MYKOLAS ROMERIS UNIVERSITY
FACULTY OF LAW
DEPARTMENT OF INTERNATIONAL AND EUROPEAN LAW

DARIUS KAZINEC

ISSUES OF CYBER WARFARE IN INTERNATIONAL LAW

Master thesis

Supervisor:
prof. dr. Justinas Žilinskas

VILNIUS, 2011

MYKOLAS ROMERIS UNIVERSITY
FACULTY OF LAW
DEPARTMENT OF INTERNATIONAL AND EUROPEAN LAW

DARIUS KAZINEC

ISSUES OF CYBER WARFARE IN INTERNATIONAL LAW

Joint International law program master thesis
Program of the studies code is 62401S118.

Supervisor:
prof. dr. Justinas Žilinskas
2011 05

Reviewer:
dr. Darius Sauliūnas
2010 05

Prepared by:
TTAmns9-01 gr.stud.
D. Kazinec
2011 05 16

VILNIUS, 2011

TABLE OF CONTENTS

INTRODUCTION....4
1. CYBER WARFARE....8
1.1 History and development....8
1.2 Definitions (“cyber warfare” and “cyberspace”)....10
1.3 Cybercrime Convention and the European Union....14
1.4 Cyber terrorism, cyber crime, cyber warfare....15
1.5 Determining the origin of cyber attacks (technical difficulties)....16
2. COMPUTER NETWORK ATTACK UNDER LAW OF ARMED CONFLICT....21
2.1 Applicability of International Humanitarian Law to cyber warfare (jus in bello)....21
2.2 Cyber attack (computer network attack) as an act of war (jus ad bellum)....24
2.2.1 Does a cyber attack (computer network attack) amount to an armed attack?....25
2.2.2 Attribution of the cyber attack (computer network attack) to a State....32
2.3 Right of self-defense against a cyber attack (computer network attack)....36
2.3.1 Right to self-defense (under United Nations Charter Article 51)....37
2.3.2 Right to an anticipatory self-defense....39
2.3.3 Right to self-defense (under customary international law)....42
2.4 Legal (combatant) status of cyber attackers (cyber combatants)....46
2.4.1 Civilian and combatant statuses....47
2.4.2 Civilians and cyber attacks (computer network attacks)....49
2.4.3 Adequacy of the four Geneva Convention criteria for cyber attacks (computer network attacks)....53
2.5 Is there need for a cyber warfare regulating treaty?....55
CONCLUSIONS....64
LITERATURE....66
SUMMARY....76
SANTRAUKA....77
ANNOTATION....78
ANOTACIJA....79

INTRODUCTION

Issues. One of the main problems that is still present is the lack of common definitions of the basic terms, such as cyber warfare and cyberspace. This is also the main obstacle for creation of any kind of international framework to regulate cyber conflict. Cyber warfare is favoured because of it's covert nature, this although might be against certain international obligations of States. Additional issues stem from this fact. Because cyber attacks are not easily traceable back to their origin, how should a victim-State react and, if the right to self-defense in such a situation exists, at whom it should be directed, this in turn raises more questions, such as distinction. Tracing and tracking cyber attacks is one of the current technological shortcomings, solutions to which have been developed, although there is still a long road ahead of us before they become fully implemented. With cyber tools becoming increasingly widespread, not only States are the sole beneficiaries of this technology. New non-State actors come into play. Cyber attacks can be the doing of private entities, such as terrorist organizations or even a single person. States can even delegate or contract private companies to accomplish their goals. Our currently existing international laws do not encompass these playes as parties to a conflict or proper combatants. Cyber warfare is not as any other type of warfare, it is not fought or seen in the physical plane, even though the consequences can. Cyber warfare is waged primarily and nearly exclusively via the cyberspace, an ephemeral place, which does not have borders.

Actuality and novelty of the topic. Cyber warfare of itself is not novel, it has been for over a decade and prior to that it existed and was synonymous with Information warfare (or Information operations) (IW or IO), only later due to it's significance it was separated as one of five core IO's military capabilities. The actuality of the issues at hand is that after such a long time there is still no specific international treaty relating to cyber warfare. Because of that we need to make due with what we have. This means we must try to accommodate cyber warfare under the existing international treaties.

Authors who dealt with this topic. The majority of publications relating to cyber warfare have come from scholars from United States. One of the first authors to provide any guidance in the matter is M. N. Schmitt[1], who provided a criteria for evaluation of cyber attacks as armed attacks, so they can fit under current international treaties. This criteria has gained

[1] M. N. Schmitt.
1. Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework// The Columbia Journal of Transnational Law. 1999, Nr.37(2). P.885-937
2. Wired warfare: Computer network attack and jus in bello// International Review of the Red Cross (IRRC). 2002, Nr.846. P.365-399.

significant support and was backed by such authors as Jeffrey Carr[2], Knut Dörmann[3], as well as general references were made to the work of M. N. Schmitt by Scott J. Shackelford[4], Lech J. Janczewski and Andrew M. Colarik and others[5], Jeffrey T.G. Kelsey[6], Marco Roscini[7], Sean Watts[8]. A few authors have also criticized M. N. Schmitt's criteria, among those is Matthew Hoisington[9].

The object is cyber warfare in international law.

The subject are international treaties and customs potentially applicable to regulation of cyber warfare.

The aim is to analyze the existing international law and determine it's adequacy to deal with the issues presented by modern cyber warfare.

The tasks raised are:

1. To ascertain the specifics of cyber warfare and cyberspace.
2. Analysis of legal scholars' works in order to find common points of the legal community.
3. Analyze the capabilities of the potentially applicable international law to cyber warfare.

Methodology. The author employs traditional theoretical methods: abstraction, analysis, analogy, generalization, deduction, induction, etc.[10] The thesis is based on international treaty and customary law, their commentaries, State practices, decisions of international courts, as well as the opinions of leading and less known scholars, researchers and experts.

Structure. The thesis is comprised of two chapters.

Chapter one deals with general information on cyber warfare, such as it's history, development, it's and other closely related terms' definitions, as well as European Union's (EU) view on cyber warfare and finally, a non-legal section on technical difficulties.

---

2 Carr J. Inside Cyber Warfare: Mapping the Cyber Underworld. Sebastopol: O'Reilly Media, 2009.

3 Dörmann K. Applicability of the Additional Protocols to Computer Network Attacks. Stockholm: International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, 2004.

4 S. J. Shackelford. From Nuclear War to Net War: Analogizing Cyber Attacks in International Law// Berkeley Journal of International Law. 2009, Nr.25(3). P.191-251.

5 Cyber Warfare and Cyber Terrorism. /ed. L. J. Janczewski, A. M. Colarik. New York: IGI Global, Inc, 2008.

6 J. Kelsey. Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare// Michigan Law Review. 2008, Nr.106. P.1427-1452.

7 M. Roscini. World Wide Warfare – Jus ad bellum and the Use of Cyber Force// Max Planck Yearbook of United Nations Law. 2010, Nr.14. P.85-130.

8 S. Watts. Combatant Status and Computer Network Attack// Virginia Journal of International Law. 2010, Nr.50(2). P.392-447.

9 M. Hoisington. Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense// Boston College International and Comparative Law Review. 2009, Nr.32(2). P.439-454.

10 Tidikis R. Socialinių Mokslų Tyrimų Metodologija. Vilnius: Lietuvos teisės universiteto Leidybos centras, 2003.

Chapter two focuses more on legal aspects of this thesis and consists of sections relating to cyber warfare in *jus in bello* and *jus ad bellum*, the right of self-defense, the status of cybercombatants under international law and lastly, attempts to answer the question if we need a cyber treaty.

Notions:

Cyberspace – a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Cyber warfare – the use of computers and the Internet in conducting warfare in cyberspace.

Cyber terrorism – a criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda.

Cyber crime – it is a form of crime where the Internet or computers are used as a medium to commit crime.

Information Warfare (IW) – the use of information or information technology during a time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.

Information Operations (IO) – employment of the core military capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, with specified supporting and related capabilities to influence, disrupt, corrupt, or usurp adversarial human and automated decision-making while protecting our own.

Computer Network Operations (CNO) or Cyber Operations (CO) – is a classification of military operations that use Computer Network Attack (CNA), Computer Network Defense (CND), Computer Network Exploitation (CNE) against an enemy to achieve military objectives.

Computer network attack (CNA) – operations to disrupt, deny, degrade, manipulate, or destroy information resident in computers and computer networks, or the computers and networks themselves; it may be waged against industries, infrastructures, telecommunications, political spheres of influence, global economic forces, or even against entire countries

Cyber combatants – also referred to as cyberwarriors, these are the „hackers“, civilian or military, these are the people with significant cyber security knowledge and skill, acting as independent players or employed to conduct cyber operations.

1. CYBER WARFARE

The first section is going to deal with general concepts beginning with a brief history of Cyber warfare, Internet and their origins. Followed by an analysis of available to date definitions of specific cyber warfare related terms and choosing the one's that are most precise to the current work. Because this work is taking a non-European approach to cyber warfare, in short the differences between the global and European approaches will be shown. Then a comparison of three very similar concepts of cyber terrorism, cyber crime and cyber warfare will be presented showing a thin yet significant line between them, proving an important guideline in properly treating any given cyber action. Finally technical aspects of why we are having problems with tracing, tracking, preventing and prosecuting the entities committing cyber crimes as well as most viable solutions.

1.1 History and development

Cyber warfare finds its roots in hacking, which predates even the Internet. “Hacking” and “hacker” have become terms that most people associate with talented computer programmers who have learned to exploit computer systems, which the average person not only does not understand, but maybe even do not grasp how a hacker operates and what he actually does. Certain hackers have made themselves famous due to their skill, some were even hired by security companies for example. However, when hacking was in its infancy, Internet as we know it today did not exist. The term hacker has existed even before the emergence of the silicon chip based computers that most of people are currently familiar with.

The hacker culture stayed with telephone equipment as their medium of choice through the 1980s. The Bell phone networks became a target for hackers who specifically called themselves *phone phreaks*[11]. Early *phone phreaks* would whistle a sound at 2600 hertz into a telephone, which the system would recognize and allow access to the long distance phone network. The *phone phreak* would then have access to the entire system the way an operator would. This iconic frequency has become the title of one of the more influential hacker publications titled simply: 2600.[12]

Few of the most known and successful people alive today have been those pioneers of hacking. Steve Jobs, chairman and CEO of Apple Inc., and Steve Wozniak, co-founder of Apple

[11] pheark – read as “freak”

[12] Goldstein E. The best of 2600: A hacker odyssey. Indianapolis: Wiley Publishing, Inc, 2009.

Inc., were some of these early “phone phreaks”, who explored the phone networks and tricked the system into doing what they wanted.[13]

As home computers began to emerge in the 1980s, hackers have switched their mediums to more powerful machines and began to explore their potential and possibilities. With the advent of the computer in homes, hackers began to learn more and more about computer code. This is essentially where the skill of the hacker lies today. The concept of modern hacking is quite simple. Exploit errors or loopholes[14] in a computer system's operating code thus allowing access to and manipulation of the system. Early hackers seemed more concerned with what could be done rather than hacking a system to get something from that system.[15] The possibilities of hacking became obvious very quickly as government, financial, educational, and security systems became more connected in the 1980s to promote efficiency of information transfer. In the 1990s the Internet granted the public unprecedented access to a variety of networks for financial transactions, communication, and commerce. The hacker community continued to grow throughout the 1980s and 1990s.

Hacking became more public with the increase of malicious code in the form of viruses and software (malware). As people began to use the Internet more and more, personal computers began to be affected. Self Replicating Computer Viruses had been present since the early 1970s, but mainstream citizens did not take notice until Happy99 and ILOVEYOU worms appeared in the 1990s. These worms had global effects that reached the lives and systems of everyday citizens. This self replicating global reach signals the start of real concern about a strategic level attack capable of striking throughout the globe, paralyzing systems, and preventing the flow of accurate information. People and governments started to fear computer hackers and their potential to disrupt systems that governments and economies relied on. Governments started to worry that if a single hacker can wreak havoc with an ILOVEYOU worm, then what could a nation accomplish with the full weight of national spending. In the late 1990s cyber warfare appeared to be a viable way to disrupt other nations, though how and to what extent was unclear at that time.[16]

These developments were of course not ignored. The shift from conventional ways to wage war to cyber warfare, which has been rumored as the new type of war for nearly ten years back then, began with the Kosovo War showing that the present has caught up with the future

---

13 S. Wozniak, G. Smith. iWoz. New York: W.W. Norton and Company, 2006.

14 A weakness or exception that allows a system, such as a law or security, to be circumvented or otherwise avoided.

15 Erickson J. Hacking: The art of exploitation. San Francisco: No Starch Press, Inc, 2008.

16 Boyd B. L. Cyber Warfare: Armageddon in a Teacup?: master thesis: military art and science general studies. U.S. Army Command and General Staff College. Fort Leavenworth, 2009.

and appropriate technologies that make it possible already exist. Since then most of the rumored technologies and tactics have become military doctrine and are receiving the utmost attention from the governments today. Initially it was called "information warfare"[17] without separating it from "cyber warfare", which at the time did not even exist as we understand it today. Nowadays the two terms are closely related, but not the same, despite them sometimes being used to describe the same act, which is not entirely wrong. Cyber warfare is both IW[18] and IO[19], but neither of those is cyber warfare. IW and IO are both broader terms used to describe the use of information in any kid of form to conduct war or operations against another entity. Cyber warfare on the other hand requires the use of cyberspace to conduct war.[20]

Advances in technology have made access to cyber warfare capability widespread, cheap and easy to use. Smaller States with weaker militaries have invested heavily into their cyber programs and now they can rely on them, because future warfare is happening in cyberspace, everything is wired and interconnected.[21] For this reason cyber warfare capability has become available even to non-State actors. The reality of today is that virtually anyone can have access to the proper tools and become a hacker. "The distinction between traditional threat actors – hackers, terrorists, organized criminal networks, industrial spies and foreign intelligence services – is increasingly blurred. With the border-less, anonymous nature of the internet, attribution of the source of attacks is difficult."[22] Looking in retrospect, when hacking was in it's early stages, it was crude and hardly understandable to the average computer user, it required a lot of technical knowledge and skill to operate, but nowadays the sophistication of the average hacker is falling down, while the selection of tools is growing in number and complexity at an increasing rate.[23]

1.2 Definitions ("cyber warfare" and "cyberspace")

To better understand the subject one must begin by defining what cyber warfare is. However, in order to do that it is necessary to define cyberspace first. Key issues with both terms

[17] W. Church. Information warfare// International Review of the Red Cross. 2000, Nr.837.

[18] IW is primarily an American concept involving the use and management of information technology in pursuit of a competitive advantage over an opponent.

[19] Most of the rest of the world use the much broader term of IO, which, although making use of technology, focuses on the more human-related aspects of information use, including (amongst many others) social network analysis, decision analysis and the human aspects of Command and Control.

[20] See supra note 16.

[21] H. I. Touré, the Permanent Monitoring Panel on Information Security World Federation of Scientists. The Quest For Cyber Peace. International Telecommunication Union. 2011.

[22] Australian Cyber Security Strategy// http://www.ema.gov.au/www/agd/agd.nsf/Page/CyberSecurity_CyberSecurity, accessed 2011-03-17.

[23] K. Geers. Cyber Weapons Convention// Computer Law & Security Review. 2010, Nr.26(5). P.547-551.

are that they do not have internationally accepted definitions, this makes it difficult and prevents the international community to establish a unified legal definition and create any kind of common agreement as to how international law should be applied to warfare conducted in cyberspace.

"Cyberspace" as defined by the United States (U.S.) Department of Defense (DoD) Dictionary of Military and Associated Terms[24]: "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers". "Cyberspace" according to the National Military Strategy for Cyberspace Operations of the U.S. is: "a domain characterized by the use of computers and other electronic devices to store, modify, and exchange data via networked systems and associated physical infrastructures."[25] T. Wingfield, in his book The Law of Information Conflict: National Security Law in Cyberspace defines "cyberspace" in a more plain language. "Cyberspace is not a physical place – it defies measurement in any physical dimension or time space continuum. It is a shorthand term that refers to the environment created by the confluence of cooperative networks of computers, information systems, and telecommunication infrastructures commonly referred to as the World Wide Web."[26] A 2001 Congressional Research Service (CRS) Report for Congress defined "cyberspace" as the "total interconnectedness of human beings through computers and telecommunication without regard to physical geography."[27] Graham H. Todd defines "cyberspace" as "an evolving man-made domain for the organization and transfer of data using various wavelengths of the electromagnetic spectrum. The domain is a combination of private and public property governed by technical rule sets designed primarily to facilitate the flow of information".[28] European Commission provides a very vague definition: "it describes the virtual space in which the electronic data of worldwide personal computers circulate"[29], adding the origins of the word being writer's W. Gibson's novel "Neuromancer"[30]. One of the most recent proposed definitions of "cyberspace" has been done by Rain Ottis and Peeter Lorents

---

[24] U.S. DoD. Chairman of the Joint Chiefs of Staff. Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms. Washington, DC: Government Printing Office. 2006. P.99.

[25] C. T. Lopez. Fighting in Cyberspace Means Cyber Dominance// Air Force Print News. 2007// http://www.af.mil/news/story.asp?id=123042670, accessed 2011-03-17.

[26] Wingfield T. C. The Law of Information Conflict: National Security Law in Cyberspace. Falls Church: Aegis Research Corp. 2000. P.17

[27] S. A. Hildreth. Cyberwarfare// The Library of Congress. CRS Report for Congress. 2001, Order Code RL30735. P.1.

[28] G. H. Todd. Armed Attack in Cyberspace: Deterring Asymmetric Warfare With an Asymmetric Definition// Air Force Law Review. 2009. P.3.

[29] Europe's Information Society: Thematic Portal. European Commission. Glossary and Acronyms (Archived)// http://ec.europa.eu/information_society/tl/help/glossary/index_en.htm#c, accessed 2011-03-17.

[30] Gibson W. Neuromancer. New York: Ace Books. 1984.

from the Cooperative Cyber Defense Center of Excellence in Tallinn, Estonia. Their definition reads: "cyberspace is a time-dependent set of interconnected information systems and the human users that interact with these systems".[31] Attention should primarily be drawn, in regards to this definition, at it's components, as authors state, there are three: the technology component, the human component, the communication and control components. Previous definitions completely disregard the human component. Rain Ottis and Peeter Lorents believe that due to the nature of cyberspace, that of an artificial space created by humans for humans, said human input, maintenance and development are needed, otherwise cyberspace would stagnate and eventually cease to exist. Secondary focus of this definition is the term "time-dependent", which means that cyberspace is not static and changes, given its nature, changes can be extremely rapid – minutes, seconds or even fractions of seconds. Analogies have been made between military actions in cyberspace and in the physical world – deployment of new firewall rules to fend of intruders can be done near instantly, whereas building military installations can take a significant amount of time. The author of the current work agrees with Rain Ottis and Peeter Lorents and their proposed definition as it is truly one of the most exhaustive and well thought out definitions, and would like to use it as the default definition of cyberspace within this work.

"Cyber warfare" has been defined as simply as "warfare conducted in the cyberspace"[32] with emphasis on the term cyberspace as being the key. This definition is although insufficient to understand the term due to the specifics of how warfare in cyberspace is conducted and does not clarify on that point at all. The U.S. DoD Dictionary of Military and Associated Terms defines "cyber operations" as "the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace."[33] and the phrase "computer network attack" as "actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[34] CRS Report for Congress from 2001 notes that "cyber warfare can be used to describe various aspects of defending and attacking information and computer networks in cyberspace, as well as denying an adversary's ability to do the same."[35] And CRS Report for Congress from 2006 defined the phrase "computer network attack" as "operations to disrupt or destroy information resident in computers and computer networks."[36] Kevin Coleman

---

31 R. Ottis, P. Lorents. Cyberspace: Definition and Implications. Academic Publishing Limited. 2010. P.267-270.

32 See supra note 16. P.7.

33 See supra note 24. It further notes that such operations include computer network operations and activities to operate and defend the Global Information Grid.

