FACULTY OF LAW
Stockholm University

Applicability of International Law on Cyber Espionage Intrusions

Ella Shoshan

Thesis combined with practical experience in
International Law, 30 HE credits
Examiner: Said Mahmoudi
Stockholm, Autumn 2014

ABSTRACT

Cyberspace is a space that epitomizes technological development, at the same time highlighting the uncertainty regarding legal issues that arise from it. Technology develops faster than do most types of laws and regulations, and this is true also for the relation between cyberspace and public international law. With the creation of cyberspace, its increased use and the dependency of a majority of societal actors thereupon, legal questions arise. Already, states are purported perpetrators of antagonistic cyberactions, for example denial-of-service-attacks, sabotage and cyber espionage. There are currently only a few conventions or treaties that have bearing on cyber issues, and there is even less consensus on how putative treaties and conventions should be designed, or if they should at all exist. Therefore this essay will instead focus on existing international law and its applicability on questions related to actions in cyberspace, specifically the applicability of public international law to state-conducted cyber espionage targeting other states. The first main finding is that cyber espionage violates the rights that a state enjoys under the principles of sovereignty and territorial jurisdiction. Cyber espionage is unfailingly an intrusive act, as it aims at gathering information that is protected and not available for public view. Data that a state has stored on servers within its territory are subject to that state's territorial jurisdiction. If the data is intruded upon by another state through cyber espionage, the spying state is violating the targeted state's sovereignty and jurisdiction by denying it the right to enact its territorial jurisdiction on that server and its contents. The second finding is that a wide interpretation of the principle of non-intervention, where a coercive element of the intrusive act is not a prerequisite for the applicability of principle, leads to the conclusion that cyber espionage is unlawful also under the principle of non-intervention.

LIST OF ABBREVIATIONS

BCC	Budapest Convention on Cybercrime
CNA	Computer Network Attack
CNE	Computer Network Exploitation
Draft Articles	2001 Articles on Responsibility of States for Internationally Wrongful Acts
EU	European Union
ICJ	International Court of Justice
ICJ Statute	Statute of the International Court of Justice
ILC	International Law Commission
IT	Information Technology
NATO	North Atlantic Treaty Organization
NSA	National Security Agency
PCIJ	Permanent Court of International Justice
TM	Tallinn Manual on the International Law Applicable to Cyber Warfare
UK	United Kingdom
UN	United Nations
UN Charter	The Charter of the United Nations
US	United States
VCCR	Vienna Convention on Consular Relations
VCLT	Vienna Convention on the Law of Treaties

CONTENTS

1 INTRODUCTION

1.1 A BACKGROUND ON THE SUBJECT

There are many types of unfriendly cyber actions: alleged Russian cyber attacks on Estonia in 2007, malware affecting Iranian uranium enriching centrifuges in 2010, and a Trojan horse infiltrating computer systems of embassies, foreign ministries and other government offices, including the Dalai Lama's exile centre in India, and in over 102 other countries.[1] Some of these actions have the character of an intrusion and are therefore regularly referred to in for example the media or doctrines as cyber intrusions. Simply put, a cyber intrusion takes place when protected data is intruded upon via cyberspace. Cyber intrusions can be attempted in order to cause damage or destruction to such a high extent that they are considered to cross the threshold for use of force or even armed attacks.[2] If so, they are often discussed within the field of cyber warfare. Close to this field, but present in situations separate from armed conflict, lies the broader subject of this essay: peacetime cyber espionage. Many states prohibit economic or industrial espionage in their domestic criminal law. When a perpetrator steals or gains unauthorized access to for example trade secrets stored in digital formats or on computer and information technology (IT) networks, this is referred to as cyber espionage. This form of espionage is usually conducted for commercial rather than national security purposes. However, cyber espionage is not limited to non-state actors; state actors can also commit cyber espionage and have indeed been accused of doing so, and not only for commercial reasons, but for reasons of national security. All states seek to establish or maintain national security, and cyber espionage for purposes said to pertain to national security is sometimes argued to

---

[1] Further reading can be found here: N Hopkins, 'Stuxnet attack forced Britain to rethink the cberwar' *The Guardian* (London 30 May 2011) <http://www.theguardian.com/politics/2011/may/30/stuxnet-attack-cyber-war-iran> accessed 28 April 2014; Directorate-General for External Policies, Policy Department 'Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action Within the EU' Study, (European Parliament 2011) 17. <http://www.europarl.europa.eu/RegData/etudes/etudes/join/2011/433828/EXPOSEDE_ET%2820 11%29433828_EN.pdf > accessed 15 March 2014; P Warren, 'Smash and grab, the hi-tech way' *The Guardian* (London 19 January 2006) <http://www.theguardian.com/politics/2006/jan/19/technology.security> accessed 28 April 2014.

[2] Cf. M C. Waxman 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)' (2011) 36 YJIL 431, 432.

be a means of attaining such security. It should be noted that states avoid the term espionage when referring to its own state-sponsored activities since espionage is often punishable according to domestic law.

Cyber espionage by states is both similar to and different from conventional espionage. Conventional espionage refers to a process involving human agents or technical means to acquire information normally not publically available.[3] Just like its conventional counterpart, cyber espionage involves unauthorized intrusions, exploiting for example security weaknesses to bypass encrypted servers and access data of embassies and foreign government agencies. One of the main differences from conventional espionage is the high geographical and physical independence enjoyed by cyber espionage. In order to spy on data of another state's agency there is no need of a physical person or a device being placed in the target state. Instead, cyber commands issued from potentially anywhere can be used. Hence, cyber espionage can be committed regardless of state borders. Because of the vagueness of virtual borders, cyber espionage raises issues regarding intruding on other states' sovereignty. This essay asks if it is legal or should be legal under international law for peacetime for states to use cyber espionage, and consequently to intrude, in order to access hidden or otherwise protected data on another state's cyberspace. Specifically, can extraterritorial cyber intrusions through cyberspace by a state into protected data located and belonging to another state, referred to as cyber espionage, constitute unlawful intrusion under peacetime international law into the sovereignty of the state intruded upon?

1.2 AIMS AND MATERIAL

The aim of this essay is to provide clarification, from the viewpoint of public international law, of the putative legality or illegality of cyber espionage by states into foreign states. It is examined if and under which circumstances and to what extent cyber espionage by states into other states' servers is allowed, and from which legal sources such activities may draw its potential legitimacy.

---

[3] The MI5, '*What is Espionage*?' <https://www.mi5.gov.uk/home/the-threats/espionage/what-is-espionage.html> accessed 4 April 2014.

The reasoning in this essay is based on sources of public international law therefore, legal conventions and treaties of international law combined with customary international law have been important. This body of law encompasses codified sources and customary principles. Of these, the most relevant were those that concern sovereignty, prohibition of use of force and the principle of non-intervention.

Articles in several law reviews were read in order to form an understanding of the developing and on-going debate on the subject and in order to define the arguments of opposing views. The main difficulty was that codification on the subject of cyberspace and espionage in general and cyber espionage specifically, and case law related to these subjects, was limited. Therefore, the main material has been found in doctrine. The doctrine used was many times found in law journals and reports by organizations such as the North Atlantic Treaty Organization (NATO) or the European Union (EU). Because new instances of cyber espionage are continuously revealed and reported, sources that explain such instances were often found in digital news media, which tend to report news faster than sources of printed paper, and were therefore used to keep the material of this essay as much up to date as possible. I have also attended a seminar about cybersecurity at the Swedish Institute of International Affairs.

The findings are partly based on interviews and information obtained during a 20 week internship at the Swedish Ministry of Defence. During the internship I presented my findings at an internal seminar and distributed a memorandum within units of the ministry. The internship enabled me to come into contact with people working on questions relating to cybersecurity and defence. These professionals include Runar Viksten, former district court chairman and chairman of the Swedish Defence Intelligence Court and Erik Wennerström, director-general at the Swedish National Council for Crime Prevention. Also, persons with professionally qualified technical knowledge were consulted for explaining the general components of cyber espionage and certain processes of for example encryption and cyber intrusions, one of these persons was Dr. Ulrik Franke of the Royal Institute of Technology in Stockholm and the Swedish Defence Research

Agency. In order to ascertain a correct technical terminology, these professionals helped review such issues.

1.3 METHOD

The method has been to select sources that specialize in the areas of interest, and from these, derive a general understanding of the wider background of the subject of cyber espionage. Customary principles of international law do not specifically address cyber espionage, and a challenge was therefore to test if these principles could be analogously applied to cyber espionage. The lack of a generally accepted definition of cyber espionage provided both freedom and difficulty in creating a definition. The sources that focused on a special field were prioritized before other sources focusing on other aspects. For example, a text on cyber threats would be used as a reference for cyber threats specifically, but even if the same source would explain for example the principle of non-intervention in general, a text focusing primarily on non-intervention would be used in the essay instead. The aim was thus to keep the references of the essay as relevant as possible.

