TALLINN UNIVERSITY OF TECHNOLOGY

Faculty of Social Sciences

Tallinn Law School

Kateryna Gorbanova

INTERNATIONAL NORMATIVE FRAMEWORK OF CYBER ESPIONAGE

Master thesis

Supervisor: Agnes Kasper, PhD

Tallinn 2017

I hereby declare that I am the sole author of this Master's Thesis and it has not been presented to any other university of examination.

Kateryna Gorbanova

" ..... " 2017

The Master Thesis meets the established requirements

Supervisor Dr. Agnes Kasper

" ..... " 2017

Accepted for examination

"..... "..... 2017

Board of Examiners of Law Master's Thesis

.....

Table of contents

Abbreviations

AMSC – American Superconductor Corporation

ASEAN – Association of South-East Asian Nations

C2 – command and control

CCD COE – Cooperative Cyber Defense Centre of Excellence

CWC – Chemical Weapons Convention

FBI – Federal Bereau of Investigation

ICJ – International Court of Justice

ICRC – International Committee of Red Cross

IHL – International Humanitarian Law

IHR – International Health Regulation

IP (addresses) – Internet Protocol

IPSs – Intrusion Prevention Systems

IT – Information Technology

ITU – International Telecommunications Union

LOAC – Law of Armed Conflict

NATO – North Atlantic Treaty Organization

NSA – National Security Agency

OSCE – Organization for Security and Co-operation in Europe

UK – United Kingdom

UN GGE – United Nations Group of Governmental Experts

UNGA – United Nations General Assembly

US – United States

WHO – World Health Organization

ZIP – Zone Improvement Plan

Introduction

The active development and expansion of cyberspace leads to the emergence of different cyber threats both on national and international levels. The huge and global ones are cyber attacks which occur between states and, therefore, require special attention from the international legal norms. The 2013 UN GGE Report basically affirmed that international law norms are applied to the cyberspace and the following 2015 UN GGE Report mentioned how they should and should not apply by dividing them into limiting norms and good practices principles. But still the question of applicability these norms to cyber operations, remains open.

Since it can be hardly to identify who is behind an incident if it is discovered unless the perpetrator steps forward or unless the incident is investigated thoroughly (which usually takes months if not years), the common practice in government circles is to assume and communicate the worst that could be possibly conducted through the cyberspace when break-ins are discovered, the worst-case scenario usually being that of enemy state actors stealing the most sensitive data. Hacking incidents that were prominently discussed nowadays in the media - such as the intrusions into high-level computers perpetrated by the Milwaukee-based 414s - were turned into call for action: If teenagers (the 414s) were able to penetrate computer networks that easily, it was assumed to be highly likely that better organized entities such as states would be even better equipped to do so.[1]

Espionage is a method of gathering intelligence and describes "the consciously deceitful collection of information, such as sensitive data or hidden strategically important data, ordered by a government or organization hostile to or suspicious of those the information concerns, accomplished by humans unauthorized by the target to do the colleting".[2] Unlike traditional spying, cyber espionage can be (and is) done from across the globe and without any need for physical exposure to risk by the perpetrator.[3]

Linking cyberspace to the national threat was not only unjustified, but also had a lot of conceptual consequences. The national security strategy, propagating the idea of a nation's threat, promotes the confrontational form "we are against them". But the cyber threat is global, and

[1] Myriam Dunn Cavelty, From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse, International Studies Review, 2013
[2] Russell Buchan, The International Legal Regulation of State-Sponsored Cyber Espionage. Chapter 4, International Cyber Norms Legal, Policy & Industry Perspectives, Anna-Maria Osula and Henry Rõigas (Eds.), NATO CCD COE Publications, Tallinn 2016
[3] Wolfgang McGavran, Intended Consequences: Regulating Cyber Attacks, Tulane Journal of Technology and Intellectual Property, p. 259

international cooperation at different levels to address the global cyber threat is important. This form of thinking "we are against them" forms a perception of the threat and may not facilitate the implementation of mechanisms of cooperation with several other states. For example, many malicious programs or attacks are often reported by cyber security providers from China or Russia, but the connection with the governments coordinating the attacks has never been proven. Therefore, cooperation with these governments for the exchange of information is important for limiting the number of cyber-criminal acts.[4]

While some countries define these intrusions or unauthorized access to data or an automated information system as an "attack" most of the observed activity today is not qualified as an attack under international law. It is believed that this theft of commercial intellectual property and proprietary information, the data of significant economic value, or the theft of confidential and classified government information. These considerations are determined by almost all nations as criminal acts in the first place, and espionage in the second. This is also a simple necessity: with the growth of alleged industrial spying sponsored by the state, it is often not clear whether to describe activities that can certainly be categorized as cyber-espionage, like cyber espionage.[5]

Important questions are now rightly being raised as to whether cyber espionage is a permissible cat-and-mouse exercise that is part of the ebb and flow of a competitive international environment, or whether it is a pernicious practice that undermines international cooperation and is prohibited by international law.[6]

There is no specific international treaty that regulates cyber espionage.[7] There is also no specific international treaty that regulates espionage in its traditional form and which could be adapted to regulate cyber espionage as mentioned in Chapter 4 of NATO CCD COE Publication regarding regulation of state-sponsored cyber espionage. And, consequently, cyber espionage is not specifically regulated by international law, but it can be illegal if it is assessed in relation to the general principles of international law.[8]

[4] Clement Guitton, Cyber insecurity as a national threat: overreaction from Germany, France and the UK?, European Security, 2013
[5] Melissa E. Hathaway, Alexander Klimburg, National Cyber Security, Framework Manual, CCDCOE
[6] Russell Buchan (2016), *supra nota* 2
[7] Major Arie J. Schaap, Cyber Warfare Operations: Development and Use under International Law, Air Force Law Review, 2009
[8] Ibid.

So, basically, it leads us to the problem how actually cyber espionage can be regulated by international legal provisions and when there is lack of these norms what actions should be conducted instead.

Therefore, **it is hypothesized that there are legal gaps in international regulation of cyber espionage that should be treated differently than traditional espionage, hence lead to the new regulation.** And the hypothesis by itself raises legal questions:

1) How do existing international legal norms apply/regulate (to) cyber espionage?
2) Are there any legal gaps in regulation which leads to the new regulation?

As for the applicable law, trans-boundary computer attacks are regulated by international law, in contrast to cyber crime, which is a matter of domestic criminal law and law enforcement. As for the second point of difference, there is some subtle difference in it. Cybercrime is not purely domestic legislation that eludes international law.[9]

The European Cybercrime Convention is an excellent example of efforts undertaken at the intergovernmental level to form a common policy on cyber crime. Cyber force is also different from cyberspionage. They share the commonality of using the same methods to penetrate the target state's computer networks, but they diverge in terms of the finality. The purpose of espionage is to obtain confidential information for various purposes, unlike cyberattacks, which are aimed at creating harmful effects similar to the act of force. From a legal point of view, espionage is usually punishable under national law and is legal, if unfriendly, act under international law, while cyber attacks violate international law relating to the use of force.[10]

The international law governing conflict consists of two distinct bodies of law: the jus ad bellum and the jus in bello. Jus ad bellum norms regulate when States, as an instrument of their national policy, may resort to force. They concern, in particular, the prohibition of the use of force by states and the exceptions thereto, primarily the right of self-defense and authorization or mandate by the UN Security Council. The jus in bello, by contrast, is concerned with how the military and other armed actors can use force, including who and what can be targeted.[11]

In the context of espionage, it is often argued that even if espionage does constitute a prima facie violation of the principle of territorial sovereignty or the non-intervention principle, state practice

[9] Marco Benatar, The Use of Force: Need for Legal Justification?, Goettingen Journal of International Law, p. 375
[10] Ibid.
[11] Michael N. Schmitt, "Attack" as a Term of Art in International Law: The Cyber Operations Context, IEEE, 2012

has established a customary international law that alters the scope of these principles. In other words, state practice has generated a resolving norm of customary international law, which views espionage as a legally recognized exception to the principles of territorial sovereignty and non-intervention.[12]

By the method of conducting, espionage can take any form, but the addition in the form of cyber space makes from the traditional espionage something more developed and thus more difficult to track and identify the perpetrators. Cyber space provides unlimited opportunities for states and non-state actors for espionage, while remaining unidentified over a long period and sometimes unidentified at all. This state of affairs cannot be unattractive, and the absence of specific international norms governing this type of cyber activity, allows states to collect data among themselves that are not publicly available and authorized, often by placing malware tracking data for long periods. Therefore, the traditional espionage and methods of its regulation cannot be equated with cyber espionage to the full, since the latter is a more advanced version of traditional espionage and includes more difficult methods of conducting in terms of investigation and identifying the responsible person or persons, but more accessible and not requiring a personal presence in terms of carrying out this type of espionage.

The aim of the research is to clarify the level of applicability of existing international legal norms to the cyber espionage and identify gaps in international regulation with possible ways of their filling.

The research will contain descriptive, comperative and analitical methods to describe the current position of international law provisions in regulation of cyber space and cyber-espionage in details, to identify existing gaps by analyzing international regulation and, basically, demonstrate that cyber espionage differs from the traditional meaning of espionage.

The structure of the thesis will consist of three chapters.

In the first chapter, the author will define the nature of cyber espionage, describe the most well-known offensive cyber operations and observe the impact of cyber espionage.

In the second chapter, the author mainly focuses on international law bodies which govern cyber conflicts, meaning customary international law and international humanitarian law and also will discuss the ways of state self-defense.

[12] Russell Buchan, The International Legal Regulation of State-Sponsored Cyber Espionage. Chapter 4, International Cyber Norms Legal, Policy & Industry Perspectives, Anna-Maria Osula and Henry Rõigas (Eds.), NATO CCD COE Publications, Tallinn 2016

In the third chapter, the author will analyze the current international law norms with regard to cyber espionage and the legal treatment of cyber espionage as a separate notion from traditional espionage, identify legal gaps in present international regulation with possible approaches to fill them.

1. Legal interpretation (qualification) of cyber espionage nature

1.1. Offensive cyber operations

For a computer or network, vulnerability is an aspect of the system that can be used to compromise that system. "Compromise" is used here as a verb meaning to attack or exploit. Weaknesses may be introduced accidentally through design or implementation flaws. A defect or "bug" may open the door for opportunistic use of that vulnerability by an adversary. A lot of vulnerabilities are widely publicized after discovery and may be used by anyone with moderate technical skills until a patch can be disseminated and installed.[13]

Adversaries with the time and resources may also detect unintentional defects, whih they protect as valuable secrets, also known as zero-day exploits. While those defects are not eliminated, the vulnerabilities they create can be used by adversaries. Vulnerabilities may also be introduced intentionally. Of course, vulnerabilities are of no use to an adversary unless the adversary knows they are present on the system or in a compromised network. But an adversary can have some special way of finding vulnerabilities, and in particular, nation states often have special advantages. For example, although proprietary software producers jealously protect their source codes as intellectual property on which their businesses depends, some of these producers are known to provide source code access to governments under certain conditions. The availability of source code for verification increases the likelihood that the inspecting party will be able to identify vulnerabilities not known to the general public.[14]

In order to take advantage of vulnerability, an adversary must have access to it. Targets that are "easy" to compromise are those that require relatively little preparation on the part of the adversary and where access to the target can be obtained without much difficulty, for example, target that is known to be connected to the Internet. "Difficult" targets require a lot of preparation on the part of the adversary, and access to the target can be obtained only with great effort, or may even be impossible for all practical purposes.[15]

Access paths to a target can suggest a way of differentiating between two categories of compromise:

- Remote access: Where a compromise is launched at some distance from the adversary

[13] Herbert S. Lin, Offensive Cyber Operations and the Use of Force, Journal of National Security Law & Policy, 2010, p. 63
[14] Ibid.
[15] Ibid.

computer or network of interest. The canonical example of a remote access compromise is using the access path provided by the Internet, but other examples may include accessing an adversary computer through a dialup modem attached to it or through penetration of the wireless network to which it is connected.[16]

- Close access: Where a compromise takes place through the local installation of hardware or software functionality by friendly parties (e.g., covert agents, vendors) in close proximity to the computer or network of interest. Close access is a possibility anywhere in the supply chain of a system that will be deployed. It may well be easier to obtain access to the system before it is deployed.[17]

With regard to operational considerations, cyber exploitation and cyber attack are very similar. Both cyber attack and cyber exploitation require a vulnerability, access to the vulnerability, and a payload that needs to be performed. The process of intelligence gathering necessary to penetrate an adversary's computer or network is almost identical for both cyber exploitation and cyber attack. Both cyber attack and cyber exploitation use the same kind of access paths to achieve their targets and also take advantage of the same vulnerabilities to deliver their payloads.[18]

Cyber exploitations are aimed at the confidentiality of information stored on or transmitted through a system or a network. Under normal circumstances, such information should be available only to authorized parties. The successful cyber exploitation compromises the confidentiality of such information and makes the information accessible to the adversary.[19]

Cyber attacks (as opposed to cyber exploitations) target one of several attributes of these components or devices and tend to cause a loss of integrity, a loss of authenticity, or a loss of availability, which includes theft of services:

- Integrity: A compromise of integrity refers to the modification of information (a computer program, data, or both) so that under some circumstances of operation, the computer system does not provide the accurate results or information that one would normally expect even though the system may continue to operate.[20]

[16] Herbert S. Lin, Offensive Cyber Operations and the Use of Force, Journal of National Security Law & Policy, 2010, p. 63
[17] Ibid.
[18] Anna Wortham, Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Chartern Provisions Prohibiting the Threat or Use of Force?, Federal Communications Law Journal, 2011
[19] Herbert S. Lin (2010), *supra nota* 16
[20] Ibid.

- Authenticity: A compromise of authenticity hides or forges the source of a given piece of information. A message whose authenticity has been compromised will deceive a recipient into thinking it was correctly sent by the approved originator.[21]
- Availability: A compromise in availability means that the functionality provided by the target system or network is not available to the user: email sent by the targeted user does not go through, the target user's computer simply freezes, or the response time for that computer becomes intolerably long, possibly leading to unpredictable results if a physical process is being controlled by the system.[22]

Due to the fact that there are so many similarities between cyber attack and cyber exploitation, it is often difficult to identify whether a party has been exploited or attacked. Vulnerabilities in many cases can be used for either cyber attack, cyber exploitation, or both.[23]

1.1.1. Well-known international offensive cyber operations

The one of the most well-known offensive cyber operation is Stuxnet. On June 1, 2012, officials of President Barack Obama's administration admitted that the computer worm, Stuxnet, was a joint project between the United States and Israel designed to disrupt Iran's nuclear program. The "Olympic Games" program began in 2006 under President George W. Bush's administration and flourished under the Obama administration. The Stuxnet worm, developed within Olympic Games, was first introduced into the Iranian computer system in 2008, at an underground facility at Natanz, through an employee's flash drive. Stuxnet was originally designed to suddenly speed up or slow down the spinning of centrifuges used to enrich uranium, causing their parts to break and thereby crippling the entire uranium enrichment operation. The most impressive aspect of the Stuxnet worm that made it interesting for us in course of the topic of cyber operations, was that while it was changing the speeds of the centrifuges, the computers in the operation room would report normal functioning of the centrifuges indicating no problems. The Stuxnet operation was working successfully until an error in the programming allowed the worm to be released after infecting an engineer's computer. The engineer took his computer home with him, and the worm spread when he connected to the Internet, thereby infecting over 100,000 computers worldwide and exposing Stuxnet to the public. Stuxnet's intent and objective were not immediately clear to those persons who encountered it. After much consideration the Obama

[21] Herbert S. Lin, Offensive Cyber Operations and the Use of Force, Journal of National Security Law & Policy, 2010, p. 63
[22] Ibid.
[23] Anna Wortham, Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Chartern Provisions Prohibiting the Threat or Use of Force?, Federal Communications Law Journal, 2011

administration decided to continue the Stuxnet attacks since the worm was still effectively dismantling the Iranian nuclear program. The overall effectiveness of Stuxnet is unclear, with the United States government arguing that it delayed Iran's nuclear development by one-and-a-half to two years, while others report that Iran was able to successfully contain much of the damage caused by Stuxnet. Stuxnet was programmed to self-destruct on June 24, 2012.[24]