34 Ibid.

35 See supra note 27. Summary.

36 W. Clay. Information Operations and Cyberwar: Capabilities and Related Policy Issues// The Library of Congress. CRS Report for Congress. 2007, Order Code RL31787. P.5

from Technolytics Institute[37] defined "cyber war" as "a conflict that uses hostile, illegal transactions or attacks on computers and networks in an effort to disrupt communications and other pieces of infrastructure as a mechanism to inflict economic harm or upset defenses." Recognizing that military operations in cyberspace could be viewed as warfare, the phrase "cyber warfare operations" is the most appropriate to be used in analyzing the wide range of military operations in cyberspace. However, many terms that do exist tend to overlap in meaning despite seemingly being different. "The use of technology to both control and disrupt the flow of information has been generally referred to by several names: IW, electronic warfare, cyberwar, netwar, and IO."[38] It is apparent that the terms "cyber warfare (cyber warfare operations)" and "information operations" are used somewhat synonymous, although this is not completely correct. Currently, IO activities are grouped by the U.S. DoD into five core military capabilities[39]:

- Psychological Operations,
- Military Deception,
- Operational Security,
- Computer Network Operations (CNO)
- Electronic Warfare.

Any cyber acts fall under the general domain of CNO.[40] In this sense "cyber warfare (operations)" should be understood as CNO. This work is interested in particular in computer network attacks (CNA), which along with computer network defense (CND) and computer network exploitation (CNE) comprise the CNO. Thus for the purpose of this work the following definition of "computer network attack" by Knut Dörmann, which is shared by the U.S. DoD, is most accurate: "operations to disrupt, deny, degrade, manipulate, or destroy information resident in computers and computer networks, or the computers and networks themselves; it may be waged against industries, infrastructures, telecommunications, political spheres of influence, global economic forces, or even against entire countries."[41] "Computer network" in this definition also encompasses the network infrastructure, which includes all of the physical

---

37 The Technolytics Institute (U.S., Pittsburgh, Pennsylvania) is an executive think-tank that focuses on the needs of management in business, government and industry. The Institute operates three centers of excellence: Business and Commerce, Security and Intelligence and the Center for Science and Technology. The Technolytics Institute is a leading international security training and services provider.

38 See supra note 36. Summary.

39 U.S. DoD. Chairman of the Joint Chiefs of Staff. Joint Publication 3-13, Information operations. Washington, DC: Government Printing Office. 2006.

40 Ibid.

41 K. Dörmann. Computer Network Attack and International Humanitarian Law// Cambridge Review of International Affairs. 2001. P.1

devices, transmission lines and network and internet protocols needed for that network to function.

There's a multitude of definitions to choose from, they do not contain mind blowing differences, but rather subtle nuances, which nonetheless do carry enough value to warrant every single one of them very important to a legal study.

1.3 Cybercrime Convention and the European Union

The European community has a different approach to cyber warfare than the Unites States or the eastern counterparts (e.g.: China, Russia). U.S. military is very progressive in this field as it is seen via the above sources of definitions and varying opinions, which are based mostly on U.S. military publications. U.S., Russian[42] and Chinese[43] militaries have all acknowledged the strategic importance of cyber warfare and are intensely working on developing defensive and offensive means. Whereas European militaries have not shown such enthusiasm and involvement. European military literature regarding cyber warfare is not prevalent at all, military publications which are open source are completely devoid of the terms cyber warfare, information warfare or operations or computer network attack. The reason for this is that cyber warfare is viewed not as a component of military doctrine, but a criminal action. Europe is not ignoring the potential for cyber warfare and its strategic threat, but the European militaries do not appear to be contributing to the generation of doctrine relating to cyber warfare. The European Union (EU) Policy is directed towards the protection of Critical Information Infrastructures,[44] which in most cases is a target for cyber warfare and not cyber crime.

Council of Europe has drawn up the Convention on Cybercrime in 2001,[45] which completely does not address the issues of cyber warfare instead dealing only with crimes in cyberspace. The convention however is not regional, despite that, 29 of the current 30 members for whom it has entered into force are European States and members of the Council of Europe, the 30th are the United States. 17 signatures have not been followed by ratifications of which 3 are non-members of the European Council: Japan, Canada and South Africa. During the draft phase European Council's observer States – Japan, Canada and China – took an active part in in

---

42 O. Odnokolenko. Controversial aspects of new Russian military doctrine questioned// Open Source Center. 2003.

43 Thomas T. L. Cyber Silhouettes: Shadows Over Information Operations. Fort Leavenworth: Foreign Military Studies Office. 2006.

44 Europe's Information Society: Thematic Portal. European Commission. Critical Information Infrastructure Protection// http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm, accessed 2011-03-17.

45 Council of Europe. Convention on Cybercrime. Adopted 2001-11-08. Open for signatures 2011-11-23. Entered into force 2004-07-01// http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm, accessed 2011-03-17.

the process. There is also an additional Protocol that outlaws acts of a racist and xenophobic nature committed through computer systems.[46] This convention is however one of a kind to date. It provides the basis for State cooperation, unification of laws and practices and investigative techniques.[47] It also lays down guidelines for governments wishing to develop legislation against cybercrime. The convention criminalizes and provides some solutions for basic cyber crimes, such as illegal access (hacking) and data interception, however it leaves more serious cyber incursions, such as sabotage or espionage, unattended. Establishment of a unified law in this way is quite slow, if not completely impossible.

It is going to be shown in the next section in brief what the differences between cybercrime and cyber warfare are. Because they are not the same, addressing only one does not mean that the other can be as well covered by the same measures.

1.4 Cyber terrorism, cyber crime, cyber warfare

The term cyber terrorism was coined in 1996 by simply combining the terms cyberspace and terrorism. It stands to logic to search for a definition in those core terms, primarily in "terrorism". The U.S. State Department defines terrorism as "politically motivated acts of violence against non-combatants."[48] In a study of 109 academic and official definitions of terrorism, three common elements were identified[49]: the use of violence, political objectives and the purpose of sowing fear within a target population – all of which are also present in the following definitions of cyber terrorism. According to the U.S. Federal Bureau of Investigation: "cyber terrorism is any premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents."[50] "Cyber terrorism", as defined in the Article 1.2 of the Proposal for an International Convention on Cyber Crime and Terrorism, means "intentional use or threat of use, without legally recognized authority, of violence, disruption, or interference against cyber systems, when it is likely that such use would result in death or injury of a person or persons, substantial damage to physical property, civil disorder, or significant

---

[46] Council of Europe. Cybercrime: a threat to democracy, human rights and the rule of law// http://www.coe.int/t/dc/files/themes/cybercrime/default_EN.asp, accessed 2011-03-17.

[47] See supra note 45.

[48] M.M. Pollitt. Cyberterrorism – Fact or Fantasy?// http://www.cs.georgetown.edu/~denning/infosec/pollitt.html, accessed 2011-03-17.

[49] K. Kerr. Putting cyberterrorism into context// http://www.auscert.org.au/render.html?it=3552, accessed 2011-03-17.

[50] S. Krasavin. What is Cyber terrorism?// http://www.crime-research.org/library/Cyber-terrorism.htm, accessed 2011-03-17.

economic harm."[51] And the U.S. National Infrastructure Protection Center provides this extensive and most accurate definition: "a criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda."[52]

Now we have come to a point where we have three previously mentioned terms: cyber terrorism, cyber crime and cyber warfare. The distinction between these terms is extremely important because there are non-technology-related issues and solutions that will impact strategies in combating these distinct cyber actions. The issue arises because in the physical world these three acts might manifest themselves in the exact same form, but in reality they would be different. The reason for this is that in order to make a distinction between them we need to know the intent behind the actions and not the mechanics of the event. According to Lech J. Janczewski and Andrew M. Colarik[53] intentionally tampering with data, which results in death, would be murder in addition to cybercrime, adding any kind of demands or threats of more similar acts if the demands are not met would be cyber terrorism, and if in addition to all that the person responsible would be an agent of a foreign State that would constitute an act of cyber warfare. This is relevant to this work in order to correctly classify the cyber act and treat it accordingly. If proven without a doubt to be the work of independent or rogue factions and acting on their own accord, the actions of culprits committing similar cyber acts cannot be treated as cyber warfare and subsequently as acts of war against a State, however the State from which the attacks have originated has various obligation under international law, thus by not acting and attempting to prevent the attacks, this State is in breach and can bear partial and indirect responsibility for the actions of the original attackers. However, proof without a doubt in such cases is nonetheless a completely different and very difficult matter. These issues will be discussed in more detail in the second chapter of this work.

1.5 Determining the origin of cyber attacks (technical difficulties)

It is appropriate to begin by asking the question: "why it is difficult to determine the origin of cyber attacks?" before going into the specific problems of the issue. The answer is

[51] A. D. Sofaer, S. E. Goodman, M.-F. Cuéllar and others. A Proposal for an International Convention on Cyber Crime and Terrorism. 2000// http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm, accessed 2011-03-17.

[52] See supra note 49.

[53] See supra note 5. P.XIV

simple: because of how the Internet is. Understanding the Internet is important as it is the primary and nearly the only delivery method of any cyber attack.[54]

The Internet as we know it today is a telecommunications super-network spanning around the globe, a network of networks, this includes hardware and software. The Internet (originally "ARPANET") began as a research project in 1969 sponsored the Advanced Research Projects Agency (ARPA) of the U.S. DoD, which was the world's first operational packet switching network and the core network of a set of network types developed over the years (X.25[55], Telenet[56], UUCP[57], NPL[58]) that came to compose the global Internet in the years to come. Primary use of such networks (ARPANET) was research and military purposes, it was strictly forbidden to use them for commercial purposes, except for those networks which were specifically established with the commercial intent in mind (X.25, Telenet). During the unification of the myriad of the networks a standard network protocol suite to support inter-networking communications was established 1982. This protocol suite consisted of Internet Protocol (IP) and Transmission Control Protocol (TCP) and became widely known as IP/TCP, which still forms the foundation of network communications up until today. In December 1988, as a direct result of the first major computer security incident on the Internet (the Morris Worm), Defense Advanced Research Projects Agency (DARPA, renamed from ARPA) founded the Computer Emergency Response Team (CERT) Coordination Center to provide a central place for coordinated responses to Internet cyber attacks. Today, the Internet comprised of approximately 769 million hosts worldwide.[59] The number of computer security incidents handled by the CERT Coordination Center (CERT/CC) has grown from 6 in 1988 to 137,529 in 2003.[60] The statistic unfortunately ends that same year. The reason for this given by CERT/CC is as follows:

---

[54] Only alternative being: equipment, hardware has malicious software embedded into it, which gets activated at some point and wrecks havoc or it might need outside activation via the Internet, in any case the importance of the Internet cannot be disputed. Additionally, hacking via a wireless connection, not necessary requiring an Internet connection can be qualified as cyber attack.

[55] X.25 is International Telecommunication Union's Telecommunication Standardization Sector's standard protocol suite for packet switched wide area network communication.

[56] Telenet was a commercial packet switched network which went into service in 1974. It was the first packet-switched network service that was available to the general public.

[57] UUCP is an abbreviation for Unix-to-Unix Copy. The term refers to a suite of computer programs and protocols allowing remote execution of commands and transfer of files, email and net-news between computers.

[58] In 1965, Donald Davies of the National Physical Laboratory (United Kingdom) proposed a national data network based on packet-switching, which was not however taken up nationally.

[59] Internet System Consortium// http://www.isc.org/solutions/survey, accessed 2011-03-17, and http://ftp.isc.org/www/survey/reports/2010/07/, accessed 2011-03-17.

[60] Computer Emergency Response Team Statistics (Historical)// http://www.cert.org/stats/, accessed 2011-03-17.

"Given the widespread use of automated attack tools, attacks against Internet-connected systems have become so commonplace that counts of the number of incidents reported provide little information with regard to assessing the scope and impact of attacks."[61]

The above data is obviously dated and it can only be speculated as to the amount of incidents that would have been documented in addition to undetected intrusions up until today. However, from the available data till 2003, a pattern of a constant and steady increase can be observed – a nearly double gain of cyber incidents every year. In light of major cyber attacks taking place in the recent years, knowledge and tools being available to almost anyone, these hypothetical figures can be significantly higher.

Despite serious security shortcomings, the TCP/IP is still the standard protocol suite for network communications on the Internet now, greatly limiting the ability to track and trace cyber attacks to their source.[62] As we can see historically the Internet was developed without this functionality in mind, the developers most certainly could not foresee the importance that the Internet has today and for what purposes it could be used. The users were considered to be trustworthy and the motivations and rewards for malicious activity were negligible. But because of this design flaw it is extremely easy for experienced hackers to make their trail disappear permanently. There have been certain technological advances over the last decades that provide several methods to ease the determination of the origin of a connection. These methods although are not perfect should be discussed along with the possibility of their implementation.

Legal perspective aside, technical difficulties are an essential part in the process of determining the origin of a cyber attack and being able to attribute the attack to someone. If it proves to be impossible to trace the subject responsible any legal debate loses its value and remains only a theory which cannot be applied in practice.

The current technical ability to track and trace Internet-based attacks is still primitive at best. It is also needed to emphasize that a pure technological solution cannot be achieved, so in addition certain policy changes have to be made, be it by Internet Service Providers (ISPs) or whole States, in cooperation efforts. Over the year there has been developed a significant number of different methods, both long- and short-term, which were meant to mitigate the issues of tracking and tracing. These methods however were not meant to be permanent solutions, as many of them had drawbacks – technological limitations (such as increased bandwidth) or issues with implementation. Most primitive trace-back[63] would involve manual checking of ISPs router

[61] Ibid.

[62] Lipson H. F. Tracking and Tracing Cyber-Attacks – Technical Challenges and Global Policy Issues. Pittsburgh: Carnegie Mellon University. 2002.

[63] Any attribution technique that begins with the defending computer and recursively steps backward in the attack path towards the attacker.

logs upstream, going backwards to the origin of the attack, up to the point when a border of another ISP or a State is reached. In order to continue the trace-back the cooperation of these entities is required, moreover the success and effectiveness of this depends on the trustworthiness and skill of the upstream ISPs. In case of State cross-border trace-back international agreements are essential to facilitate the required cooperation, as well as agreements to share trace-back technology to raise the overall level of skill, in addition to hardware enhancements, are needed to complete a trace across multiple ISPs. This suggests that significant investment and financial support is required in these sectors too.

The most prominent solutions without any drawbacks for the issues of tracing and tracking at hand are the new internet security protocols: Internet Protocol Version 6 (IPv6) and Internet Protocol Security (IPsec). Despite having developed these solutions, they are far from being implemented. IPsec is most commonly used to secure Internet Protocol Version 4 (IPv4) traffic due to slow deployment of IPv6. It provides new security protocols:

– the Authentication Header, which provides packet integrity by authenticating all IP header fields, except those that may legitimately change in transit, and the data portion of the packet;

– the Encapsulating Security Payload, which provides packet confidentiality and integrity.

However, it does not provide explicit support for vigilant resource consumption, fine-grained authentication of trust, and situation-sensitive processing, which are three of the requirements for next generation Internet protocols.[64] Although fulfilling these requirements is technically possible with IPsec, further exploration and development is needed.

IPv6 has been developed in conjunction with IPsec as a replacement for IPv4 since 1998[65] and has IPsec build into it, although IPsec is present, its use is optional. Main advantage of IPv6 over IPv4 is its enormous address space, 128 bits over 32 bits respectively. The shortage of IPv4 addresses lead to sharing of global IP addresses through the use of Network Address Translation and dynamic IP assignment. This was detrimental to tracing and tracking, since there was no long-term link between an IP address and a physical machine or device. Such information could be stored in an ISP's logs or network administration documents, but it was certainly ephemeral. IPv6 on the other hand provides for a static IP address assignment. In addition, IPv6 header is quite flexible and efficient, providing for a sequence of extension

[64] See supra note 62.

[65] IPv6 was developed by the Internet Engineering Task Force to deal with the long-anticipated IPv4 address exhaustion, and is described in Internet standard document RFC 2460, published in December 1998, http://tools.ietf.org/html/rfc2460, accessed 2011-03-17.

headers to carry optional information, such as tracking or other audit data. This relatively new technology would greatly enhance our ability to trace and track cyber attacks, however over a decade has already passed since its birth and as of 2008 the penetration of IPv6 was still less than one percent of Internet traffic in any country, with leaders being Russia – 0.76%, France - 0.65% Ukraine – 0.64%, Norway – 0.49%, U.S. – 0.45%.[66]

[66] S. H. Gunderson. Global IPv6 statistics. Measuring the current state of IPv6 for ordinary users. RIPE57 (*Réseaux IP Européens*, french for European IP Networks)// http://www.ietf.org/proceedings/73/slides/v6ops-4.pdf, accessed 2011-03-17; http://www.ripe.net/ripe/meetings/ripe-meetings/ripe-57, accessed 2011-03-17.

2. COMPUTER NETWORK ATTACK UNDER LAW OF ARMED CONFLICT

The second part of this work will deal with the main issues posed by the topic of this work. How are cyber attacks (CNAs) treated under law of armed conflict (LOAC) and international law, or, more precisely, when and under what conditions does a cyber attack (CNA), if at all, amount an armed conflict or armed force – cyber force if you will. This chapter will begin by a dual distinction of two sets of rules provided by LOAC: *jus in bello* and *jus ad bellum*. We will touch upon the non-kinetic nature of cyber attacks (CNA). We will in short recap the already discussed technical part, which is the identification cyber attackers. Then ways of possible attribution of cyber attacks (CNA) – committed by both State and non-State actors – to States will be discussed. A significant part of this chapter will be devoted to understanding if cyber attacks (CNAs) grant a right for self-defense. Final sections are going to deal with the issue that there as of yet, is no specialized international treaty for regulation of cyber attacks (CNAs) and cyber warfare in general.

2.1 Applicability of International Humanitarian Law to cyber warfare (*jus in bello*)

In order to effectively analyze and answer the question posed by the current section of this work it is necessary to establish a clear relation between cyber warfare and international humanitarian law (IHL). Main issue here lies with the nature of cyber warfare – it is conducted in cyberspace and not in the physical plane, although consequences can be felt or seen in both of them.

IHL was designed for methods and means that are kinetic in nature, which is for armed conflicts. One may claim that since there is literally nothing "physical" in a computer network attack, therefore it is not "armed" and should completely fall out of the scope of IHL, because the existence of an armed conflict is in fact a prerequisite that activates *jus in bello*. According to Article 2 common to the four 1949 Geneva Conventions, they apply, aside from specific provisions that pertain in peacetime, "to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them".[67] 1977 Additional Protocol I, which also applies to international

[67] Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. 1949-08-12. Art. 2 , United Nations Treaty Series (UNTS) Nr.75(31) (GC I); Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of the Armed Forces at Sea. 1949-

armed conflict, adopts the same "armed conflict" standard, one that has become an accepted customary law threshold for humanitarian law.[68] Although in a different context of non-intenational conflict, 1977 Additional Protocol II also embraces the term "armed conflict", which means that armed conflict is a condition determined by its nature rather than by its participants, location or the declaration of war by the belligerents.[69]

But what is an armed conflict? Originally IHL related only to armed conflict between two or more States, however over time it's application has been expanded to non-international armed conflicts, consequently expanding the definition of what actually constitutes armed conflict. Therefore IHL recognizes only two types of armed conflicts, however it is possible for one type of conflict to evolve into another. This work is primarily concerned with State-on-State type of conflict and use of cyber warfare within it.

Commentaries published by the International Committee of the Red Cross (ICRC) on the 1949 Geneva Conventions and the 1977 Additional Protocols take a very expansive approach towards the meaning of the term of armed conflict – "any difference or dispute". The former define armed conflict as "any difference arising between two States and leading to the intervention of armed forces... even if one of the Parties denies the existence of a state of war. It makes no difference how long the conflict lasts, or how much slaughter takes place."[70] Similarly, the Commentary on AP I gives us that "humanitarian law... covers any dispute between two States involving the use of their armed forces. Neither the duration of the conflict, nor its intensity, play a role".[71] And the Commentary on AP II describes armed conflict as "the existence of open hostilities between armed forces which are organized to a greater or lesser degree".[72] But simple engagement of armed forces cannot be considered a sole criterion for an armed conflict. In addition, it is generally accepted that isolated incidents such as border clashes or small-scale raids do not reach the level of armed conflict as that term is employed in international humanitarian law. More recently, ICRC has published its opinion[73] on the definition of armed conflict in 2008. The analysis of the prevailing legal opinion gives us such definitions:

08-12. Art. 2.UNTS Nr.75(85) (GC II); Geneva Convention Relative to the Treatment of Prisoners of War. 1949-08-12. Art. 2. UNTS Nr.75(135) (GC III); Geneva Convention Relative to the Protection of Civilian Persons in Time of War. 1949-08-12. Art. 2. UNTS Nr.75(287) (GC IV).

