Darius Kazinec

Issues of cyber warfare in international law

LAP LAMBERT Academic Publishing

Darius Kazinec

Issues of cyber warfare in international law

LAP LAMBERT Academic Publishing

Impressum / Imprint
Bibliografische Information der Deutschen Nationalbibliothek: Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Bibliographic information published by the Deutsche Nationalbibliothek: The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.d-nb.de.

Coverbild / Cover image: www.ingimage.com

Verlag / Publisher:
LAP LAMBERT Academic Publishing
ist ein Imprint der / is a trademark of
OmniScriptum GmbH & Co. KG
Heinrich-Böcking-Str. 6-8, 66121 Saarbrücken, Deutschland / Germany
Email: info@lap-publishing.com

Herstellung: siehe letzte Seite /
Printed at: see last page
ISBN: 978-3-659-51307-7

TABLE OF CONTENTS

TABLE OF CONTENTS

This work has been written at the Mykolas Romeris University, Faculty of law, Vilnius, Lithuania, and supervised by Prof. Dr. Justinas Žilinskas. The work has been completed in May 2011, a minor revision and corrections have been completed in March 2015.

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 favored because of its 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 should it 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 players 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 its 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 do 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 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 its adequacy to deal with the issues presented by modern cyber warfare.

The tasks raised are:

1.1. To ascertain the specifics of cyber warfare and cyberspace.

1.2. Analysis of legal scholars' works in order to find common points of the legal community.

---

[1] Schmitt M. N.

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.

[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] Shackelford S. J. 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. Janczewski L. J., Colarik A. M. New York: IGI Global, Inc., 2008.

[6] Kelsey J. 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] Roscini M. 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] Watts S. Combatant Status and Computer Network Attack // Virginia Journal of International Law. 2010, Nr.50(2). P.392-447.

[9] Hoisington M. 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.

1.3. 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 work 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 work is comprised of two chapters.

Chapter one deals with general information on cyber warfare, such as its history, development, its 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.

Chapter two focuses more on legal aspects of this work and consists of sections relating to cyber warfare in *jus in bello* and *jus ad bellum*, the right of self-defense, the status of cyber combatants 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.

---

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

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), and 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 ones 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

[11] phreak – read as "freak"

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 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

---

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

[13] Wozniak S., Smith G. 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.

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 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

---

[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.

[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.

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 its 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 are that they do not have internationally accepted definitions, this makes it difficult and prevents the international community from establishing a unified legal definition and creating 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: "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks,

---

[21] Touré H. I., 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.

computer systems, and embedded processors and controllers".[24] "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 from the

---

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

[28] Todd G. H. 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.

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 its components, as the 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,

---

[31] Ottis R., Lorents P. 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.

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 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), and

---

[34] Ibid.

[35] See supra note 27. Summary.

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

[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.