Another example, Operation Shady rat, the invasive hacking intrusion, which was able to gain the access to secret information of different types including legal, governmental, personal data in 14 countries by infiltrating several states' computer systems and non-governmental corporations and organizations as well.[25]

And one more example, Flame. In late May 2012, experts discovered a computer virus dubbed "Flame". Unlike Stuxnet, Flame operated as an espionage tool because it infiltrated computers and exfiltrated information from them. The experts believe that a government or governments created Flame to spy on other countries. This large and complex virus was mainly found in computers in the Middle East, with Iran being particularly affected. Some information indicated that Flame had been operating for many years prior detection and shared some code with early versions of Stuxnet. The Iran and Stuxnet aspects called for speculation that the United States and/or Israel were responsible for Flame. Although cyber espionage is not a new problem, Flame garnered international attention, including the warning from the International Telecommunications Union ("ITU") and assertion by the ITU's cyber security coordinator that Flame constituted "a much more serious threat than Stuxnet".[26]

The experience indicates that cyber threats will be propagated from those jurisdictions that criminals, terrorists, or other malicious actors find most favorable, i.e., those with the least stringent domestic regulations and the greatest inability to monitor or curtail malevolent Internet traffic.[27] And the recent cyber-related incidents - ranging from cyber crises in Estonia and Georgia to reports of the Stuxnet cyberworm allegedly infecting Iranian computers - that have contributed to a growing perception that "cyberwar" is inevitable, if not already underway.[28]

[24] David Weissbrodt, Cyber Conflict, Cyber-Crime and Cyber-Espionage, Minnesota Journal of International Law, 2013
[25] Gross M.J., "Exclusive: Operation Shady rat - Unprecedented Cyber-espionage Campaign and Intellectual Property Bonanza", Vanity Fair, 2011
[26] David P. Fidler, Recent Developments and Revelations Concerning Cybersecurity and Cyberspace: Implications for International Law, Insights, 2012
[27] Sean Kanuck, Sovereign Discourse on Cyber Conflict under International Law, Texas Law Review, 2009-2010, p. 1571
[28] Charles J. Dunlap Jr., Perspectives for Cyber Strategists on Law for Cyberwar, Strategic Studies Quarterly 2011

Before the Estonian incident, organizations tended to treat their risks and arrangements in isolation. Since 2007, however, the United Nations, NATO, the European Union, OSCE and other international organizations have introduced new cyber-security policies or revised existing ones.[29]

The current situation occurred on July 2, 2014 with regard to cyber espionage where a German federal government employee was arrested on suspicion of spying for Russia claimed to have been transmitted German intelligence documents to the United States. Shortly thereafter, German officials raided the apartment of another individual suspected of espionage; news reports suggested that U.S. intelligence agents had recruited another agent, this one linked to Germany's Defense Ministry.[30]

Tensions between Germany and the United States over espionage had already started to emerge in 2013 after documents leaked by former National Security Agency (NSA) operative Edward Snowden revealed that U.S. intelligence agencies had monitored the electronic data of millions of Germans and had tapped Merkel's cell phone. After the Snowden leak, Germany requested a "no espionage" agreement with the United States, arguing that similar agreements already existed with certain U.S. allies that are currently participants to an intelligence-sharing arrangement. The Obama administration maintained the position that both legislation and policy should keep up with changes in surveillance technology and that the United States is committed to reforms and further communications with its allies in order to solve the issues related to espionage.[31]

Therefore, at the moment, domestic and global consequences of human society's increasingly critical dependence on the Internet makes necessary the ability to deter, detect, and minimize the unpleasant effects of cyber attack.[32]

1.1.2. Cyber force and its types

For the purpose of research, cyber force is defined as coercive measures that are (1) taken by a state or an entity whose actions are attributable to the state and (2) travel through cyberspace using the interconnection of computer networks to cause harmful effects in another state.[33]

[29] Eneken Tikk, Ten Rules for Cyber Security, Survival, 2011, p. 119-132
[30] Kristina Daugirdas and Julian Davis Mortenson, In Wake Of Espionage Revelations, United States Declines To Reach Comprehensive Intelligence Agreement With Germany, American Journal of International Law, 2014
[31] Ibid.
[32] Scott J. Shakelford, Richard B. Andres, State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem, Gergetown Journal of International Law, 2011, p. 971
[33] Marco Benatar, The Use of Force: Need for Legal Justification?, Goettingen Journal of International Law, p. 375

The varying greatly in intensity, ranging from web vandalism to attacking critical infrastructures, cyber force ultimately takes on one of three forms. The first type, syntactic attack, is aimed at the operating system of a computer with help of malicious code or hacking. Examples include worms which consistently replicate themselves leading to significant slowdown, trap doors that provide attackers unauthorized access to enter a computer system, and logic bombs that are in sleep mode in computers for long periods of time until a trigger activates them upon which they unleash havoc. The hacking involves breaking into a computer in order to spy or exploit an operating system. Access can be obtained by relying on human weakness (social engineering), using sniffer software to intercept passwords, user names etc. (eavesdropping) or using a dictionary program to check all possible code combinations (brute-force intrusion).[34]

The second type of cyber force is semantic attacks, which are not aimed at operating systems but rather the accuracy of information retained by computers. The main goal is to corrupt data so as to mislead users into thinking that information is true. This is espesially dangerous when a governmental website is targeted, for the public at large will be inclined to trust the data and act accordingly.[35]

Thirdly, mixed attacks involve a combination of syntactic and semantic attacks. It is clear that this category of cyber warfare has the ability to lead to extreme levels of devastation if well-organized. In order to outline the concept of cyber force, the latter should be distinguished from similar acts. Such a distinction is between cyber force and cyber crime. The difference is twofold. From the point of view of the perpetrator, acts of cyber force are committed by a state or state-related entity, whereas private entities commit cyber crime.[36]

1.2. Use of force – assesment criteria

States are seeking to keep their actions as free as possible, while do not want to suffer from such actions of the other states, which could definitely give rise to unexpected consequences. This position is based on factors which border the line between cyber operation and use of force and determine when the first one becomes the latter one. The states' assessment criteria as those set forth below will demonstrate the balancing of these issues in order to identify the golden mean.[37]

[34] Marco Benatar, The Use of Force: Need for Legal Justification?, Goettingen Journal of International Law, p. 375
[35] Ibid.
[36] Ibid.
[37] Michael N. Schmitt, Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts, Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, The National Academies, 400 pages, 2010

Severity: The consequences involving physical harm to individuals or property will constitute the use of force, while those that creating only minor inconvenience or negative perception will never do so. Therefore, it is obvious that the most important interests of the nations can be affected by above mentioned impacts, so the use of force will be represented as a consequence of cyber operation, meaning the substitution of cyber operation notion in such a context. The degree of severity can be identified by such an important factor as self-evidently.[38]

Immediacy: States, as a rule, focus their attention on those consequences that arise immediately and after that they resort to the solution of those that gradually arise with the course of time. It is very important that such consequences to be determined as soon as possible, thus, it would reduce the likelihood that states will seek ways to peacefully prevention of these disastrous consequences.[39]

Directness: Unlike immediacy, directness is more focused on causality, when immediacy affects temporal aspects. Thus, when there is ambiguity in the chain of cause and effect, the likelihood that states violating the ban on the use of force will bear the responsibility is decided to be reduced to a minimum. For example, if we consider the consequences of an economic recession that is caused by a series of factors, then the actions and their consequences are usually not directly connected with each other. At the same time, as in actions of an armed nature, such concepts as cause and effect are interconnected, meaning in simple words that the explosion usually leads to victims and destruction.[40]

Invasiveness: Undoubtedly, the more secure system causes an equally large buzz around it and numerous attempts to penetrate this very system. Considering the aspect of invasiveness by the example of economic coercion and armed actions, the author can again determine their difference, where in the first case there is no intrusion into the state, and in the second one, sovereignty is inevitably violated by the movement of troops. In the case of cyber space, it is customary to assume that cyber exploitation is the mean for carrying out cyber espionage. International law does not define cyber espionage as such, which is defined as the use of force or

[38] Michael N. Schmitt, Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts, Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, The National Academies, 400 pages, 2010
[39] Ibid.
[40] Ibid.

an armed attack, despite the high degree of invasiveness of this operation. Thus, the invasiveness factor in the cyber context is not considered as the use of force.[41]

Measurability: This factor serves as an assistant in determining the consequences, namely, their quantity. Returning again to economic coercion, international law does not define it as the use of force and it is difficult enough to determine the quantitative level of damage in this case, although in the second case, namely the military attack, it is quite simple to determine the damage simply by victims and destructions.[42]

Presumptive legitimacy: International law is generally of a prohibitive nature, so everything that is not prohibited by international law is permitted. It follows that cyber espionage, for instance, is presumably a legitimate act, as is propaganda, since they are not prohibited by international law. The alleged legitimacy allows cyber operations to be carried out because they are presumably not illegal.[43]

Responsibility: This factor determines when the state will be responsible for the cyber operations. Responsibility should be imposed on states not only for the cyber operations conducted by states, but also for cyber operations where the states take place or participated in. This is necessary, since other states can determine any relation of the state (minimal or global) to cyber operations as the use of force and the development of international instability.[44]

The Estonian cyber attacks can be illustrative here. It is obvious, that cyber operations are more secure in some sense and since they are not perform any damages or deaths, they are considered like non use of force. But, if we look more precisely to the damage caused by the above mentioned cyber attacks to the Estonian society, it become obvious that everything and everyone were affected greatly. These cyber attacks didn't lead to the consequences destroying human lives, but they definitely destroy the entire operation system of the country.[45]

[41] Michael N. Schmitt, Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts, Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, The National Academies, 400 pages, 2010
[42] Ibid.
[43] Ibid.
[44] Ibid.
[45] Ibid.

1.3. Espionage. Cyber espionage

1.3.1. Types of espionage

The occurrence of cyber espionage is determined by the fact of states' desire to represent their interests in the cyberspace.[46]

A significant amount of intelligence collected by states is from sources which are publically available. Espionage violates domestic law; but it is not illegal under international law.[47] A literature has only begun to emerge regarding cyber espionage. There are aspects of cyber espionage that may change the optimal outcome. On the one hand, as was the case with satellite surveillance, the lack of territorial invasion makes cyber surveillance less problematic.[48]

But on the other hand, the drastic reduction in the cost of surveillance and the lower probability of apprehension may lead firms to participate in it when before the benefits did not justify the costs. Some consider this as an advantage, because the nonlethal aspects of cyber capabilities make them preferable to other means. Others hold the opposite view, arguing that since cyber espionage increases the scale of intelligence-gathering capability, it should be limited by treating it more strictly than traditional espionage. Still others support doing nothing and allowing state practices to develop. In any case, general agreement has never arisen with regard to traditional espionage, and there seems little reason to expect that consensus is more likely to emerge in the cyber context.[49]

English historian Michael Burn inspects the particular motives for spying by dividing such activity into the following four categories:

1. The espionage one government practices against another.

2. The espionage used to defeat this.

3. The secret watch a government keeps on its own people.

[46] Ronald J. Deibert and Masashi Crete-Nishihata, Global Governance and the Spread of Cyberspace Controls. Global Governance: A Review of Multilateralism and International Organizations: July-September, 2012, pp. 339-361

[47] Alexander Melnitzky, Defending America against Chineese Cyber Espionage through the Use of Active Defences, Cardozo Journal of International and Comparative Law, 2012, p. 537

[48] Yoo, Christopher S., Cyber Espionage or Cyberwar?: International Law, Domestic Law, and Self-Protective Measures, University of Pennsylvania Law School, 2015

[49] Ibid.

4. The secret watch some of its people keep upon the government.[50]

Burn's second category, espionage used to defeat the espionage one government practices against another, is better called counterespionage, a subtype of counterintelligence. Counterespionage, a common specialty found practiced by intelligence organizations worldwide, can be active or passive, and designed to prevent, confuse, or modify hostile intelligence development. Counterintelligence is the "spy against spy" work of countering secret human intelligence collection, but does not fall under the definition of espionage proposed earlier. Counterspies are supported by the sense of high purpose spies use to overcome municipal legal barriers and garden variety ethical standards.[51]

Burn's third category, the secret watch a government keeps on its own people, addresses domestic surveillance. This form of "spying" infringes on the individual rights of a society's members, but depending upon the internal and external threats to a polity, some domestic surveillance is justified. Although important, the spying of a government against its members is not examined in the present analysis.[52]

Burn's fourth category is the secret watch some of a government's people keep upon the government. At its extreme, this category of spying evokes a crime closely related to espionage: treason. Treason, a statutory crime in most countries, typically involves the conscious transmittal of information to another country's agents or spies by a citizen of the target country. Usually the information transmitted must have some significance for national security. Espionage and treason have a curious relationship. The key activity of traditional espionage is that it constitutes the recruitment and development of traitors, and, although a traitor also may be a spy, the traitor aspect will receive greater disrespect and loathing.[53]

Espionage comes in different forms. Traditional espionage covers a government's efforts to obtain clandestinely classified or otherwise protected information from a foreign government. Economic espionage is associated with attempts by the state to acquire covertly commercial secrets held by foreign private enterprises. "Corporate espionage" or "industrial espionage" describes a company's illegal acquisition of another company's commercial secrets with no

[50] Demarest, Geoffrey B., Espionage in International Law, Denver Journal of International Law and Policy 24 Denv. J. I., 1996, p.321
[51] Ibid.
[52] Ibid.
[53] Ibid.

government participation. Many countries have long considered economic espionage important to national security and economic development.[54]

Cyber tactics employed by adversaries are fundamentally similar to traditional methods involving fraud, deception, covert access, insider recruitment, vendor visits, and specialized technical operations. However, each of these tactics has its potential effectiveness which is increased when current technology is used to enhance its impact.[55]

At least three characteristics of cyberspace render it a unique medium for the conduct of espionage and covert action: the possibility of remote access, the difficulty of attributing intrusions and attacks to identifiable entities, and the difficulty of distinguishing between exploitation and attack. Upon reflection, the third of these features appears to present particularly significant challenges for the conduct of espionage and covert action.[56]

1. Remote Access

The first characteristic distinguishing cyberspace from traditional domains is remote access. In discussing the "changing nature of criminal espionage", Professor Susan Brenner and information analyst Anthony Crescenzi describe the remote-access problem thus, a key characteristic of traditional crime - proximity between victim and offender - is no longer a requirement for the targeting of sensitive critical infrastructure information. Spyware and keystroke loggers can be inserted into networks by insiders or by Trojan software downloaded surreptitiously and written for the express purpose of permitting remote access to sensitive data present on information networks. Spies do not need physically located near sensitive information, or even in the nation to which that information belongs, in order to hack into critical networks and steal secret data. Once a computer is compromised by, for example, a Trojan horse software program, an unauthorized user can take control of the infected computer and steal data on the machine or configure it to become part of a botnet that automatically infects other machines. Territorial limits on the exercise of police power may constrain the capacity of law enforcement agencies to deter espionage conducted from remote locations.[57]

[54] David P. Fidler, Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies, Insights, 2013
[55] Susan W. Brener, Anthony C. Crescenzi, State-Sponsored Crime: The Futility of Economic Espionage Act, Houston Journal Of International Law, 2006, p. 389
[56] Robert D. Williams, (Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action, George Washington Law Review 79 Geo. Wash. L. Rev., 2010-2011, p. 1162
[57] Ibid.