68 Additional Protocol I to the Geneva Convention of 1949-08-12, and Relating to the Protection of Victims of International Armed Conflicts. 1977-12-12, UNTS Nr.1125(3) (AP I).

69 Additional Protocol II to the Geneva Conventions of 1949-08-12, and Relating to the Protection of Victims of Non-International Armed Conflicts. 1977-06-08. UNTS Nr.1125(609) (AP II).

70 ICRC Commentary on the Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field /ed. Jean Pictet. Geneva. 1952. P.32-33 (GC I Commentary).

71 ICRC Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 /ed. Y. Sandoz, Ch. Swinarski, B Zimmerman. Geneva. 1987. Para.62. (AP Commentaries).

72 Ibid. Para.4341.

73 ICRC. How is the Term "Armed Conflict" Defined in International Humanitarian Law?. Opinion Paper. 2008.

1. *"international armed conflicts* exist whenever there is resort to armed force between two or more States"

2. *"non-international armed conflicts* are protracted armed confrontations occurring between governmental armed forces and the forces of one or more armed groups, or between such groups arising on the territory of a State [party to the Geneva Conventions]. The armed confrontation must reach a *minimum level of intensity* and the parties involved in the conflict must show a *minimum of organization*."[74]

The original definitions of can be easily explained from a historical perspective. At the time when these documents were drafted these definition and use of "armed forces" was actor-based. Citing the said actors of undesirable conduct by the Conventions and their Commentaries was sufficient enough to regulate them. In comparison, even the newest definitions still relate to the actor-based criteria. That said, we are in need of new or additional criteria and thus our focus is shifting from actors to the above mentioned undesirable conduct, which, in a sense, is contained within IHL itself. A review of it's instruments and principles gives us a clear understanding what is the purpose of IHL – that is to protect the individuals who are not directly participating in hostilities, as well as their property.[75] Entities protected by IHL are civilians and civilian objects, those who are *hors de combat* or those who provide humanitarian services. Protection granted to these individuals is framed in terms of injury or death and in case of property as damage or destruction. These Geneva Law purposes are complemented by Hague Law norms intended to limit suffering generally through restrictions on certain weaponry and methods of warfare.[76] In short, an armed conflict occurs when a group takes measures that injure, kill, damage or destroy. The term also includes actions intended to cause such results or which are the foreseeable consequences thereof. At this point the issue is just *jus in bello* rather than *jus ad bellum*, thus the motivation underlying the actions is irrelevant, so too is their wrongfulness or legitimacy. These last key issues in relation to *jus ad bellum* shall be discussed later.

To continue on topic, the same consequence based test should and can be applied to cyber attacks in order for IHL principles to apply:

- not sporadic or isolated incident
- intended to cause injury, death, damage, destruction or analogous effects or such consequences are foreseeable.

---

74 Ibid.

75 AP I Preamble: "it is necessary to reaffirm and develop the provisions protecting the victims of armed conflicts and to supplement measures intended to reinforce their application."

76 The designation "Geneva Law" refers to that portion of the law of armed conflict addressing protected categories of persons: civilians, prisoners of war, sick wounded or shipwrecked, medical personnel. It is distinguished from "Hague Law", which governs methods and means of combat, occupation, and neutrality.

In this sense, IHL is sufficient at first glance to afford minimal protection to protected persons and objects. However there are still numerous issues. Interpretation of cyber attacks undertaken by any non-State actors are incredibly vague and difficult, things are even more complicated if it is impossible to attribute these attacks to a concrete State or at least as State sponsored. Moreover, civilian personnel performing cyber operations for the military are in a difficult position in relation to their combatant status, which actually makes them illegal combatants.[77]

In order to expand or rather adapt IHL to the realities of modern days, change is needed. The change in the form of a switch from actor-based to consequence-based threshold of application of IHL in *jus in bello.* This hardly a jurisprudential epiphany according to M. N. Schmitt, who in his work of 1999[78] and 2002[79] mentions this, pointing out differences between *jus in bello*, where consequence-based approach is already settled in, and *jus ad bellum*, where he proposes a slightly amended approach, by additionally introducing his six criteria. M. N. Schmitt draws parallels between chemical and biological warfare and cyber warfare. The former are lacking the delivery by a kinetic weapon as well as the latter, but no one is disputing that they are subject to IHL. Intentionally targeting civilian or other protected objects is unlawful regardless of the means used. This tramples any claim that a cyber attack by itself cannot be subject to IHL because it is not "armed". Therefore, a cyber attack might or might not qualify as being "armed". Disturbing a universities intranet would obviously not suffice for example. The answer is never clear cut though, as it depends on cyber attack's nature and likely consequences.

2.2 Cyber attack (computer network attack) as an act of war (*jus ad bellum)*

It has to be stressed that there is no international definition of what is an act of war, therefore the international community relies on the definitions of armed conflict, which, to an extent, has nearly uniform understanding and have been already covered by ICRC commentaries. It is also important to point out that most scholars who have discussed cyber attacks in *jus ad bellum* were from the U.S. and were contemplating the issues within their legal framework and only considered the right of self-defense of the U.S. against cyber attacks only. The rest of the international community is still undecided as to what is the appropriate course of action in

[77] If their cyber attacks amounted to "attacks", i.e.: causing injury, death, damage or destruction.
[78] See supra note 1.
[79] Ibid.

serious cases of cyber attacks, there is still fear of creating a precedent that is not adequate or would backfire in the future.

The three key points in answering the main question if a cyber attack (CNA) can be treated as an act of war are[80]:

- does it mount to an armed attack,
- identification of the culprits and
- attribution of the attack to a State.

The issues and solutions for intensification, or more precisely, tracing and tracking, have been discussed in Chapter 1.5. The chapter in question is devoid of practical examples however. What is meant by the technical term of IP spoofing? Anonymity is one of the greatest advantages of cyber warfare – attacks might appear to originate in a certain country, but that does not necessary mean that that country, or even that the owners of the computers involved, were behind such actions. The saying "looks are deceiving" fits like no other within the context of anonymity of cyber attacks. For example, an attack that broke into the U.S. DoD's system in 1998 was carried out by an Israeli teenager and two Californian students through a computer based in the United Arab Emirates.[81] Attacks on Estonia in 2007 originated from U.S., Egypt, Peru and the Russian federation.[82] Note the wording: "originated" - there is still little data available about the original perpetrators of the attacks, any accusations are unfortunately merely speculations.

2.2.1 Does a cyber attack (computer network attack) amount to an armed attack?

Since we are going to speak about "armed attack", it has to be noted that this term as well does not have a uniform definition contained in any convention. This, unlike with other terms, however is not as problematic. The framework for analyzing armed attacks is well-settled along with core legal principles relating to its meaning. The international community generally accepts the Jean S. Pictet's[83] test of scope, duration, and intensity to serve as a guide and to be able to evaluate if a particular use of force is equal to an armed attack. When a use of force is of sufficient scope, duration, and intensity, then it is an armed attack and this would bring the

[80] Not expressly pointed out as such three key elements, however M. Roscini follows a similar logic.
[81] See supra note 4, P.204
[82] Ibid. P.203,231.
[83] Doctor of Laws and Director for General Affairs of the International Committee of the Red Cross in 1952-1959, General Editor of the Commentary on the Geneva Conventions.

operation under the aegis of the Geneva Conventions and the law of war. The test, despite being widely accepted, is interpreted differently by States, non-governmental organizations (NGO's) and scholars, once again creating many varying opinions, moving further away from a uniform view. However varied these opinions are, via State declarations, they help understand which uses of force are of sufficient scope, duration and intensity in order to constitute an armed attack.

In 1974 the United Nations General Assembly (UN GA) passed the Definition of Aggression resolution.[84] The resolution requires an attack to be of "sufficient gravity" (Article 2) before it is considered an armed attack. There is no definition of armed attacks, although it provides examples that are accepted by the international community instead. The resolution has helped settle the meaning of armed attacks for conventional attacks only. This means that with new technological advances come new forms of attack, which previously were not covered by State declarations or practices. States recognize that unconventional uses of force may warrant treatment as an armed attack when their scope, duration, and intensity are of "sufficient gravity" as well. One of such unconventional uses of force are cyber attacks (CNA).

Before proceeding to the next two points it is necessary to assess if a cyber attack (CNA) can at all be called an armed attack in order to trigger the application of *jus ad bellum* rules. This means that we must determine if a State may actually respond to it with force, this is governed by the UN Charter. The relevant article here is Article 2(4) prohibiting threat of or use of force:

"*All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the Purposes of the United Nations.*"[85]

Purposes of the UN expressly cited in the Charter include the maintenance of international peace and security. The article itself does not authorize a State to respond with force, it merely provides us with a guideline showing which use of force is wrongful under the Charter. UN Charter Chapters VI and VII deal with bases for proper response with force.

It should be determined if cyber attacks (CNA) fall under the definition of "force". Since the drafting of the UN Charter, the reach of the term "force" has proven contentious. The Vienna Convention on the Law of Treaties[86] sets forth the core interpretive principle that international instruments are to be interpreted in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in light of its object and scope. But what is

---

[84] United Nations General Assembly Resolution 3314 (XXIX). Definition of Aggression. Adopted at it's twenty-ninth session. 1974-12-14

[85] UN Charter. Art.2, para.4.

[86] Vienna Convention on the Law of Treaties. 1969-05-23. Art.31(1). UNTS Nr.1155(331).

the plain meaning of the term "force"? Is it only "armed" force, i.e. force by military units or does it apply to other forms of coercion? For this analysis of the text of the UN Charter, it's Preamble, annexes and *travaux preparatoires* are needed. The Preamble mentions "armed force"[87]. For purposes of consistency, if Article 2(4) would be intended to extend beyond "armed force", the term "armed" would not have been included there. Article 44 further supports restrictive interpretation: "When the Security Council has decided to use force it shall, before calling upon a Member not represented on it to provide armed forces..." Although "force" in Article 2(4) appears without the qualifier "armed", it nonetheless makes reference to "armed force". We find term "armed force" only twice in the text of the Charter itself, which might suggest that the drafters wanted to distinguish it from simply "force". However, both cases involved enforcement of Charters Chapter VII, in which armed force is but one of multiple options available to the Security Council in response to threats to the peace, breach of the peace, or acts of aggression. Article 2(4) precludes nothing but "force", therefore there was no need to distinguish it through qualification. *Travaux preparatoires* are most useful in the context of Article 2(4). At the San Francisco Conference[88], the Brazilian delegation submitted amendments to the Dumbarton Oaks proposals that would have extended Article 2(4) range to economic coercion.[89] Though the proposition received a majority vote in committee, the Conference declined adopting it by a vote of 26 to 2.[90] Thus this short analysis leads us with the conclusion that economic, and political for matter, coercion was left out of the sphere of Article 2(4) of the UN Charter.

Additionally, as per Article 31 (3 (b)) of the Vienna Convention on the Law of Treaties, any subsequent practice of the contracting States is to be taken into account when interpreting a treaty. In this sense States have clearly expressed that they view cyber force as a type of armed force. U.S. are calling cyber attacks as one of "weapons of mass effect", attributing even greater economic and psychological impact to such weapons than any kinetic or biological agent could achieve.[91] The Russian Federation has been pushing within the UN for a treaty to limit development, production and use of particularly dangerous cyber weapons for many years, the U.S. was mostly opposed to this, however recent developments show a change is coming.[92]

---

87 The Preamble includes among Charter purposes the goal that "armed force shall not be used, save in the common interest ."

88 Formally United Nations Conference on International Organization, 1945-04-25 – 06-26. The international meeting that established the UN.

89 Dumbarton Oaks Conference, 1944-08-21 – 10-07. The representatives of China, the Soviet Union, the U.S., and the United Kingdom formulated proposals for a world organization that became the basis for the UN.

90 Documents of the United Nations Conference on International Organization, 1945, Vol.VI.

91 Chairman of the Joint Chiefs of Staff. The National Military Strategy of the U.S. of America: A Strategy for Today; A Vision for Tomorrow. 2004.

92 J. Markoff. At Internet Conference, Signs of Agreement Appear Between U.S. and Russia. The New York

When submitting it's views to the UN Secretary-General, the Russian Federation declared that "information weapons" can have "devastating consequences comparable to the effect of weapons of mass destruction."[93] Therefore, "the use of Information Warfare against the Russian Federation or its armed forces will categorically not be considered a non-military phase of a conflict whether there were casualties or not."[94] Similar statements have been by the United Kingdom Under-Secretary for security and counter-terrorism, saying that a cyber attack that took out a power station would be an act of war,[95] and by Estonian Defense Minister, who equated cyber blockades to naval blockades on ports preventing State's access to the world.[96] From these examples is it clear that States desire and are inclined to treat cyber attacks as armed force.

Certain cyber attacks (CNA), which are specifically intended to cause physical damage to tangible property (e.g., creating a hammering phenomenon in oil pipelines so as to cause them to burst) or injury or death to human beings (e.g., shutting down power to a hospital with no back-up generators) can be easily categorized as use of armed force and therefore easily included in the prohibition. Therefore, armed coercion is not defined by whether or not kinetic energy is employed or released, but rather by the nature of the direct results caused, specifically physical damage and human injury. The fact that a cyber attack (CNA) employs electrons to cause a result from which destruction or injury directly ensues is simply not relevant to characterization as armed force.

The above mentioned category of cyber attacks (CNA) is quite narrow and limited. A more problematic category of cyber attacks (CNA) are those which actually do not cause physical damage or injury, or do so indirectly. How should those be classified under the prohibition on the use of force? Because up till now the international community did not manage to create a new international legal system to deal with cyber warfare, we have to view cyber attacks (CNA) through the existing paradigm of use of force. We need to comeback to the term of "force". From the previous paragraphs it can be seen that the controversy over the term was not whether the concept was limited to "armed force", but rather if it included economic, and by proxy political, coercion. The qualifier "armed" was needed to counter any argument for extension of the concept of "force". And at that time cyber warfare was not contemplated at all,

---

Times// http://www.nytimes.com/2010/04/16/science/16cyber.html, accessed 2011-03-17.

93 P. A. Johnson. Is it Time for a Treaty on Information Warfare? in M. N Schmitt, B. T. O'Donnell. Computer Network Attack and International Law. 2001. P.187.

94 Quote from the speech of a senior Russian military officer, reported in: V. M. Antolin-Jenkins. Defining the Parameters of Cyberwar Operations: Looking for Law in all the wrong places?// Naval Law review. 2005, Nr.51. P.132.

95 J. Doward. Britain fends off flood of foreign cyber-attacks. The Observer// http://www.guardian.co.uk/technology/2010/mar/07/britain-fends-off-cyber-attacks, accessed 2011-03-17.

96 North Atlantic Treaty Organization (NATO) Parliamentary Assembly. 173 DSCFC 09 E bis – NATO and Cyber Defence. 2009. Para.59// http://www.nato-pa.int/default.asp?SHORTCUT=1782, accessed 2011-03-17

therefore there was no need to look beyond armed force in it's simplest sense. However, International Court of Justice (ICJ) in the Nicaragua Case[97] has determined, in what was tantamount to an application of agency theory, that force apparently includes actively and directly preparing another to apply armed force, but not merely funding the effort:

"While arming and training of the contras can certainly be said to involve the threat or use of force against Nicaragua, this is not necessarily so in respect of all assistance given by the United States Government. In particular, the Court considers that the mere supply of funds to the contras, while undoubtedly an act of intervention in the internal affairs of Nicaragua... does not itself amount to a use of force."

ICJ was not actually applying UN Charter Article 2(4) *qua* 2(4). The application of the Charter was barred by the U.S. acceptance of jurisdiction (pursuant to Article 36(2) of the ICJ's Statute) only on the condition that all States involved in the case be party to any multilateral treaty used by the Court to adjudicate the issue. Therefore, the Court applied the customary international law prohibition on the resort to force.

However, from this ruling we can still deduce that other forms of force are not necessary excluded from the concept of "force" of Article 2(4). This in turn gives us two opposites of the spectrum: economic and political coercion on one end, which falls out of the use of force prohibition, and armed force, which does fall withing the prohibition, on the other. Therefore, the line of use of force lies somewhere between those two opposites. Economic and political coercion can be delimited from the use of armed force by reference to various criteria.

There has been developed several analytical models to deal with such unconventional uses of force as cyber attacks (CNA's) in order to ease attack classification and to help put the classic already scope, duration and intensity analysis into more concrete terms. There are three main models:

- instrument-based,
- consequence-based (or alternatively referred to as: effects-based),
- strict liability.

Instrument-based approach. Here it is checked whether the damage caused by a new attack method previously could have been achieved only with a kinetic attack. For instance a cyber attack is used to shutdown a power grid. It is automatically qualified as an armed attack. This is because previously shutting down a power grid required typically dropping a bomb on a power station or some other kinetic use of force to incapacitate the grid. Since conventional

[97] Military and Paramilitary Activities in and against Nicaragua (Nicaraguea v. U.S.). ICJ Reports 1986. P.119.

munitions were required to achieve the same result, a cyber attack under this approach is treated as if it was kinetic.

Consequence-based approach. Here a cyber attack's similarity to a kinetic attack is completely irrelevant and the focus altogether shifts to the overall effect that the cyber attack has on a victim-State. For instance, a cyber attack that manipulated information across a State's banking and financial institutions to seriously disrupt commerce in the State is an armed attack. The manipulation of information does not resemble a kinetic attack, as required under an instrument-based approach, but the disruptive effects that the attack had on the State's economy is a severe enough overall consequence that it warrants treatment as an armed attack.

Strict liability approach. Here cyber attacks against critical infrastructure are automatically treated as armed attacks, due to the severe consequences that can result from disabling those systems. This approach has been proposed by W. G. Sharp Sr[98] in order to justify anticipatory self-defense before any harm comes from a potential cyber attack. Reasoning behind this approach is the speed at which cyber attacks operate and that a mere computer breach can quickly escalate into a major destructive attack against defense critical infrastructure and cause harm of extreme scope, duration, and intensity.

Scholars agree that of all the methods mentioned, the consequence-based approach is most suitable to deal with cyber attacks.[99] Consequence-based approach can account not only for situations that the instrument-based approach covers, but it also provides a base for cyber attacks that cannot be equated easily to kinetic attacks. Instrument-based approach is satisfied under the consequence-based approach because results of cyber attacks mirror results previously achievable only with kinetic force. Consequence-based approach is also superior to the strict liability approach, which has its share of legal pitfalls. Responding to cyber attacks with under the consequence-based approach is in conformity with international legal norms and customs, whereas responding with force under the strict liability approach a victim-State might violate *jus ad bellum.*

M. N. Schmitt, an advocate of the consequence-based model, has advanced the most useful analytical framework for evaluating cyber attacks. In his seminal article "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework"[100], M. N. Schmitt lays out six criteria for evaluating cyber attacks as armed attacks:

---

98 Sharp W. G. CyberSpace and the Use of Force. Falls Church: Aegis Research Corp. 1999

99 See supra note 1,2.

100 See supra note 1.

Severity: Armed attacks threaten physical injury or destruction of property to a much greater degree than other forms of coercion. Physical well-being usually occupies the apex of the human hierarchy of need.

Immediacy: The negative consequences of armed coercion, or threat thereof, usually occur with great immediacy, while those of other forms of coercion develop more slowly. Thus, the opportunity for the target State or the international community to seek peaceful accommodation is hampered in the former case.

Directness: The consequences of armed coercion are more directly tied to the actus reus than in other forms of coercion, which often depend on numerous contributory factors to operate. Thus, the prohibition on force precludes negative consequences with greater certainty.

Invasiveness: In armed coercion, the act causing the harm usually crosses into the target State, whereas in economic warfare the acts generally occur beyond the target's borders. As a result, even though armed and economic acts may have roughly similar consequences, the former represents a greater intrusion on the rights of the target State and, therefore, is more likely to disrupt international stability.

Measurability: While the consequences of armed coercion are usually easy to ascertain (e.g., a certain level of destruction), the actual negative consequences of other forms of coercion are harder to measure. This fact renders the appropriateness of community condemnation, and the degree of vehemence contained therein, less suspect in the case of armed force.