1.4 SCOPE AND LIMITATIONS

This essay focuses on cyber espionage rather than on the wider category cyber intrusions. Thus, other types of cyber intrusions, for example cyber crime unrelated to state-actors, were beyond the scope of this essay. Furthermore, the legal assessment covers only cyber espionage conducted by states, and therefore the attribution of hackers acting independently from a state, and questions of state responsibility for harbouring or tolerating cyber espionage by non-state actors were omitted. Consequently, situations where no relationship between states and non-state actors who commit cyber espionage exists are not examined. Examples of such situations can include industrial espionage conducted exclusively by private corporations, where the data received are gathered solely upon request of non-state actors, without the state's knowledge or possible knowledge.

Finally, this essay is written from a legal point of view, and does therefore not discuss technical details.

1.5 DISPOSITION

Although many aspects of cyber espionage and sovereignty are intertwined, in the first parts of the essay they are divided into different sections. This is done to facilitate specific understanding of the various aspects before bringing them together in the analysis and final conclusion.

First, the reader will become generally acquainted with cyberspace and the possibilities of cyber intrusions, followed by a more detailed presentation of the intrusion sub-category of cyber espionage. Secondly, a condensed account of the legal discussion on the legality or illegality of peacetime espionage generally and cyber espionage specifically under international law will be presented. Thirdly, sovereignty will be explained through the perspective of international law. This section presents the reader with a discussion on the sovereignty of cyberspace and its challenges. The following section discusses the prohibition of use of force and the principle of non-intervention. The applicability of these principles of international law onto the activity of cyber espionage by states will be analysed, resulting in a summary and conclusion. Finally, the discussion is also broadened into the field of human rights law and on future developments of cyber espionage and possible consequences thereof.

2 EXPLAINING THE FIELDS OF CYBER AND CYBER ESPIONAGE

2.1 INTRODUCTION

This chapter describes features and technical aspects of cyberspace and cyber espionage. The technical descriptions and cases provided do not imply any opinions on the legal or political acceptability of the aspects described. It furthermore aims at assisting the reader's understanding of what activities cyber espionage encompasses and closely related fields of relevance for this essay.

2.2 CYBERSPACE

William Gibson, a science-fiction writer, first used the term cyberspace in a short story in 1982. Some years later he expanded the term in the novel 'Neuromancer', where cyberspace is described as 'a consensual hallucination experienced daily by

billions of legitimate operators' and 'a graphic representation of data abstracted from the banks of every computer in the human system'.[4] The literary creation of Gibson turned out to be quite applicable to the term cyberspace as it is used today. Today we describe cyberspace as an electronic and digital dimension. It is a global network involving linked computers located around the world. It is also a 'space of virtual reality; the notional environment within which electronic communication (especially via the Internet) occurs'.[5] This electronic medium of digital networks is used to store, modify and communicate information. Within it, the Internet and other information systems supporting businesses, infrastructure and services are found. The definition of cyberspace has many components. One important component is the virtuality of cyberspace, referring to its independence from any specific spatiotemporal location. This means that cyberspace does not require the interacting parties to be at a specific location at a specific moment in order to meet. Another important component refers to the putative relation between cyberspace and the Internet. Cyberspace is dependent on the Internet because it is a space that supervenes on the interconnected networks of computers.[6]

2.3 CYBER INTRUSIONS

Malicious cyber actions affecting for example infrastructure or national security can be attempted through cyber intrusions. A cyber intrusion can in practical terms generally be described as breaking through or circumventing a security, for example a firewall, or doing so by technical means, false signals or false key, or by disguising, such as using a stolen username or password. The United States (US) Department of Defense defines an intrusion as 'an incident of unauthorized access to data or an automated information system'.[7] A cyber intrusion can be the first

---

[4] M Giles, 'Special report: Cyber-security, Defending the digital frontier' *The Economist* (London 12 July 2014) digital edition for android.
[5] 'Cyberspace, n' Oxford English Dictionary Online (Oxford University Press November 2010) <http://www.oed.com.ezp.sub.su.se/view/Entry/240849?redirectedFrom=cyberspace&accessed> accessed 14 March 2014.
[6] T Ploug, *Ethics in Cyberspace: How Cyberspace May Influence Interpersonal Interaction* (1st edn Springer, 2009) 70.
[7] US Department of Defense Dictionary of Military Terms, '*Computer Intrusion*' <http://www.dtic.mil/doctrine/dod_dictionary/data/c/11171.html> accessed 14 March 2014.

step in a so-called cyber attack[8] if it provides the intruding actor enough access to alter data in order to for example black out an electrical grid system. Therefore, basically all cyber attacks are cyber intrusions; however, cyber intrusions are not always cyber attacks. It should therefore be noted that an intrusion is not synonymous with an attack, as it is only a means of access in order to commit an attack.[9]

The information and communication technology has developed quickly, and so has the perceived threat of cyber intrusions. It is increasingly reported that states are developing information and communication technology for tools of warfare, political and intelligence purposes.[10] Many types of cyber intrusions are committed by criminal organizations and are increasingly considered to be the most profitable of all criminal enterprises.[11] In addition, states have been suspected or accused of either tolerating criminal activities originating from within their territory, or actually backing these organizations as their private proxies in cyberspace.[12]

2.4 CYBER ESPIONAGE

The first part of the term cyber espionage belongs to the modern age, whereas the latter part, espionage, is an old trade. The earliest surviving record of espionage dates from the war between Pharaoh Ramses with the Hittites and the battle of

---

[8] One definition of a cyber attack, which is also used by NATO, is CNA, an acronym for 'Computer Network Attack'. It is '[a]ctions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves'. See 'Computer Network Attack' (*US Department of Defense Dictionary of Military Terms*) <http://www.dtic.mil/doctrine/dod_dictionary/data/c/10082.html> accessed 14 March 2014.

[9] This essay defines cyber espionage as an intrusion and not an attack. A more thorough discussion on why cyber espionage is not synonymous with an attack can be found in chapter 4.

[10] UN General Assembly, Group of Governmental Experts 'Developments in the Field of Information and Telecommunications in the Context of International Security' (30 July 2010) UN Doc A/65/201 7.

[11] Directorate-General for External Policies, Policy Department 'Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action Within the EU' Study, (European Parliament, 2011) 9.

[12] See for example: A Segal, 'Chinese Computer Games: Keeping Safe in Cyberspace' *Foreign Affairs* (New York March/April 2012) <http://www.foreignaffairs.com/articles/137244/adam-segal/chinese-computer-games> accessed 15 March 2014; S W. Brenner, *Cyberthreats and the Decline of the Nation State*, (1st edn Routledge, New York 2014) 55.

Kadesh (ca. 1274 BCE).[13] From then on, history offers countless examples of intelligence gathering and espionage.[14] Espionage is undertaken by spies, i.e. unofficial state agents, who are working abroad covertly and engage in intelligence gathering with regard to military, political, or industrial value. International law does not regulate peacetime espionage as an activity on its own, but it does regulate some activities related to peacetime espionage. Examples of regulations of such activities are found in the Vienna Convention on Diplomatic Relations, in which, among other things, the privileges of a diplomatic mission in a foreign country are regulated, and in the Vienna Convention on Consular Relations (VCCR).[15] However, activities related to espionage are punishable under the national law of practically every state.[16]

There are many definitions of espionage available. While international law does not specifically define espionage as such, some common aspects can be found described in doctrine: it must be conducted clandestinely or otherwise covertly, by a state organ or agent, or otherwise be attributable to a state; and must target information not available to the public. Just as international law does not regulate espionage as such, but merely some activities related to espionage, neither does it specifically regulate cyber espionage. It is therefore emphasized that this essay only examines the activity, by technical means using cyberspace, of a state intruding into another state's organ's or institution's hidden and/or protected data. Because of the similarity of this activity with what is commonly referred to as espionage, for example the covert character and the element of an intrusion into hidden information, the term cyber espionage is in this essay applied to describe the activity of a state intruding into another state's data for the purpose of