2. Attribution Problem

A second unique characteristic of cyber activity is known as the attribution problem. The problem lies in the fact that, since cyber intrusions and attacks can be launched largely in secret, the identities of the actors carrying them out often cannot easialy be determined. For example, a cyber attack seemingly originating in China might have been launched by the Chinese government, by some unofficial group of hackers in China or elsewhere, or by terrorists in the Middle East who disguise their identities. In addition to identifying the responsible party, determining whether a given cyber intrusion was intentional or inadvertent is associated with difficulty. Thus, the attribution problem creates considerable difficulties for those seeking effective methods of deterrence against cyber intrusions.[58]

However, not knowing the actor does not mean that defensive actions are prohibited. According to the U.S. Defense Department, international law does not require that an actor must be known before defensive action can be taken. Rather, the responsibility for the attack would be imputed "to the state to whose territory the attack was traced".[59]

3. Exploitation/Attack Quandary

A third distinctive aspect of cyber operations is the thorny issue of distinguishing cyber intrusions that constitute theft or exploitation from those that rise to the level of "armed attack" or "use of force." States are at pains to distinguish between acts of cyber espionage ("the use of information technology systems and networks to gather information about an organization or a society that is considered secret or confidential without the permission of the holder of the information") and information war ("cyber conflict at the nation-state level involving either direct military confrontation or indirect competition via disruption and deception").[60]

The exploitation of cyberspace for the purpose of espionage has emerged as a particularly attractive method to acquire confidential information because of the large amount of information that is now stored in cyberspace and because cyberspace affords a considerable degree of anonymity to perpetrators of espionage and is thus a relatively risk free enterprise.[61]

[58] Robert D. Williams, (Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action, George Washington Law Review 79 Geo. Wash. L. Rev., 2010-2011, p. 1162
[59] Anna Wortham, Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Chartern Provisions Prohibiting the Threat or Use of Force?, Federal Communications Law Journal, 2011
[60] Robert D. Williams (2010-2011), *supra nota* 58
[61] Russell Buchan, The International Legal Regulation of State-Sponsored Cyber Espionage. Chapter 4, International Cyber Norms Legal, Policy & Industry Perspectives, Anna-Maria Osula and Henry Rõigas (Eds.), NATO CCD COE Publications, Tallinn 2016

1.3.2. Impact of cyber espionage

For most daily Internet uses, the hidden world of international cyber espionage may seem too distant to be of any real importance. But to the most individual citizens, cyber espionage may not seem to influence their lives very much, but its value in a nation state are significant. The impact can vary significantly from monetary loss to physical infrastructure damage to civilian casualties, and the cost can range from insignificant to devastating. In this section, the author will discuss the different impacts of cyber espionage and their costs on any given society, as well as explore ideas about how nation state cyber espionage impacts the future of international relations and national security.[62]

Although the amount and type of cost associated with cyber espionage can vary, in extreme cases it can be very high. When cyber attacks are coupled with actual warfare, as in Russia's preferred strategy, the loss of communication systems can severely restrict the victim nation's ability to defend itself and its citizens. In this case such an attack results in loss of property, infrastructure, and human life.

When Russia used this strategy on Estonia, Georgia, and Ukraine, the tree victim countries lost much of their ability to defend themselves or to reach out and appeal to the outside world. Coupled with physical strikes, the cost on the victim state can be enormous. It is also important to consider the impact that politics and media have had on the public perception of cyber espionage. It is likely that politicians would prefer that the perceived threat of cyber war remain high because then they can direct public policy toward combating cyber espionage.[63]

Physical damage to the civilian infrastructure can seriously damage the economy of the target state. When the damaged objects are legitimate military targets, or targets whose neutralization confers a military advantage that outweighs the negative impact on the civilian population, the economic damage is collateral. Information warfare is also capable of attacking civilian facilities, not for the purpose of doing physical damage, but to disable them in some fashion. Examples include shutting down the computer system that manages the national stock market, disabling the computer systems of major banks, or shutting down telephone lines in areas in which military forces have no interest. Such targets have no military use and their neutralization confers no definite military advantage.[64]

---

[62] Dana Rubenstein, Nation State Cyber Espionage and its Impacts, Washington University, St. Louis, 2014
[63] Ibid.
[64] Davis Brown, A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict, Harvard International Law Journal 47 Harv. Int'l L.J., 2006, p. 179

2. International law bodies governing cyber conflicts

2.1. *Jus ad bellum* – customary international law

It is today widely accepted that cyberspace is regulated by existing positive law. Following this view, the law on the use of force, jus contra bellum as well as jus in bello, applies to cyber operations.[65]

The jus ad bellum seeks to maintain peaceful relations within the community of nations by setting strict criteria as to when states may move beyond non-forceful measures such as diplomacy, economic sanctions and counter-measures. Of particular note is the right to do so in self-defense when either facing an "armed attack" or coming to the aid of another state which is defending itself (collective self-defense).[66]

Article 51 of the United Nations Charter:

"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".[67] Article 51, recognized as reflective of customary international law by the vast majority of legal scholars, is an express exception to Article 2(4) of the Charter.

Article 2(4) of the United Nations Charter:

"[a]ll 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".[68] Taking the Articles together, a state may "use force" without violating Article 2(4) when it is the victim of an "armed attack", as that term is envisaged in Article 51. Self-defense requires no *ex ante* authorization from the Security Council, states alone enjoy the right of self-defense, and the right only attaches to armed attacks with a transnational element.[69]

By contrast, in international humanitarian law, "attack" refers to a particular category of military operations. Article 49(1) of the 1977 Additional Protocol I to the 1949 Geneva Conventions

[65] Marco Roscini, Cyber Operations and the Use of Force in International Law, Oxford Press, 2014
[66] Michael N. Schmitt, "Attack" as a Term of Art in International Law: The Cyber Operations Context, IEEE, 2012
[67] See, The Charter of the United Nations, 1945
[68] Ibid.
[69] Michael N. Schmitt (2012), *supra nota* 66

defines "attacks" as "acts of violence against the adversary, whether in offence or in defense".[70] It is a neutral term in the sense that some attacks are legitimate, whereas others are not, either because of the status of the object of the attack or how the attack is conducted.[71]

The question at hand, however, is when does a cyber operation qualify as an armed attack, that is, when does an action against a State legally merit a response with either cyber or kinetic actions that are at the level of a use of force? The challenge lies in interpreting the adjective "armed". "Armed" is not to be equated with "force" in the sense of Article 2(4). The International Court of Justice recognized this normative "gap" in the *Nicaragua Judgment* when it found that there are "measures which do not constitute an armed attack but may nevertheless involve a use of force" and distinguished "the most grave forms of the use of force from other less grave forms".[72]

The arrival of cyber operations challenged this presupposition because dire consequences could now be caused by operations that did not fit neatly into the notion of an attack that was "armed" in the kinetic sense. While the International Court of Justice had opined in its Nuclear Weapons advisory opinion that the type of weapon used is immaterial to the application of Articles 2(4) and 51, cyber operations seemed distant from the concept of "armed".[73]

A recurring question in the cyber context is whether the damage or destruction or manipulation of data that does not generate such consequences is capable of qualifying as an armed attack. Generally it does not, for so qualifying such action would dramatically lower the threshold at which States would enjoy a right to forcefully respond to actions directed at them. This would contradict international law's general presumption against the resort to force in the absence of authorization by the Security Council.[74]

In light of the ever-increasing reliance of society on computers and computer networks, many readers, like the author, will find the "physical consequences" standard too narrow. But it does represent the lex lata, that is, the law that presently exists.[75]

2.2. *Jus in bello* – international humanitarian law

The notion of armed attacks under the jus ad bellum must not be confused with international

[70] See, Additional Protocol I to the Geneva Conventions, 1949
[71] Michael N. Schmitt, "Attack" as a Term of Art in International Law: The Cyber Operations Context, IEEE, 2012
[72] Ibid.
[73] Ibid.
[74] Ibid.
[75] Ibid.

humanitarian law's usage of the term "attack". In the latter body of law, an "attack" triggers a wide array of legal protections. The principle of distinction determines the restrictions which enable the parties to a conflict "to set the clear distinction between military people and civilians and to conduct operations only against military objectives".[76]

Article 51 is illustrative. Just by putting the prohibition on directing military operations against civilians, civilian objects and other protected persons and objects must be understood as essentially a prohibition on attacking them. Conducting military operations that do not qualify as attacks against them is, in a general sense, lawful (absent a specific prohibition to the contrary). A careful reading of Additional Protocol I's prohibitions and restrictions on attacks discloses that the concern was not so much with acts which were violent, but rather with those that have harmful consequences (or risk them), in other words, violent consequences. In great part, the treaty's object and purpose is to avoid, to the extent possible in light of military necessity, those very consequences.[77]

It is apparent that international humanitarian law, despite adopting an instrumentality-based definition of attack, takes a consequence-based approach to it normative prescriptions when operationalizing that term. The Bothe, Partsch and Solf commentary to Article 49 supports this conclusion by noting that attack refers to "those aspects of military operations that most directly affect the safety of the civilian population and the integrity of civilian objects".[78]

Through the process of induction, we can derive a general principle regarding the concept of attack, which has sense in the cyber context. Attacks can be redefined as operations that lead to or in the event that it was initially expected that unsuccessful attempts result in death or injury to people or destruction or damage to objects. The concept of injury includes a disease that can result from a cyber operation, for example, in the event of an attack on a wastewater treatment plant to infect drinking water.[79]

It is also reasonable, for example, based on the prohibition of terrorist attacks and hunger, to extend this concept to actions that lead to serious suffering, which otherwise are not justified by the notion of military necessity. Destruction includes operations that, without causing physical damage, nevertheless "break" the object, making it unworkable, as in the case of cyber

[76] Michael N. Schmitt, "Attack" as a Term of Art in International Law: The Cyber Operations Context, IEEE, 2012
[77] Ibid.
[78] Ibid.
[79] Ibid.

operation, which leads to the fact that the computer dependent system ceases to function if it is not repaired. Thus, a legal analysis of an attack in the context of international humanitarian law leads roughly to the same conclusion as with jus ad bellum.[80]

At the 37th International Conference of the Red Cross and Red Crescent Society in 2011, the ICRC circulated a background paper articulating a different approach. It began by noting that Article 49's reference to "acts of violence denote physical force". Accordingly, "cyber operations by means of viruses, worms, etc., that result in physical damage to persons, or damage to objects that goes beyond the computer program or data attacked could be qualified as 'acts of violence', i.e. as an attack in the sense of IHL".[81] There is universal agreement on this point.[82]

Once a cyber operation qualifies as an attack, Article 52(2)'s criteria for qualification as a military objective apply… and not before that determination is made. Should an object not constitute a military objective, a prospective attack thereon is prohibited. If it does, the object may, as a military objective, be attacked by any method or means of warfare that otherwise complies with the rule of proportionality, the requirement to take precautions in attack and other applicable standards. For instance, even when cyber operation can be employed to neutralize a military objective, an attacker may elect to bomb it doing so is not expected to exacerbate incidental harm to civilians, civilian objects and other protected persons and places.[83]

The creation of a legal line with regard to the Charter of the United Nations and the use of force standards generates geostrategic winners and losers, so the debate on the interpretation of the Charter has always reflected the distribution of power and vulnerability. This helps to explain what appears to be the emerging, though not yet formalized and publicized, US legal framework for cyberattacks, as well as some nascent rethinking from the standard US position on the use of force throughout much of the Charter's history.[84]

Even if the US government's assumptions about threats and conflicts are manifested in an uncertain future, other major state actors in this area are likely to have different views on drafting the legal line, as they perceive various strategic risks and opportunities. Therefore, it will be difficult to reach an agreement on interpretation. Moreover, the special characteristics of cyberattacks, including the low visibility of attacks and counter-actions, probable disputes about

[80] Michael N. Schmitt, "Attack" as a Term of Art in International Law: The Cyber Operations Context, IEEE, 2012
[81] Ibid.
[82] Ibid.
[83] Ibid.
[84] Ibid.

key facts and difficulties in establishing attribution and causation, will make it difficult to achieve a legal consensus around the US position. In the foreseeable future, the United States will have to continue its offensive and defensive strategy in an uncertain and volatile international legal framework.[85]

2.3. Passive and active state self-defense

The Tallinn Manual recognized that "a victim state is entitled to take proportionate measures to end harmful ongoing cyber operations if the state of origin fails to meet its obligations to end them".[86]

The use of only passive measures is no longer sufficient to protect networks in the face of rising threat levels.[87] The protective action which constitutes direct effect and seeks to diminish the scope of cyber attacks is considered to be the active cyber defense. On the other hand, the opposite notion – passive cyber defense – basically the actions which are the preparation stage for the active cyber defense. A lot of popular security controls employ active cyber defenses. Access controls block users from accessing unauthorized files and other resources. Passwords and other user authentication mechanisms block login attempts from adversaries spoofing legitimate users. Anti-malware systems, intrusion prevention systems (IPSs), and firewalls block malicious software and packets matching threat signatures or exhibiting anomalous behavior. Active cyber defenses also include operations against systems owned or used by an attacker, including counter-attacks.[88]

By contrast, passive cyber defenses include cryptography, security engineering and verification, configuration monitoring and management, providing enrichment for users by educating them, vulnerability assessment, risk assessment, making backup copies and initiating lost information restoration.[89]

Basically, the active cyber defense can be characterized by four features which identify the nature of this type of cyber defense: the scope of effects, types of effects, degree of automation and cooperation.[90]

---

[85] Matthew C. Waxman, Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), Yale Journal of International Law, Vol. 36, 2011
[86] Tallinn Manual 1.0 on the International Law Applicable to Cyber Warfare, 2013
[87] Pascal Brangetto, Tomáš Minárik, Jan Stinissen, From Active Cyber Defence to Responsive Cyber Defence: A Way for States to Defend Themselves – Legal Implications, Nato Legal Gazette, Dr. Petra Ochmannova, ACT SEE Deputy Legal Advisor, NATO CCD COE Publications, Tallinn, 2014
[88] Dorothy E. Denning, Framework and principles for active cyber defense, Computers & Security, 2014, p. 108-11
[89] Ibid.
[90] Ibid.

Scope of effects. This feature distinguishes between internal defenses, whose effects are limited to the network being defended, and external defenses, whose effects go beyond the network. Most cyber security controls such as access controls and IPSs are internal. An example of active defense with external effects is a botnet takedown that involves taking over the IP addresses and domain names used for command and control (C2).[91]

Degree of cooperation. This feature distinguishes between active defenses that are cooperative, meaning that action is one that performed against a system with the knowledge and consent of the system owner, from those that are non-cooperative, meaning it is not. Cyber defense that involve hacking back or attacking the attacker fall in the category of non-cooperative, external operations. A good example is an operation performed by the Georgian government against a Russian-based hacker who had waged a persistent, month-long campaign to steal confidential data from Georgian systems. Using a "water-hole" attack, the hacker had managed to infect Georgian computers with malware that exfiltrated files matching certain criteria to a drop site belonging to the hacker. To counter the hacker, the government planted a decoy ZIP archive on one of its infected machines, which the malware dutifully exfiltrated to the drop site. Once the hacker downloaded and opened the archive, it unleashed spyware that passed data from the hacker's machine back to the Georgian government, including a photo of the hacker taken by his own webcam. This example demonstrates the non-cooperative operation conducted by Georgia in order to protect their confidential data, but although the operation to plant spyware on the hacker's system was non-cooperative, it was the hacker's own actions and code that caused his system to be infected. The Georgian government did not directly hack his machine or any of the servers be used, but it constitutes active self-defense.[92]

Types of effects. This feature distinguishes four types of effects. The first, sharing, refers to actions that distribute threat information such as the IP addresses of attacking computers or the signatures of attack packets to other parties. Sharing occurs when anti-malware vendors ship out new signatures to their customers or victims report the domain names or IP addresses of malicious sites.[93]

The second type is a collection in which actions are taken to obtain additional information about the threat, for example, by activating or deploying additional sensors or by serving a court order or subpoena against the source or an IPS likely to have relevant information. When the

[91] Dorothy E. Denning, Framework and principles for active cyber defense, Computers & Security, 2014, p. 108-11
[92] Ibid.
[93] Ibid.