Presumptive Legitimacy: In most cases, whether under domestic or international law, the application of violence is deemed illegitimate absent some specific exception such as self-defense. The cognitive approach is prohibitory. By contrast, most other forms of coercion—again in the domestic and international sphere--are presumptively lawful, absent a prohibition to the contrary. The cognitive approach is permissive. Thus, the consequences of armed coercion are presumptively impermissible, whereas those of other coercive acts are not (as a much generalized rule).

Taken together, these criteria allow States to measure cyber attacks along several different axes. While no one criterion is decisive, cyber attacks that satisfy enough criteria can be characterized as armed attacks. Since their publication in 1999, M. N. Schmitt's criteria have gained traction in the legal community, with several prominent legal scholars advocating for their use.[101] Many hope that M. N. Schmitt's criteria will help bring some uniformity to State efforts to classify cyber attacks. However, until these criteria gain wider acceptance, States are

[101] Ibid.

likely to classify cyber attacks differently, depending on their understanding of armed attacks as well as their conception of vital national interest.

Despite M. N. Schmitt's created criteria being back up by legal scholars,[102] there are opponents[103] with claims of serious flaws in Schmitt's framework for analyzing cyber warfare under Article 2 (4) of the UN Charter. Matthew Hoisington has compiled the views of several other authors[104] who reproach M. N. Schmitt's position. Their view is that by using presumptive legitimacy as a factor, M. N. Schmitt's approach requires determining the legitimacy of an attack under international law by asking whether the attack is legitimate. In effect, the approach is backwards. Furthermore, unlike other types of warfare, instances of cyber warfare cannot be assessed readily at the time of the attack to determine their magnitude and the permitted responses. This problem will arise with any framework that requires an *ex post* analysis.

Valid points have been presented, however the author of the current work nonetheless supports M. N. Schmitt. There are alternatives to his approach, but those are even easier discarded, more faulty. Because of this, it is need to fall back on the best option available due to lack of better suggestions even from the opposing authors. On one hand, arguments of M. Hoisington and others are very much on point in the context of self-defense under Article 51 of the UN Charter, where rapid reaction is needed. On the other hand, M. N. Schmitt's criteria have the potential to work very well in the context of *jus ad bellum* as presented in the previous paragraphs of this section. More on the subject of self-defense is going to be covered in the subsequent section 2.3.

2.2.2 Attribution of the cyber attack (computer network attack) to a State

According to the U.S. DoD:

"State sponsorship may be convincingly inferred from such factors as the State of relationships between the two countries, the prior involvement of the suspect State in computer network attacks, the nature of the systems attacked, the nature and sophistication of the methods and equipment used, the effects of past attacks, and the damage which seems likely from future attacks."[105]

---

[102] See supra note 4.

[103] See supra note 9.

[104] See supra note 94. P.172; J. Barkham. Information Warfare and International Law on the Use of Force// New York University Journal of International Law and Politics. 2001, Nr34. P.86-87; E. T. Jensen Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self Defense// Stanford Journal of International Law. 2002, Nr.38. P.239-240.

[105] Department of Defense Office of General Counsel. An Assessment of International Legal Issues In Information Operations. 1999. P.21-22.

This is however too vague and according to M. Roscini[106] the proper answer should be searched for in the Articles on the Responsibility of States for internationally Wrongful Acts (Articles on State Responsibility).[107] Keeping this in mind several groups can be identified.

Although details of State military cyber capabilities are obviously classified, nonetheless it appears that several national armies have already established cyber units: China – cyberspace battalions and regiments[108], Israel – soldiers working in Internet Warfare team[109], U.S. – Cyber Command[110], Germany – Department of Information and Computer Network Operations[111], Italy – considers establishing it's own cyber unit[112]. These are the "uniformed" hackers. This is the easiest group. It is clear that conduct of such "uniformed" hackers will be attributed to the State of which they are *de jure* organs.[113] Moreover, their status is completely irrelevant, whether they are civilian or military, the conclusion would be the same. Such hackers could be members of independent agencies or privatized corporations or independent contractors, nonetheless they are empowered by law to exercise some degree of governmental authority and thus their conduct can be easily attributed to the State, provided that "the person or entity is acting in that capacity in the particular instance"[114]

Hackers do not necessary need to be *de jure* organs in order to attribute their actions to States. They might be individuals or even corporations hired by States to conduct cyber attacks on their behalf.[115] According to Article 8[116] the individuals must be acting under "instructions of, or under the direction or control of, that State in carrying out the conduct." There is however case law based established two attribution standards. ICJ in the Nicaragua case[117] has established an "effective control" test, which requires the State in question not only to have helped by planing, financing, organizing, training, supplying and equipping their proxies, but to actually have control over them during the time of violations. The other test is "overall control", adopted

---

106 See supra note 7.
107 Articles on the Responsibility of States for internationally Wrongful Acts// Yearbook of International Law Commission. /ed. International Law Commission. 2001. Vol.II, Part Two.
108 S. M. Condron Getting it right: Protecting American critical infrastructure in cyberspace// Harvard Journal of Law and Technology. 2007, Nr.20. P.373.
109 D. Eshel. Israel adds cyber-attack to IDF// www.military.com/features/0,15240,210486,00.html, accessed 2011-03-17.
110 P. Beaumont. U.S. appoint first cyber warfare general// The Observer, 2010 May 23// http://www.guardian.co.uk/world/2010/may/23/us-appoints-cyber-warfare-general, accessed 2011-03-17.
111 J. Hoetz, M. Rosenbach, A. Szandar. War of the Future – National Defense in Cyberspace// Spiegel Online, 2009 Feb 11// http://www.spiegel.de/international/germany/0,1518,606987,00.html, accessed 2011-03-17.
112 T. Kington. Italy weighs cyber-defense command// Defense News, 2010 May 31// www.defensenews.com/story.php?i=4649478, accessed 2011-03-17.
113 See supra note 107. Art.4.
114 Ibid. Art.5.
115 J. A. Ophardt. Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield// Duke Law and Technology Review. 2010, Nr.3.
116 See supra note 107. Art.8.
117 See supra note 97.

by the International Criminal Tribunal for the former Yugoslavia (ICTY). It said that taking into account the factual circumstances the degree of control may be different, therefore it provided a more lax test[118]. Under it the requirement is only for the State to play a role in organization, coordination and planing in addition to financing, training, equipping or supporting their proxies, irrespective of any instructions provided by the State. But which of these is most appropriate for cyber attacks (CNA)? S. J. Shackelford[119] is of the opinion that "overall control" is better because of it's clandestine nature and technical difficulties of identifying the authors of attacks. However, for the exact same reasons "effective control" should be preferred, with a more lax test there is a chance that victim States might accuse other States of cyber attacks that they did not commit and were unaware of. It is hard to agree with Shackelford. Such careless accusations and possibly even preemptive or anticipatory use of force might lead to a situation where the victim-State itself is going to be in breach of *jus ad bellum* because its use of force was wrongful. M. Roscini also points out a possibility of faulty thinking on part of S. J. Shackelford. In the sense that, the ICTY adopted "overall control" test applies only to organized and hierarchically structured groups, such as military units or, in case of war, armed bands of irregulars or rebels.[120] Organized and hierarchically structured cyber insurgents do not seem to exist yet, although there are speculations of such armed groups as Hamas to have hired cyber criminals to conduct cyber operations.[121] However unlikely the possibility of emergence of such cases in the future is quite possible or not certainly known to exist to us at the moment. ICTY retains the view of ICJ in cases of unorganized, non-military and non-hierarchical groups of individuals who, on orders by their home State, commit illegal acts in another State, that "effective control" applies.

There might be cases when hackers are neither *de jure* nor *de facto* State organs. In such cases actions of such hackers could have been incited by State agents via websites, blogs, chat rooms, forums etc. This was very obvious during attacks on Estonia in 2007 and Georgia in 2008, with tools and instruction how to attack both widely accessible to virtually anyone.[122] Unfortunately the Articles on State Responsibility do not provide any regulation of incitement. In respect to the previous paragraph, such incitement might be able to constitute "direction or control" of a State (Article 8). However there is a possibility that after incitement of actions a

---

[118] ICTY. Prosecutor v. Tadic, Case No. IT-94-1-A. Appeals Chamber, Judgment. 1999-07-15. Para.137

[119] See supra note 4. P.235.

[120] See supra note 118. Para.120.

[121] J. A. Lewis. The "Korean" Cyber Attacks and Their Implications for Cyber Conflict// Center for Strategic and International Studies, 2009 Oct 23// http://csis.org/publication/korean-cyber-attacks-and-their-implications-cyber-conflict, accessed 2011-03-17.

[122] E. Tikk, K. Kaska, K. Rünnimeri and others. Cyber Attacks Against Georgia: Legal Lessons Identified// Cooperative Cyber Defence Centre of Excellence (CCDCOE) Report. 2008// http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf, accessed 2011-03-17.

State may publicly endorse them. As was in the case of the Hostages case.[123] ICJ ruled that an initial attack on the U.S. Embassy in Teheran was not attributed to Iran, but by endorsement of such actions by Iranian authorities transformed the occupation of the embassy and detention of the hostages in acts of the State. This is backed up by Article 11.[124] However, public acknowledgment of cyber attacks by States or their agents is highly unlikely – cyber attacks are perfect tools for covert operations.

Last group is a case when cyber attacks originate from computers located in a certain State without any State involvement. Such cyber attacks cannot be attributed to the State. However the State might still bear some responsibility. The State did not take necessary and reasonable measures to prevent or stop the cyber attacks originating from their territory. This can be done swiftly and painlessly simply by disabling Internet access to the attackers, or more precisely to the offending computers, because attacked might be on the other side of the globe. The State's wrongful act would be not the cyber attack, but the breach of it's obligations. UN GA recommends in one of its resolutions that states should ensure "that their laws and practice eliminate safe havens for those who criminally misuse information technologies."[125] In the case of recent Estonian and Georgian attacks, the involvement of the Russian Federation was not established, however the government has tolerated the cyber attacks that have originated from their territory. Moreover, the Russian Supreme Procurature has declined the Estonian request for cooperation under the Mutual Legal Assistance Treaty (MLAT) between the two countries.[126]

With such toleration of cyber attacks by States, additional issues of responsibility arise as pointed out by J. A. Lewis in his brief note[127]**.** According to J. A. Lewis cyber attacks raise what can be called the "overflight" issue. Almost all cyber exploits require traversing third country networks to reach their target. Few States now have knowledge as to what passes through their territory, or what the intent of that traffic may be, due to the covert or clandestine nature of these cyber attacks. Attacks are disguised as legitimate commercial traffic that is permitted to cross frontiers under existing commercial law and agreements among service providers. This could be interpreted as a violation of sovereignty unless the attacker asked permission to transit the network en route to an attack. Depending on the circumstances, harboring and support of terrorists may breach a number of a State's international obligations under treaties, customary international law, and Security Council resolutions. To begin with,

[123] U.S. Diplomatic and Consular Staff in Tehran (U.S. of America v. Iran), ICJ Reports 1980
[124] See supra note 107. Art.11.
[125] UN GA A/RES/55/63 of 2000-12-04. Para.1(a).
[126] Russia Refused Legal Assistance in Cyber Attacks Investigation// Estonian Review. Vol.17, Nr.27, 2007 Jul 4-10
[127] J. A. Lewis. A Note on the Laws of War in Cyberspace// Center for Strategic and International Studies, 2010 Apr// http://csis.org/publication/note-laws-war-cyberspace, accessed 2011-03-17.

States should not knowingly allow anyone to use their territory in a way that endangers other States, including as a base for attacks.[128] In a way, this obligation can be applicable to cyber attacks as well.

2.3 Right of self-defense against a cyber attack (computer network attack)

The right to self-defense is inherent to every State, however when does one resort to it's use against a cyber attack (CNA) and what is the extent of an appropriate response, without overstepping the allowed boundaries, when a State does not even know who is attacking it.

There are two exceptions to the prohibition on the use of force Under the UN Charter:

- Security Council action pursuant to article 42, and
- an individual or collective self-defense under article 51.

Article 42 does not cause much trouble in applying and understanding it, it is straightforward. Whereas Article 51 is not that simple. The scope of Article 51 is the main source of controversy among scholars.[129] The article reads as:

"Nothing in the present Charter shall impair the inherent right of individual or collective self-defense 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. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security."[130]

Some scholars are interpreting this article in a restrictive manner, claiming that a State may not respond with self-defense unless it has suffered an armed attack. UN Security Council (UN SC) shares the same view. This of course means that a State may not act in anticipation of an immediate attack. The international community however is leaning in the opposite, counter-restrictionist, direction, saying that in certain circumstances it may be lawful to use force in advance of an armed attack. Scholars supporting the latter opinion argue that Article 51 incorporates customary international law as articulated by the Caroline doctrine, allowing anticipatory self-defense.[131] As defined by then Secretary of State, D. Webster in the Caroline

[128] The Corfu Channel (United Kingdom v. Albania). ICJ Reports 1949, Merits. P.22.
[129] See supra note 104, 108.
[130] UN Charter. Art.51.
[131] British-American Diplomacy. The Caroline Case// http://avalon.law.yale.edu/19th_century/br-1842d.asp, accessed 2011-03-17.

case, this point in time occurs when the "necessity of that self-defense is instant, overwhelming and leaving no choice of means, and no moment for deliberation."

2.3.1 Right to self-defense (under United Nations Charter Article 51)

A State response to a cyber attack that amounts to an armed attack must meet three principles to qualify as self-defense[132]:

- necessity;
- proportionality;
- immediacy.

Necessity. The use of force is a means of last resort and all other available means have failed or are likely to fail. As a minimum, it implies an obligation to identify and author, verify that the cyber attack is not an accident and that the matter cannot be settled by less intrusive means.

Proportionality. The force used in the response must be proportional to the original attack. However simple that might be, it's not that easy and an equal "payback" might be hampered by such matters as: a victim-State does not have the appropriate technology to conduct cyber operations or because the aggressor does not have a sufficiently developed computer network to hit for example.

Immediacy. It prohibits a response from occurring after too much time has passed after the original attack. It also reflects the fact that the underlying purpose of this principle is not to punish the attacker, but rather to repel an armed attack. In cases of cyber attacks this principle should be applied flexibly. An adversary might use logic or time bombs, the actually damage would altogether occur well after the original cyber attack. Additionally, if a State's military computer network becomes incapacitated by a cyber attack, it might take some time before the State is ready to react in self-defense.

Cyberspace creates opportunities for attacker anonymity and possibility of remote attacks, thus there is a high chance that the perpetrators of cyber attacks are likely to go unidentified at the moment of attack. In order to respond with force, a victim-State must first identify the attacker's intentions as hostile. However, due to the speeds at which cyber attacks operate, which are near instantaneous[133], unlike conventional kinetic warfare, evaluation of cyber attacks (CNA) for a victim-State on the spot are incredibly difficult. There is simply not enough

[132] Y. Dinstein. War, aggression and self-defense. New York: Cambridge University Press. 2005. P.208-211.
[133] S. Brenner. At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare// Journal of Criminal Law and Criminology. 2007, Nr.97. P.379.

time and the victim-State is therefore denied the opportunity to preemptively contemplate a proper response altogether. Attribution is needed to ensure that a State does not target an innocent person or place by using force in self-defense. Furthermore, it's necessary to determine who the attacker is due to the fact that the law governing permissible response varies depending on if the attacker a State or a non-State actor. This distinction is important because the already discussed Article 2(4) of the UN Charter on prohibition on the use of force applies only to States and not to individuals. This means that States are prevented under international law from threatening or using force against each other, while similar acts committed by individuals fall under domestic criminal laws.

Summarizing the above, it seems that it is not easy to satisfy the given three principles in the context of cyber attacks (CNA). We have the conditions for activation of self-defense under Article 51, generally speaking they can be fulfilled and the right of self-defense can be applied. However, the reality is that the test ultimately fails at the very beginning, not being able to formally satisfy the necessity principle. It's possible that the necessity principle would be satisfied if given enough time, but coupled with immediacy principle it becomes irrelevant, because the use of force in self-defense would not have been used in time, thus preventing it's use at all. The principle of proportionality plays a minor role, because if a State is considering this principle it must have satisfied the necessity principle and is contemplating the adequate force to be used in self-defense. It is difficult to propose anything more concrete at this point. In conclusion, it seems that although a legal basis exists, our technological advances are not adequate enough to facilitate a timely response to a cyber attack in order to be able to take advantage of Article 51. The author's opinion is that at the current juncture in time, it is not technologically possible to properly invoke Article 51 of the UN Charter.

There is however a difference of opinion between scholars, a significant enough difference that can change the conclusions made in the previous paragraph. Y. Dinstein[134] and M. Roscini[135] are requiring that all three previously mentioned principles must be met in order to qualify for use of self-defense; anticipatory self-defense is explained via the same principles along with Caroline doctrine.[136] Whereas the groundbreaking opinion belongs to J. Carr[137], who requires only two of the three principles to be satisfied for self-defense: necessity and proportionality, and all three, of which immediacy principle receives special treatment, because he attributes it to anticipatory self-defense only. Anticipatory self-defense is going to be looked

[134] See supra note 132. P.207
[135] See supra note 7. P.120.
[136] See next section 2.3.2 on Anticipatory self-defense
[137] See supra note 2. P.56.

into in the next section 2.3.2, at this point it is irrelevant to the argument. What is relevant is the reasoning behind the differences in opinion, which is not clear. If we would rethink our previously made conclusions within the new frame provided by J. Carr, we would have to without a doubt proclaim that there is nothing stopping States, after satisfying the two relevant principles, from being able to use Article 51.

2.3.2 Right to an anticipatory self-defense

In cases when cyber attacks (CNA) do not yet reach the threshold of an "armed attack", a State might invoke anticipatory self-defense against an imminent attack via conventional means that the cyber operations are only preparing for. The situation was very similar during the Russian-Georgian conflict in 2008. Before the invasion certain Georgian governmental websites have been already targeted, crippling communication from the Georgian government.[138]

The only question is how imminent an armed attack must be, because this determines whether the reaction is anticipatory or preventive. This wording should not be confused with the doctrine of preventive self-defense, which has no basis in international law, either customary or conventional.[139] However, in this sense, "anticipatory" is referring to self-defense against imminent attacks, whereas "preventive" is against non-imminent attacks. The terminology used by M. Roscini is controversial, the author admits it. Such segregation and creation "preventive self-defense" might be even redundant, since this "type" of self-defense by definition coincides with self-defense under Article 51 of the UN Charter. Rationale behind this is that, if an attack is not immediate, therefore it either has already happened giving rise for self-defense under Article 51, or alternatively it "subsided" and never took place.

Focusing on anticipatory self-defense only, the right to exercise it against an imminent armed attack is consistent with both customary international law and Article 51.[140] Textually looking at the article is seems to require for an armed attack to "occur", however, according to Article 32 of the 1969 Vienna Convention on Law of Treaties, the application of criteria entrenched in Article 31 should not lead to an interpretation which is "manifestly absurd or unreasonable". Surely, it is unrealistic to expect of a State to wait for an attack to commence before acting. The whole point of self-defense is to prevent an armed attack. Recalling the already mentioned Caroline doctrine: if danger is "instant, overwhelming, leaving no choice of

[138] supra note 122. P.4-5,15.
[139] A. Cassese. International Law. Oxford University Press. 2005. P.361.
[140] Report of the Secretary-General, A/59/2005. In larger freedom: towards development, security and human rights for all. 2005. P.33

means, and no moment for deliberation"[141], the victim-State is entitled to invoke the right of self-defense. M. N. Schmitt has given us yet another test, which is a reasonable application of the Caroline doctrine in the context of cyber attacks (CNA). In order to establish a right to respond in anticipatory self-defense against a cyber attack that does no amount in itself to an armed attack under Article 51, we must consider these three factors[142]:

1. the cyber attack (CNA) is part of an overall operation culminating in armed attack;

2. the cyber attack (CNA) is an irrevocable step in an imminent (near-term) and probably unavoidable attack; and

3. the defender is reacting in advance of the attack itself during the last possible window of opportunity available to effectively counter the attack.