---

[13] T Crowdy, *The Enemy Within: A History of Spies, Spymasters and Espionage* (1st edn Osprey Publishing, Oxford 2006) 14.
[14] For further examples cf. S W. Brenner & A C. Crescenzi, 'State-Sponsored Crime: The Futility of the Economic Espionage Act' (2006) 28 HJIL 389, 395 (with further references).
[15] See for example, Art 24 of the Vienna Convention on Diplomatic Relations, on outlawing covert examination of the archives and documents of a diplomatic mission, Arts 27 and 40 protecting mission communications of being monitored, Arts 30,36 and 40 that extend the above guarantees to an official diplomat's private residence and property, and similar regulations in the VCCR, Arts 35, 50 and 54.
[16] Cf. Y Dinstein, 'Computer Network Attacks and Self-Defense' (2002) 76 Int'l L Stud. Ser. US Naval War College 99, 105; Greenberg, Goodman et al., *Information Warfare and International Law* (National Defense University Press, Washington DC 1998) 26.

gathering information. It may be noted that these elements stand in contrast to for example cyber attacks, which disrupt, deny, degrade or destroy data.[17]

2.4.1 Defining a Debated Term

Cyber espionage may be viewed as a subcategory of espionage. It is the act of stealing or gaining unauthorized access to secrets stored in digital formats or on computer and IT networks. Cyber espionage can for example target governments, the military, businesses and individuals. The actor uses computer networks to covertly steal sensitive data hidden or otherwise protected. Such sensitive data may consist of intellectual property, research and development projects and material or any other information that the owner wants to protect.[18] It therefore allows a hostile actor to steal information from a remote place, doing this covertly, quite cheaply and possibly on a large scale.

A useful and comprehensive description of cyber espionage can be found in the NATO volume Peacetime Regime for State Activities in Cyberspace which describes cyber espionage as the:

> [C]opying of data that is publicly not available and which is in wireless transmission, saved or temporarily available on IT-systems or computer networks located on the territory or area under the exclusive jurisdiction of another State by a State organ, agent, or otherwise attributable to a State, conducted secretly, under disguise or false pretences, and without the (presumed) consent or approval of the owners or operators of the targeted IT-systems or computer networks or of the territorial State. Copying includes also the temporary copying of data into the random access or virtual memory of an IT-system for the purpose of mere visualization or acoustic exemplification of (e.g., voice over IP) data.[19]

Finally, it must be mentioned that the term cyber espionage is subject to debate. Some authors contend that it includes both so-called CNE (computer network exploitation or spying) and CNA (computer network attack or sabotaging) and this

---

[17] See definition in note 8.
[18] The MI5, '*Cyber Threats*' <https://www.mi5.gov.uk/home/the-threats/cyber.htmlviewed> accessed 12 March 2014 accessed 12 March 2014.
[19] K Ziolkowski, 'Peacetime Cyber Espionage – New Tendencies in Public International Law' in K Ziolkowski (ed), *Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy* (1st edn NATO CCD COE Publication, Tallinn 2013) 429. See note 8 for a definition of CNA.

is because they hold that CNE is needed for a CNA in order to be effective.[20] The author Schneier argues that 'what may be preparations for cyber warfare can well be cyber espionage initially or simply be disguised as such'.[22] In this essay the view that it is possible to distinguish between CNE and CNA is maintained. CNE does not necessarily result in cyber warfare, since this would require elements of CNA. Importantly, CNE differs from many other forms of cyber intrusions as it does not in any way alter the data it targets. Thus, it is limited to merely being an intrusion, and not, for example, an intrusive cyber attack in accordance with the CNA definition. As described, cyber espionage consists of intruding in networks to collect data, without resulting in an actual action that disrupts, denies, degrades, manipulates, damages or destroys the target. By analogy, there is a difference between breaking into an air force base to take pictures and to attach explosives to planes and blowing them up. Therefore, in the following, the view is maintained that cyber espionage and other intrusions that fall within the scope of the CNE definition are distinguishable from CNA.

2.5 USE OF PROXIES

There are many suspected examples of states indirectly or directly backing criminal cyber organizations or other non-state actors. Cyber espionage by states is often conducted by a command within the defence department or an intelligence unit, or by government organs or agencies. States may also use proxies in the form of e.g. technologically skilled individuals or groups. These actors can have full support by the nation-state, for example in cases where they receive funding or are directly employed by the state, or they might be supported in a less direct way. Examples of indirect support may include instances when a state purposely neglects to intervene in the non-state actor's activities even though the state is

---

[20] Cf. The MI5, '*Cyber Threats*' <https://www.mi5.gov.uk/home/the-threats/cyber.htmlviewed> accessed 12 March 2014; The Vice Chairman of the Joint Chiefs of Staff '*Joint Terminology for Cyberspace Operations*' Memorandum (US Department of Defense 2010) <http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace %20Operations .pdf> accessed 12 March 2014.

[22] B Schneier, 'There's No Real Difference Between Online Espionage and Online Attack' *The Atlantic* (Washington DC 6 March 2014). <http://www.theatlantic.com/technology/archive/2014/03/theres-no-real-difference-between-online-espionage-and-online-attack/284233/> accessed 12 March 2014.

aware of them.[23] Instances of unofficial command chains that connect the cyber espionage activities with high-level political leadership are also reported.[24] There are many ways states can collaborate or otherwise be involved with non-state actors in the area of cyber espionage. A thorough examination of when, and to what extent states assume state responsibility in such cases, is as remarked in section 1.4, beyond the scope of this essay, but one may well believe states are unlikely to voluntarily accept such responsibility.

Furthermore, a state will be unsuccessful in trying to avoid state responsibility by using proxies for conducting cyber espionage. This is because the concept of 'organs of a state' in the context of state responsibility is broad. It encompasses every person or entity that has that status under the state's internal legislation. This applies regardless of the person's or entity's function or place in the governmental hierarchy.[25] In turn, this means that it is clear that cyber activities conducted by intelligence, military or other state agencies will engage state responsibility if the activities in question violate an international legal obligation applicable to that state. Additionally, persons or entities, while not organs of the state, which are empowered by domestic law to exercise 'governmental authority' are according to the International Law Commission's (ILC) 2001 Articles on Responsibility of States for Internationally Wrongful Acts (Draft Articles), Art 5 (and accompanying commentary) equated with state organs. If for example a group of hackers has been empowered by a state to conduct cyber espionage against another state, this act would also engage state responsibility. Furthermore, Art 8 of the Draft Articles states that 'the conduct of a person or a group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct'. However, the material scope of

---

[23] C Czosseck, 'State Actors and Their Proxies in Cyberspace' in K Ziolkowski (ed), *Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy* (1st edn NATO CCD COE Publication, Tallinn 2013) 16.
[24] Directorate-General for External Policies, Policy Department 'Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action Within the EU' Study (European Parliament 2011) 51.
[25] Draft Articles, Art 4(2).

applicability of Art 8 is limited to instructions, direction or control. The state needs to have issued specific instructions or directed or controlled a particular operation to engage state responsibility. In summary, the use of proxies, 'patriotic hackers' or similar agents in order to conduct cyber espionage would, in cases where the relation to the state falls under Art 8, not free a state from the rule of state responsibility.

2.6 PRACTICAL PROBLEMS

While it is not a purely judicial issue, the reader should remember that although a foreign state organ intrudes on the data of another state, the target state will in practice have difficulties identifying the intruding state, and even greater difficulties in holding or proving a state responsible of such a violation.

Clearly, one of the main advantages for the actor conducting cyber espionage is that if it is at all uncovered, it is very difficult to track its source. Therefore, a retaliation by the victim state is improbable. There might be diplomatic or other political reasons to suspect specific states to be behind the cyber espionage, but it would be difficult to provide sufficient material to technically attribute a state to a specific case of cyber espionage or other antagonistic cyber actions.

The difficulty in defining the location, nature and substance of cyberspace creates is a major cause of the disagreements as to whether cyberspace is subject to state sovereignty or not. Representatives of states overwhelmingly argue that their state has sovereignty over the cyberspace spheres they attribute to their state (for example the top level domain '.gov' is limited to governmental entities and agencies of the US).[26] However, there are also persons and organizations that argue that cyberspace governs itself, that it is not subject to sovereignty by any state and should not be interfered with.[27]

---

[26] J Postel, 'Domain Name System Structure and Delegation' (The Internet Engineering Task Force 1994) Memo <http://tools.ietf.org/html/rfc1591> accessed 2 May 2014; General Services Administration, 'Gov Domain Name Registration Services'(General Services Administration) <https://www.dotgov.gov/portal/web/dotgov> accessed 2 May 2014.

[27] S J. Shackelford, *Managing Cyber Attacks in International Law, Business and Relations: In Search of Cyber Peace* (1st edn Cambridge University Press, UK 2014) 53.