Coreflood botnet was taken down, for example, its attacker-controlled C2 servers were effectively replaced with C2 servers operated by the non-profit Internet Systems Consortium in collaboration with the federal government. The servers were set up to collect the IP addresses of the bots when they checked in for instructions. These addresses were then shared with the FBI, which in turn shared them with their associated ISPs so that the victims could be notified.[94]

Blocking is decided to be the third type of effect. The main task it performs is blocking unsecure or hostile activity, for instance, specific IP addresses or programs. The Coreflood example demonstrates the issue of lost control of the botnet by people who were regulated the connection and communication of bots and botnet. The outcome of that issue was the disability of addressing commands to the bots, and afterwards the command "to stop any activity" finished the hostile activity of the bots conducted by C2 servers. The illustrative were always firewalls, access controls, anti-malware controls for blocking purposes.[95]

The command take down, as in Coreflood, demonstrates the preemptive effect, which means attack source elimination. The unsecure servers (C2) were neutralized, meaning that they became total functioning disable.[96]

Degree of automation. This human involvement is related to the feature degree of automation. The human involvement with regard to this feature is considered to be important in order to finalize the operation. Such kind of process – the human involvement widely used in the manual active defense, where specific human actions are required, an automatic active defense, obviously, does not need any human assistance. Basically, humans' main function is the security software installation and updating when required by using the signature database. The final response is demonstrating no need in human involvement due to the fact that it is automated as well as malicious software detection.[97]

Active and cyber defenses should be employed only when doing so is ethical and legal. The following six principles aim to promote that only based on them the active cyber defense will consider to be appropriate and not prohibited: authority, third party immunity, necessity, proportionality, human involvement, and civil liberties.[98]

Authority. Active cyber defenses should be conducted only with authorities granted by laws,

[94] Dorothy E. Denning, Framework and principles for active cyber defense, Computers & Security, 2014, p. 108-113
[95] Ibid.
[96] Ibid.
[97] Ibid.
[98] Ibid.

contracts, and policies. The issue of the authority becomes especially problematic when defenses produce non-cooperative, external effects, say shutting down a botnet's C2 servers. In those cases additional authorities may be needed from the government, such as a court order. In general, governments, particularly their law enforcement, national security, and homeland defense arms, have greater authority than the private sector to conduct external, non-cooperative active defenses.[99]

The third party immunity. The principle in general prohibited any harm to the third party. Active cyber defenses should not internationally harm third parties. This includes any third party systems compromised by the attacker and used in the attacks. For example, an operation to shut down a botnet should not harm victim machines on the botnet.[100]

Necessity. The notion of necessity basically underlines that active cyber defenses should not be deployed unless they are necessary to mitigate the threat. This principle applies especially to operations that affect third parties: they should not be attacked or harmed in any way unless doing so is essential.[101]

Proportionality. One of the core principles of active cyber defenses that should not be deployed unless the harm incurred is proportionate to the benefits gained. In the domain of cyber, it is incumbent on those applying active defenses to know what effects they may have. Without that knowledge, the principle of proportionality cannot be reliably applied to determine whether an active defense is morally permissible.[102] According to the self-defense proportionality requirement, states' actions after, or in anticipation of, an armed attack must not exceed the amount of force necessary in order to stop the threat. Meaning that countermeasures taken against a state for a wrongful action, however, must be equivalent in effects to the injury suffered by the state taking the countermeasures. A somewhat broader approach was taken in the *Air Services case*, which incorporated into the assessment of proportionate countermeasures an evaluation of the right involved in the wrongful act, stating "it is essential in a dispute between states, to take into account not only the injuries suffered by the companies concerned but also the importance of the questions of principles arising from the alleged breach".[103]

[99] Dorothy E. Denning, Framework and principles for active cyber defense, Computers & Security, 2014, p. 108-113
[100] Ibid.
[101] Ibid.
[102] Ibid.
[103] Catherine Lotrionte, Countering State-Sponsored Cyber Economic Espionage Under International Law, The North Carolina Journal of International Law and Commercial Regulation, 2014

Human involvement. The principle of active cyber defenses that is refers to one of the main features meaning that there is a requirement of humans at some stage.[104]

Civil liberties. Active cyber defenses should respect the civil liberties of all persons affected, including their rights of privacy, free speech, and association.[105]

Furthermore, it is requisite that the act of self-defense is appropriately limited in scope to that which is necessary to prevent the infringement. Because of the requirement that the threat of attack be immediate, simply recognizing an accessed vulnerability would not seem to be enough to justify the use of anticipatory self-defense. Under this legal regime, the only instance in which cyber exploitation would appear to ever justify anticipatory self-defense is in the case where both (1) a cyber exploitation vulnerability that can be used at a future date is located and (2) where intelligence information that the particular vulnerability will in fact be used for an imminent attack has been obtained.[106]

[104] Dorothy E. Denning, Framework and principles for active cyber defense, Computers & Security, 2014, p. 108-113
[105] Ibid.
[106] Anna Wortham, Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Chartern Provisions Prohibiting the Threat or Use of Force?, Federal Communications Law Journal, 2011

3. International regulation of cyber espionage

3.1. The criminal law approach. Cyberspace weapon

Almost all states have enacted domestic laws that both restrict access to classified information as well as criminalize the act of an unauthorized taking of such information in order to deny intelligence gathering within their territories. Actual or threatened prosecution under these domestic laws takes the form of denial of information rather than an assertion by the state that the act is a *per se* in violation of international law, the legal issue is about individual criminal liability and not state responsibility. The suggestion that intelligence collection is illegal under international law is often based on the reasoning that espionage is criminalized in the domestic legal systems of most states and therefore, there is a sense that states must then view such activities as unlawful under international law.[107]

The only substantial international legal document developed to address issues related to cyberspace is the European Union's Convention on Cybercrime (Cybercrime Convention).[108] While the Cybercrime Convention does not address cyberspace attacks as possible acts of war and instead focuses on criminal acts, it does help establish a framework for a new methodology of analyzing cyberspace attacks.[109] The main objectives of the Convention on Cybercrime are as follows: to define criminal offenses, some of which are already determined in the Convention; to identify types of investigative powers that can fit into developing information technologies and harmonize procedures between states and also to identify options for international cooperation for the fruitful use of the Cybercrime Convention in the judicial practice and at the stages of the investigation.[110] There are some illustrative articles of the Cybercrime Convention.

Article 3 – Illegal interception:

"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such

[107] Catherine Lotrionte, Countering State-Sponsored Cyber Economic Espionage Under International Law, The North Carolina Journal of International Law and Commercial Regulation, 2014
[108] See, Convention on Cybercrime of the Council of Europe (CETS No.185), 2001
[109] Major Arie J. Schaap, Cyber Warfare Operations: Development and Use under International Law, Air Force Law Review, 2009
[110] Roderic Broadhurst, Developments in the global law enforcement of cyber-crime, 29 Policing Int'l J. Police Strat. & Mgmt. 408, 2006

computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system".[111]

Article 4 – Data interference:

"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right".[112]

Article 23 – General principles relating to international co-operation:

"The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence".[113]

Article 28 – Confidentiality and limitation on use:

"When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof…"[114]

The above presented articles from Cyber Crime Convention demonstrate, basically, general definitions of existing cyber threats and put an emphasis on the fact of necessity of international cooperation in any event, which could lead to the fruitful regulation of cyber space in international level.

Instead of focusing on the end result of a cyberspace event, the effects, and trying to determine whether such an act is a use of force or armed attack under international law, a criminal law methodology places increased emphasis on the genesis of a cyberspace event. The criminal law approach thus focuses on defining the beginning of a cyberspace event and not the effects, and

[111] See, Convention on Cybercrime of the Council of Europe (CETS No.185), 2001
[112] Ibid.
[113] Ibid.
[114] Ibid.

those definitions can then be applied to international law and military operations in cyberspace.[115]

The criminal law approach and methodology help resolve the issues of ambiguity, enforceability, and attribution for two reasons. First, it provides strong definitions that can withstand judicial scrutiny and allow for fair application to a variety of fact patterns. A nuance of this first strength is that criminal law definitions must also clearly put everyone on notice as to prohibited activities. The second strength is that the criminal law methodology requires the definition of a prohibited act to have some degree of intent, also known as the scienter element. Relying on these strengths, the criminal law approach creates a definition of a cyberspace crime that is clear, flexible, and requires a minimum level of intent. The criminal law methodology will then enable us to reverse engineer the definition of a cyberspace crime in order to establish the definition of a cyberspace weapon.[116]

As noted earlier, the Convention on Cybercrime of the Council of Europe is an international treaty intended to create consistency in criminal laws related to internet activities. Unfortunately, the Cybercrime Convention does not offer a definition of malicious logic or cyberspace weapon. Instead, the Cybercrime Convention identifies specific activities states should criminalize. Logically, the reason to prohibit certain activities is to avoid unwanted effects. The criminal law methodology is able to transform unwanted effects into specific definitions and prohibitions, whereas the current approach under international humanitarian law relies on an ambiguous analysis of facts using undefined prohibitions.[117]

The intent of the Cybercrime Convention was to set up a basic framework whereby the parties agreed to create their own state criminal codes to address broadly defined prohibited activities. Because the Convention defines prohibited activities broadly, it does not provide the detailed definitions of actual effects in cyberspace necessary to specifically define a cyberspace weapon. Nevertheless, the Convention's aspirational criminal law definitions of unlawful activity in cyberspace can help identify the international community's thoughts regarding unlawful cyberspace effects and thus the weapons that cause those effects. By looking at what types of activities the Cybercrime Convention intends to criminalize, it is possible to reverse engineer the definition of a cyberspace weapon.[118]

---

[115] Major Arie J. Schaap, Cyber Warfare Operations: Development and Use under International Law, Air Force Law Review, 2009
[116] Ibid.
[117] Ibid.
[118] Ibid.

Although the Cybercrime Convention does not provide definitions of key terms such as "damaging" or "altering", the Cybercrime Convention points us to the criminal codes of party states, such as the United States, to specifically define the *actus reus*. The criminal code of the United States is considered for several reasons: the United States invented the internet; the United States is arguably the largest user of cyberspace; the United States is a leading prosecutor of cyberspace crimes; and many nations work with the United States to solve cyberspace crimes. Section 1030 of Title 18 of the U.S. Code[119] criminalizes intentionally causing damage to a protected computer. Section 1030 is often used by U.S. Attorneys to prosecute persons who steal or corrupt data located on computer systems and persons who engage in denial of service attacks. Section 1030 defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information". This definition of "damage" recognizes the reality of what happens during a criminal hack or a cyberspace attack: "damage" in cyberspace does not require smashing, burning, or blowing things up. The U.S. Code provides a clear, judicially accepted and internationally recognized definition of damage in the cyberspace realm. From the above, we see that in its most simple terms, the definition of a weapon is "something that causes damage".[120]

First, one must consider whether particular cyberspace "tools" constitute weapons under international law.[121]

The ICRC Commentary on Article 35 of Additional Protocol I states:

"The words "methods and means" include weapons in the widest sense, as well as the way in which they are used."[122]

Next, one must analyze how the proposed definition of a cyberspace weapon can be applied in the real-world context of two recent "cyberspace attacks" in Estonia and Georgia. Considering the realities of these two events, does the proposed definition provide sufficient clarity for use in international law? Clearly, the event in Estonia resulted in reduced availability and impaired the integrity of the information located on computer systems in Estonia. Applying the attacker's methods to the proposed definition, it is clear these methods constituted "cyberspace weapons". The methods used by cyberspace attackers in Georgia caused a loss of access and impaired the

[119] See, Title 18 of the United States Code
[120] Major Arie J. Schaap (2009), *supra nota* 115
[121] Ibid.
[122] Ibid.

integrity of the data. Consequently, it is appropriate to label these methods as "cyberspace weapons".[123]

Thus, just as it is now generally recognized that it is the effect of the cyber-attack that determines whether or not the law of armed conflict is operationalized, a malicious code might be deemed a 'weapon' not solely by its intrinsic properties but also by the outcome it is designed to produce. In other words, only if it is established that a malicious code possesses an offensive capability and there is an intention to use it in a manner which comports with its offensive capability might the malware be deemed a 'cyber-weapon'. Accordingly, it is both the offensive capability of the malicious code and the intended outcome or effect produced by that code that transforms it into a weapon that would be governed, as with any conventional weapon, by the law of armed conflict.[124]

In June 2011, it was reported that the Pentagon had developed a classified list of cyber-weapons and cyber-tools including viruses with the capacity to sabotage an adversary's critical networks. This announcement would seem to suggest that the absence of international consensus on a definition for a 'cyber-weapon' might be indicative of a political impasse rather than there being any intrinsic attribute that precludes cyber-weapons from definition.[125] Even if agreement can be reached on what constitutes a cyber-weapon, whether their very properties make cyber-weapons simply incompatible with the rationale upon which arms control treaties are founded is warrants consideration.[126]

In order to regulate the cyber weapons, the author compares the Chemical Weapons Convention (CWC)[127] with not yet existing Cyber Weapons Convention which could possibly proceeding the first one in future. But one may distinguish that cyber warfare is not chemical warfare. Although they share some similarities – including ease of acquisition, asymmetric damage, and polymorphism – the tactics, strategies and effects are fundamentally different. Chemical warfare kills humans; cyber warfare kills machines.[128] There are some illustrative articles that could be applicable to cyber space and cyber weapons furthermore.

Article 7 – National implementations measures:

[123] Major Arie J. Schaap, Cyber Warfare Operations: Development and Use under International Law, Air Force Law Review, 2009
[124] Louise Arimatsu, A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations, NATO CCD COE Publications, 2012
[125] Ibid.
[126] Ibid.
[127] See, Chemical Weapons Convention, 1993
[128] Kenneth Geers, Cyber Weapons Convention, Computer Law & Security Review, 2010

"Each State Party shall, in accordance with its constitutional processes, adopt the necessary measures to implement its obligations under this Convention. In particular, it shall: … prohibit natural and legal persons anywhere on its territory or in any other place under its jurisdiction as recognized by international law from undertaking any activity prohibited to a State Party under this Convention, including enacting penal legislation with respect to such activity ..."[129]

Article 9 – Consultations, cooperation and fact-finding:

"States Parties shall consult and cooperate, directly among themselves, or through the Organization or other appropriate international procedures, including procedures within the framework of the United Nations and in accordance with its Charter, on any matter which may be raised relating to the object and purpose, or the implementation of the provisions, of this Convention …"[130]

Article 11 – Economic and technological development:

"The provisions of this Convention shall be implemented in a manner which avoids hampering the economic or technological development of States Parties, and international cooperation in the field of chemical activities for purposes not prohibited under this Convention including the international exchange of scientific and technical information and chemicals and equipment for the production, processing or use of chemicals for purposes not prohibited under this Convention …"[131]

Article 14 – Settlement of disputes:

"When a dispute arises between two or more States Parties, or between one or more States Parties and the Organization, relating to the interpretation or application of this Convention, the parties concerned shall consult together with a view to the expeditious settlement of the dispute by negotiation or by other peaceful means of the parties' choice, including recourse to appropriate organs of this Convention and, by mutual consent, referral to the International Court of Justice in conformity with the Statute of the Court. The States Parties involved shall keep the Executive Council informed of actions being taken …"[132]

It is obvious, that present articles seek to represent the mutual states' cooperation with regard to the all possibly emerged issues – the principle, which could be used in the future draft of Cyber

[129] See, Chemical Weapons Convention, 1993
[130] Ibid.
[131] Ibid.
[132] Ibid.

Weapons Convention and which could be recognized as the core principle in the field of usage of cyber weapons regulation.

Talking about Cyber Weapons Convention, we could see its development through the principles applied in Chemical Weapons Convention, such as first three principles – political will, universality, and assistance – are easy to apply in the cyber domain. None of them is a perfect fit, but as with CWC, all of them are appropriate to the nature and challenges of managing Internet security and the final two principles – prohibition and inspection – are not helpful at this time. It is difficult to prohibit something that is hard to define, and not easy to inspect something that grows by orders of magnitude on a regular basis.[133] If we refer to the issue of prohibition of cyberspace weapons as such, one must recognize that by contrast to other weapons that command public condemnation because they appear unambiguously indiscriminate or inflict unnecessary suffering, cyber-weapons are often regarded as a panacea that can achieve precisely the opposite: sanitize warfare and even prevent the use of kinetic force. Thus, rightly or wrongly, there is little public appetite to support a total ban.[134]

The line between what is a cyber-weapon and what is not a cyber-weapon is subtle. But drawing this line is important. For one, it has security consequences: if a tool has no potential to be used as a weapon and to do harm to one or many, it is simply less dangerous. Secondly, drawing this line has political consequences: an unarmed intrusion is politically less explosive than an armed one. Thirdly, the line has legal consequences: identifying something as a weapon means, at least in principle, that it may be outlawed and its development, possession, or use may be punishable. It follows that the line between weapon and non-weapon is conceptually significant: identifying something as not a weapon is an important first step towards properly understanding the problem at hand and to developing appropriate responses.[135]

The most common and probably the most costly form of cyber-attack targets to spy. But even a highly sophisticated piece of malware that is developed and used for the sole purpose of covertly exfiltrating confidential data from a network or machine is not a weapon. A bug is not a weapon either.[136] Therefore, the notion of cyber-weapon requires more precise definition to qualify it as weapon in the meaning as kinetic weapon.