Let's consider the imminent character of a cyber attack (CNA): it depends on the intensity of the attack, the target of the attack, the reaction time required in order to successfully preempt the attack, and the speed with which the damage may move throughout the computer networks."[143] The defensive reaction should also be proportionate, however not to the cyber attack, but rather to the overall attack of which the cyber attack is a preliminary part. By same rationale the self-defense attack does not have to be against the facility that launched the cyber attack (CNA) or not even designed to counter the current or other cyber attacks (CNAs).[144]

Legal scholars however have put forward certain new concepts, which do not fundamentally change the existing framework of *jus ad bellum* but which try to remedy the regulation of the still novel threat of cyber attacks (CNA). W. G. Sharp, for example, has proposed that all States should adopt a rule of engagement that allows them to use force in anticipatory self-defense against any identified State that demonstrates hostile intent by penetrating a computer system which is critical to their respective vital national interests.[145] This is an interesting approach that has some merit to it, although the direction of this idea is proper indeed, there might still be a better solution. M. Hoisington suggests to skip the attribution and characterizing of a cyber attack altogether. Because State survival may depend on an immediate, robust, and aggressive response, international law should not impose inflexible and outdated requirements on States to fully satisfy the traditional necessity requirements when acting in self-defense of vital State interests. International law should afford protection for States acting in

[141] See supra note 131.
[142] See supra note 1. Computer Network Attack... P.28
[143] C. C. Joyner, C. Lotrionte. Information Warfare as International Coercion: Elements of a Legal Framework// European Journal of International Law. 2001, Nr.12. P.860.
[144] See supra note 142.
[145] See supra note 98. P.130.

cyber self-defense who initiate a good-faith response to an attack. The law should evolve to recognize a State's inherent right to self-defense, including anticipatory self-defense, in response to a cyber attack, especially when the attack targets critical national infrastructure.[146] He continues by providing an idea how to incorporate his view as an exception to the rule governing use of force: that the international community should create a list of critical national infrastructures that a State may protect with active defensive measures.

However the above views cannot be accepted and are inherently illogical according to M. Roscini.[147] One can hardly disagree with such a statement. It is difficult to imagine at whom the reaction in self-defense is going to directed, if it has not yet been established where the attack is coming from or to whom it can be attributed. The U.S. DoD shares the same opinion and rejects such views arguing that "the international law of self-defense would not generally justify acts of "active defense" across international boundaries unless the provocation could be attributed to an agent of the nation concerned, or until the sanctuary nation has been put on notice and given the opportunity to put a stop to such private conduct in its territory and has failed to do so, or the circumstances demonstrate that such a request would be futile."[148]

To clarify, critical national infrastructure is a term used by governments to describe assets that are essential for the functioning of a society and economy, these include core facilities such as:

- electricity generation, transmission and distribution;
- gas production, transport and distribution;
- oil and oil products production, transport and distribution;
- telecommunication;
- water supply (drinking water, waste water/sewage)
- agriculture, food production and distribution;
- heating (e.g. natural gas, fuel oil, district heating);
- public health (hospitals, ambulances);
- transportation systems (fuel supply, railway network, airports, harbors, inland shipping);
- financial services (banking);
- security services (police, military);
- chemical and nuclear industry;

[146] See supra note 9. P.453
[147] See supra note 7. P.119.
[148] See supra note 105. P.21.

– space and research.[149]

This is however a non-exhaustive list, as prescribed by the UN GA, each country has to determine it's own critical information infrastructures.[150] The term "critical information infrastructures" is used in relation to cyber attacks, however cyber attacks are actually far more reaching than just critical information infrastructures, therefore the term encompassing the whole infrastructure is more appropriate: "critical (national) infrastructure". There is no internationally agreed definition as to what "critical (national) infrastructure", as a general term, of a State actually is. M. Hoisington tried to remedy this situation by proposing a "global" list of critical infrastructures that deserve protection. Attempts at exploring additional venues seem to not bear any fruit, since we are still at the conclusion that self-defense response to a cyber attack is practically not possible.

In conclusion, a right to anticipatory self-defense exists only exclusively against a conventional attack preceded by or with a cyber attack (CNA) component. Additionally, attacks on a nations' critical (national) infrastructures, if clearly attributable to a State agent or a State that does not take measures to prevent the attacks, can also give rise to anticipatory self-defense.

2.3.3 Right to self-defense (under customary international law)

In the Nicaragua case, the ICJ acknowledged that there is no complete relation between the customary international law rules and the use of force and the relevant provisions of the UN Charter and that the customary international law continues to exist and to apply, separately from international treaty law, even where the two categories of law have identical content.[151] Because the two can exist and apply separately it is relevant to see if there is any customary international law relating to cyber warfare or cyber attacks (CNA).

M. Roscini[152] provides us with an opinion of M.N. Schmitt that cyber attacks (CNA) are still a relatively new phenomenon and no custom or State practice has emerged.[153] Roscini however disputes this opinion, an opinion which is ten years old. Cyber attacks might be as old as computer networks, however even despite that, their significance, potential threat and ease of

[149] Commission of The European Communities. Green Paper on a European Programme for Critical Infrastructure Protection. 2005// http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0576:FIN:EN:PDF, accessed 2011-04-15
[150] UN GA A/RES/58/1999 of 2003-12-30.
[151] See supra note 97.
[152] See supra note 7. P.39.
[153] See supra note 1. Computer network attack... P.22.

access have become evident only recently in comparison. Setting that aside, the argument that a phenomenon such as cyber attacks did not have time to evolve into a custom or that States did not develop a practice is not valid and easily discarded. "The passage of only a short period of time is not necessarily, or of itself, a bar to the formation of a new rule of customary international law".[154] According to the International Law Association (ILA) "some customary rules have sprung up quite quickly: for instance sovereignty over air space, and the regime of the continental shelf, because a substantial and representative quantity of States practice grew up rather rapidly in response to a new situation"[155] It is evident that time is not an issue. Concrete State practice is however harder to find, nevertheless *usus* as part of a custom also includes "verbal acts, and not only physical acts, of States", "diplomatic statements (including protests), policy statements, press releases, official manuals (e.g., on military law), instructions to armed forces, comments by governments on draft treaties, legislation, decisions of national courts and executive authorities, pleadings before international tribunals, statements in international organizations and the resolutions those bodies adopt".[156] Interpreting State practice means looking at what States say, not necessarily even at what they do.[157] "The role of usage in the establishment of rules of international customary law is purely evidentiary: it provides evidence on the one hand of the contents of the rules in question and on the other hand of the *opinio juris* of the States concerned. Not only is it unnecessary that the usage should be prolonged, but there need also be no usage at all in the sense of repeated practice, provided that the *opinio juris* of the States concerned can be clearly established."[158] Therefore actual practice is also not an issue.

Certain States have expressed their opinions in regard to the issue of self-defense in response to a cyber attack. Such practice should be "extensive and virtually uniform" according to ICJ, regardless of how short the period in question is.[159] Creation of many rules of customary international law has been dominated by State practice of powerful States. However this circle might grow even smaller once we consider only States who have a stake in an issue. The ILA Report[160] on the formation of customary international law also points out that the extensive character of State practice is more a qualitative than a quantitative criterion. When all major interests, especially the affected States, are represented, it is not necessary for a majority of all

[154] North Sea Continental Shelf, ICJ Reports 1969. Para.74.
[155] Statement of Principles Applicable to the Formation of General Customary International Law. International Law Association. Report of the Sixty-Ninth Conference. 2000. P.731
[156] Ibid, P.725.
[157] C. Gray. International Law and the Use of Force. Oxford University Press. 2008. P.418.
[158] Cheng B. United Nations Resolutions on outer Space: Instant International Customary Law?// International Journal of Innovation and Learning. 1965 Nr.5. P.23.
[159] See supra note 154.
[160] See supra note 155, P.737.

States to have participated. An example of this is outer space. Only two States had the technology to exploit it and their convergence facilitated a fast creation of rule of customary international law. By analogy, the same should apply to cyber attacks, so in order to determine existence of State practice we must look at States that have developed military cyber technologies to see whether a "general practice accepted as law"[161] has evolved in the field.

Practical examples of the above are abundant within the U.S. The U.S. are in favor of the right of self-defense against cyber attacks. Their belief to protect the country and nation at any cost is very strong and echoes through nearly all documents relating to this subject. According to U.S. DoD's 1999 Assessment of International Legal Issues in Information Operations, "State-sponsored cyber attacks may well generate the right of self-defense."[162] The Assessment continues, if such assets as air traffic controls systems, banking and financial systems, public utilities, dams or others would be affected by a cyber attack and would result in deaths and property damage, that no one would challenge the State if it concluded that it was a victim of an armed attack, or of an act equivalent to an armed attack. According to the 2003 U.S. National Strategy to Secure Cyberspace, all large scale incidents will be investigated, perpetrators arrested and prosecuted or a diplomatic or even a military response would follow the incident if it were discovered to be State sponsored.[163] "When a nation, terrorist group, or other adversary attacks the United States through cyberspace, the U.S. response need not be limited to criminal prosecution. The United States reserves the right to respond in an appropriate manner.[164]" According to the head of U.S. Strategic Command the U.S. reserves the option to use military force, possibly even nuclear weapons, in response to a disabling cyber attack against U.S. computer networks.[165] A Pentagon official, J. Miller, stated that they would consider means of responding to a cyber attack outside of the cyber domain.[166]

According to one Russian senior military officer, Russia retains the right to use nuclear weapons first against means and forces of information warfare, and then against the aggressor State itself.[167] Also, a new law proposed would give Moscow the authority to define and respond to acts of cyber warfare. According to K. Zenz[168], a Russia specialist at iDefense (infrastructure

[161] ICJ Statute. Art.38(1)(b).
[162] See supra note 105. P.21-22.
[163] U.S. National Strategy to Secure Cyberspace. 2003// http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf, accessed 2011-03-01
[164] Ibid. P.50.
[165] E. M. Grossman. U.S. General Reserves Right to Use Force, Even Nuclear, in Response to Cyber Attack// Global Security Newswire, 2009 May 12// http://gsn.nti.org/gsn/nw_20090512_4977.php, accessed 2011-05-01.
[166] Pentagon: Military Response To Cyber Attack Possible, 2010 May 12, http://www.defensenews.com/story.php?c=AME&i=4623599&s=TOP
[167] See supra note 94.
[168] A senior threat analyst at VeriSign Inc.'s iDefense Labs. VeriSign Inc. is a company that operates a diverse array of network infrastructure, including two of the Internet's thirteen root nameservers, as well as offering a range of

defense) Labs, these statements basically mean that, if it can be determined that a cyber attack of any kind came from the government of another State, it would be able to treat it as an act of war.[169]

United Kingdom on the other hand has not given such strong promises of severe retaliation in case of a cyber attack. 2009 United Kingdom Cyber Security Strategy leaves open every option by saying that "we recognize the need to develop military and civil capabilities, both nationally and with allies, to ensure we can defend against cyber attack, and take steps against adversaries where necessary."[170]

Additionally, we have to consider not only practice of States, but also practice of relevant international organizations, such as the North Atlantic Treaty Organization (NATO), when assessing the existence a rule of customary international law.[171] NATO recognizes that the next significant attack on the Alliance might come down a fibre optic cable[172], however the position of NATO itself or its Member States on the issue of applicability of Article 5 of the treaty in case of a cyber attack is not clear. It's ambiguous at best. When one official completely excludes any military action against a cyber attack, another does not.[173] Although NATO admits to being under cyber attacks against NATO systems, all of them however are below the threshold of political concern. Furthermore, the response to a cyber attack is not being placed under Article 5 but instead under Article 4 of the treaty, which calls upon the members to "consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened."[174] On the other hand, large-scale cyber attacks against NATO's command and control systems or energy grids could warrant consultations under Article 4 and only then could possibly lead to collective defense measures under Article 5.[175] However, whether an unconventional attack such as a cyber attack would trigger the application

---

security services, including managed DNS, Distributed Denial of Service (DDoS) mitigation and cyber threat reporting.

169 McAfee Report. In the Crossfire – Critical Infrastructure in the Age of Cyber War. 2010. P.30// http://img.en25.com/Web/McAfee/NA_CIP_RPT_REG_2840.pdf, accessed 2011-03-05

170 United Kingdom Government. Cyber Security Strategy of the United Kingdom. 2009. P.14// http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf, accessed 2011-02-20.

171 See supra note 155. P.730.

172 NATO 2020: Assured security; Dynamic engagement. Analysis and recommendations of the group of experts on a new strategic concept for NATO. 2010// http://www.nato.int/nato_static/assets/pdf/pdf_2010_05/20100517_100517_expertsreport.pdf, accessed 2011-05-01.

173 NATO agrees common approach to cyber defence, 04 April 2008, http://www.euractiv.com/en/infosociety/nato-agrees-common-approach-cyber-defence/article-171377, accessed 2011-04-15

174 R. B. Hughes. NATO and Global Cyber Defense. in The Bucharest Conference Papers /ed. R. Sheperd. 2008. P.48// http://www.chathamhouse.org.uk/files/11276_bucharest08.pdf, accessed 2011-04-04.

175 See supra note 172. P.45.

of Article 5 of the treaty will have to be decided by the North Atlantic Council, based on the nature, source, scope, and other aspects of the particular security challenge.[176]

From the above we can conclude that State practice in fact exists or at the very least the process of creating a rule of customary international law is ongoing, it is already evident that there is a certain level of State practice and *opinio juris*. Some States choose to entrench that in their legislation, be it as a warning and deterrent to anyone attempting to engage the State or just to show a strong position on the subject, others on the other hand are taking a more restrictive approach, not completely casting away the possibility of a military response or a response outside of the cyber domain, but neither taking a firm stance for or against it. Despite that we have already seen some effective and large-scale cyber attacks, for example, cyber attacks on Estonia, none of them have yet amounted to an act equivalent to an armed attack that would in turn trigger any of the provisions discussed in the current section. The current practice might lead in the years to come to some rules of customary international law directly relating to cyber attacks. Unfortunately at the moment none still exist.

2.4 Legal (combatant) status of cyber attackers (cyber combatants)

Although in some respects timeless, the 1949 Conventions appear in other respects dated. As we have already seen, there is need for expansive interpretation of armed conflict in order for it to give a chance to encompass cyber warfare in the definition. Up until now the Conventions have served us well and have been without a doubt a highly evolutionary body of law, responding and adapting to the sufferings of victims of past wars. However, even the Conventions' approach to their primary function, protecting victims of war, may be showing its age, as majority of the protection afforded by the Conventions is solely tied in with the nationality of a person.[177] In modern armed conflicts, war victims' need for legal protections often has less to do with nationality than in past conflicts, undoubtedly leaving persons in the hands of an enemy outside the scope of the Conventions' protections. For instance, although captured or wounded in intense combat operations with U.S. forces, a number of fighters detained in Afghanistan in 2001 and 2002 were nationals of States not at war with the U.S., including Yemen, Saudi Arabia, and Pakistan.[178] Even greater evidence of poor aging is apparent in matters the Conventions have come to regulate more recently. Despite certain shortcomings

[176] Ibid. P.20.
[177] GC IV. Art.4.
[178] J. Diamond. U.S. Rejects POW Label. Chicago Tribune, 2002 Jan 28// http://articles.chicagotribune.com/2002-01-28/news/0201280167_1_white-painted-school-buses-defense-secretary-donald-rumsfeld-detainees, accessed 2011-03-05.

the Conventions still are treaties in force, which dictate not only treatment in custody of belligerents, but also, according to the 1977 AP I, whether a person is susceptible to lawful targeting and prescribes who is entitled to participate in hostilities – civilians and combatants respectively.

2.4.1 Civilian and combatant statuses

Civilian Status. Quite some time has passed after the Geneva Conventions until States have finally agreed on a widely accepted definition entrenched only in 1977 in the Additional Protocol I. Article 50 of the Protocol says:

"A civilian is any person who does not belong to one of the categories of persons referred to in Article 4(A)(1), (2), (3), and (6) of the Third Convention and in Article 43 of this Protocol."[179]

This is a negative definition, which grants civilian status to all persons not describes elsewhere, this however does no one any good since this article neither describes the civilian status nor gives any criteria for assigning it. The use of such an approach carries two important implications. First, there are only two statuses available under law of war, that is civilian or the class described in the referenced provisions. Second, understanding Article 50 requires familiarity with the referenced provisions, which most scholars and lawyers agree to be describing the combatant class.

Combatant Status. The combination of the above mentioned articles constitutes the most widely accepted definition of combatant class. The existing law did not account for the full range of persons fighting in a modern armed conflict, and therefore 1977 AP I has introduced a new definitional framework for prisoners of war (POW). The Protocol embedded the criteria of its combatant class in this POW framework. AP I defines combatants as "members of the armed forces of a Party to a conflict"[180] and the preceding section elaborates on what are "armed forces":

"The armed forces of a Party to a conflict consist of all organized armed forces, groups and units which are under a command responsible to that Party for the conduct of its subordinates, even if that Party is represented by a government or an authority not recognized by an adverse Party. Such armed forces shall be subject to an internal disciplinary system

[179] AP I. Art.50.
[180] AP I. Art.43(2).

which, inter alia, shall enforce compliance with the rules of international law applicable in armed conflict."[181]

In the subsequent Article 44[182], combatants are to distinguish themselves from the civilian population and carry arms openly during hostilities. These requirements serve the important function of facilitating opposing forces' efforts to limit their attacks to combatants. In regard to tactics employed by guerrilla fighters and insurgents, Article 44 relaxes this distinction criteria when, owing to the nature of hostilities, observance is impracticable.

The GC III actually enumerates six classes of prisoners of war (POW), but the much later AP I and it's negative criteria enumerates only four as being distinct from the civilian class. The four groups constitute classes of POWs generally acknowledged to take active or direct part in hostilities as combatants. These groups include:

- members of the armed forces of a party;[183]
- militia, volunteer corps, and organized resistance movements belonging to a party;[184]
- armed forces of parties to the Conventions not diplomatically recognized by their enemy;[185]
- citizens who respond spontaneously to invasion (*levée en mass)*[186].

There were requests for extending the protection to unconventional fighters or members of resistance movements as long as these groups conducted themselves similarly to volunteer corps. The drafters have struck middle ground and have restricted POW status to resistance movements and groups that adhered to these four criteria:

- being commanded by a person responsible for his subordinates;
- having a fixed distinctive sign visible at a distance;
- carrying arms openly;
- conducting operations in accordance with the laws and customs of war.[187]

These criteria however are not the unique work of the drafters of the Conventions, it can be traced back to 1899, it first appeared in the Second Hague Convention. Interestingly enough, the criteria in the Second Hague Convention employs a broader definition of belligerents than GC III, meaning that the above criteria apply to armies and to volunteer corps.

---

[181] AP I. Art.43(1).
[182] AP I. Art.44(3).
[183] GC III. Art.4(A)(1).
[184] GC III. Art.4(A)(2).
[185] GC III. Art.4(A)(3).
[186] GC III. Art.4(A)(6).
[187] GC III. Art.4(A)(2).

Some legal implications arise from these statuses. Some are clearer than others. In general, civilians enjoy protection from intentional targeting and belligerents must distinguish between civilians and combatants, and may direct attacks only upon the latter ones. It is widely asserted that civilians only forfeit protection from targeting by taking direct part in hostilities and only for such time as they do so.[188] Moreover, because combatant status has been defined by reference to POW, all persons who qualify for combatant status enjoy the protection provided under POW status. Certain civilians, such as contractors and suppliers accompanying armed forces, air crews, and merchant marine crews qualify for POW status if captured.[189] Even civilians who fail to qualify for POW status get protection by virtue of their nationality. In addition, examining AP I Article 43 we can observe that combatants have the right to participate directly in hostilities. Thus, members of the combatant class may not be prosecuted for warlike acts, including killing, that comply with the law of war. It may be concluded that a combatant's right to participate in hostilities is therefore exclusive and under AP I Article 43, by negative implication, it prohibits civilians from engaging directly in hostilities. Despite that, the GC IV Article 5 and AP I clearly anticipate civilian participation in hostilities, even allowing suspension or derogation from protection of persons suspected of participation in hostilities. In addition, positive provisions of international criminal law, such as the grave breaches regime of the Geneva Conventions and the Rome Statute of the International Criminal Court, do not include such an offense as civilian participation in hostilities. Nor has the ICTY produced a conviction for the offense, despite widespread civilian involvement in combat during the war that dissolved Yugoslavia. This can be viewed as a deliberate omission, expressing the will of States to deal with such incidents domestically rather than internationally.