Cyberspace can provide those who commit cyber espionage with an alluring cloak of anonymity, making attribution unlikely. Importantly, cyber espionage intruders can run their actions through a chain of intermediaries located in various third states, making it difficult to track an intrusion to its original source. Moreover, lack of cooperation from the state in question may increase the difficulties to determine the source or cause of a purported intrusion, especially if it does not receive cooperation by the concerned state or states. This is mainly due to the national legal authority being confined by the conventional limits of sovereignty. Even if the state intruded upon would be able to determine the source, counter intrusions would still prove difficult both from a practical and legal point of view, as the original intrusion likely involved the infrastructure of third states as well.[28] Legally, an examination would need also to examine the third state's involvement, for example; whether it was purposely collaborating with the main intruding state, or whether it was being used as a platform without its knowledge or possible knowledge.

2.7 CASES OF SUSPECTED PRACTICES OF STATE CYBER ESPIONAGE

Although some examples of state practice of cyber espionage are presented below, one must be aware that both the conducting actor and those targeted have interests not to report spying or intrusions. If, for example, a government agency makes it public that it has been spied upon, this public knowledge can harm diplomatic relations and hurt security credibility. For the 'cyber spying states', to admit ongoing and/or past spying would clearly be counterproductive, as it would alert suspicion and strain diplomatic relations.

Cyber issues are receiving increasing attention and the costs of cyber security are increasing too.[29] The reader is already acquainted with the phenomenon of state proxies in the form of non-state actors who conduct or contribute to cyber

---

[28] G Kerschischnig, *Cyberthreats and International Law*, (1st edn Eleven International Publishing, The Netherlands 2012) 12.
[29] S Gorman, 'Annual US Cybercrime Costs Estimated at $100 Billion' *The Wall Street Journal* (New York City 22 July 2013) <http://online.wsj.com/news/articles/SB10001424127887324328904578621880966242990> accessed 3 May 2014.

espionage activities. However, some of the most notable attacks have, although not with full certainty and without confirmation from the purposed acting state, been associated with the specific states that are discussed below. Not to be forgotten is that states, including those listed below, can be both actors and targets of cyber intrusions.

2.7.1 China

Although usually firmly denied by Chinese officials, it is likely that the Chinese state is highly involved in various forms of cyber intrusions including cyber espionage.[30] The republic has repeatedly been accused of using government proxies or 'patriotic hackers' to commit cyber espionage targeting foreign companies' intellectual and property development.[31] Cyber hackers backed by the Chinese Republic are known as 'patriotic hackers'. They commit intrusions into for example high-tech companies, stealing their data to the gain of Chinese companies that are state-owned or which have a close or unclear relation to the state.[32]

Beginning in 2003, the US was targeted by a massive cyber espionage campaign code named Titan Rain. Among its targets were the National Security Agency (NSA), the Department of Defense and private institutions. Partly due to the enormous resources needed to commit an attack of this extent, the espionage is believed to at least be backed by the Chinese government.[33] The US Congress annual report on China in 2013 reported that in 2012 numerous computer systems

---

[30] Directorate-General for External Policies, Policy Department 'Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action Within the EU' Study, (European Parliament 2011) 16.

[31] See for example, J Markoff & D Barboza, '2 China Schools Said to Be Tied to Online Attacks' *The New York Times* (New York City 18 February 2010) <www.nytimes.com/2010/02/19/technology/19china.html?th&emc=th> accessed 4 April 2014; S Elegant 'Cyberwarfare: The Issue China Won't Touch' *Time Magazine* (New York City 18 Nov 2009) <http://content.time.com/time/world/article/0,8599,1940009,00.html> accessed 4 April 2014.

[32] Even though not always direct attacks on extraterritorial government institutions, the espionage character and national security purpose of many Chinese-linked attacks make them relevant in the context of this essay.

[33] See C Arthur, 'Google the Latest Victim of Chinese 'State-Sponsored' Cyberwar' *The Guardian* (London 25 August 2005) <http://www.guardian.co.uk/technology/2010/jan/14/google-hacking-china-cyberwar> accessed 17 March 2014.

all over the world, including some owned directly by the US government, were subject to intrusions likely directly related to the Chinese government.[34]

2.7.2 Russia

In another eastern power, Russia, 'hacker patriots' are believed to be coordinated with the Russian armed forces. The same source reports that Russian cyber espionage has increased.[35] One of the main focuses of Russian information and cyber security strategy is the perceived threat of American 'information control' in cyber space. Russia is believed to have significant cyber capabilities, derived from a tradition of for example 'Information Warfare' and the strong position of the state's intelligence.[36]

2.7.3 The United States

The US is the world's foremost cyber power today. Other major cyber powers, notably Russia and China, have accused the US of conducting cyber intrusions including cyber espionage, and vice versa the US has accused primarily China of the same.[37] One example of the US being a victim of cyber espionage is the reports by the US Department of Defense admitting to having 24,000 Pentagon files intruded upon.[38] On the other hand, the US has not only been a victim of cyber espionage, it has also been a perpetrator; the so-called Snowden documents have revealed that the US has conducted considerable espionage activities through the NSA, for example bugging and infiltrating computer networks of countries and

---

[34] Cf. Office of the Secretary of Defense '*Military and Security Developments Involving the People's Republic of China*' Annual Report to Congress, (US Department of Defense 2011) <http://www.defense.gov/pubs/pdfs/2011_cmpr_final.pdf> accessed 18 March 2014.

[35] European Commission and High Representative, 'Cybersecurity Strategy of the European Union: An Open Safe and Secure Cyberspace', Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, JOIN(2013)1, 2013,17. <http://www.europarl.europa.eu/RegData/etudes/etudes/join/2011/433828/EXPO-SEDE_ET%282011%29433828_EN.pdf > accessed 15 March 2014.

[36] *Ibid* 58.

[37] See for example: Z Wa & F Jing, 'Washington Tries to Shift Spying Blame to China' *China Daily* (Beijing 24 December 2013) <http://www.chinadaily.com.cn/china/2013-12/24/content_17192169.htm> accessed 30 April 2014; European Commission and High Representative, 'Cybersecurity Strategy of the European Union: An Open Safe and Secure Cyberspace', Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, JOIN(2013)1, 2013, 58.

[38] S J. Schackelford, *Managing Cyber Attacks in International Law, Business, and relations: in Search of Cyber Peace*, (1st edn Cambridge University Press, United States 2014) 8.

institutions. The targeted countries and institutions include the United Nations (UN), the EU and the International Atomic Energy Agency.[39] The former chief technology officer for the Defense Intelligence Agency of the US, did admit that the agency conducted reconnaissance in foreign countries' networks and evaluated its suspects without engaging them, thereby seemingly admitting to US use of cyber espionage.[40] The US has under the defence plan of the Comprehensive National Cybersecurity Initiative adopted a defence policy specifically for issues of cybersecurity.[41] It employed its first cyber command in 2010.[42]

2.7.4 Others

Non-super power states have reported that they have been subject to cyber espionage linked to foreign government agencies. There are countless examples, and the following provides only a small selection. It should also be noted that these countries are also likely to conduct cyber espionage against other states, although perhaps on a smaller scale than the cyber-powers listed above.

One of the most prominent cases of cyber espionage was discovered in 2009 after Tibetan authorities suspected they had fallen victim. The investigation conducted by the Information Warfare Monitor, an independent venture group based in Canada, revealed that a wide range network of computers had been compromised by a so-called Trojan, capable of fully controlling the compromised systems. This major cyber espionage operation was named GhostNet. There was circumstantial evidence pointing toward Chinese elements being behind the attack, but the investigation still concluded that there was not enough evidence to implicate the Chinese government.[43]

---

[39] L Poitras, M Rosenbach & H Stark, 'Codename 'Apalachee': How America Spies on Europe and the UN' *Der Spiegel International* (Hamburg 26 August 2013) <http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html> accessed 30 April 2014.
[40] Cf. H Shane, 'The Cyberwar Plan' *National Journal Magazine* (11 November 2009) 15.
[41] The Executive Office of the President of the United States, *The Comprehensive National Cybersecurity Initiative* (The White House 2010).
[42] United States Army, '*Establishment of the US Army Cyber Command*' (US Army Cyber Command) <http://www.arcyber.army.mil/history.html> accessed 25 February 2014.
[43] G Kerschischnig, *Cyberthreats and International Law*, (1st edn Eleven International Publishing, The Netherlands 2012) 68.