It is possible to outline the following typical elements of a cyber-weapon:

[133] Kenneth Geers, Cyber Weapons Convention, Computer Law & Security Review, 2010
[134] Louise Arimatsu, A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations, NATO CCD COE Publications, 2012
[135] Thomas Rid, Cyber-Weapons, The RUSI Journal, 2012
[136] Ibid.

- the aim must be specific, therefore, the "part of equipment, a device, or any set of computer instructions" do not have to be created with the aim of reaching their maximum diffusion, as it happens for generic malware (except for the case of concealment of the real purposes of an attack);[137]
- the information systems which have been hit must be classified as a sensitive target of the attacked subject;[138]
- the purpose must be to actively penetrate the target's information systems (not just to cause a simple dysfunction) and with malicious ends;[139]
- the information systems of the target must be protected;[140]
- tangible or significantly detectable damage must be caused.[141]

3.2. Existing international law norm with regard to cyber space

According to West's Encyclopedia of American Law, espionage is "[t]he act of securing information of a military or political nature that a competing nation holds secret," and it is "commonly known as spying ..."[142] As stated previously, federal criminal laws prohibit the practice of espionage, but it is a generally accepted activity in the international community.[143]

Until recently, there was significant consensus about international law's relation to espionage. With a few exceptions discussed below, most scholars agree that international law either fails to regulate spying or affirmatively permits it.[144]

The general starting point for determining the international legality of state conduct is the well-known *Lotus* principle. Stated succinctly, this principle provides that international law leaves to states "a wide measure of discretion which is limited only in certain cases by prohibitive rules"[145] and that in the absence of such rules "every state remains free to adopt the principles which it regards best and most suitable".[146] There is no specific international treaty that regulates

[137] Stefano Mele, Cyber-weapons:legal and strategic aspects, Observatory Inforwarfare and Emerging Technologies, Italian Institute of Strategic Studies 'Niccolò Machiavelli', 2013
[138] Ibid.
[139] Ibid.
[140] Ibid.
[141] Ibid.
[142] Lehman J., and Phelps S., West's Encyclopedia of American Law, Detroit: Thomson/Gale, 2005, available at: http://www.worldcat.org/title/wests-encyclopedia-of-american-law/oclc/57301521 (16.05.2017)
[143] Anna Wortham, Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Chartern Provisions Prohibiting the Threat or Use of Force?, Federal Communications Law Journal, 2011
[144] Ashley Deeks, An International Legal Framework For Surveillance, Virginia Journal of International Law, 2015
[145] See, P.C.I.J. (ser. A) No. 10 (Sept. 7) 1927, *S.S. Lotus case* (France v. Turkey), para. 40
[146] Ibid.

cyber espionage. There is also no specific international treaty that regulates espionage and which could be adapted to regulate cyber espionage. However, in an international legal order premised upon the sovereign equality of states, it is inherent in the nature of an intrusive trans-boundary activity such as cyber espionage that this type of conduct can run into conflict with general principles of international law. In this sense, whilst cyber espionage is not specifically regulated by international law it may be nevertheless unlawful when appraised against general principles of international law.[147]

In international law the emergence of the concept of sovereignty "coincided with the emergence of the state as a political unit following the apportionment of territories and the political and legal recognition of such territorial compartmentalization by the Treaty of Westphalia".[148] As a result, sovereignty is typically understood as the right of states to exercise exclusive authority over their territory.[149]

In order to constitute a violation of the principle of territorial sovereignty is the mere intrusion into a state's territory unlawful or, in addition, must the intrusion produce physical damage? This is an important question in the context of cyber espionage because this is a practice that describes the accessing and copying of confidential information and is committed regardless of whether information is lost or damaged (in the sense that it is modified or deleted); in short, cyber espionage cannot be said to produce physical damage.[150]

In the *Lotus case*, the Permanent Court of International Justice explained that the "first and foremost restriction imposed by international law upon a state is that – failing the existence of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another state".[151] Several government officials and scholars believe that the *Lotus* approach provides the best way to think about espionage in international law. For them, the idea is simply that nothing in international law forbids states from spying on each other; states therefore may spy on each other - and each other's nationals - without restriction. Espionage is therefore unregulated in international law. Further, this group would point to the widespread practice of espionage to counter any suggestion that a customary international law had developed against spying. In this view, ideas such as non-intervention and sovereignty developed against a

[147] Russell Buchan, The International Legal Regulation of State-Sponsored Cyber Espionage. Chapter 4, International Cyber Norms Legal, Policy & Industry Perspectives, Anna-Maria Osula and Henry Rõigas (Eds.), NATO CCD COE Publications, Tallinn 2016
[148] Ibid.
[149] Ibid.
[150] Ibid.
[151] See, P.C.I.J. (ser. A) No. 10 (Sept. 7) 1927, *S.S. Lotus case* (France v. Turkey), para. 39

background understanding that states do and will spy on each other, thus establishing a carve-out for espionage within those very concepts.[152]

Other scholars interpret the widespread state practice of espionage as indicating that states affirmatively recognize a right to participate in such type of conduct. Indeed, government officials have publicly asserted that spying is permissible. President Obama recently stated that "few doubt[[ ] the legitimacy of spying on hostile states".[153] Though legitimacy and legality are not identical, this is a relatively bold affirmation that the United States spies, at least on non-friendly states. British Prime Minister David Cameron reportedly pointed out at a European Union summit that espionage capabilities have prevented many terror attacks.[154] The former French foreign minister, Bernard Kouchner, stated, "The magnitude of the eavesdropping is what shocked us . . . . Let's be honest, we eavesdrop too. Everyone is listening to everyone else".[155] The fact that certain states have entered into arrangements with other states to limit such spying is additional evidence that international law either permits or does not prohibit spying. If international law prohibited such espionage, these agreements would be unnecessary. At the very least, the existence of these arrangements proves that international law is unclear about whether it regulates espionage and states seek to secure themselves from unauthorized intrusion.[156]

In the *Corfu Channel case* the ICJ determined that "the UK's decision to send warships into Albania's territorial waters to collect evidence of illegal mining represented an unauthorized incursion into Albania's territory and thus constituted a violation of Albanian sovereignty".[157] Although physical evidence was collected from Albanian territory, a careful reading of the ICJ's judgment reveals that the Court determined that the UK's conduct was unlawful solely on the basis of its unauthorized intrusion into Albania's territorial sea.[158]

However on the face of it cyberspace would appear immune from territorial sovereignty because

---

[152] Ashley Deeks, An International Legal Framework For Surveillance, Virginia Journal of International Law, 2015

[153] President Barack Obama, Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014) [hereinafter Obama NSA Speech]

[154] Appelbaum J. et al., The NSA's Secret Spy Hub in Berlin, Der Spiegel (Kristen Allen & Charly Wilder trans., Oct. 27, 2013, 7:02 PM), available at: http://www.spiegel.de/internation al/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html (16.05.2017)

[155] Hinnant L. and Dahlburg J-T, Let's be honest, we eavesdrop too: former French foreign minister on NSA spying claims, The Associated Press Published Wednesday, 2013, available at: http://www.ctvnews.ca/sci-tech/let-s-be-honest-we-eavesdrop-too-former-french-foreign-minister-on-nsa-spying-claims-1.1509912 (16.05.2017)

[156] Ashley Deeks (2015), *supra nota* 152

[157] I.C.J. 1949 I.C.J 4. 22, *Corfu Channel case* (United Kingdom v. Albania), p. 28, para. 2

[158] Russell Buchan, The International Legal Regulation of State-Sponsored Cyber Espionage. Chapter 4, International Cyber Norms Legal, Policy & Industry Perspectives, Anna-Maria Osula and Henry Rõigas (Eds.), NATO CCD COE Publications, Tallinn 2016

it is a virtual, borderless domain, it must nevertheless be appreciated that cyberspace is a man-made environment that "requires physical architecture to exist", including fibre-optic cables, copper wires, microwave relay towers, satellite transponders, Internet routers etc. As a result, where computer networks are interfered with, or where information is interfered with that is located on those networks, and those networks are supported by cyber infrastructure physically located in a state's territory, that state's territory can be regarded as transgressed and thus a violation of the principle of territorial sovereignty occurs.[159]

State practice in this area is instructive and indicates that where computer systems are accessed and information is obtained that is resident on or transmitting through those computer networks, states consider their territorial sovereignty violated where those networks are supported by cyber infrastructure located within their territory. To put the same matter differently, there is state practice to suggest that where a state considers itself to have been the victim of cyber espionage it regards such behaviour as falling foul of the principle of territorial sovereignty.[160]

It is possible that a state's confidential information may be intercepted as it is being transmitted through cyber infrastructure located on the territory of another state. In addition, since the emergence of cloud computing (and indeed its now widespread use), many states may even store confidential information in a central server that is located in the territory of another state. In such situations, although a state may assert ownership over the information that has been intercepted, there is no territorial basis on which it can claim a violation of its territorial sovereignty. Here is that the principle of non-intervention becomes important. The non-intervention principle therefore represents international law's attempt to protect a state's sovereign right to determine its internal and external affairs free from external intervention.[161]

As the Tallinn Manual noted, "[c]yber operations into another state violate the principle of non-intervention, and accordingly qualify as internationally wrongful acts, when intended to coerce (as opposed to merely influence) the targeted state's government in matters reserved to that state".[162]

In order for an unlawful intervention to occur it must be established that:

1) the act committed intervenes in a state's sovereign affairs;

[159] Russell Buchan, The International Legal Regulation of State-Sponsored Cyber Espionage. Chapter 4, International Cyber Norms Legal, Policy & Industry Perspectives, Anna-Maria Osula and Henry Rõigas (Eds.), NATO CCD COE Publications, Tallinn 2016
[160] Ibid., p. 71
[161] Ibid.
[162] Tallinn Manual 1.0 on the International Law Applicable to Cyber Warfare, 2013

2) that the act is coercive in nature. The application of these two elements to acts of cyber espionage against information which is being stored on or transmitted through cyber infrastructure located within the territory of another state will now be considered.[163]

First and foremost, in order to establish an unlawful intervention the act in question must have a bearing upon matters which, by virtue of the principle of state sovereignty, a state is entitled to decide freely. The purpose of this criterion is to assess whether the alleged intervention pertains to a matter that is permissibly regulated by states on the basis that it falls within their sovereign authority, or whether states have instead determined through international law that it is a matter that falls outside of the realm of state sovereignty. In the context of the current discussion, the important question is whether states exercise sovereignty over information that they have authored and compiled but which is stored on or being transmitted through cyber infrastructure located on the territory of another state.[164]

The recent *East Timor v Australia* litigation before the ICJ is also instructive here. East Timor alleged that Australia had sent its agents into the office of an Australian lawyer acting as legal counsel for East Timor to collect confidential information relating to existing litigation between the two states. The office was physically located in Australia. East Timor applied to the ICJ for a provisional order that declared "[t]hat the seizure by Australia of the documents and data violated the sovereignty of Timor-Leste and that "Australia must immediately return to the nominated representative of Timor-Leste and all of the aforesaid documents and data, and to destroy beyond recovery every copy of such documents and data that is in Australia's possession or control".[165] In addressing these requests, the ICJ noted that "[a]t this stage of proceedings, the Court is not called upon to determine definitively whether the rights which Timor-Leste wishes to see protected exist; it need only decide whether the rights claimed by Timor-Leste on the merits, and for which it is seeking protection, are plausible".[166] Importantly, the ICJ did consider East Timor's claim "plausible" and granted a provisional order that "Australia must not interfere in any way in communications between Timor-Leste and its legal advisers",[167] indicating that this conclusion "might be derived from the principle of the sovereign equality of states, which is

[163] Russell Buchan, The International Legal Regulation of State-Sponsored Cyber Espionage. Chapter 4, International Cyber Norms Legal, Policy & Industry Perspectives, Anna-Maria Osula and Henry Rõigas (Eds.), NATO CCD COE Publications, Tallinn 2016
[164] Ibid.
[165] Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia), 147 Reports of Judgments, International Court of Justice 2014, para. 2
[166] Ibid., para. 26
[167] Ibid., para. 55

one of the fundamental principles of the international legal order and is reflected in Article 2, paragraph 1, of the Charter of the United Nations".[168]

State's sovereignty extends to its property (providing this property is used for exclusively non-commercial purposes) even when this property is physically located in the territory of another state and, as such, is considered inviolable. The data which belongs to a state but which is being stored on or transmitted through cyber infrastructure located on the territory of another state possesses "national data sovereignty" and interference with that data (for the purpose of espionage, for example) can be regarded as an intrusion into state sovereignty.[169]

In order to establish an unlawful intervention it must then be determined that the intervention is coercive in nature. The leading authority on the meaning of coercion is the *Nicaragua judgment*. In this case the ICJ defined coercion as acts interfering with "decisions" and "choices" of the victim state in relation to matters falling within its sovereignty. In this sense, the dividing line between permissible influence and impermissible intervention in sovereign affairs is whether the act in question compels the state to act, or to abstain from acting, in a manner that it would not have voluntarily chosen.[170]

This broader reading of the term coercion finds support within academic commentary. McDougal and Feliciano argue that a finding of coercion can be made whenever there is an attack against the "value" of sovereignty.[171]

This expansive understanding of coercion also finds support in state practice and the practice of international organizations, notably the UN General Assembly. The 1965 UN Declaration on the Inadmissibility of Intervention and the 1970 Friendly Relations Declaration employ identical language in articulating the scope of the non-intervention principle, explaining that no state has "the right to intervene, directly or indirectly, for any reason whatever, in sovereignty of any other State" or use "any…measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights".[172]

Additional support for this broader reading of the non-intervention principle is evident from the

[168] Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia), 147 Reports of Judgments , International Court of Justice 2014, para. 27
[169] Russell Buchan, The International Legal Regulation of State-Sponsored Cyber Espionage. Chapter 4, International Cyber Norms Legal, Policy & Industry Perspectives, Anna-Maria Osula and Henry Rõigas (Eds.), NATO CCD COE Publications, Tallinn 2016
[170] Ibid.
[171] Ibid.
[172] Ibid.

reaction of the Soviet Union to the US's exploitation of outer space for purpose of unauthorized surveillance in the 1960s. Even in the absence of a violation of its territorial sovereignty the Soviet Union asserted that the US's conduct constituted a violation of its political integrity and in making this determination explained that "in all cases an intrusion into something guarded by a sovereign state in conformity with its sovereign prerogative" is unlawful.[173]

Customary international law emerges on the basis of "general practice accepted as law". There are thus two elements of customary international law. First, state practice and second, the requirement of this practice to be accompanied by a belief that it is permitted under international law (*opinio juris*). The burden is on those asserting the existence of customary rule to demonstrate that these two criteria are met.[174]

In relation to state practice, in the North Sea Continental Shelf Cases the ICJ explained that in order to find that a customary rule has emerged there must be "extensive and virtually uniform" state practice in favour of that rule.[175]

However, in order to qualify as state practice it must be conducted publically and openly and state practice committed in secret is irrelevant to the formation of customary international law. In relation to state practice committed in secret, the International Law Commission's Second Report on the Identification of Customary International Law explains that "[i]t is difficult to see how [such] practice can contribute to the formation or identification of general customary international law".[176]

Almost by definition, espionage is a practice conducted in secret. As a result, regardless of how frequently states engage in espionage, where this practice is engaged in covertly and secretly it cannot be classified as state practice for the purpose of customary law formation. In the context of espionage, the International Law Association's Committee on the Formation of Customary International Law explains that "a secret physical act (e.g. secretly "bugging" diplomatic premises) is probably not an example of the objective element [of state practice]".[177]

The events surrounding *Sony case* in late 2014 are also illustrative. As is well known, Sony intended to release a film entitled The Interview which depicted the assassination of the leader of

[173] Russell Buchan, The International Legal Regulation of State-Sponsored Cyber Espionage. Chapter 4, International Cyber Norms Legal, Policy & Industry Perspectives, Anna-Maria Osula and Henry Rõigas (Eds.), NATO CCD COE Publications, Tallinn 2016
[174] Ibid.
[175] Ibid.
[176] Ibid.
[177] Ibid.