This treaty-based distinction of civilian and combatant could be interpreted as restraining individual conduct as well as the compositions of States' fighting forces. This is not merely a means of classifying individuals upon capture for the purposes of proper treatment, but also as a limit how States organize combat. Furthermore, a State that employ civilians to take direct part in hostilities would be in breach of such limits.

2.4.2 Civilians and cyber attacks (computer network attacks)

Lawyers and scholars assessing the question of civilian participation in CNAs resort almost universally to the GC POW framework and its four combatant criteria outlined above.

[188] AP I. Art.51(3).
[189] GC III. Art.4(A)(4-5).

The following opinions of L. Doswald-Beck, formerly Legal Adviser with the ICRC[190], M. N. Schmitt, of the U.S. Army Marshall Center[191], Major J. R. Heaton, Air Force Lawyer[192], professor S. Brenner[193], D. Brown[194] and professor G. Corn, former Special Assistant to the U.S. Army Judge Advocate General for Law of War[195] shall be provided.

L. Doswald-Beck concludes that rules guiding combatant classification and privileges should be no different in cyber attacks (CNA). It is possible that persons engaging in CNA would be considered civilians who would have no POW status if captured. Her recommendation is to incorporate CNA personnel so a State can avoid such issues. She goes as far as putting the CNA operators in uniforms in anticipation of capture.

According to M. N. Schmitt, civilians participating in CNA that actually or foreseeably could result in injury, death, damage, or destruction would be illegal combatants. Schmitt's advice is simply to employ military personnel for conducting CNAs.

Building further on M. N. Schmitt's work, Major J. Ricou Heaton has provided a view on State practice in regard to use of civilians performing functions relating to combat. State practice is that the prohibition on civilian participation in hostilities is being interpreted narrowly, thus employing civilian contractors and employees to perform functions that might formerly have been regarded as combatant functions. These observation confirm the traditional approach to the question. Despite States' manipulation of the direct participation standard to avoid application of the four combatant criteria, the Geneva POW regime still remains as the most relevant test.

S. Brenner takes a more critical approach to the issue. First, she agrees with Doswald-Beck and Schmitt that Geneva Conventions' framework most likely prohibits civilians from participating in CNA. Secondly, she calls for reassessment of the rules governing participation in hostilities in light of practical realities of CNA today. S. Brenner predicts an inevitable migration of civilians into the conduct of CNAs, unlike with conventional hostilities, civilians can be quite adept at cyber warfare.

---

190 Doswald-Beck. L. Computer Network Attack and the International Law of Armed Conflict. in Computer Network Attack And International Law. /eds. M. N. Schmitt, B. T. O'Donnell. 2002. P.163.

191 See supra note 1. Wired Warfare: Computer... P.187.

192 J. R. Heaton. Civilians at War: Reexamining the Status of Civilians Accompanying the Armed Forces// Air Force Law Review. 2005. Nr.57. P.155.

193 Brenner S. W. Cyberthreats: The Emerging Fault Lines of The Nation State. Oxford University Press. 2009

194 D. Brown. A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict// Harvard international Law Journal. 2006, Nr.57. P.179-187.

195 G. Corn. Unarmed but How Dangerous? Civilian Augmentees, the Law of Armed Conflict, and the Search for a More Effective Test for Permissible Civilian Battlefield Functions// Journal of National Security Law & Policy. 2008, Nr.2. P.257.

In order to account for the erosion of the traditional rationale supporting the provisions on participation in hostilities, S. Brenner hints at the need to adapt the law of war. However, like Schmitt and many others, her suggestions shift focus more to organizational adjustments to national security institutions. Instead of questioning the applicability of the Geneva regime, she in the end suggests creation of a Cyber Security Agency, employing enforcement, intelligence and military personnel.

D. Brown notes that laws of war are not situation specific, that targeting principles of military necessity, proportionality and unnecessary suffering govern all uses of force, whatever the means used. He goes as far as proposing a new cyber convention, yet also incorporating the four POW criteria in this convention's definition of combatant. He ultimately reaches the same conclusion as others, that only armed forces of member States or any other groups meeting the Geneva POW criteria are permitted to conduct cyber attacks (CNAs).

G. Corn, although confirms the use of the Geneva criteria to evaluate the scope of permissible civilian functions, he still departs from the traditional standard. To put it simply, Corn argues that civilians should not be permitted to perform functions regulated by existing law of war. They should be left to armed forces governed by military disciplinary systems and steeped in military culture, battlefield functions are less likely to depart from accepted restraints on the conduct of hostilities. G. Corn's test offers the advantage of looking beyond civilian means of participation and towards more meaningful ends or consequences of civilian acts in conflict. Despite an innovative approach, G. Corn's test remains committed to Geneva POW criteria.

All these example demonstrate that an over century old criteria is still relevant and scholars from various backgrounds nearly in unison resort to its application in order to determine lawful participation in hostilities.

Unfortunately the reality is different from the proposals of scholars and civilians do get employed by States, and certain military functions get outsourced to private companies. Intelligence gathering for example, is key to success of military operations, the more valuable and integrated it is to the targeting process, the greater likelihood that the gatherer is taking direct part in hostilities, in turn he would be subject for evaluation of combatant status. This is not a problematic for military intelligence gatherers such as scouts, but civilians on the other hand if not meeting the criteria would implicate legal concerns connected to civilian participation in hostilities. The argument that intelligence collection, or even intelligence analysis, constitutes taking direct part in hostilities is far stronger when such information increases the destructive effects or lethality of an attack. So even serving as an intelligence agent may constitute direct

participation in hostilities.[196] By analogy, a computer network specialist that performs intelligence gathering can be considered being equivalent to a military scout, especially if information gathered is essential and a military operation would fail otherwise. Regular or real time updates from such a specialist increase his contribution to the CNA and thus look more like direct participation in hostilities. The more his work is integrated with those who actually launch a cyber attack (CNA), the more he resembles a forward artillery observer who directs fire onto an enemy. Another example of civilian involvement would be a CNA weapon designer – a civilian employee whose job is to simply write code. He is responsible for all aspects of the tool that is used in CNA. This designer might be compared to the tank production plant worker or designer of firearms used by soldiers. These categories of people however do not participate directly in hostilities, they are civilians supporting the war effort. Their participation is too remote to be considered as direct.[197] But suppose, if such a programmer is writing the code on the move, he cooperates closely with the previously mentioned computer reconnaissance expect and works directly with the information produced by the expert to adjust the code, to maximize it's effectiveness and minimize it's collateral damage, up to the moment of attack. In such a case the permissible contribution of a civilian to combat might be overstepped and his civilian protection would be greatly jeopardized as a consequence of his activities. Granted, that there is still need for additional evaluation if the actions of the civilian caused actual harm to the personnel and equipment of the enemy armed forces, taking into consideration that this is in fact CNA, various effects, such as degraded service, denial of service, destruction of information, destruction of a computer, destruction of a network of computers, or physically destructive effects, and if any of these have caused any harm.[198] Even further complications would arise in case one person is performing multiple CNA functions – reconnaissance, design and coding of the CNA weapon, and finally "pulling the trigger" and launching the attack.

The analysis of the existing legal base strongly suggests that States employing civilians in many of the roles described above would be in breach of limits on civilian participation in hostilities. Currently, the only legal combatants are only those who meet the POW criteria. Employment of civilians is full of legal pitfalls, with just a few shown above, however these developments to call for a change in the combatant definitions applicable to cyber warfare.

---

[196] M. E. Guillory. Civilianizing the Force: Is the United States Crossing the Rubicon?// Air Force Law Review. 2001, Nr.51. P.111-117

[197] AP Commentary. Para.619.

[198] Ibid.

2.4.3 Adequacy of the four Geneva Convention criteria for cyber attacks (computer network attacks)

Despite the four Geneva Conventions criteria providing clear requirements and easily helping us understand POW and combatant status in general, according to the GC III Article 4(2) this criteria only applies to unconventional belligerents. The criteria do not appear in sections about armed forces or persons accompanying armed forces or *levée en masse*. This appears to be deliberate. In a way, the 1977 AP I addresses this issue by defining armed forces and combatants in consecutive articles and explicitly referring to the criteria. A problem at this point is that the AP I has not received a global ratification. However, the U.S. for example, despite opposing the Protocol, have long regarded it as reflecting customary international law, binding both on parties and non-parties alike.[199] Regardless, this issue is still heavily disputed and most definitely unsettled.

According to S. Watts[200], "while the interpretive case against application of the criteria to the combatant class is unsettled, there are strong arguments for applying the four criteria as a normative matter." Although the four criteria are perfect for traditional warfare, S. Watts raises a question of it being relevant to the new reality of cyber attacks (CNA).

The requirement of a hierarchical chain of command reinforces the idea that war is not an individual pursuit. Chaos of war attracts rioter, looters and other violent elements. Existence of of a command structure eliminates both rogue actors and gives the ability to trace unlawful war acts to respective leaders of belligerent parties from whom reparations can be demanded. Chain of command is also necessary to ensure that operations performed by the armed forces on the battlefield are limited only to military objectives. That subunits and subordinates that are geographically separated, would not take initiative and derogate from the goals set by the State.

The requirement of wearing a distinctive insignia or uniform visible at a distance operates primarily through targeting practices, in order to distinguish legitimate military targets from civilians and their property. According to AP I, combatants must direct their weapons only against specific military objectives[201] and targeting distinction requires that combatants do not employ weapons that are inherently incapable of distinguishing between enemy combatants and

---

[199] Memorandum from W. H. Parks to Mr. J. H. McNeill, Assistant Gen. Counsel, Office of the Secretary of Defense. 1977 Protocols Additional to the Geneva Conventions: Customary International Law Implications. 1986. Reprinted in The Judge Advocate General's Legal Center & School, Law Of War Documentary Supplement /ed. S. Watts. 2006. P388-389.

[200] See supra note 8. P.437.

[201] AP I. Art.51(4)(a),52(2).

civilians.[202] Additionally, combatants have a duty to distinguish themselves from civilians. By complying with this requirement, combat becomes more effective and humane in respect to the protected entities.

The requirement of carrying arms openly operates similarly to the principle of distinction, setting apart belligerents with arms and peaceful civilians.

Lastly, the requirement to conduct military operations in accordance with laws of war. The traditional battlefield is a dangerous place, full of temptations to abuse the innocent – civilians and their property are completely at the mercy of the belligerents. Because of this combatants are subject to military criminal jurisdiction, coupled with good order and discipline it provides a relatively good system of checks against potential inhumane chaos of war.

However, when this criteria first appeared it was quite adequate for waging line-of-sight war, mechanized or air warfare, which expanded and sped up the engagements was not foreseen. The criteria was interned for warfare as it was at the end of the nineteenth century and not how it would evolve later.

Today we have remote means and methods of warfare, and cyber attacks (CNA) are only a subset of such capabilities, the importance of which constantly is growing. Engagements arise between forces that are continents apart. Chances of physically being captured are minimal and traditional temptations associated with presence on a battlefield, such as pillage, looting or abuse of the innocent, are greatly reduced under the conditions of remote warfare. Leaders and commanders can literally be at arms length from the cyber combatant. The implications for the relevance of the four combatant criteria are profound in regard to cyber attacks (CNA).

Line-of-sight combat needs distinction of insignia, uniforms or carrying arms openly, however in light of remote warfare, the appearance of the person attacking has become nearly completely irrelevant. Victims of a cyber attack (CNA) are going to respond to the means and methods of the attack, instead of the traditional combatant, this in turn completely removes the combatant from the battlefield and the distinction equation, making it the greatest advantage.

Command still remains relevant in cyber attacks (CNA) only in a much looser sense. There is no separation from the headquarters of political leadership, therefore cyber combatants are highly unlikely going to have to make autonomous discretionary decisions.

The importance of internal disciplinary system is also fading away. It was relevant for combatants that are on foreign soil, however cyber combatants can be conducting cyber attacks (CNA) from within the territory of their State, where national criminal laws apply. Therefore the

[202] Ibid. Art.51(4)(b).

issues of internal military disciplinary system and civilian responsibility under it are completely mitigated because they're subject to national criminal laws.

State affiliation in regard to cyber attacks (CNA) however plays an important role, even more so than before. In order to resort to the use of force a State has to know it's adversary. State affiliation coupled with principle of distinction gives us an interesting issue that is not easily dealt with and raises some red flags. The concern with principle of distinction lies not with the participants, e.g. civilians, but with their weapons and appearance generated by an attack. Effective cyber attacks (CNAs) are well disguised. It is hardly expected that a State would hold its fire, kinetic or non-kinetic, for long, when faced with a series of cyber attacks (CNAs) against it's critical information infrastructure, which appear to be coming from a civilian server. The State would certainly resort to rationalizing launching an attack on the source as self-defense in the name of protection. Civilian and military networks are already as it is very interconnected and in the future their distinction can become completely meaningless. This is the true challenge for principle of distinction. Cyber attacks (CNAs) routed through civilian server or programmed to appear as though they originated from civilian institutions may in fact constitute a breach of the States duty to bear arms openly in an attack.

In conclusion, it is obvious that the four GC criteria are on the most part almost rendered useless in the context of cyber attacks (CNA), with only some aspects still being able to accommodate the new reality of cyber attacks (CNA), therefore a more adequate system is most definitely needed.

2.5 Is there need for a cyber warfare regulating treaty?

Opinions on the subject are quite varied among scholars and experts, ranging from very enthusiastic “most definitely”, with ideas and proposals of a new cyber warfare regulating treaty, to a quite pessimistic “it is not going to work in reality, even if the treaty gets created” and enters into force.[203]

The analysis so far of works of scholars is showing that despite the fact that the Geneva Conventions can in theory be applied to cyber warfare, albeit by using elaborate and expansive interpretations. The current legal framework is already strained and cannot cover cyber warfare effectively, either by analogizing it to nuclear weapons as new means of warfare as some have tried or in any other way. The drafters of the conventions could not possibly imagine the

[203] E. Fischer. Cyber Warfare – Do We Need a New Geneva Convention? 2011 Apr 8// http://www.army-technology.com/features/feature115500/, accessed 2011-04-25.

technological development which would follow and result in emergence of cyberspace and cyber warfare. Some scholars do actually point out the flaws of the current legal framework and the fact that it is dated, they however refrain from providing radical solutions, such as creation of a new convention, and attempt to make the current system work, to an extent. An even smaller number of scholars is actually resorting to proposing drafts of possible treaties. Such scholars are A. Merezhko[204], a Ukrainian professor of International Law, D. Brown[205], whose proposal and conclusions have already have been reviewed in short in section 2.4.2.

A. Merezhko has developed a project called the International Convention on Prohibition of Cyberwar in Internet. According to this project, cyber war is defined as the use of Internet and related technological means by one State against political, economic, technological and information sovereignty and independence of any other State. The project suggests that the Internet ought to remain free from warfare tactics and be treated as an international landmark. A. Merezhko goes even further stating in the project that the Internet cyberspace is a common heritage of mankind (Article 2 of the proposed convention). This is a very interesting idea indeed, considering the global significance of the Internet cyberspace and the heavy reliance of society on it, its importance simply cannot be denied. The author of this work can only hope that such a regime would be accepted by the international community. If implemented, the threat and unimaginable economic and societal fallout of an actual all out State-on-State cyber war occurring would be permanently eliminated. However enforcing such a complete disarmament in cyberspace can be extremely difficult if not completely impossible, as States' reliance on their cyber capability constantly grows, they would hardly be inclined to forfeit all of those advances. Moreover, the convention leaves out cyber crime and cyber terrorism.

There are also not only opponents of a new cyber warfare treaty, but cyberlaw in general. However before continuing with this line of thought, it's appropriate to point that the opinions on this subject matter are over a decade old and in the opinion of the author of this work should have been discarded as holding no merit to a modern discussion. That said, as it will be shown below, some still do refer to these opinions and hold them relevant.

A term “law of the horse” has been promoted by Frank H. Easterbrook[206] in 1996 in a paper[207] in which he argues against cyberlaw. F. H. Easterbrook's argument is that the best way

---

[204] А.А. Мережко. Конвенция о запрещении использования кибервойны в глобальной информационной сети информационных и вычислительных ресурсов (Интернете)// http://www.politik.org.ua/vid/publcontent.php3?y=7&p=57, accessed 2010-11-02

[205] See supra note 194.

[206] The Chief Judge of the U.S. Court of Appeals for the Seventh Circuit.

[207] F. H. Easterbrook. Cyberspace and the Law of the Horse. University of Chicago Legal Forum. 1996// http://www.law.upenn.edu/fac/pwagner/law619/f2001/week15/easterbrook.pdf, accessed 2010-10-15.

to learn specialist applications of legal controls is by being intimately familiar with the general principles. Specialist areas of law are no more than an application of these principles, which may be seen as foundations of knowledge. Without the foundations the structure will collapse. With the right foundations you can construct many different designs of structure (or specialism). Cyberlaw is a false attempt to give structure to a disparate collection of legal problems caused by technology. F. H. Easterbrook ideas were later challenged by L. Lessig.[208] Lessig argues that as Code and Law compete, additionally with Markets and Norms, to regulate conduct and greater use is made of indirect regulation - using law to regulate code to regulate individuals. Unlike other applications such as "the law of the horse" there is greater scope for social effects to flow in either direction and as such there is a value in the law of cyberspace as a distinct entity as it influences society at a wider level than with other specialized subject matter. L. Lessig further expanded the ideas from his article in a book[209].

L. Lessig's code argument is only partially successful against F. H. Easterbrook. He demonstrated why there was a value to cyber regulatory theory, but he failed to demonstrate why cyberlaw should not be seen as, as F. H. Easterbrook referred to it,'dilettantism'. A. Murray[210] provides us with an academic integrity argument: it examines the relationship between legal research and other social sciences. Law as a social science cannot be examined in isolation. Thus, for example, we have socio-legal studies, law and anthropology, law and economics and law and politics. If computer science or information systems exist as a viable subjects for social science research, then cyberlaw is a viable academic subject too.

J. Sommer[211] provides three key arguments against cyberlaw:

1. *technological argument.* Fields of law are seldom demarcated by technology. There never was the law of the steam engine despite it's role in society, nor is there law of the car today. Laws are rather dictated by societal practice.

2. *introspection argument.* Developing and teaching a law of cyberspace leads to excessive specialization and insufficient perspective and a disdain for history.

3. *technophilia argument.* Cyberlawyers ignore the complex interactions between society and technology.

---

[208] L. Lessig. The Law of the Horse: What Cyberlaw Might Teach// Harvard Law Review. 1999, Nr.113. P.501-546

[209] Lessig L. Code and Other Laws of Cyberspace. New York: Basic Books.1999 The book was later updated: Lessig L. Code: Version 2.0. 2006. http://codev2.cc/download+remix/Lessig-Codev2.pdf

[210] Murray A. The Regulation of Cyberspace: Control in the Online Environment (Glasshouse). London: Routledge-Cavendish, November 2006.

[211] Sommer J. H. Against Cyberlaw// Berkeley Technology Law Journal. 2000, Nr.15

The society argument effectively debunks J. Sommer's position.[212] This argues that there is a flourishing social context to cyberspace and this society both demands and dictates regulation. Additionally, cyberlawyers do not deny the existence of other areas of law such as banking practice, they only wish to mold the laws to meet the requirements of their society, something different from the requirements of the banking community. Finally cyberlaw is not defined by technology but in fact represents attempts to regulate a complex social society, which has members from a variety of cultural and social backgrounds. The technology enables it does not necessarily constrain.

D. West[213], a decade later, comes back to the J. Sommer arguments, granted on the subject of cyber warfare, however the idea of such line of thought is *déjà vu*. He is claiming that the current rules of war can address the issues raised by cyber warfare, because according to UN Charter 2 (4) prohibits all uses of force, D. West includes cyber warfare in the use of force, as well as since law of war applies to absolutely all military operations without any exceptions, therefore cyber warfare is not exempt. Additional arguments provided are, linking to J. Sommer argument, that there is no cyber warfare no more than there is a law of the horse or bows and arrows, despite that at some point in time the use of horses or bows and arrows was revolutionary. Therefore any kind of revolutionary technology cannot be the basis for an emergence of any kind of body of international law.[214] D. West adds that he considers cyber warfare as a primarily non-lethal deterrent. Moreover, a global compliance with the newly created treaty would be hardly feasible. Lastly, D. West is confident that the technological development will outpace any new international treaty and its cyber regime to a point when it will not be able to produce a working international policy, whereas UN Charter is able to absorb any new advances.