In May 2010, a leaked memo from the Canadian Security and Intelligence Service said that cyber espionage had targeted among others Canadian computer and combinations of networks of the Canadian government.[44]

In 2012 it was reported that a highly sophisticated malware named Flame was affecting countries primarily in the Middle East and that this was ongoing since at least 2010. The malware did not appear to alter the data in order to cause physical damage; instead, it seemed to aim at collecting vast amounts of sensitive data. The malware was for example able to take screen-shots of ongoing activity, record Skype calls or other audio. Its targets included individuals, businesses, academic institutions and governments. Due to mainly the size and sophistication of Flame it is believed to be the product of a state or at least to be state-backed.[45] The Flame malware is a real-life example of cyber espionage as defined in this essay, as it did not seek to alter or otherwise affect protected, private or hidden data, but to collect it.

Another substantial case of cyber espionage was uncovered when Kaspersky, the Russian-founded security firm and privately held vendor of software security products, initiated a new threat research in October 2012 after attacks against computer networks of many international diplomatic service agencies. It was indicated that the cyber espionage campaign, named Red October had been active since 2007, with a main objective of gathering intelligence from targets such as governmental and scientific research organizations.[46]

---

[44] GovInfoSecurity.com 'Time Line of Major Global Cyber Incidents 2010-2011' *Bank Info Security Magazine* (Princeton 17 March 2011) <http://www.bankinfosecurity.com/articles.php?art_id=3440> accessed 17 March 2014.

[45] Kaspersky Labs and ITU Research, 'Kaspersky Labs and ITU Research Reveals New Advanced Cyber Threat' (Kaspersky Lab 29 May 2012) <http://usa.kaspersky.com/about-us/press-center/press-releases/kaspersky-lab-and-itu-research-reveals-new-advanced-cyber-threa > accessed 25 March 2014.

[46] '"Red October" Diplomatic Cyber Attacks Investigation' (SecureList) <http://www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation,> accessed 2 April 2014.

A spokesperson of the Swedish National Defense Radio Establishment said in an interview that in 2013 Swedish government agencies were subject to cyber intrusions in the form of cyber espionage conducted by foreign state agencies.[47]

2.8 SUMMARY

In this chapter the reader has been guided into understanding technical aspects of cyberspace and cyber espionage. To summarize, the definition of espionage entails the covertness of the activities being conducted. Furthermore, cyber espionage differs from other forms of cyber intrusions, as it is limited to being an intrusion, and does not for example alter the data intruded upon. Although states use policies of denial or simply do not comment on matters of espionage, the reader has learned that many state-actors are suspected of conducting cyber espionage to various extents. And, just as states themselves are conducting cyber espionage, other states also target them. The involvement of states conducting cyber espionage highlights the need to examine the legality of these types of actions.

3 ESPIONAGE AND INTERNATIONAL LAW

3.1 INTRODUCTION

The first leads in determining the possible legality of cyber espionage are found within the larger category of espionage. There are different opinions within the legal and sometimes the political debate on the legality of espionage. Some view it as illegal, others claim it to be lawful and some say it is neither legal nor illegal.[48] This chapter will guide the reader into the discussion about espionage's legality in international law, subsequently enabling the reader to apply similar arguments in the narrower field on the legality of cyber espionage in the context of territoriality.

---

[47] K Örstadius 'Företag utsätts för intrång av utländsk makt' *Dagens Nyheter* (Stockholm 8 January 2014) <http://www.dn.se/nyheter/sverige/foretag-utsatts-for-intrang-av-utlandsk-makt/> accessed 20 March 2014.

[48] K Ziolkowski, 'Peacetime Cyber Espionage – New Tendencies in Public International Law' in K Ziolkowski (ed), *Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy* (1st edn NATO CCD COE Publication, Tallinn 2013) 430.

3.2 ILLEGALITY OF ESPIONAGE – SOME ARGUMENTS

Those who suggest that cyber espionage is illegal argue that espionage is penalized within domestic law systems. This line of reasoning is based upon the view that '[u]nder international law, if something were truly legal (or at least not illegal), no state should prosecute those who do it'.[49] However, the sources of international law, for example the 'principles of law recognized by civilized nations' of Art 38(1) of the Statute of the International Court of Justice (ICJ Statute), hold otherwise. The article elevates those principles of national law that are applicable to inter-state relations, to the level of international law. Activities of espionage are penalized within all principal systems of domestic law, but the mere existence of such penalization is not enough to deem espionage prohibited under international law. Importantly, the subjects of domestic law are not states, but individuals, and domestic law governs only the individual criminal liability for espionage activities, not the liability of states. Hence, domestic laws of states criminalizing espionage cannot be elevated to a principle of international consisting of a prohibition of espionage.[50] Another hindrance for extracting a principle of illegality of espionage is that issues of inter-state political relations are found within the sphere of international relations and not within municipal law.

Yet another argument of the illegality of espionage is that which refers to Art 2(4) of the Charter of the United Nations (UN Charter) and its prohibition of the 'use of force' in international relations. However, this view confuses trespassing, physical intrusion by state aircraft, vessels etc. into the target state's territory with espionage per se.[51] This article together with the prohibition of use of force and the applicability of cyber espionage intrusions will be discussed further in chapter 4.

---

[49] A J. Radsan, 'The Unresolved Equation of Espionage and International Law' (2006-2007) 28 Mich J Int'l L 595, 604.
[50] K Ziolkowski, 'Peacetime Cyber Espionage – New Tendencies in Public International Law' in K Ziolkowski (ed), *Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy* (1st edn NATO CCD COE Publication, Tallinn 2013) 432.
[51] *Ibid* 432.

3.3 LEGALITY OF ESPIONAGE – SOME ARGUMENTS

3.3.1 Espionage as Self-Defence or as a Purported Right of Pre-Emptive Self-Defence

The predominant argument among those who view espionage as expressly permitted under international law is that espionage is a component of a right of self-defence or anticipatory or pre-emptive self-defence. Self-defence is allowed according to Art 51 of the UN Charter, if it is lawful and in conformity with the Charter. However, the scope of this essay is limited to peacetime cyber espionage, whereas cyber espionage justified as self-defence intrinsically belongs only to situations of conflict. If one goes further and believes in the controversial putative right of pre-emptive or anticipatory self-defence, cyber espionage could consequently be conducted in periods where a conflict might be imminent but has not yet developed. If one holds the view that such a right exists, espionage is a legitimate means whereby states defend themselves. In support of this argument the 'Gary Powers U-2 incident' can be referred to, a case where a US reconnaissance plane flew over Soviet territory on an espionage mission, but was shot down by a Soviet rocket unit. In the aftermath, when the incident became known to the public, the then US President Dwight D. Eisenhower stated that there was a '[…] distasteful necessity of espionage activities in a world where nations distrust each other's intentions.' Eisenhower also emphasized that the espionage was defensive, without any aggressive intents and was conducted in order to assure the safety of the US and the 'free world' against surprise attacks.[52] According to Eisenhower's statement, the justification of espionage is derived from the spying state's incentive. Thus, if a state's incentive is based on a presumed right to anticipatory self-defence the espionage would be allowed, whereas if espionage is conducted as a preparatory means of an act of aggression, it would be prohibited. An evident counterargument of this incentive-based view is that it gives the espionage perpetrators an 'easy way out' as they could, perhaps too easily, rely on claiming that their (subjective) incentive was based on a right of

---

[52] The United States, The Office of Public Services, Bureau of Public Affairs, '*President's Statement of May 16*' *The Department of State Bulletin,* XLII, No. 109 (Washington D.C. 6 June 1960) 905.

anticipatory self-defence and that they did not intend to conduct an act of aggression. Consequently, unless an actual act of aggression takes place it would be hard to show that the state conducting espionage intended to commit such an act.

Another argument for the legality of espionage is that espionage may be viewed as an unfriendly act. Unfriendly acts can be committed without being in breach of any binding norm of international law. The author Dinstein specifically mentions espionage as an example of unfriendly act, thereby holding that espionage is 'strictly speaking' legal as it does not violate international law.[53] Such acts are liable to upset the state the targeted state, but as long as no breach of international law is committed the targeted state has no *jus standi*, i.e., legal standing, for objecting to the unfriendly conduct.