North Korea. Days before its release Sony's computer networks were accessed without authorization and malware was introduced which wiped a substantial amount of confidential information. In addition, certain confidential information was exfiltrated and published on the Internet, including sensitive email correspondence between the company and its employees (well-known actors) and storylines for forthcoming films. The US Federal Bureau of Investigation (FBI) determined that North Korea was responsible for this malicious cyber conduct.

Although the US did not specify on what basis this conduct constituted a violation of international law, the U.S. explained that it would "respond proportionally and in a space, time and manner that we choose".[178] Indeed, on 2 January 2015 the U.S. imposed economic sanctions against North Korea, including freezing its assets in the U.S. As we know, under international law a state that is subject to an internationally wrongful act is entitled (subject to caveats) to adopt proportionate countermeasures in order to compel the wrongdoing state to discontinue its internationally wrongful conduct and make appropriate reparations.[179]

One stark example of the difficulty of prosecuting international cyber espionage is the plight of AMSC, a U.S. firm specializing in software for wind turbines whose core product was allegedly stolen by Chinese turbine manufacturer Sinovel Wind Group Co. in 2011. Sinovel reportedly convinced an AMSC engineer to misappropriate code from Wisconsin, decrypt it in Austria, and email it to China. AMSC did not promptly detect the IT breach; rather, it identified the leak only after accidentally discovering its code in a Sinovel test facility in China.[180]

By the time AMSC launched a cyber investigation, contacted the FBI, and ultimately obtained an indictment, counterfeit copies of their software had already been sold back into the United States in Sinovel's products. Hamstrung by deficient cyber-intelligence, AMSC's legal action proved to be too little too late. The named defendants are now all in non-extradition countries and Sinovel has deployed litigation defense tactics that have stalled the case in U.S. courts while AMSC's stock has fallen from $370 per share to $5 per share.[181]

Therefore, this chapter does not deny the importance of intelligence-gathering in the contemporary world order. However, one must distinguish between intelligence-gathering from

[178] Russell Buchan, The International Legal Regulation of State-Sponsored Cyber Espionage. Chapter 4, International Cyber Norms Legal, Policy & Industry Perspectives, Anna-Maria Osula and Henry Rõigas (Eds.), NATO CCD COE Publications, Tallinn 2016
[179] Ibid.
[180] David J. Kappos, Pamela Passman, Cyber Espionage Is Reaching Crisis Levels, Fortune, 2015
[181] Russell Buchan (2016), *supra nota* 178

publically available sources and intelligence-gathering from private, unauthorized sources, namely espionage. Information collection constitutes unproblematic issue if it obtains this information from open source. One must also distinguish between authorized and unauthorized intelligence gathering. Intelligence that is gathered pursuant to a treaty regime or Chapter VII Security Council Resolution, for example, can be regarded as authorized, and for this reason is not properly regarded as espionage.[182]

This chapter has examined the international legality of trans-boundary state-sponsored cyber espionage and has argued that cyber espionage constitutes a violation of the territorial sovereignty of a state where information is accessed that is resident on computer networks that are supported by cyber infrastructure located on that state's territory. It has been identified recent state practice which supports this conclusion. It has been also argued that cyber espionage violates the principle of non-intervention where it has a more than insignificant impact on the authority structures of a state. The utility of the non-intervention principle is particularly apparent in relation to information that belongs to a state but is located on cyber infrastructure in the territory of another state. Finally, it has been argued that customary international law develops on the basis of transparent, publically observable state conduct that is committed in the belief that it is permissible under international law. As espionage is a practice that is by definition committed in secret, and where states overwhelmingly refuse to admit responsibility for such conduct let alone justify it as acceptable under international law, it has been concluded that there is no customary "espionage exception" to the principles of territorial sovereignty and non-intervention.[183]

For the evolution of international norms on espionage: domestic laws, which continue to evolve, but provide at least basic substantive and procedural rules about domestic and transnational surveillance, will affect the way in which those international norms develop. These laws have proven to work effectively in practice (at least as far as they govern domestic and transnational surveillance); have been the subject of public debates during which legislators have considered how to balance privacy and security; and are (mostly) publicly accessible. Furthermore, to the extent that general international norms track common concepts reflected in states' domestic laws, external observers may have greater confidence that states will comply with the international

[182] Russell Buchan, The International Legal Regulation of State-Sponsored Cyber Espionage. Chapter 4, International Cyber Norms Legal, Policy & Industry Perspectives, Anna-Maria Osula and Henry Rõigas (Eds.), NATO CCD COE Publications, Tallinn 2016
[183] Ibid.

norms, because governments tend to comply more rigorously with domestic laws than international law.[184]

3.3. The legal treatment of cyber espionage as a separate notion

Cyber espionage operations have been taking place since at least the 1990s, with the emergence of the Internet allowing governments to collect information more pervasively than traditional human methods of collecting information clandestinely. Similar to traditional, political, or military espionage, cyber espionage, or cyber exploitation, constitutes the acquisition of information to inform policymakers about actual or potential threats, and does not rise to the level of a use of force or armed attack under international law. Given that they are similar in their objectives, cyber security experts have argued that cyber espionage should have the same legal status as traditional, political, and military espionage. By extension, cyber espionage in line with the same objectives of traditional espionage may be seen as acceptable state practice under international law as long as such activities stay within the bounds of acceptable limits analogous to those rules of traditional espionage that have been accepted by states.[185]

Many forms of malware are strictly tools of espionage: they do not directly damage the targeted nation's information systems, or cause damage via these information systems. In this sense, they are not themselves cyber weapons. In such cases, it is only through the use of gathered information by an enemy that a nation's interest may be harmed. Traditionally, mere espionage has not been viewed as a *casus belli* (customary or legitimate reason for going to war), but may bring non-military retaliation, such as the expulsion of diplomats or the limiting of foreign aid or commerce.[186]

Open societies enjoying strong international relationships and possessing such advanced industries as telecommunications, mining, agriculture, biotechnology, and the aerospace industry make for especially attractive cyber-espionage targets. The cyber dimension has changed the character of espionage. Hitherto, espionage was a practice of intelligence professionals.[187]

Today, along with attempts at statecraft, non-state entities have embarked on cyber-espionage and cyber-sabotage efforts, often motivated by ideological, political, and economic considerations. Proxies and technologies make detection and attribution difficult. The espionage

[184] Ashley Deeks, An International Legal Framework For Surveillance, Virginia Journal of International Law, 2015
[185] Catherine Lotrionte, Countering State-Sponsored Cyber Economic Espionage Under International Law, The North Carolina Journal of International Law and Commercial Regulation, 2014
[186] Randall R. Dipert, The Ethics of Cyberwarfare, Journal of Military Ethics, 2010
[187] Martin Rudner, Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge, International Journal of Intelligence and Counter Intelligence, 2013

objective of gaining strategic advantage by stealing secrets to identify an adversary's capabilities, strengths, and weaknesses can now be achieved through proxies and virtual means which are deniable and considerably more diverse and ephemeral. That the same *modus operandi* may be utilized by opportunistic criminals, activists, corporate competitors, or foreign governments can make the task of identifying perpetrators, their intentions, and targets an elusive exercise, at least in the early stages.[188]

Indeed, there is no clear consensus among states on the legal nature of espionage or whether states enjoy a right at international law to complain of it. Oddly, espionage remains "ill-defined under international law, even though all developed nations, as well as many lesser-developed ones, conduct spying and eavesdropping operations against their neighbors".[189] Although no international agreement expressly condones espionage, "states do not reject it as a violation of international law".[190] This historical acceptance has given espionage the appearance of lawful activity, "grounded in the [states'] recognition that "custom" serves as an authoritative source of international law".[191] To the extent states are concerned with espionage at all, it is espionage at wartime that vexes them most.[192]

While the International Group of Experts agreed that there is no prohibition of espionage *per se*, they likewise concurred that cyber espionage may be conducted in a manner that violates international law due to the fact that certain of the methods employed to conduct cyber espionage are unlawful. In other words, if an aspect of a cyber espionage operation is unlawful under international law, it renders the cyber espionage unlawful.[193]

Due to the fact that all the states conduct espionage, this type of activity is considered as acceptable under international law and constitutes no violation. The problem is that states constantly violate national law; therefore such acts as unauthorized intelligence gathering constitute criminal offences, which lead to prosecution and investigation processes. One might keep in mind that sensitive data can be lost because of several possibilities, not only by cyber espionage.[194]

---

[188] Martin Rudner, Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge, International Journal of Intelligence and CounterIntelligence, 2013
[189] Christina Parajon Skinner, An International Law Response to Economic Cyber Espionage, Connecticut Law Review, 2014
[190] Ibid.
[191] Ibid.
[192] Ibid.
[193] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2017
[194] Herbert Lin, Why Computer Scientists Should Care About Cyber Conflict and U.S. National Security Policy, Communications of the ACM, 2012

On the issue of espionage, the capability necessary for network exploitation is generally lower than that required for destructive attacks, particularly in the realm of economic espionage where private sector companies are targeted. What we lack is not so much an ability to attribute attacks, but international norms that keep espionage limited. Espionage is generally recognized to be permissible under certain circumstances and many scholars will argue that it has a stabilizing effect on the international system by reducing paranoia. As has been recently demonstrated by the discovery of a Russian spy ring in the United States, engaging in espionage is not necessarily considered a hostile act and can be resolved without further escalation. The challenge with cyber espionage is that we lack norms that limit the extent to which states engage in it. This problem is exacerbated by the fact that cyber espionage is not constrained by the costs, consequences and limitations of traditional espionage.[195]

Whatever country or countries are behind this espionage campaign, the people who are carrying it out are working safely from within the borders of their own country at little risk of being discovered or imprisoned. The low cost and low risk of cyber espionage is the problem, not the difficulty in attributing the source of the activity. It may be time that we recognize cyber espionage to be a different phenomenon from traditional espionage, one that requires a different set of norms and responses.[196]

The American point of view on the current threat of a cyber espionage basically noted that is too difficult to control such a problem under existing criminal law due to the lack of appropriate legal norms related to cyber way of conducting espionage.

The problem of cyber-espionage, whether economic or industrial, is too complex a problem at this time to be individually prosecuted through a single federal criminal statute. The aims of criminal law, such as deterrence and retribution, are unattainable when it is nearly impossible to investigate and assign blame to an actor using traditional criminal law formulas.[197]

However, it would be a mistake to afford the same legal treatment to different type of cyber espionage. For one, unlike traditional espionage, cyber espionage takes place on a much larger scale. The volume of information stolen via cyberspace, using cyber tools, is much more significant and happens at a quicker pace than traditional human or technical intelligence gathering. Moreover, the penetration of computer systems and databases is far more difficult to

[195] Robert K. Knake, Untangling Attribution: Moving to Accountability in Cyberspace, The Council on Foreign Relations, 2010
[196] Ibid.
[197] Gerald O'Hara, Cyber-Espionage: A Growing Threat to the American Economy, Journal of Communictions Law and Policy, 2010

detect and stop than traditional human espionage. Finally, with cyber espionage, there is no custom of reciprocity or cooperation that states should be concerned about preserving. For these reasons, it is a mistake not to draw any legal distinction between traditional espionage and cyber espionage.[198]

The lack of meaningful international law on traditional spying and economic espionage allows cyber espionage to operate in a legal black hole. The legal black hole surrounding cyber espionage adversely affects the search for norms of responsible behavior in cyberspace because it increases incentives for states to develop capabilities and engage in activities that heighten suspicion among countries and also weaken interest in robust international cooperation and rules that could mitigate cyber security threats.[199]

The technology needed to launch a cyber attack or exploitation is widely available today. Non-state actors can launch cyber attacks and exploitations quite easily and can often do just as much harm as state actors. The inability to know whether an actor is a state actor or not makes applying LOAC and the UN Charter difficult because these laws are built upon the presumption that it is clear when LOAC should be applied and when national criminal laws should be applied.[200]

In many cases, the cyber activity of non-state actors falls squarely within a broad category of cyber crime, but perhaps can also be categorized as cyber espionage. Some acts, however, pose a threat not just to private companies or industry, but in a more comprehensive way to the national security of the state. The transition from domestic and cross-border law enforcement to more forceful responses depends on an analysis of how and when international law establishes a right for states to use force and in what manner.[201]

The International Group of Experts agreed that cyber operations conducted by non-state actors that are not attributable to states do not violate the sovereignty of the state into which they are launched, constitute intervention, or amount to a use of force because these breaches can be committed only by states. This is so irrespective of any consequences caused by such operations.

[198] Christina Parajon Skinner, An International Law Response to Economic Cyber Espionage, Connecticut Law Review, 2014
[199] David P. Fidler, Tinker, Tailor, Soldier, Duqu: Why cyberespionage is more dangerous than you think, International Journal of Critical Infrastructure Protection, 2012
[200] Anna Wortham, Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Chartern Provisions Prohibiting the Threat or Use of Force?, Federal Communications Law Journal, 2011
[201] Laurie R. Blank, International Law and Cyber Threats from Non-State Actors, International Law Studies, 2013

With respect to a violation of sovereignty, the Experts acknowledged the existence of a contrary view.[202]

Resultantly, states cannot resort to countermeasures in response to cyber operations by non-state actors unless those operations are attributable to another state. However, in some cases the failure of a state to terminate cyber operations conducted by non-state actors on its territory will constitute a breach of the requirement to exercise due diligence. Additionally, certain non-state cyber operations permit the target states to directly respond against the non-state actors abroad conducting them. Furthermore, responses directed against non-state actors may be permissible pursuant to the law of self-defense.[203]

In some circumstances, non-state actors may engage in cyber operations that are contrary to international human rights law or the law of armed conflict such that individual criminal responsibility attaches pursuant to international criminal law.[204] Nations seem to agree that espionage, among other activities, is not enough to count as a use of force. And many nations recognize cyber exploitation as a new method of espionage.[205]

Many of the considerations that the new laws should take into account are the difficulties discussed previously with applying LOAC and the UN Charter to cyber threats: the new governing laws need to take into consideration that today's society is heavily reliant on an infrastructure that is controlled by information technology, that cyber weapons are easily available and can easily be used by non-state actors, that conflict is not just between nations and national military forces anymore, that military and civilian sectors are interconnected and share information technology, that cyber exploitation is different from traditional espionage, and that the actors of cyber attacks often cannot be identified.[206]

It must be cautioned that it can be challenging for a target state to distinguish cyber espionage activities from other cyber operations, including offensive cyber operations. Technical realities contribute to the risk that an act of cyber espionage will be misconstrued as another type of activity, such as a cyber use of force or even an imminent armed attack.[207] The author defines the lack of certainty of the notion of cyber espionage, thus it can be determines in many

[202] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2017
[203] Ibid.
[204] Ibid.
[205] Anna Wortham, Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Chartern Provisions Prohibiting the Threat or Use of Force?, Federal Communications Law Journal, 2011
[206] Ibid.
[207] Tallinn Manual 2.0 (2017), *supra nota* 202

inappropriate ways, which do not constitute the cyber espionage as such and, therefore, will lead to the unexpected consequences. The states must distinguish cyber espionage from other cyber threats in order to be capable reduce possible risks and protect themselves in accordance with legal norms.