The author of the current work cannot agree with the arguments of D. West however, the first part can be easily discarded. In the process of writing this work, it has been already established that it's possible to cover cyber warfare under current international laws, however with significant drawbacks and imperfections, therefore this cannot be a permanent solution to a problem which is only going to escalate in the future. The J. Sommer argument has been

---

[212] See supra note 211.

[213] A Senior Cyber Intelligence and Policy Analyst at Booz Allen Hamilton. He holds a B.S. in Mathematics, a M.S. in Applied Information Technology, and a Juris Doctor degree from The University of Maryland School of Law, where he was an Editor of the Maryland Law Review.

[214] D. West. A Survey and Examination of the Adequacy of the Laws Related to Cyber Warfare. 2010// http://www.google.co.uk/url?sa=t&source=web&cd=1&ved=0CB0QFjAA&url=http%3A%2F%2Fhakim.ws%2FDEFCON18%2FWest%2FDEFCON-18-West-Laws-Cyber-Warfare.WP.pdf&rct=j&q=sommer%20argument%20against%20cyber%20warfare&ei=19bLTdy9Lcix8QP2xOigBA&usg=AFQjCNFTFzEvy1DMNQ2xccGqc7kr6XsQTg, accessed 2011-03-13.

previously defeated and the last key points made by D. West do have some merit. Enforcement of a new treaty can prove to be difficult, as well as while drafting it, future technological advancements need to be kept in mind. However these last arguments cannot be the sole criteria for dismissal of a cyber treaty.

The reality of the modern world is that there is movement in the direction of a cyber treaty, it stands to reason that the international community, or at least the States with major stakes in the matter, have admitted that there was and is a need for a treaty. Soon enough this legal deficiency should be rectified. Main roles in these developments are being played by Russia and the U.S. However the states have not always seen eye to eye. "The U.S. has for years objected to Russian proposals to establish a kind of arms-control treaty for cyber weapons, arguing that international cooperation should first focus on reducing cyber crime." Russia has been working to marshal support for a United Nations treaty to limit the use of cyber weapons, such as software code that could destroy an enemy's computer systems."[215] Negotiations although have begun earlier[216], but due to difference of opinions they have stopped for a while. The mere fact of negotiations going on between Russia and the U.S. is a significant enough event to warrant it as good progress. The negotiations have been renewed some half year later with signs of an agreement between the parties.[217] The result of these negotiations is a cyber proposal produced by EastWest Institute in New York,[218] which was presented at the annual Munich Security Conference in 2011. It describes rendering the Geneva and Hague conventions in cyberspace. Those attending the conference include UK Prime Minister David Cameron, German Chancellor Angela Merkel, U.S. Secretary of State Hillary Clinton and Russian Foreign Minister Sergei Lavrov. According to the institute, the ambiguity about what constitutes cyber conflict is delaying international policy to deal with it. The draft document makes five recommendations:[219]

1. *Detangling Protected Entities in Cyberspace*: "promote the preservation of the observed principles of the Hague and Geneva Conventions that protect humanitarian critical infrastructure and civilians".

2. *Application of the Distinctive Geneva Emblem Concept in Cyberspace*: "The Geneva and Hague Conventions direct that protected entities, protected personnel and protected

[215] S. Gorman. U.S. Backs Talks on Cyber Warfare// The Wall Street Journal, 2010 Jun 4// http://online.wsj.com/article/SB10001424052748703340904575284964215965730.html, accessed 2011-02-06

[216] J. Markoff, A. E. Kramer. In Shift, U.S. Talks To Russia On Internet Security// The New York Times, 2009 Dec 12// http://www.nytimes.com/2009/12/13/science/13cyber.html, accessed 2011-01-28

[217] J. Markoff. At Internet Conference, Signs of Agreement Appear Between U.S. and Russia// The New York Times 2010 Apr 15// http://www.nytimes.com/2010/04/16/science/16cyber.html, accessed 2011-03-25

[218] S. Watts. Proposal for cyber war rules of engagement// BBC, 2011 Feb 3// http://news.bbc.co.uk/2/hi/programmes/newsnight/9386445.stm, accessed 2011-03-17.

[219] B. Rooney. Calls for Geneva Convention in Cyberspace// The Wall Street Journal, 2011 Feb 4// http://blogs.wsj.com/tech-europe/2011/02/04/calls-for-geneva-convention-in-cyberspace/, accessed 2011-03-17.

vehicles be marked in a clearly visible and distinctive way. This recommendation proposes analogous markers in cyberspace to designate protected entities, personnel and other assets.

3. *Recognizing New Non-State Actor and Netizen*[220] *Power Stature*: "The digital revolution has unleashed non-State actors and individuals to occupy, control and operate in cyber territory. This creates new power asymmetries and magnifies the clout of new participants who can violate Convention principles on a massive scale."

4. *Consideration of the Geneva Protocol Principles for Cyber Weaponry*: "Russian and U.S. governments must be open to the possibility that some weapon attributes may be unacceptable because they are offensive to the principles of humanity and from dictates of public conscience."

5. *Examination of a Third, 'Other-Than-War' Mode*: "There is no clear, internationally agreed upon definition of what would constitute a cyber war. In fact, there is considerable confusion."

Alongside these developments however there are still critics, some of which point out valid potential future issues. Creation of a cyber treaty might prove to be premature, despite that this is the right step in the direction of international collaboration, it does not however include all stakeholders.

Chief security officer at the U.S.-based cyber security company Tenable Network Security, M. J. Ranum is certain that a cyber treaty would not be effective at all.[221] Weak States would do well advocating rules for cyber war, however superpowers would be able to ignore them when it suits them. He goes even further claiming that the threat of a cyber attack might be just a hype, aggravated by big military companies, because this technology is a product that can still be sold, unlike heavy military equipment. The author of this work would like to propose an additional argument, however not particularly beneficial for M. J. Ranum, that cyber security companies would as well benefit from such a hype – their trade is mitigation or damage control of cyber attacks (CNA).

The most important critique comes from professor P. Sommer from the Information Systems and Innovation Group, London School of Economics, who was not very impressed by the proposal.[222] He points out that it is very easy to disguise the source of a cyber attack (CNA) and that is not going to change in the future. Then there's the protection of objects, such as hospitals, which is difficult to accomplish due to the structure of the internet. These

[220] Netizen – a combination of words "internet", the "'net", and "citizen".
[221] See supra note 204.
[222] See supra note 220.

technological aspects are difficult to tackle in general and a treaty cannot amend this situation. The nature of cyber attacks (CNAs) is that they are covert, any entity conducting them would not be willing to obey the rules of any treaty. The proposal at the moment is giving us a "physical world solution to a digital world problem."[223] P. Sommer suggests that a better solution is for nations to focus their cyber defense policies on increasing resilience of computer systems and having detailed contingency plans to enable them to recover from a cyber attack (CNA). In addition, conflicting interests between state security and commercial profit exist, as up to 80% of developed countries critical national infrastructure is in private hands.

There have been other attempts to address the issue of cyber security[224]:

- In April 2010, the Twelfth United Congress on Crime Prevention and Criminal Justice drafted a set of declarations which included a provision calling for an intergovernmental expert group to study the problem of cybercrime and international responses to it.
- The UN Economic and Social Council opened its 2010 session with a briefing on the challenges of cyber security, as well as the threats posed and opportunities provided by ever-expanding use of the Internet. They cautioned that the international scope and dire consequences of an actual cyberwar require a coordinated response and current ad hoc solutions and defense strengthening are now inadequate strategies.
- NATO implemented its own policy on cyber defense in 2008 in order to protect its technological resources and those of its member countries. The alliance created a Cyber Defense Management Authority, a Computer Incidence Response Capability, which provides for the dispatch of Rapid Reinforcement Teams to individual member countries, and a Cooperative Cyber Defense Center for Excellence, Located in Estonia.
- Individual States have also attempted to build relationships with other countries in regard to cyber security in the form of bilateral treaties (e.g.: India and South Korea) or memoranda of understanding (Morocco and Malaysia).
- International Telecommunication Union has established a smart grid[225] focus group, which consists of representatives from different member states and will collaborate with worldwide smart grid communities, in order to produce recommendations for smart grid standards to deal with cyber security challenges related to smart grids.

---

[223] Ibid.

[224] See supra note 45.

[225] A smart grid is a form of electricity network using digital technology. Smart grids increase the connectivity, automation and coordination between electricity suppliers, consumers and networks that perform either long distance transmission or local distribution tasks.

Permanent Monitoring Panel on Information Security of the World Federation of Scientists has drafted up a The Erice Declaration on Principles for Cyber Stability and Cyber Peace and adopted in 2009[226]. These are the principles that have been proposed in order to achieve and maintain cyber stability and peace:

1. All governments should recognize that international law guarantees individuals the free flow of information and ideas; these guarantees also apply to cyberspace. Restrictions should only be as necessary and accompanied by a process for legal review.

2. All countries should work together to develop a common code of cyber conduct and harmonized global legal framework, including procedural provisions regarding investigative assistance and cooperation that respects privacy and human rights. All governments, service providers, and users should support international law enforcement efforts against cyber criminals.

3. All users, service providers, and governments should work to ensure that cyberspace is not used in any way that would result in the exploitation of users, particularly the young and defenseless, through violence or degradation.

4. Governments, organizations, and the private sector, including individuals, should implement and maintain comprehensive security programs based upon internationally accepted best practices and standards and utilizing privacy and security technologies.

5. Software and hardware developers should strive to develop secure technologies that promote resiliency and resist vulnerabilities.

6. Governments should actively participate in United Nations' efforts to promote global cyber security and cyber peace and to avoid the use of cyberspace for conflict.

In contrast to the recommendations given by the EastWest Institute, these principles are more general purpose rules rather than principles actually capable of regulating cyber warfare. The draft proposal on the other hand, especially in light of the above attempts of strengthening cyber security, appears to be most suited for the task of regulation of cyber warfare, as it attempts to tackle the key issues that were present since the dawn of cyber warfare.

It is too early to dismiss the draft since it has only appeared a few months ago and as of writing of this work there were no more new developments. This work will not see the outcome what this future treaty might become and therefore any prediction would only be speculation. The author of this work is inclined to support the efforts and the direction of the EastWest

[226] See supra note 45; World Federation of Scientists. Erice Declaration on Principles for Cyber Stability and Cyber Peace, Adopted By The Plenary of The World Federation Of Scientists on The Occasion of The 42nd Session of The International Seminars on Planetary Emergencies in Erice (Sicily) On August 20, 2009// http://Www.Ewi.Info/System/Files/Erice.Pdf

Institute's draft proposal. In the opinion of the author the five recommendations provided are adequate and currently it would be difficult to supplement the list as it exhaustive and refers to all issues that have been raised. The main question posed by this section however has been answered: a new cyber treaty is indeed needed and, coincidentally, a treaty is in the making.

CONCLUSIONS

1. It has been shown that even the currently existing definitions of "cyber warfare" and "cyberspace" are not uniform and may wary not only from State to State, but also from institutions to institution to a degree, within the same State, however these differences present themselves as more of nuances rather than major deviations. The definitions have many points at which they intersect.

2. Based on analysis of the Geneva Conventions and the Additional Protocols as well as the work of M. N. Schmitt, it has been established that *jus in bello* can in fact cover cyber attacks (CNAs) if the consequence-based approach is applied instead of the actor-based. Minimal protection to protected persons and objects can be therefore afforded**,** however the application of this regime does not solve the questions of combatancy, determination of the origin of attacks and what is a proper response to an unknown adversary.

3. In regard to *jus ad bellum*, with the six criteria provided by M. N. Schmitt, it is possible to extend the application of current international norms to cyber attacks (CNAs), however certain cyber attacks (CNAs) against civilians and civilian objects that do not injure, kill, damage or destroy (or otherwise produce the requisite level of suffering) can on whole be allowed. Therefore some legal *lacunae* still exist.

4. Attribution of cyber attacks (CNAs) to a State can be accomplished easily if the hackers are *de jure* organs of States, or proxies who are not even *de jure* organs, over which States exercise "effective control", or if a State condones actions of entities who are neither *de jure* nor *de facto* its organs. It is more difficult if a State has no control over the attacking computer, therefore the attack cannot be attributed to a State, and however it might still bear some indirect responsibility for inaction under its international obligations.

5. Right to self-defense under Article 51 of the UN Charter exists, however it requires meeting a three step criteria of necessity, proportionality and immediacy, which is impossible to accomplish given our current technological level of development. The test fails at immediacy, it is not possible to use force even in self-defense when our adversary is not known. Therefore this right is not usable in practice, unless we have a clear adversary.

6. A right to anticipatory self-defense exists only against a conventional attack preceded by or with a cyber attack (CNA) component. There have been proposals of anticipatory self-defense being especially applicable in order to protect critical (national) infrastructure. It is appropriate to attempt to protect critical (national) infrastructure more, however we are still faced with the issue of identification of our adversary.

7. A right of self-defense under international customary law does exist or at the very least, it's the intention of States to make it real, there is significant amount of State practice and *opinio juris* to back up it's use, however until we see actual application of this in a cyber attack amounting to an armed attack, the rule of customary international law has not yet been spelled out.

8. In regard to combatancy issues, the analysis of the existing legal base strongly suggests that States employing civilians to conduct cyber operations would be in breach of limits on civilian participation in hostilities. Additionally, the four GC criteria are on the most part almost rendered useless in the context of cyber attacks (CNA), with only some aspects still being able to accommodate the new reality, therefore a more adequate system is most definitely needed.

9. Based on the currently applicable international laws to cyber warfare in general, a multitude of issues arise. The international law has adapted to cyber warfare as much as it is possible, however the issues present cannot be dealt with accordingly with the legal instruments that are available. Analysis of recent legal developments as well point to the fact that the major stakeholders are inclined to look into options for creation of a new international cyber treaty.

LITERATURE

International treaties

1. Additional Protocol I to the Geneva Convention of 1949-08-12, and Relating to the Protection of Victims of International Armed Conflicts. 1977-12-12, UNTS Nr.1125(3) (AP I).
2. Additional Protocol II to the Geneva Conventions of 1949-08-12, and Relating to the Protection of Victims of Non-International Armed Conflicts. 1977-06-08. UNTS Nr.1125(609) (AP II).
3. Cheng B. United Nations Resolutions on outer Space: Instant International Customary Law?// International Journal of Innovation and Learning. 1965 Nr.5.
4. Council of Europe. Convention on Cybercrime. Budapest, 2001-11-23
5. Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. 1949-08-12. Art. 2 , United Nations Treaty Series (UNTS) Nr.75(31) (GC I)
6. Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of the Armed Forces at Sea. 1949-08-12. Art. 2.UNTS Nr.75(85) (GC II)
7. Geneva Convention Relative to the Treatment of Prisoners of War. 1949-08-12. Art. 2. UNTS Nr.75(135) (GC III); Geneva Convention Relative to the Protection of Civilian Persons in Time of War. 1949-08-12. Art. 2. UNTS Nr.75(287) (GC IV).
8. Vienna Convention on the Law of Treaties. 1969-05-23. Art.31(1). UNTS Nr.1155(331).

Periodic sources

9. A. Cassese. International Law. Oxford University Press. 2005.
10. B. Rooney. Calls for Geneva Convention in Cyberspace// The Wall Street Journal, 2011 Feb 4// http://blogs.wsj.com/tech-europe/2011/02/04/calls-for-geneva-convention-in-cyberspace/, accessed 2011-03-17.
11. D. Brown. A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict// Harvard international Law Journal. 2006, Nr.57. P.179-187.

12. E. M. Grossman. U.S. General Reserves Right to Use Force, Even Nuclear, in Response to Cyber Attack// Global Security Newswire, 2009 May 12// http://gsn.nti.org/gsn/nw_20090512_4977.php, accessed 2011-05-01.

13. E. T. Jensen Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self Defense// Stanford Journal of International Law. 2002, Nr.38.

14. G. Corn. Unarmed but How Dangerous? Civilian Augmentees, the Law of Armed Conflict, and the Search for a More Effective Test for Permissible Civilian Battlefield Functions// Journal of National Security Law & Policy. 2008, Nr.2. P.257.

15. G. H. Todd. Armed Attack in Cyberspace: Deterring Asymmetric Warfare With an Asymmetric Definition// Air Force Law Review. 2009. P.3.

16. J. A. Ophardt. Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield// Duke Law and Technology Review. 2010, Nr.3.

17. J. Barkham. Information Warfare and International Law on the Use of Force// New York University Journal of International Law and Politics. 2001, Nr.34.

18. J. Kelsey. Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare// Michigan Law Review. 2008, Nr.106.

19. J. Markoff, A. E. Kramer. In Shift, U.S. Talks To Russia On Internet Security// The New York Times, 2009 Dec 12// http://www.nytimes.com/2009/12/13/science/13cyber.html, accessed 2011-01-28.

20. J. Markoff. At Internet Conference, Signs of Agreement Appear Between U.S. and Russia// The New York Times 2010 Apr 15// http://www.nytimes.com/2010/04/16/science/16cyber.html, accessed 2011-03-25.

21. J. R. Heaton. Civilians at War: Reexamining the Status of Civilians Accompanying the Armed Forces// Air Force Law Review. 2005. Nr.57. P.155.

22. K. Dörmann. Computer Network Attack and International Humanitarian Law// Cambridge Review of International Affairs. 2001.

23. K. Geers. Cyber Weapons Convention// Computer Law & Security Review. 2010, Nr.26(5).

24. L. Lessig. The Law of the Horse: What Cyberlaw Might Teach// Harvard Law Review. 1999, Nr.113.

25. M. E. Guillory. Civilianizing the Force: Is the United States Crossing the Rubicon?// Air Force Law Review. 2001, Nr.51.

26. M. Hoisington. Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense// Boston College International and Comparative Law Review. 2009, Nr.32(2).

27. M. N. Schmitt. Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework// The Columbia Journal of Transnational Law. 1999, Nr.37(2).

28. M. N. Schmitt. Wired warfare: Computer network attack and jus in bello// International Review of the Red Cross (IRRC). 2002, Nr.846.

29. M. Roscini. World Wide Warfare – Jus ad bellum and the Use of Cyber Force// Max Planck Yearbook of United Nations Law. 2010, Nr.14.

30. Russia Refused Legal Assistance in Cyber Attacks Investigation// Estonian Review. Vol.17, Nr.27, 2007 Jul 4-10

31. S. A. Hildreth. Cyberwarfare// The Library of Congress. CRS Report for Congress. 2001, Order Code RL30735. P.1.

32. S. Brenner. At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare// Journal of Criminal Law and Criminology. 2007, Nr.97.

33. S. Gorman. U.S. Backs Talks on Cyber Warfare// The Wall Street Journal, 2010 Jun 4// http://online.wsj.com/article/SB10001424052748703340904575284964215965730.html, accessed 2011-02-06.

34. S. J. Shackelford. From Nuclear War to Net War: Analogizing Cyber Attacks in International Law// Berkeley Journal of International Law. 2009, Nr.25(3).

35. S. M. Condron Getting it right: Protecting American critical infrastructure in cyberspace// Harvard Journal of Law and Technology. 2007, Nr.20.

36. S. Watts. Combatant Status and Computer Network Attack// Virginia Journal of International Law. 2010, Nr.50(2).

37. S. Watts. Proposal for cyber war rules of engagement// BBC, 2011 Feb 3// http://news.bbc.co.uk/2/hi/programmes/newsnight/9386445.stm, accessed 2011-03-17.

38. Sommer J. H. Against Cyberlaw// Berkeley Technology Law Journal. 2000, Nr.15.

39. W. Church. Information warfare// International Review of the Red Cross. 2000, Nr.837.

40. W. Clay. Information Operations and Cyberwar: Capabilities and Related Policy Issues// The Library of Congress. CRS Report for Congress. 2007, Order Code RL31787.

41. Wingfield T. C. The Law of Information Conflict: National Security Law in Cyberspace. Falls Church: Aegis Research Corp. 2000.