3.3.2 A Rule of International Custom

One more argument of the lawfulness of espionage refers to its widespread state practice. Of particular weight to this argument is the existence of government intelligence agencies that provide espionage services as legitimate functions of the state, and these agencies do so without incurring the other state's official statements of illegality of espionage, – therefore insinuating legality under customary international law. The International Court of Justice (ICJ) has confirmed that a rule of 'international custom, as evidence of a general practice accepted as law' as stated in Article 38(1)(b) of the ICJ Statute requires two conditions to be fulfilled: first, that the acts concerned must amount to a generally uniform and consistent state practice, and second, that there must be a belief that the behaviour is required or permitted under international law – described in the notion of *opinio juris sive necessitatis*.[55] The first, objective requirement is certainly fulfilled; intelligence gathering, is a common and integral function of a state. The second, subjective requirement is more difficult to prove fulfilled. Numerous cases of state practice of espionage that have been uncovered, but when governments have issued official statements on such activities, they have seldom

---

[53] Y Dinstein, 'Computer Network Attacks and Self-Defense' (2002) 76 Int'l L Stud. Ser. US Naval War College 99, 101.
[55] See for example: *North Sea Continental Shelf (Federal Republic of Germany v Denmark; Federal Republic of Germany v Netherlands)* (Judgment) [1969] ICJ Rep 54, para 77.

referred to espionage as a necessity or requirement (and the states targeted by espionage have certainly not viewed the spying state's activity as necessary in this sense). In well-known cases of alleged espionage, states have responded by protesting or condemning the activities, by referring to other aspects than espionage as grounds of illegality or by not commenting them at all.[56] Two examples of states officially protesting against espionage activities include the aforementioned Gary Powers U-2 incident, which the Soviet president Khrushchev protested against,[57] and the recent allegations of German Chancellor Merkel's phone being tapped by the US, after which the Chancellery stated such activities to be 'totally unacceptable'.[58] When a Soviet submarine ran aground in Swedish internal waters, inside the protection area of the Karlskrona naval base on 27 October 1981, the Swedish government issued diplomatic protest notes, in which Sweden protested the grave violation of Swedish territoriality and the fundamental principles of international law. However, the protest notes did not refer to espionage as such, but to 'illicit activities'.[59]

Official comments providing an *opinio juris* on cyber espionage are scarce. Neither the 'Moonlight Maze' incident in 1998-1999, in which supposedly Russian hackers penetrated computer networks of e.g. the US Department of Defense and the The National Aeronautics and Space Administration, nor the 'Titan Rain' incident of 2003-2007 in which supposedly Chinese state-sponsored hackers gained access to various departments of the US, resulted in any official statements by the US toward the two suspected states, nor were there any statements by Russia or China. Other examples of espionage with no indications of

---

[56] For more examples see: K Ziolkowski, 'Peacetime Cyber Espionage – New Tendencies in Public International Law' in K Ziolkowski (ed), *Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy* (1st edn NATO CCD COE Publication, Tallinn 2013) 439.

[57] Union of Soviet Socialist Republics, Draft Resolution Concerning Alleged Aggressive Acts by the United States Air Force Against the Soviet Union, UNSC Doc S/4321(23 May 1960, not adopted). The draft resolution condemns the intrusion by the US as an act of aggression.

[58] J Appelbaum, H Stark, M Rosenbach & J Schindler, 'Berlin Complains: Did US Tap Chancellor Merkel's Mobile Phone?' *Der Spiegel International* (Hamburg 23 October 2013) <http://www.spiegel.de/international/world/merkel-calls-obama-over-suspicions-us-tapped-her-mobile-phone-a-929642.html> accessed 18 April 2014.

[59] B J. Theutenberg, 'U 137 – Folkrätt och neutralitetspolitik i tillämpning' (1982) 2 Kungliga Krigsvetenskapsakademins handlingar och tidskrift, 112.

an *opinio juris* in this respect, include the joint effort of the NSA and the United Kingdom (UK) Government Communication Headquarters to tap into various communications closely related to the other members of the UN Security Council and the monitoring of the communications of the UN Secretary General and the PRISM mass-surveillance by the NSA 'discovered' in 2007.[60] In the aforesaid case of Operation Red October (see section 2.7.4) there were no grounds for attributing the espionage to a specific state. Any official statement from a state targeted by it, is in terms of *opinio juris* not probable, since a target state would lack grounds to accuse another state of being behind the espionage. Hence, there is little substance to provide for an *opinio juris*, and what exists is highly conflicting regarding the legality or illegality of espionage.

The Head Secretary for Sweden's ongoing Committee on a strategy for information security, Wennerström, said that the current practice of states regarding espionage and intelligence gathering is contradictory. States are sanctioning espionage or intelligence gathering while national law criminalizes espionage (for the benefit of another state). Wennerström agreed that there is known state practice of intelligence gathering and that there is no *opinio juris* on neither the legality of espionage nor cyber espionage.[61]

In all, there are only few examples of states commenting on the legal and necessary, or on the illegal aspects of espionage, and there is certainly no uniformity in comments from states regarding espionage and its necessity under international law. Therefore, under the provision that the second requirement (i.e. *opinio juris*) is not fulfilled, espionage cannot be regarded as a rule of international custom.

---

[60] K Ziolkowski, 'Peacetime Cyber Espionage – New Tendencies in Public International Law' in K Ziolkowski (ed), *Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy* (1st edn NATO CCD COE Publication, Tallinn 2013) 440.
[61] Interview with E Wennerström, Head Secretary in the Committee on a strategy on information security (*Regeringens utredning om Strategi och mål för hantering och överföring av information i elektroniska kommunikationsnät och it-system*) Dir 2013:110 (Stockholm, Sweden, 24 November 2014).

3.4 CONCLUSION – ESPIONAGE IS NOT PROHIBITED AS SUCH

The above arguments of the illegality and legality of espionage, respectively, were here both found to be insufficient. One has therefore to find an intermediate path, and look beyond these arguments. The ICJ has arguably had opportunities to take a position of peacetime espionage they have not done so. Although the US was alleged by Iranian and Nicaraguan representatives, respectively, of committing activities of espionage the ICJ's judgments in the *Tehran Hostages case* and the *Nicaragua case* focused on other aspects than espionage.[62] In the Permanent Court of International Justice (PCIJ) *Lotus case* of 1927 a principle applicable to situations that are not, or only partly regulated by international law, is presented. The Court stated that:

> International law governs relations between independent States. The rules of law binding upon States therefore emanate from their own free will as expressed in conventions or by usages generally accepted as expressing principles of law and established in order to regulate the relations between these co-existing independent communities or with a view to the achievement of common aims. Restrictions upon the independence of States cannot therefore be presumed.[63]

From this statement follows the principle that, defined here in a simplified and short version, a state may exercise jurisdiction on any matter, as long as international law does not expressly prohibit it to do.[64] Peacetime espionage as such is not expressly prohibited under international law but there are specific acts of espionage that are prohibited. For example, Art 41(1) of the Vienna Convention on Diplomatic Relations states that diplomatic staff stationed abroad must comply with the domestic law of the state that they are stationed in, and indeed, states do generally criminalize different acts of espionage in their domestic systems of law.

In conclusion, because espionage as such is not prohibited under international law, there might be instances where it could be permitted. The author Forceses

---

[62] D Fleck, 'Individual and State Responsibility for Intelligence Gathering' (2006-2007) 28 Mich J Int'l L 678, 691-692.
[63] *The Case of the S.S. 'Lotus' (France v Turkey)* (Judgment) [1927] PCIJ Rep Series A No 10, 18.
[64] *Ibid*, paras 46-47; *North Sea Continental Shelf (Federal Republic of Germany v Denmark; Federal Republic of Germany v Netherlands)* (Judgment) [1969] ICJ Rep 54, para 77. Cf. the Statute of the ICJ Art 38 on applicable law.

emphasises that the question of international law and espionage should not be reduced to one of legality or illegality. Instead, the answer depends on an assessment of the method, location and other relevant factors of the assessed espionage activities.[65] In accordance with Forceses' suggestion, this essay will now examine the specific factors that adhere to cyber espionage in the context of the provisions of international law.

3.5 SUMMARY

Above, arguments of the illegality or legality, respectively, of espionage under international law were presented. Because it was found that espionage as such is not forbidden, there is room to continue and to narrow the discussion into espionage's subcategory of cyber espionage, and the aspects that adhere with the latter.

4 CYBER ESPIONAGE AND INTERNATIONAL LAW

4.1 INTRODUCTION – WHY INTERNATIONAL LAW IS APPLICABLE TO CYBERSPACE

The previous section concluded that espionage activities must be individually tried under a case-to-case basis under the rules of international law. In the following it will be shown that international law is applicable to cyberspace and consequently cyber espionage.

Many states have taken the position that international law is applicable to cyberspace.[66] In 2011, the US International Strategy for Cyberspace acknowledged that '[t]he development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing norms obsolete. Long-standing international norms guiding state behaviour – in times of peace and conflict – also apply in cyberspace'.[67] The UN Group of Governmental

---

[65] C Forcese, 'Spies Without Borders: International Law and Intelligence Collection' (2011) 5 J Nat'l Sec L & Pol'y 179, 181.
[66] Cf. UN General Assembly, Group of Governmental Experts, Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc A/68/98 (24 June 2013) para 19.
[67] The White House, '*International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World'* (2011). See also the US position as set forth for the UN in UN Doc A/66/152.