While cyber exploitation falls within the above definition of espionage, as it is a means of obtaining secret national information, cyber exploitation does not fit the traditional understanding of espionage, where nations send attaches and spies in order to gather intelligence information. Because cyber exploitation is so much more intrusive than traditional espionage and can be conducted effectively by non-state actors in ways that can undermine a targeted nation's infrastructure or launch an attack on another nation, it needs to be treated as a higher concern than traditional espionage.[208]

3.4. Legal gaps in current international regulation of cyber espionage and possible alternative approaches

The one reason due to which cyber exploitation should be treated differently than traditional espionage is because of the greater breadth of material that cyber exploitation can provide access to.[209]

The second reason is that while the problem of unintended consequences is often discussed in relation to cyber attack, cyber exploitation can also have unintended consequences. Although the exploitation may begin with a very specific target, because of the way computers become infected and then perpetuate the infection in order to gain access to more vulnerabilities and more computers, the exploitation can often end up infecting unintended targets and producing unintended results.[210]

Furthermore, because of the problems of attribution, investigations into cyber exploitation can go on for years and result in very little conclusive information.[211] Therefore the cyber espionage should distinguish from the traditional espionage in a manner of treating it and in order to protect states from this threat, it should be prohibited by international law, not only by domestic law of nations.

The majority of the Experts was of the view that exfiltration violates no international law prohibition irrespective to the attendant severity. They suggested that the legal issue is not

[208] Anna Wortham (2011), *supra nota* 205
[209] Ibid.
[210] Ibid.
[211] Ibid.

severity, but instead whether the method employed is unlawful. A few experts took the position that at a certain point of consequences suffered by a target state are so severe (e.g. the exfiltration of nuclear launch codes) that the operation is the violation of sovereignty.[212] The author upholds the position of minority meaning that exfiltration may not constitute such grade of severity in comparison to other existing threats, but it definitely creates significant damages to the states with possible future outcomes raising from exfiltrated confidential information as mentionrd in the example above.

The majority of the experts agreed that although acts of cyber espionage may not be unlawful standing alone, they can nevertheless constitute an integral and indispensable component of an operation that violates international law. The majority was of the view that, once the threat has been communicated, the action in its entirety, including the integrated cyber espionage constitutes an unlawful threat of the use of force. For example, consider the case of state that executes a single plan in which it employs cyber espionage to acquire the credentials necessary to access the industrial control system of a nuclear power plant of another state with the intent of threatening to conduct cyber operations against the system in a manner that will cause significant damage or death unless the former ends particular military operations abroad. But the minority of the Experts states here that the two aspects of the operation must be assessed separately and that the acquisition of the access credentials, as distinct from the use of force, does not violate international law.[213]

The author also picks up *de lege ferenda* alternative approaches in order to gain the broader overview of possible alternatives with regard to international regulation of cyber espionage and demonstrates the verity of applicable international principles which could facilitate the process of formation future normative framework of cyber intelligence gathering. Although, the below mentioned approaches may not be fully suitable for the purpose of the thesis, but they demonstrates the regulation and protection of common spaces, and it is clear, that cyber space is falling under the present notion of common space.

The lack of defined strategies, transparency of operations and verification capacity, as well as the inherent length of the treaty-making and adoption process, render legally based arms control problematic for addressing cyber-security threats. The goal of preventing or moderating cyber-warfare, however, can probably be advanced through carefully crafted political measures. Such measures could seek to increase transparency and build confidence concerning cyber-security

[212] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2017
[213] Ibid.

intentions. They could also serve to articulate a code of responsible behaviour for states in cyberspace.[214]

Discussing emerging doctrines and operational concepts can serve deterrent functions, but can also provide a basis for identifying mutually beneficial arms control options. Even just the process of bilateral interaction can be invaluable in clarifying misperceptions, fostering understanding of respective approaches and laying a basis for eventual co-operation. Unfortunately, it would appear that other political or strategic factors have worked against the initiation of such cyber-security dialogues between some of the key states concerned (such as China, Russia and the U.S.). It will be important for decision-makers to ensure that such cyber-security confidence building channels are not ignored, especially when levels of mistrust are so high.[215]

In addition to the bilateral track, there is consider able scope for multilateral measures of confidence building, both at the regional and global level. At a basic level, issues of cyber-attack and defense should be discussed at meetings of international security organizations. It is time to support transparency exercises that would illuminate military doctrine and strategic thinking on the emerging cyber-security agenda. Research and development of verification techniques could be encouraged, given the need to resolve or minimize the problem of attribution.[216]

The capacity to identify the true origin of a cyber-attack will continue to be a chief requirement for policing cyberspace. There could also be scope for national or collective pledges not to engage in cyber-attacks. These political measures, while difficult to verify in practice, could contribute to the building of norms in cyberspace. The principle of 'non-interference', which has been applied to satellite verification technology in several nuclear and conventional arms control agreements, maybe an attractive, initial measure for a multilateral accord. Notification of and invitations to observe cyber-security exercises could prove another vehicle for confidence-building, mirroring what was accomplished in the field of conventional forces previously. Regional security organizations such as NATO, the Organization for Security and Cooperation in Europe, the Organization of American States and Asia-Pacific Economic Cooperation/ASEAN Regional Forum have taken some initial steps of this nature, but much more could be done.[217]

Using the *lex ferenda* approach, to the Internet as a resource that is shared globally among people

[214] Paul Meyer, Cyber-Security Through Arms Control, The Rusi Journal, 2011
[215] Ibid.
[216] Ibid.
[217] Ibid.

and thus to the cyber space the general principles of international law can be applied that governs the protection of the international environment, of common spaces, or the protection from globally spreading (health) infections. But the use of these principles is more likely a more philosophical idea, which undoubtedly requires further development in order to be able to apply the above principles to cyber space without prejudice to the normative nature of the law.[218]

It should be mentioned, that broad characteristics of the principles of equal sovereignty of states and the duty of cooperation all principles could lead to the indirectly formed related principles.

It can be argued that the application of *de lege ferenda* to the principle of sustainable development and the equitable use of global resources, protection against the spread of (health) infections throughout the world in cyberspace or on the Internet and the common heritage or the problem of mankind will undoubtedly support a legal obligation states to maintain international peace and security and, in a broader sense, to eliminate various threats to peace and security.[219]

The principle of sustainable development, which demonstrates the link between environmental protection and long-term development, was first mentioned in the United Nations in the 1970s. Conceptually, this principle suggests that the development of the current generation should not be in conflict with the capabilities of future generation, and the use of natural resources should be carried out for social, environmental and economic reasons in this regard.[220]

The principle of sustainable development sets many disputes in order to determine whether it is a political ideal or it can be identified as a rule of international customary law. Various international agreements, UNGA resolutions and political declarations have included the principle of equitable utilization of shared resources which was developed in the context of international water resources and the continental shelf and is confirmed by the international jurisprudence and definitely is the general international principle. The core of the principle of sustainable and equitable use of resources can be deemed a general principle of international environmental law, thus it can be applied to internet as another globally shared resource, establishing a legal obligation of states to cooperate in sustainable and equitable usage.[221]

Katharina Ziolkowski has mentioned that "despite the principle of common heritage (or concern) of humankind was not meant to constitute an independent principle, its application outside the

[218] Katharina Ziolkowski, Confidence Building Measures for Cyberspace – Legal Implications, NATO CCD COE Publications, Tallinn, 2013
[219] Ibid.
[220] Ibid.
[221] Ibid.

respective treaty regimes, i.e., to cyberspace, seems to be, in theory, adequate. This is supported by the assertion that the principle obtained the character of international customary law with regard to the use of common spaces (resulting in obligations to international cooperation, use for peaceful purposes, equal distribution of usage and exploration, and respect for future generations). If the internet, and thus cyberspace, was considered a common heritage or concern of humankind, states would have the obligation to, inter alia, use it for peaceful purposes only."[222]

"This corresponds with the general principle of international law to restrain from the threat of or the use of force in international relations, and would still allow the military use of cyberspace for, e.g., exercises, self-defense, or measures undertaken according to Chapter VI and VII of the UN Charter. Although States partly refer to cyberspace as a 'global common', the official diplomatic language partly avoids terminology which could indicate the development of cyberspace into a common heritage or concern of humankind (e.g., Germany speaks of a 'public good'). Thus, tendencies for respective developments are momentarily not detectable."[223]

In the 19th century international cooperation in the field of cross-boundary spreading of health infections had already begun. This was due to technical achievements in the field of communication and transport, which led to the intensification of economic exchanges and international relations. The application of the principles underlying the IHR to the situation of cross-border distribution of computer viruses, worms and other hostile programs does not seem justified, since the impact of malicious software on the world population groups is very different in its intensity and significance from the impact of worldwide spreading health infections and diseases. The huge negative effect of cyber-manipulation on the economy, which cannot be denied, does not justify the application of the principles of sanitary legislation on the Internet or cyberspace. However, consideration should be given to expanding the rights and capabilities of an international body with powers comparable to those of the Health Assembly and the WHO Board (see above).[224]

Most likely in the future, cyber threats will increase, as the global network continues to evolve along with technologies making everything more dependent on the services offered, then to preserve international and national security such a body could make decisions regarding:

- "reporting of cyber security incidents,

[222] Katharina Ziolkowski, Confidence Building Measures for Cyberspace – Legal Implications, NATO CCD COE Publications, Tallinn, 2013
[223] Ibid.
[224] Ibid.

- quarantine requirements for networks,

- nomenclatures of malicious software,

- standards of cyber security,

- standards of purity of software,

- advertising and labelling of software, and

- taking emergency measures in cases which require immediate action."[225]

The author applied the existing general international principles to the cyber space as to a global humankind heritage following the concepts of these principles in order to determine whether it is possible to use them in further normative acts' developments and received the outcomes representing the possible practical usage of *de lege ferenda* approach as a "fruitful soil" for future purposes.

[225] Katharina Ziolkowski, Confidence Building Measures for Cyberspace – Legal Implications, NATO CCD COE Publications, Tallinn, 2013

Conclusions

Concerns about growing security threats in cyber space are valid. These concerns are grounded on the combination of growing national dependence on cyber systems, and the existing vulnerabilities in these systems. Cyber attacks both passive and disruptive, exploit these vulnerabilities; both criminals and nation states have effectively employed cyber attacks of both types.[226] Cyber capabilities are not a subject that states discuss openly, since it is rarely beneficial for a state to publicize that it is spying on another state or that it is causing another state's networks to close down. Much is written about the vital importance of possessing a cyber capability, but while states do not directly announce their own offensive capabilities in cyberspace, as no one want to be "open" in such a field conducting cyber operations for its own state purposes, this does not prevent them from discussing and analyzing other states' capabilities and options in this area.[227]

When getting of reports of the Chinese breaking into U.S. computer networks for espionage purposes was started, firstly, it was described in some very strong language meaning how highly intrusive is an act conducted by China. We called the Chinese actions cyber-attacks. We sometimes even invoked the word cyber war, and declared that a cyber-attack was an act of war. But when Edward Snowden revealed that the NSA has been doing exactly the same thing as the Chinese to computer networks around the world, we used much more moderate language to describe U.S. actions: words like espionage, or intelligence gathering, or data collection or spying in simple words. We stressed that it's a common peacetime activity, and that everyone does it.[228]

The reality is somewhere in the middle, and the problem is that our intuitions are based on history, meaning that they apply the same qualifications to the rather different and new way of conducting espionage. Electronic espionage or cyber espionage is different today than it was in the pre-Internet days of the Cold War. Eavesdropping isn't passive anymore. It's not the electronic equivalent of sitting close to someone and overhearing a conversation by watching the object (target) through the holes in newspaper. It's not passively monitoring a communications circuit. It's more likely to involve actively breaking into an adversary's computer network - be it Chinese, Brazilian, Belgian or elsewhere - and installing malicious software designed to take

[226] Jeffrey Hunker, Cyber War And Cyber Power, Issues For NATO Doctrine, 2010
[227] Magnus Hjortdal, China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence, Journal of Strategic Security 4, no. 2, 2011
[228] Bruce Schneier, There's No Real Difference Between Online Espionage and Online Attack, The Atlantic, 2014

over that network. In other words, it's hacking which is carried out by installment if it's possible to say. Cyber-espionage is a form of cyber-attack, it's an offensive action and it cannot be measured as a traditional espionage.[229]

Cyber espionages are always hidden behind the internet and almost never exposed. While the traditional espionages are trembling, worrying the exposure of their positions, the cyber espionages are drinking a cup of coffee and eating the favorite meal leisurely in front of the computers. Let's say that a traditional espionage may use a couple of years to integrate into the adversary group and another couple of year to obtain the trust before they really can do their stuff and it will never know for sure who is behind its back suspecting all the time. However, if lucky, the cyber espionages can steal the data of couple of companies during one afternoon by engaging in full usages of internet.[230]

The legal experts hold the view that since cyber espionage expand the scope of intelligence gathering capabilities, it should be limited if we treat it more strictly than traditional espionage. Meanwhile, the others support inaction and allow state practice to develop in mentioned direction. Hence, the emergence of general agreement on traditional espionage is not likely to occur, and there seems to be no reason to expect that consensus is more likely to emerge in the cyber context.

The variety of cyber tactics which are used by adversaries are similar to traditional methods on the fundamental levels including deception, covert access, recruitment of insiders, fraud, vendor visits, and specialized technical operations. Nevertheless, each of these tactics has its potential effectiveness, which can be strengthen if the current technology is used to enhance its impact.

There are three main features of cyberspace that make it a unique tool for the cyber espionage and covert action: the possibility of remote access, the difficulty of attributing intrusions and attacks to identifiable objects, and the difficulty of distinguishing between exploitation and attack. Thinking about it, the third of these characteristics seems to represent particularly serious problems for espionage and covert actions. To look more precisely on them, the author resulted in present general description.

Remote access is the first of the main features distinguishing cyberspace from traditional one is remote access. There is no needed requirement for the targeting of sensitive and mainly

[229] Bruce Schneier, There's No Real Difference Between Online Espionage and Online Attack, The Atlantic, 2014
[230] YeZhen, Cyber Espionage, National University of Singapore, 2010, available at: http://blog.nus.edu.sg/iblog/2010/10/17/cyber-espionage/ (15.05.2017)

confidential information, due to the fact that a spyware and can be easily inserted into networks by insiders or by Trojan software downloaded and written, basically, for the express purpose of allowing remote access to confidential information present on information networks. Therefore, spies do not need to be physically located near such confidential information or at least in the state to which that information belongs, in order to hack into critical networks and steal all required secrets or even more. For instance, if computer will be targeted by a Trojan horse software program, an unauthorized actor can possess control of the infected computer and steal amounts of sensitive information on the machine or alter it in the part of a botnet that automatically infects other machines. And furthermore, the territorial restrictions on the usage of police power can limit the ability of law enforcement agencies to curb espionage, conducted from remote areas.

Attribution problem is a second unique feature of cyber activity. The main issue is arisen due to the fact that cyber intrusions and attacks can be launched in secret in most cases making not so easy to determine the responsible actors. A cyber attack seems to be originating in China, for example, might have been launched by the Chinese government, by some unofficial group of hackers in China or elsewhere, or by terrorists in the Middle East who hide their identities. Moreover, the determining of the responsible party, determining whether a given cyber intrusion was intentional or unintentional will mainly associated with difficulties. Therefore, the attribution problem originates the major difficulties for those seeking effective methods of deterrence against cyber intrusions.

And the last feature is exploitation, the distinctive aspect of cyber operations is the tissue of distinguishing cyber intrusions that constitute theft or exploitation from those that rise to the level of “armed attack” or “use of force”. The problem originates from the states’ attempts to distinguish between acts of cyber espionage, meaning the use of information technology systems and networks to collect the data about an organization or a society that is considered secret or confidential without the permission of the holder of the information and information war, meaning cyber conflict at the nation-state level involving either direct military confrontation or indirect competition via disruption and deception. The above discussed feature constitutes the lack of certainty of the notion of cyber espionage, which is considered to be not good.

But the defensive actions are not prohibited due to the fact that responsible actor remains unknown. There is no requirement in international law that an actor must be known before defensive action can be taken and it is more likely that the responsibility for the attack would be imputed to the nation-state to whose territory the attack was traced.

The exploitation of cyberspace for the purpose of espionage has emerged as a particularly attractive method to acquire confidential information because of the large amount of information that is now stored in cyberspace and because cyberspace affords a considerable degree of anonymity to perpetrators of espionage and is thus a relatively risk free enterprise.