Specialized literature

42. Brenner S. W. Cyberthreats: The Emerging Fault Lines of The Nation State. Oxford University Press. 2009

43. C. Gray. International Law and the Use of Force. Oxford University Press. 2008.

44. Carr J. Inside Cyber Warfare: Mapping the Cyber Underworld. Sebastopol: O'Reilly Media, 2009.

45. Chairman of the Joint Chiefs of Staff. The National Military Strategy of the United States of America: A Strategy for Today; A Vision for Tomorrow. 2004.

46. Cyber Warfare and Cyber Terrorism. /ed. L. J. Janczewski, A. M. Colarik. New York: IGI Global, Inc, 2008.

47. Documents of the United Nations Conference on International Organization, 1945, Vol.VI.

48. Dörmann K. Applicability of the Additional Protocols to Computer Network Attacks. Stockholm: International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, 2004.

49. Doswald-Beck. L. Computer Network Attack and the International Law of Armed Conflict. in Computer Network Attack And International Law. /eds. M. N. Schmitt, B. T. O'Donnell. 2002.

50. Erickson J. Hacking: The art of exploitation. San Francisco: No Starch Press, Inc, 2008.

51. Gibson W. Neuromancer. New York: Ace Books. 1984.

52. Goldstein E. The best of 2600: A hacker odyssey. Indianapolis: Wiley Publishing, Inc, 2009.

53. ICRC Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 /ed. Y. Sandoz, Ch. Swinarski, B Zimmerman. Geneva. 1987. Para.62. (AP Commentaries).

54. ICRC Commentary on the Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field /ed. Jean Pictet. Geneva. 1952. P.32-33 (GC I Commentary).

55. ICRC. How is the Term “Armed Conflict” Defined in International Humanitarian Law?. Opinion Paper. 2008.

56. Y. Dinstein. War, aggression and self-defense. New York: Cambridge University Press. 2005.

57. Lessig L. Code and Other Laws of Cyberspace. New York: Basic Books.1999.

58. Lessig L. Code: Version 2.0. 2006. http://codev2.cc/download+remix/Lessig-Codev2.pdf, accessed 2011-04-04.

59. Lipson H. F. Tracking and Tracing Cyber-Attacks – Technical Challenges and Global Policy Issues. Pittsburgh: Carnegie Mellon University. 2002.

60. Murray.A. The Regulation of Cyberspace: Control in the Online Environment (Glasshouse). London: Routledge-Cavendish, November 2006.

61. P. A. Johnson. Is it Time for a Treaty on Information Warfare? in M. N Schmitt, B. T. O'Donnell. Computer Network Attack and International Law. 2001. P.187.

62. R. Ottis, P. Lorents. Cyberspace: Definition and Implications. Academic Publishing Limited. 2010.

63. S. Wozniak, G. Smith. iWoz. New York: W.W. Norton and Company, 2006.

64. Sharp W. G. CyberSpace and the Use of Force. Falls Church: Aegis Research Corp. 1999.

65. Tidikis R. Socialinių Mokslų Tyrimų Metodologija. Vilnius: Lietuvos teisės universiteto Leidybos centras, 2003.

Other sources

66. Articles on the Responsibility of States for internationally Wrongful Acts// Yearbook of International Law Commission. /ed. International Law Commission. 2001. Vol.II, Part Two.

67. Boyd B. L. Cyber Warfare: Armageddon in a Teacup?: master thesis: military art and science general studies. U.S. Army Command and General Staff College. Fort Leavenworth, 2009.

68. British-American Diplomacy. The Caroline Case// http://avalon.law.yale.edu/19th_century/br-1842d.asp, accessed 2011-03-17.

69. Commission of The European Communities. Green Paper on a European Programme for Critical Infrastructure Protection. 2005// http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0576:FIN:EN:PDF, accessed 2011-04-15

70. Department of Defense Office of General Counsel. An Assessment of International Legal Issues In Information Operations. 1999. P.21-22.

71. E. Tikk, K. Kaska, K. Rünnimeri and others. Cyber Attacks Against Georgia: Legal Lessons Identified// Cooperative Cyber Defence Centre of Excellence (CCDCOE) Report. 2008// http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf, accessed 2011-03-17.

72. F. H. Easterbrook. Cyberspace and the Law of the Horse. University of Chicago Legal Forum. 1996// http://www.law.upenn.edu/fac/pwagner/law619/f2001/week15/easterbrook.pdf, accessed 2010-10-15.

73. H. I. Touré, the Permanent Monitoring Panel on Information Security World Federation of Scientists. The Quest For Cyber Peace. International Telecommunication Union. 2011.

74. ICJ Statute.

75. J. A. Lewis. A Note on the Laws of War in Cyberspace// Center for Strategic and International Studies, 2010 Apr// http://csis.org/publication/note-laws-war-cyberspace, accessed 2011-03-17.

76. J. A. Lewis. The "Korean" Cyber Attacks and Their Implications for Cyber Conflict// Center for Strategic and International Studies, 2009 Oct 23// http://csis.org/publication/korean-cyber-attacks-and-their-implications-cyber-conflict, accessed 2011-03-17.

77. McAfee Report. In the Crossfire – Critical Infrastructure in the Age of Cyber War. 2010. P.30// http://img.en25.com/Web/McAfee/NA_CIP_RPT_REG_2840.pdf, accessed 2011-03-05

78. Memorandum from W. H. Parks to Mr. J. H. McNeill, Assistant Gen. Counsel, Office of the Secretary of Defense. 1977 Protocols Additional to the Geneva Conventions: Customary International Law Implications. 1986. Reprinted in The Judge Advocate General's Legal Center & School, Law Of War Documentary Supplement /ed. S. Watts. 2006. P388-389.

79. North Atlantic Treaty Organization Parliamentary Assembly. 173 DSCFC 09 E bis – NATO and Cyber Defence. 2009// http://www.nato-pa.int/default.asp?SHORTCUT=1782, accessed 2011-03-17

80. O. Odnokolenko. Controversial aspects of new Russian military doctrine questioned// Open Source Center. 2003.

81. Report of the Secretary-General, A/59/2005. In larger freedom: towards development, security and human rights for all. 2005.

82. Statement of Principles Applicable to the Formation of General Customary International Law. International Law Association (ILA). Report of the Sixty-Ninth Conference. 2000. P.731

83. Thomas T. L. Cyber Silhouettes: Shadows Over Information Operations. Fort Leavenworth: Foreign Military Studies Office. 2006.

84. U.S. Department of Defense. Chairman of the Joint Chiefs of Staff. Joint Publication 3-13, Information operations. Washington, DC: Government Printing Office. 2006.

85. UN Charter. Signed 1945-06-26. In force 1945-10-24.

86. UN GA A/RES/55/63 of 2000-12-04.

87. UN GA A/RES/58/1999 of 2003-12-30.

88. United Nations General Assembly Resolution 3314 (XXIX). Definition of Aggression. Adopted at it's twenty-ninth session. 1974-12-14.

89. United States Department of Defense. Chairman of the Joint Chiefs of Staff. Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms. Washington, DC: Government Printing Office. 2006.

90. V. M. Antolin-Jenkins. Defining the Parameters of Cyberwar Operations: Looking for Law in all the wrong places?// Naval Law review. 2005, Nr.51. P.132.

91. World Federation of Scientists. Erice Declaration on Principles for Cyber Stability and Cyber Peace, Adopted By The Plenary of The World Federation Of Scientists on The Occasion of The 42nd Session of The International Seminars on Planetary Emergencies in Erice (Sicily) On August 20, 2009// http://www.ewi.info/system/files/erice.pdf, accessed 2011-03-29.

Case law

92. ICTY. Prosecutor v. Tadic, Case No. IT-94-1-A. 1999-07-15.

93. Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States). ICJ Reports 1986.

94. North Sea Continental Shelf, ICJ Reports 1969.

95. The Corfu Channel (United Kingdom v. Albania). ICJ Reports 1949.

96. United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran), ICJ Reports 1980

Internet sources

97. Australian Cyber Security Strategy// http://www.ema.gov.au/www/agd/agd.nsf/Page/CyberSecurity_CyberSecurity, accessed 2011-03-17.

98. C. T. Lopez. Fighting in Cyberspace Means Cyber Dominance// Air Force Print News. 2007// http://www.af.mil/news/story.asp?id=123042670, accessed 2011-03-17.

99. Computer Emergency Response Team Statistics (Historical)// http://www.cert.org/stats/, accessed 2011-03-17.

100. Council of Europe. Cybercrime: a threat to democracy, human rights and the rule of law// http://www.coe.int/t/dc/files/themes/cybercrime/default_EN.asp, accessed 2011-03-17.

101. D. Eshel. Israel adds cyber-attack to IDF// www.military.com/features/0,15240,210486,00.html, accessed 2011-03-17.

102. A. D. Sofaer, S. E. Goodman, M.-F. Cuéllar and others. A Proposal for an International Convention on Cyber Crime and Terrorism. 2000// http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm, accessed 2011-03-17.

103. D. West. A Survey and Examination of the Adequacy of the Laws Related to Cyber Warfare. 2010// http://www.google.co.uk/url?sa=t&source=web&cd=1&ved=0CB0QFjAA&url=http%3A%2F%2Fhakim.ws%2FDEFCON18%2FWest%2FDEFCON-18-West-Laws-Cyber-Warfare.WP.pdf&rct=j&q=sommer%20argument%20against%20cyber%20warfare&ei=19bLTdy9Lcix8QP2xOigBA&usg=AFQjCNFTFzEvy1DMNQ2xccGqc7kr6XsQTg, accessed 2011-03-13.

104. E. Fischer. Cyber Warfare – Do We Need a New Geneva Convention? 2011 Apr 8// http://www.army-technology.com/features/feature115500/, accessed 2011-04-25.

105. Europe's Information Society: Thematic Portal. European Commission. Glossary and Acronyms (Archived)// http://ec.europa.eu/information_society/tl/help/glossary/index_en.htm#c, accessed 2011-03-17.

106. Europe's Information Society: Thematic Portal. European Commission. Critical Information Infrastructure Protection// http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm, accessed 2011-03-17.

107. Internet System Consortium// http://www.isc.org/solutions/survey, accessed 2011-03-17, and http://ftp.isc.org/www/survey/reports/2010/07/, accessed 2011-03-17.

108. J. Diamond. U.S. Rejects POW Label. Chicago Tribune, 2002 Jan 28// http://articles.chicagotribune.com/2002-01-28/news/0201280167_1_white-painted-school-buses-defense-secretary-donald-rumsfeld-detainees, accessed 2011-03-05.

109. J. Hoetz, M. Rosenbach, A. Szandar. War of the Future – National Defense in Cyberspace// Spiegel Online, 2009 Feb 11// http://www.spiegel.de/international/germany/0,1518,606987,00.html, accessed 2011-03-17.

110. J. Markoff. At Internet Conference, Signs of Agreement Appear Between U.S. and Russia. The New York Times// http://www.nytimes.com/2010/04/16/science/16cyber.html, accessed 2011-03-17.

111. K. Kerr. Putting cyberterrorism into context// http://www.auscert.org.au/render.html?it=3552, accessed 2011-03-17.

112. M.M. Pollitt. Cyberterrorism – Fact or Fantasy?// http://www.cs.georgetown.edu/~denning/infosec/pollitt.html, accessed 2011-03-17.

113. NATO 2020: Assured security; Dynamic engagement. Analysis and recommendations of the group of experts on a new strategic concept for NATO. 2010// http://www.nato.int/nato_static/assets/pdf/pdf_2010_05/20100517_100517_expertsreport.pdf, accessed 2011-05-01.

114. NATO agrees common approach to cyber defence, 04 April 2008, http://www.euractiv.com/en/infosociety/nato-agrees-common-approach-cyber-defence/article-171377, accessed 2011-04-15.

115. P. Beaumont. U.S. appoint first cyber warfare general// The Observer, 2010 May 23// http://www.guardian.co.uk/world/2010/may/23/us-appoints-cyber-warfare-general, accessed 2011-03-17.

116. Pentagon: Military Response To Cyber Attack Possible, 2010 May 12, http://www.defensenews.com/story.php?c=AME&i=4623599&s=TOP

117. R. B. Hughes. NATO and Global Cyber Defense. in The Bucharest Conference Papers /ed. R. Sheperd. 2008. P.48// http://www.chathamhouse.org.uk/files/11276_bucharest08.pdf, accessed 2011-04-04.

118. S. H. Gunderson. Global IPv6 statistics. Measuring the current state of IPv6 for ordinary users. RIPE57 (Réseaux IP Européens, french for European IP Networks)// http://www.ietf.org/proceedings/73/slides/v6ops-4.pdf, accessed 2011-03-17; http://www.ripe.net/ripe/meetings/ripe-meetings/ripe-57, accessed 2011-03-17.

119. S. Krasavin. What is Cyber terrorism?// http://www.crime-research.org/library/Cyber-terrorism.htm, accessed 2011-03-17.

120. T. Kington. Italy weighs cyber-defense command// Defense News, 2010 May 31// www.defensenews.com/story.php?i=4649478, accessed 2011-03-17.

121. United Kingdom Government. Cyber Security Strategy of the United Kingdom. 2009. P.14// http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf, accessed 2011-02-20.

122. United States National Strategy to Secure Cyberspace. 2003// http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf, accessed 2011-03-01.

123. А.А. Мережко. Конвенция о запрещении использования кибервойны в глобальной информационной сети информационных и вычислительных ресурсов (Интернете)// http://www.politik.org.ua/vid/publcontent.php3?y=7&p=57, accessed 2010-11-02.

Kazinec D. Issues of cyber warfare in international law/ Joint International law program master thesis. Supervisor prof. dr. Justinas Žilinskas. – Vilnius: Mykolas Romeris University, Faculty of law. 2011. – P.79.

SUMMARY

Cyber has been around for over a decade and yet we are still faces with a situation of a very weak or rather no regulation. This is being heavily influenced by our weak technological development and due to the nature of cyberspace and the Internet. Cyber warfare poses interesting questions for us. It is one of a kind type of warfare, the one we cannot see or feel, but it‘s impacts are instantaneous and potentially devastating. States and scholars agree on that.

This thesis attempts to explore possibilities of application of existing international laws to amend this situation and answer the questions if it is adequate or at all possible. While scholars are still arguing about the basics of what cyber warfare and cyberspace actually is, it keeps on evolving. States on the other hand have recognized the potential threat of cyber warfare a long time ago and are attempting to mend the existing legal void, however not successfully. The effects of their efforts are limited only to a small number of States. States who are not willing to give up their cyber capability would also stay clear from such international legislation.

International treaties and State practice were analyzed in search of a way to accommodate cyber warfare under the current regime. The findings show that application of existing legal basis to cyber warfare is at best difficult and strained. The reality is that cyber warfare does not fit adequately under any of the legal umbrellas at the moment. Application of existing laws generates even more drawbacks than it in the end covers. There is potential for future development however. States are inclined to negotiate and, even as we speak, are attempting at creation of a cyber warfare regulating treaty.

The thesis concludes that current international law is not adequate in order to be applicable to cyber warfare and even in areas where it can afford minimal protection, potential for abuse exists. The criteria and standards which were appropriate to conventional warfare and armed conflict are outdated. At least a global understanding on the terms used to define cyber warfare and related terms would be a good starting point. A universally accepted convention would be the perfect solution.

Keywords: cyber warfare, computer network attack, self-defense, international humanitarian law.

Kazinec D. Kibernetinio karo problematika tarptautinėje teisėje/ Jungtinės tarptautinės teisės programos magistro baigiamasis darbas. Vadovas prof. dr. Justinas Žilinskas. – Vilnius: Mykolo Romerio Universitetas, Teisės fakultetas. 2011. – P.79.

SANTRAUKA

Kibernetinis karas jau egzistuoja daugiau nei dešimtmeti tačiau mes vis dar turime labai silpną šio reiškinio reguliavimą. Tokia situacija yra stipriai įtakota mūsų silpnu techniniu galimybių bei interneto struktūros. Kibernetinis karas yra labai keblus. Tai yra naujoviškas kariavimo būdas kurio mes nematome, bet jo pasekmes gali būti žaibiškos ir niokojančios. Mokslininkai ir pasaulio valstybės tai jau seniai pripažino.

Šis darbas bando atskleisti galimybes tarptautines teises reguliavimui kibernetinio karo atžvilgiu, jeigu tai iš viso yra įmanoma. Tačiau mokslininkai vis dar ginčijasi dėl kibernetinio karo ir kibernetines erdvės terminologijos, tuo tarpu kibernetinio karo grėsme tik didėja. Pasaulio valstybes tai suprasdamos bando ištaisyti teisės trukumus, tačiau nesėkmingai. Bet kokie pasiūlymai ir susitarimai galioja tik nedideliam valstybių ratui. O didžiosios valstybės tuo tarpu nenoriai atsisakytu savo kibernetinio pajėgumo.

Darbe buvo išanalizuotos tarptautinės sutartys bei valstybių praktika bandant pritaikyti esamus režimus kibernetinio karo reguliacijai. Darytinos išvados, kad esamos tarptautinės teisinės bazės taikymas geriausiu atveju yra sudėtingas ir nenatūralus. Realybė yra tai, kad kibernetiniam karui netinka nei vienas režimas. O toks jo taikymas, deja sukelia daugiau problemų nei buvo prieš tai. Tačiau dar nėra išsemtos visos galimybės ir ateitis gali parodyti teisingą sprendimą. Tuo tarpu valstybes yra pasiruošusios vesti derybas dėl tarptautinės sutarties, kuri potencialiai galėtu sureguliuoti kibernetinį karą.

Darbas prieina išvadą, kad dabartinė tarptautinė teisė nėra adekvati, kad efektyviai sureguliuotu kibernetinį karą. Tose srityse, kur yra galimybė suteikti minimalią apsaugą, išlieka vietos piktnaudžiauti spragomis. Kriterijai ir standartai kurie tinka tradiciniam karui, yra pasenę ir neatitinka realijų. Todėl pirmu žingsniu teisingą linkme būtų vieningų apibrėžimų sukūrimas. O tobulu sprendimu būtų viso pasaulio valstybių priimta, kibernetinį karą reguliuojanti, tarptautinė sutartis.

Raktiniai žodžiai: kibernetinis karas, kompiuterių tinklo puolimas, savigyna, tarptautine humanitarinė teisė.

Kazinec D. Issues of cyber warfare in international law/ Joint International law program master thesis. Supervisor prof. dr. Justinas Žilinskas. – Vilnius: Mykolas Romeris University, Faculty of law. 2011. – P.79.

ANNOTATION

The thesis attempts to find out if existing international laws and practices can shed light and provide solution to the existing issues arising from cyber warfare. This work consists of two parts. The first part deals with notions and definition, which even now do not have a uniform understanding, among scholars and States alike. It also briefly touches upon attribution and technical difficulties, solving which would greatly enhance the situation with tracing and tracking cyber attacks. The second part is concerned with specific legal issues, firstly can current international laws accommodate cyber warfare within their framework, and secondly self-defense against a cyber attack and combatancy are going to be answered. This part also deals with future prospects for cyber warfare regulation via an international cyber treaty.

Keywords: cyber warfare, computer network attack, self-defense, international humanitarian law.

Kazinec D. Kibernetinio karo problematika tarptautinėje teisėje/ Jungtinės tarptautinės teisės programos magistro baigiamasis darbas. Vadovas prof. dr. Justinas Žilinskas. – Vilnius: Mykolo Romerio Universitetas, Teisės fakultetas. 2011. – P.79.

ANOTACIJA

Šis darbas bando išanalizuoti egzistuojančius tarptautines teises šaltinius, kad išsiaiškinti kylančias problemas iš kibernetinio karo bei surasti galimus jų sprendimo būdus. Darbas susideda iš dviejų dalių. Pirma dalis nagrinės apibrėžimų problematiką, kurie šiuo metu neturi vieningo supratimo pasaulyje. Taip pat, trumpai bus aptarti techniniai sunkumai, kurie trukdo susekti kibernetinius puolimus. Antra dalis nagrinėja specifinius teisinius klausimus, visų pirmą ar dabartinė tarptautinė teisė yra pajėgi susidoroti su kibernetinio karo keliamomis problemomis. Toliau bus nagrinėjama savigyna kaip atsakas į kibernetinį puolimą bei kovotoju problematika. Šita dalis taip pat apžvelgs ateities galimybes kaip sureguliuoti kibernetini karą tarptautines sutarties pagalba.

Raktiniai žodžiai: kibernetinis karas, kompiuterių tinklo puolimas, savigyna, tarptautine humanitarinė teisė.