burn-industrial-motors/>.

9 Abstract and keywords

Title: Cyberspace: Ius ad bellum and Ius in bello

Keywords: cyberspace, cyber operation, cyber-attack, cyber warfare, ius ad bellum, ius in bello, use of force, right to self-defence, law of armed conflict, conduct of hostilities

Abstract: This thesis is concerned with issues of prohibition of use of force, right of self-defence and law of armed conflicts, all in relation to cyberspace and cyber operations. In the beginning it focuses on applicability of relevant legal provisions to cyber operations. Subsequently deals with prohibition of use of force in international law and conditions, which must be fulfilled in order to consider cyber operation to be use of force. At the same time the exemption, in form of self-defence, is taken into account. The conditions and specifics of this institute are analysed in relation to cyber operations. Second part of thesis deals with law of armed conflicts in relation to cyberspace. Different regimes of international armed conflicts are applied on cyber operations. The issue of legal cyber means and methods in armed conflict is addressed. This is followed with analysis of particular obligation which cyber-attack must comply with.

10 Shrnutí a klíčová slova

Název: Kybernetický prostor: Ius ad bellum and Ius in bello

Klíčová slova: kybernetický prostor, kybernetická operace, kybernetický útok, kybernetická válka, ius ad bellum, ius in bello, použití síly, právo na sebeobranu, právo ozbrojených konfliktů, vedení nepřátelských akcí

Shrnutí: Tato diplomová práce se zabývá problematikou zákazu užití síly, práva na sebeobranu a práva ozbrojených konfliktů ve vztahu ke kybernetickému prostoru a kybernetickým operacím. V úvodu se zaměřuje na aplikovatelnost relevantních právních ustanovení na kybernetické akce a jejich přičitatelnost státu. Následně diplomová práce pojednává o zákazu použití síly v mezinárodním právu a o podmínkách, které musí být naplněny, aby byla kybernetická operace považovaná za použití síly. Zároveň je brána v potaz výjimka ze zákazu použití síly ve formě práva na sebeobranu a její specifika aplikována na kybernetické operace. Druhá část diplomové práce se zabývá právem ozbrojených konfliktů v rámci kyberprostoru. Na kybernetické operace jsou aplikovány jednotlivé právní režimy ozbrojených konfliktů. Je zkoumaná problematika legálních prostředků v ozbrojeném konfliktu ve vztahu ke kybernetickým operacím. Následně jsou na potencionální kybernetický útok aplikovány jednotlivé požadavky legálního vedení boje.