The current international regulation of cyberspace nowadays is widely accepted as to be regulated by existing positive law and following this view, the law on the use of force, jus ad bellum as well as jus in bello, applies to cyber operations. In more familiar words, the cyber space is regulated by international customary and humanitarian law, where the international customary law seeks to maintain peaceful relations within the community of nations by setting precise criteria as to when states may go beyond non-forceful measures such as diplomacy, economic sanctions and counter-measures. By contrast, in international humanitarian law, "attack" refers to a particular category of military operations. International humanitarian law is obviously, despite adopting an instrumentality-based definition of attack, takes an approach to these regulatory requirements, taking into account the consequences when this term is introduced.

In order to protect themselves, states are not prohibited from usage of self-defense measures. The use of only passive measures is no longer enough to protect networks in the face of rising threat levels. The active cyber defense is direct defensive action taken to destroy or reduce the effectiveness of cyber threats against friendly forces and assets. Active cyber defense can be characterized by four main features such as scope of effects, types of effects, degree of cooperation and degree of automation. These features, basically determined whether it is permitted to conduct self-defense.

In addition, it is important that the act of self-defense be appropriately limited in scope by what is necessary to prevent violations. In connection with the requirement of an immediate threat of attack, simply recognizing the vulnerability available for access is not sufficient to justify the use of preemptive self-defense. Also states should keep in mind the principles under which the self-defense will be legitimate and will not bring more harm in response, such as the most important to the author's opinion – the principle of proportionality.

Almost all states have enacted domestic laws that both restrict access to classified information as well as criminalize the act of an unauthorized taking of such information in order to deny intelligence gathering within their territories. Here it is presented the criminal law approach with regard to cyber espionage as to the criminal act.

In these sphere one can recognized the only one international legal document developed to address issues related to cyberspace is the European Union's Convention on Cybercrime. The Cybercrime Convention does not address cyberspace attacks as possible acts of war and instead focuses on criminal acts, therefore it could be helpful in establishing of a framework for a new methodology of analyzing cyberspace attacks.

The main issues resolved with help of the criminal law approach and methodology, enforceability, and attribution for two reasons. It contains strong definitions that can withstand judicial review and allow for fair application to a variety of fact patterns. Criminal law definitions must also clearly put everyone on notice as to prohibited activities. The second strength is that the criminal law methodology requires the definition of a prohibited act to have some degree of intent, also known as the scienter element, meaning that the lack of such degree of intent will not constitute the criminal act itself. Relying on these strengths, the criminal law approach creates a definition of a cyberspace crime that is clear, flexible, and requires a minimum level of intent.

During the thesis, the author also refers to the cyber-weapon, which is became highly discussed issue, especially in a view that cyber espionage constitutes an armed attack with requirement of weapon involvement as is common for traditional meaning of an armed attack. What is a cyber-weapon and what is not a cyber-weapon is a very controversial question with slightly visible differences, but it is important to draw the line between these two notions. First of all, it has security consequences, meaning that if such weapon (cyber in this context) has no potential to be used as a weapon and constitutes no harm to the people, it is simply less dangerous. Then, the political consequences could follow, meaning that with no usage of weapon, it is an unarmed intrusion and it is less dangerous from the political point of view than an armed one. And thirdly, the emerge of legal consequences legal is also possible, due to the fact that identifying something as a weapon means that it may be legally punishable as the traditional weapon is.

Furthermore, the author expressed in the thesis an interesting suggestion in order to regulate the cyber weapons, by comparing the Chemical Weapons Convention with Cyber Weapons Convention which could emerge from the principles of the first one. The main distinction here lies in the fact that cyber warfare is not chemical warfare. However, they do share some similarities, such as ease of acquisition, asymmetric damage and polymorphism. But the tactics, strategies and effects are greatly differs, in simple words the chemical warfare kills humans, while cyber warfare kills machine. Therefore, in order to constitute the advent of Cyber Weapons Convention several significant distinctions should be taken into account.

The author mentioned, that current situation with regard to regulation of cyber espionage is unclear, meaning that it is apparently not regulated in the international level as a specific type of traditional espionage as well as the latter one does not specifically regulated by international law as well. But upon the sovereign equality of states, it is appropriate in the nature of an intrusive trans-boundary activity such as cyber espionage that this type of conduct can run into conflict with general principles of international law. Therefore, the cyber espionage might be unlawful under principles of international law, such as the principle of state sovereignty or the principle of non-intervention.

If we look precisely on the notion of the espionage, it becomes evident that it is something, which is conducted in secret. Hence, for the purpose of customary law formation, cyber espionage may not be determined as a state practice due to the fact that this state practice is engaged in secret. National laws, which continue their development, but provide at least basic substantive and procedural rules about internal and transnational surveillance, will influence the way in which those international norms develop.

The development of an international norm prohibiting states from stealing sensitive data in the cyber domain would contribute to a more stable international order. Such limitation tends to minimize the possibility of escalating violence in the cyber area and it acts as a deterrent to state actions in cyberspace based on misunderstanding and erroneous factual definitions, which are widespread in cyberspace. With regard to cyber operators, the modern international law rules should develop in order to more clearly define the criteria used to distinguish which state actions are permissible from these cyber operations which can be qualified as illegal interference.[231]

The Tallinn Manual 2.0 brings some interesting suggestions for the further consideration. The majority of the experts was of the view that exfiltration violates no international law prohibition irrespective to the attendant severity. They suggested that the legal issue is not severity, but instead whether the method employed is unlawful. Basically, they set aside the issue of severity and concentrated on the method of conducted exfiltration. But few experts took the position that at a certain point of consequences suffered by a target state are so severe (e.g. the exfiltration of nuclear launch codes) that the operation is the violation of sovereignty. Here, the author is tended to uphold the minority, arguing that exfiltration could greatly vary from one to another, therefore

[231] Catherine Lotrionte, Countering State-Sponsored Cyber Economic Espionage Under International Law, The North Carolina Journal of International Law and Commercial Regulation, 2014

focusing only on the method involved without predicting possible consequences may lead to the significant damages.

Then, the majority of the experts agreed that although acts of cyber espionage may not be unlawful standing alone, they can nevertheless constitute an integral and indispensable component of an operation that violates international law. The majority was of the view that, once the threat has been communicated, the action in its entirety, including the integrated cyber espionage constitutes an unlawful threat of the use of force. But the minority of the experts states here that the two aspects of the operation must be assessed separately and that the acquisition of the access credentials, as distinct from the use of force, does not violate international law. With regard to this point of view, the author partially agree with both of statements, arguing that cyber espionage definitely could be a part of operation that is violated the international law, but for the purpose of the thesis, cyber espionage should be assessed as a separate aspect due to the fact that is huge ill-regulated states' practice, which requires special treatment as far as information technology is involved.

As a result of conducted research by the author, it is apparently that cyber espionage is not the minor criminal act or rare used practice that could be left in a shade of international law principles and Cyber Crime Convention. It is huge hidden threat on national level and even more substantial on international level, hence, in order to minimize the treat and control the already emerged one, cyber espionage requires the new international regulation to fill the existing gaps in international governing law and develop clear, practically applicable international norms to deal with it. Also, there are several alternative approaches which derived from international principles applicable to common spaces that might be used as additional tools in order to facilitate the core international norms with regard to cyber espionage as separate notion.

List of sources

Scientific books and articles

1. Alexander Melnitzky, Defending America against Chineese Cyber Espionage through the Use of Active Defences, Cardozo Journal of International and Comparative Law, 2012, p. 537
2. Anna Wortham, Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Chartern Provisions Prohibiting the Threat or Use of Force?, Federal Communications Law Journal, 2011
3. Ashley Deeks, An International Legal Framework For Surveillance, Virginia Journal of International Law, 2015
4. Catherine Lotrionte, Countering State-Sponsored Cyber Economic Espionage Under International Law, The North Carolina Journal of International Law and Commercial Regulation, 2014
5. Charles J. Dunlap Jr., Perspectives for Cyber Strategists on Law for Cyberwar, Strategic Studies Quarterly, 2011
6. Christina Parajon Skinner, An International Law Response to Economic Cyber Espionage, Connecticut Law Review, 2014
7. Clement Guitton, Cyber insecurity as a national threat: overreaction from Germany, France and the UK?, European Security, 2013
8. Dana Rubenstein, Nation State Cyber Espionage and its Impacts, Washington University, St. Louis, 2014
9. David J. Kappos, Pamela Passman, Cyber Espionage Is Reaching Crisis Levels, Fortune, 2015
10. David P. Fidler, Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies, Insights, 2013
11. David P. Fidler, Recent Developments and Revelations Concerning Cybersecurity and Cyberspace: Implications for International Law, Insights, 2012
12. David P. Fidler, Tinker, Tailor, Soldier, Duqu: Why cyberespionage is more dangerous than you think, International Journal of Critical Infrastructure Protection, 2012
13. David Weissbrodt, Cyber Conflict, Cyber-Crime and Cyber-Espionage, Minnesota Journal of International Law, 2013

14. Davis Brown, A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict", Harvard International Law Journal 47 Harv. Int'l L.J., 2006, p. 179
15. Demarest, Geoffrey B., Espionage in International Law, Denver Journal of International Law and Policy 24 Denv. J. I., 1996, p. 321
16. Dorothy E. Denning, Framework and principles for active cyber defense, Computers & Security, 2014, p. 108-113
17. Eneken Tikk, Ten Rules for Cyber Security, Survival, 2011, p. 119-132
18. Gerald O'Hara, Cyber-Espionage: A Growing Threat to the American Economy, Journal of Communictions Law and Policy, 2010
19. Herbert S. Lin, Offensive Cyber Operations and the Use of Force, Journal of National Security Law & Policy, 2010, p. 63
20. Herbert S. Lin, Why Computer Scientists Should Care About Cyber Conflict and U.S. National Security Policy, Communications of the ACM, 2012
21. Katharina Ziolkowski, Confidence Building Measures for Cyberspace – Legal Implications, NATO CCD COE Publications, Tallinn, 2013
22. Kenneth Geers, Cyber Weapons Convention, Computer Law & Security Review, 2010
23. Kristina Daugirdas and Julian Davis Mortenson, In Wake Of Espionage Revelations, United States Declines To Reach Comprehensive Intelligence Agreement With Germany, American Journal of International Law, 2014
24. Laurie R. Blank, International Law and Cyber Threats from Non-State Actors, International Law Studies, 2013
25. Louise Arimatsu, A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations, NATO CCD COE Publications, 2012
26. Magnus Hjortdal, China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence, Journal of Strategic Security 4, no. 2, 2011
27. Major Arie J. Schaap, Cyber Warfare Operations: Development and Use under International Law, Air Force Law Review, 2009
28. Marco Benatar, The Use of Force: Need for Legal Justification?, Goettingen Journal of International Law, p. 375
29. Marco Roscini, Cyber Operations and the Use of Force in International Law, Oxford Press, 2014
30. Martin Rudner, Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge, International Journal of Intelligence and Counter Intelligence, 2013

31. Matthew C. Waxman, Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), Yale Journal of International Law, 2011
32. Michael N. Schmitt, "Attack" as a Term of Art in International Law: The Cyber Operations Context, IEEE, 2012
33. Michael N. Schmitt, Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts, Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, The National Academies, 400 pages, 2010
34. Myriam Dunn Cavelty, From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse, International Studies Review, 2013
35. Pascal Brangetto, Tomáš Minárik, Jan Stinissen, From Active Cyber Defence to Responsive Cyber Defence: A Way for States to Defend Themselves – Legal Implications, Nato Legal Gazette, Dr. Petra Ochmannova, ACT SEE Deputy Legal Advisor, NATO CCD COE Publications, Tallinn, 2014
36. Paul Meyer, Cyber-Security Through Arms Control, The Rusi Journal, 2011
37. Randall R. Dipert, The Ethics of Cyberwarfare, Journal of Military Ethics, 2010
38. Robert D. Williams, (Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action, George Washington Law Review 79 Geo. Wash. L. Rev., 2010-2011, p. 1162
39. Robert K. Knake, Untangling Attribution: Moving to Accountability in Cyberspace, The Council on Foreign Relations, 2010
40. Roderic Broadhurst, Developments in the global law enforcement of cyber-crime, 29 Policing Int'l J. Police Strat. & Mgmt. 408, 2006
41. Ronald J. Deibert, Masashi Crete-Nishihata, Global Governance and the Spread of Cyberspace Controls. Global Governance: A Review of Multilateralism and International Organizations: July-September, 2012, pp. 339-361
42. Russell Buchan, The International Legal Regulation of State-Sponsored Cyber Espionage. Chapter 4, International Cyber Norms Legal, Policy & Industry Perspectives, Anna-Maria Osula and Henry Rõigas (Eds.), NATO CCD COE Publications, Tallinn 2016
43. Scott J. Shakelford, Richard B. Andres, State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem, Gergetown Journal of International Law, 2011, p. 971
44. Sean Kanuck, Sovereign Discourse on Cyber Conflict under International Law, Texas Law Review, 2009-2010, p. 1571

45. Stefano Mele, Cyber-weapons: legal and strategic aspects, Italian Institute of Strategic Studies 'Niccolò Machiavelli' , 2013
46. Susan W. Brener, Anthony C. Crescenzi, State-Sponsored Crime: The Futility of Economic Espionage Act, Houston Journal Of International Law, 2006, p. 389
47. Thomas Rid, Cyber-Weapons, The RUSI Journal, 2012
48. Wolfgang McGavran, Intended Consequences: Regulating Cyber Attacks, Tulane Journal of Technology and Intellectual Property, p. 259
49. Yoo, Christopher S., Cyber Espionage or Cyberwar?: International Law, Domestic Law, and Self-Protective Measures, University of Pennsylvania Law School, 2015

National and EU legal acts and international conventions

1. Additional Protocol I to the Geneva Conventions, 1949
2. Chemical Weapons Convention, 1993
3. Convention on Cybercrime of the Council of Europe (CETS No.185), 2001
4. Title 18 of the United States Code
5. The Charter of the United Nations, 1945

Other international instruments

1. Melissa E. Hathaway, Alexander Klimburg, National Cyber Security, Framework Manual, NATO CCDCOE
2. Tallinn Manual 1.0 on the International Law Applicable to Cyber Warfare, 2013
3. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2017

Case law

1. I.C.J. 1949 I.C.J 4. 22, *Corfu Channel case* (United Kingdom v. Albania)
2. P.C.I.J. (ser. A) No. 10 (Sept. 7) 1927, *S.S. Lotus case* (France v. Turkey)

Research papers and news articles

1. Appelbaum J., et al., The NSA's Secret Spy Hub in Berlin, Der Spiegel (Kristen Allen & Charly Wilder trans., Oct. 27, 2013, 7:02 PM), available at: http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html (16.05.2017)
2. Bruce Schneier, There's No Real Difference Between Online Espionage and Online Attack, The Atlantic, 2014

3. Lehman J. and Phelps S., West's Encyclopedia of American Law, Detroit: Thomson/Gale, 2005, available at: http://www.worldcat.org/title/wests-encyclopedia-of-american-law/oclc/57301521 (16.05.2017)
4. Jeffrey Hunker, Cyber War And Cyber Power, Issues For NATO Doctrine, 2010
5. Hinnant L. and Dahlburg J-T, Let's be honest, we eavesdrop too: former French foreign minister on NSA spying claims, The Associated Press Published Wednesday, 2013, available at: http://www.ctvnews.ca/sci-tech/let-s-be-honest-we-eavesdrop-too-former-french-foreign-minister-on-nsa-spying-claims-1.1509912 (16.05.2017)
6. Gross M.J., "Exclusive: Operation Shady rat - Unprecedented Cyber-espionage Campaign and Intellectual Property Bonanza", Vanity Fair, 2011
7. Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia), 147 Reports of Judgments, International Court of Justice 2014
8. President Barack Obama, Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014) [hereinafter Obama NSA Speech]
9. YeZhen, Cyber Espionage, National University of Singapore, 2010, available at: http://blog.nus.edu.sg/iblog/2010/10/17/cyber-espionage/ (15.05.2017)