Experts, which includes Russia and China, agreed that international law applies to cyberspace.[68] In 2014 a committee for the Swedish Ministry of Defence stated that they viewed international law as applicable to cyberspace.[69] The authors behind the Tallinn Manual (TM), described by the authors as an academic, non-binding study on how international law apply to cyber conflicts and cyber warfare, unanimously agreed that international law apply to cyberspace. The authors also 'rejected any assertions that international law is silent on cyberspace in the sense that it is a new domain subject to international legal regulation only on the basis of new treaty law'.[70] This essay does not discuss a putative need of new treaty law, but it asserts that there are principles of international law that can be applicable to cyberspace and therefore also to relevant areas of cyber espionage.

There are obviously practical problems in applying to cyberspace the regulations and customs of international law, of which a majority originate from a time before the creation of cyberspace. An opponent of the applicability of international law on cyberspace could argue that cyber incidents or attacks are fundamentally different from traditional warfare and therefore require new legal regimes and forms of control. However, in this essay it will be shown that cyberspace can be subject to international law and that the laws of war might be analogous, but they are not irreconcilable with the digital age.

This chapter focuses on how some of the main principles of international law apply to extraterritorial cyber espionage, by using cyberspace and in the form of intrusions by states into other states' organs.

4.2 SOVEREIGNTY AND THE TERRITORIAL PRINCIPLE

The principle of sovereignty is used in international law to express a relationship between a state and its own territory.[72] Based on this principle, each state can claim from all other states full respect for its territorial integrity and also political

---

[68] M N. Schmitt 'The Law of Cyber Warfare: *Quo Vadis?*' (2014) 25 Stan L & Pol'y Rev 269, 271.
[69] Swedish Ministry of Defence, *Försvaret av Sverige – Starkare försvar för en osäker tid*, Ds 2014:20.
[70] TM Part 1 'International cyber security law' (no page number available).
[72] V Lowe, *International Law* (1st edn Oxford University Press, Oxford 2007) 138.

independence.[73] Importantly, the concept of sovereignty in international law is a legal construct as opposed to so called political sovereignty that reflects possession of power and authority in practice. There are many elements to the principle of sovereignty and providing all is beyond the scope of this essay. Briefly, they tend to revolve around territorial effectiveness: hence a close link to the territorial principle.

The territorial principle is a corollary of a state having sovereignty over its territories. The sovereignty of the state entails that it has the right to prescribe laws 'that set the boundaries of the public order of the state'.[74] This right extends also to actions within its territory that has their effects abroad, and to actions abroad that have effects inside the territory. For example, in the case of the Lockerbie bombers, where terrorists blew up a plane over the UK, the UK had jurisdiction, even though the bomb was put on board in Malta.[75]

The principle of territorial sovereignty holds that states exercise full and exclusive authority over their sovereign territories. These territories include land, internal waters, territorial sea, archipelagic waters, and national airspace or platforms (for example aircraft, satellites or vessels).[76] In the *Lotus case* the PCIJ stated 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'.[77] Furthermore, in Oppenheim's International Law it is said that a 'state is not allowed to send its troops, its men-of-war, or its police forces into or through foreign territory /…/

---

[73] A Cassese, *International Law* (2nd edn Oxford University Press, Oxford 2004) 14.
[74] M D. Evans, *International Law* (3rd edn Oxford University Press, Oxford 2010) 320.
[75] M Inazumi, *Universal Jurisdiction in Modern International Law: Expansion of National Jurisdiction for Prosecuting Serious Crimes Under International Law* (1st edn Intersentia, 2005) 165 and *Questions of Interpretation and Application of the 1971 Montreal Convention arising from the Aerial Incident at Lockerbie (Libyan Arab Jamahiriya v. United Kingdom)* [Judgment] 1998 ICJ Rep 3 and *Questions of Interpretation and Application of the 1971 Montreal Convention arising from the Aerial Incident at Lockerbie (Libyan Arab Jamahiriya v. United States of America)* [Judgment] 1998 ICJ Rep 3.
[76] Cf. for example United Nations Convention on the Law of the Sea, part 2, Art 2.
[77] *The Case of the S.S. 'Lotus' (France v Turkey)* (Judgment) [1927] PCIJ Rep Series A No 9, paras 18-19c.

without permission'.[78] Thus, an unauthorized entry into and presence in a state's sovereign areas of a foreign organ, in the form of for example an agent who acts in official capacity, would violate the territorial sovereignty of the state intruded upon.

4.3 SOVEREIGNTY OF CYBERSPACE

It is important to determine whether cyberspace can be subject to state sovereignty because this would give the state right to exercise its functions within cyberspace. A description of what sovereignty is can be found in the *Island of Palmas* Arbitral Award of 1928. The Court held that sovereignty is signified by states being independent from one another in the sense that within a state's sovereign territory the state has the right to exercise, among other things, the functions of a state.[79] Furthermore, sovereignty implies that a state may control access to its territory and enjoys (within the limits set by customary international law and treaty law) the exclusive right to exercise jurisdiction and authority on its territory.

Because cyber espionage is conducted without authorization, it is therefore a violation of the principle of sovereignty. Because data is stored on servers, and servers are included in the definition of cyber infrastructure, this means that if data intruded upon is located on the target state's territory the target state has a right to exercise 'sovereign prerogatives' over that data.[80] In line with this the TM holds that 'A state may exercise control over cyber infrastructure and activities within its sovereign territory'.[81] In the context of this essay, an application of sovereignty results in the conclusion that a state that enjoys sovereignty over the territory where a server is located, also has the right to decide over access to that server – and the data stored in the server. Through territorial sovereignty and the physical presence of for instance servers, the state thus has the right to control cyber infrastructures, including servers.

---

[78] L Oppenheim, H Lauterpacht (ed) *International Law: A Treatise* (8th edn Longmans, Green, and Co., 1955) 288.
[79] *Islands of Palmas (Netherlands v US)* (1928) 2 RIAA 829, 838.
[80] *Ibid* 838.
[81] TM 15.

The global, non-physical, conceptual element of cyber space clearly differs from the traditional spaces onto which the principle of sovereignty is applied: land, sea, air and space.[83] By some, cyberspace is claimed to be a space unregulated or only partly regulated by law. If cyberspace were indeed unregulated and unaffected by law this essay would soon reach its end concluding that cyber espionage is not prohibited due to it being a law-less Wild West. However, this view is in the following found to be inadequate, and it is on the contrary found that cyberspace is affected by and can be subject to international law. Yet, for the sake of discussion, the main arguments for an 'independent cyberspace' are presented below.

4.3.1 Arguments for an Independent Cyberspace

One of the main proponents of the independence of cyberspace is J P. Barlow, a political activist and cyberlibertarian. In his 'A Declaration of the Independence of Cyberspace' from 1996, he states that cyberspace is a space subject to internal governance.[84] This governance emerges from social contracts that are present within cyberspace's borders. Perhaps close or within this view, are those who see cyberspace as an independent dimension, outside the reach of rules and regulations of other human spheres.[85] The view of a cyberspace as a terra nullius, a place not yet under regulation of any government, was common among the early users of cyberspace.[86] Agreeing with an independent cyberspace not being subject to state sovereignty or international law, puts to an end the discussion of extraterritorial data intrusions by states, since no state has a cyber territory. If so, what happens in cyberspace would only be subject to regulations within for example the social contracts mentioned by Barlow.

4.3.2 Arguments for Cyberspace Being Subject to Sovereignty

This view argues that although cyberspace is an abstract dimension it still has physical locations, for example, the locations of servers. The location of the server is subject to state jurisdiction, placing the 'slice' of cyberspace that is located on

---

[83] V Lowe, *International Law* (1st edn Oxford University Press, Oxford 2007) 151.
[84] J P. Barlow, 'A Declaration of the Independence of Cyberspace' (1998) <https://projects.eff.org/~barlow/Declaration-Final.html> accessed 3 March 2014.
[85] M N. Schmitt, 'Reaction: Cyberspace and International Law: the Penumberal Mist of Uncertainty' (2013) 126 HLR F 176, 176.
[86] A Schwabach, *Internet and the Law: Technology, Society, and Compromises* (2nd edn ABC-CLIO, California 2014) 57.

that server, under that state's jurisdiction. Furthermore, the actors that exist in cyberspace, are also subjects of state jurisdiction. Together, this makes it clear that cyberspace does not exist in a vacuum. Instead, both the machines and the actors that constitute and effectuate cyberspace, are subject to state sovereignty.[87]

4.4 CYBER ESPIONAGE, SOVEREIGNTY AND JURISDICTION

Now we have found that data located on servers within a state are subject of that state's sovereignty. The next step is to examine if the intrusive element of cyber espionage violates a state's sovereignty and the closely related principle of territorial jurisdiction.

4.4.1 Cyber Espionage and Sovereignty

As written in section 4.3, the principle of sovereignty allows states 'to exercise to the exclusion of any other State, the functions of a State' on their territory.[88] In the context of cyber espionage this principle entails that states may regulate all cyber activities and control the use of any cyber infrastructure that take place within its territory, and exercise legal jurisdiction over such activities.[89]

One can have the view that cyber espionage does not constitute an unlawful intrusion into the sovereign territory of a foreign state, mainly because it lacks an altering element. Cyber espionage can be conducted without inducing alterations in the target state's sovereign areas, and it does not aim for or result in an effect in the target state. Cyber espionage intrusions can thus be argued to not be comparable to traditional espionage 'platforms' such as state vessels, submarines or aircraft intruding into the sovereign areas of the target state. It may be viewed as an unauthorized virtual trespass and therefore not comparable to a physical entry or presence in a foreign state.

However, in the view of this essay, cyber espionage, i.e., extraterritorial intrusions through cyberspace into protected data of a foreign state, should be seen as a violation of a state's sovereignty. Cyber espionage is comparable to an agent who

---

[87] J P. Trachtman, 'Global Cyberterrorism, Jurisdiction, and International Organization' in M F. Grady & F Parisi (eds), *The Law and Economics of Cybersecurity* (1st edn Cambridge University Press, 2005) 268.
[88] *Islands of Palmas (Netherlands v US)* (1928) 2 RIAA 829, 838.
[89] M N. Schmitt 'The Law of Cyber Warfare: *Quo Vadis?*' (2014) 25 Stan L & Pol'y Rev 269, 274.

breaks into a governmental office to find and collect secret and protected information of the target state. Similarly, cyber espionage involves an unauthorized presence in the target state by a foreign organ or entity acting in official capacity. What differs is the medium used to commit this type of espionage. Whereas an agent conducts his or hers espionage activities in the physical spaces of land, sea, air or space, cyber espionage takes place only in the virtual medium of cyberspace. Nonetheless, this difference lacks importance in this context because of the previous conclusion that servers, where the data intruded upon is stored, are subject to state sovereignty due to their physical location, and are therefore under a state's territorial jurisdiction.

Furthermore, the author Wright has an approach that focuses on the object and character of a state's actions.[90] He writes that a state has a right of sovereign dominion that should not be interfered with:

> Domain, like property in systems of national law, implies the right to use, enjoy and transfer without interference from others, and the obligation to each state to respect the domain of others. The precise definition of this obligation is the major contribution which international law can make toward maintaining the peaceful co-existence of states.[91]

Although the cyberspace that we know today was yet to be when Wright wrote the above in 1960, it is not far-fetched, when applying Wright's concept of interference, to view the intrusion into a server as interference into the sovereign dominion of the target state. The ICJ states that a prohibited intervention 'must be one bearing on matters in which each state is permitted, by the principle of state sovereignty to decide freely'.[92] If a state enjoys sovereignty over a territory, this sovereignty also entails the state's right to territorial jurisdiction over the area in question (cf. section 4.4.2). When a state conducts cyber espionage against another

---

[90] Q Wright's approach can also be applied onto an assessment of the ill- or legality of an act of intervention. Doing this result in an assessment based not on the presence of coercive intention or effect but on the object and character of an intervention (cf. the discussion on a purported need for a coercive element for an act to comprise prohibited intervention in section 4.6.2).
[91] Q Wright, 'Subversive Intervention' (1960) 54 Am J Int'l L 521, 528.
[92] *Case Concerning the Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America)* (Merits) [1986] ICJ Rep 14, para 205.

state's data that is located on a server on the targeted state's territory, this act is in violation of the targeted state's right to freely decide who or what may enter its territory. One could therefore argue that cyber espionage is prohibited because it constitutes an intrusion into the target state's right to decide freely regarding access to data located on servers within its sovereign territory.

Another argument for cyber espionage violating the rights enjoyed by a sovereign state can be found in the *R v Hape case* of the Canadian Supreme Court. The Court confirmed that enforcement may not take place on another state's territory without that state's consent, and also that a state may not exercise public authority on another state's territory.[93] Enforcement actions can be authorized only by the territorial state. This entails that acts that are prohibited for a non-state actor to conduct where state A has territorial sovereignty, are prohibited also for state B to conduct in the same areas. As the author Wrange explains, domestic law does typically not authorize search of premises by non-state actors, and this is neither allowed for a foreign state on another state's territory. Cyber espionage entails that a foreign state 'breaks in' on protected data of another state in the target state's territory, an act that can be compared with state-level search of premises. Similar to national non-state actors not being authorized to conduct search of premises, neither is a foreign state allowed to conduct the comparable act of cyber espionage within the target state.[94]

4.4.2 Cyber Espionage and Jurisdiction

The jurisdiction of a state encompasses the state's authority to prescribe, enforce and adjudicate. Jurisdiction extends to matters of civil, criminal, or administrative nature. In international law, jurisdiction concerns to which extent a state is permitted to exercise its jurisdiction over persons or things in its territory and/or abroad. Jurisdiction in international law is closely linked to sovereignty of states –

[93] R v Hape SCC (CanLII) (2007) 2 SCR 292, para 104-105.
[94] P Wrange, 'Intervention in National and Private Cyberspace and International Law' in Ebbesson, et al.: *International Law and Changing Perceptions of Security*, (Brill | Nijhoff, 2014) 307, 314.

this is reflected in the principles of equality of states and non-interference in other states' domestic affairs.[95]

A subcategory of jurisdiction is territorial jurisdiction. The territorial principle holds that a state is free, with some exceptions, to legislate and enforce its legislation within its territory. A 'constructive presence (a certain degree of contact with the territorial state)'[96] can provide enough basis for a state to apply its legislation on for example legal persons or corporations. The location of a server within a state's territory, for example, is considered to provide enough basis for a state to apply its legislation on the data stored on the server. According to TM Rule 2 (b) a state may exercise its jurisdiction over cyber infrastructure located on its territory. The Manual emphasizes the connection between the territorial location of cyber infrastructure and the applicability of international law.

Territorial jurisdiction can be divided into two types: subjective and objective territoriality. The objective territoriality is most relevant for this essay as it describes the jurisdiction that 'permits a state to deal with acts which originated abroad but which were completed, at least in part, within its own territory…'.[97] If objective territorial jurisdiction is applied to acts of cyber espionage, one finds that the target state has jurisdiction over acts of cyber espionage originating abroad, because cyber espionage is, at least in the part that involves the intrusion on a server located in the target state, completed within the target state's territory.

In practice it may be difficult to determine jurisdiction within cyberspace since many systems, data and processing within cyberspace span national borders. Technically, data can be located in multiple jurisdictions simultaneously. However, I want to emphasize that the existence of technical challenges should not deprive a state of its legal right to exercise jurisdiction over servers (and other cyber infrastructure) located on its territory.

---

[95] A Aust, *Handbook of International Law,* (1st edn Cambridge University Press, 2005) 43.
[96] *Ibid* 44.
[97] Joined Cases 89, 104, 114, 116, 117 and 129/85, *Ahlström Osakeyhtiö and Others v Commission* [1994] ECR I-100, Opinion of AG Darmon.

4.5 CYBER ESPIONAGE AND THE PRINCIPLE OF NON-INTERVENTION

This section focuses on the applicability of the non-intervention principle on cyber espionage.[98] The principle of non-intervention – in contrast to the prohibition of the use of force in Art 2(4) of the UN Charter – refers not only to armed force, but also to lower intensities of force. This essay argues that although cyber espionage does not in itself consist of armed force, it is an intrusion that takes place covertly in order to gain information and is not intended to cause collateral damage or leave other traces behind.[99]

It is, however, common that issues of cyber intrusions and/or attacks are approached from the perspective of *jus ad bellum*; specifically, if cyber attacks can be regarded as an unlawful use of force.[100] Therefore, this section will start with analysing the applicability of Art 2(4) of the UN Charter on cyber espionage.

4.5.1 Why Cyber Espionage is Not Equivalent to Use of Force

Cyber espionage is by some argued to amount to unlawful use of force. Although cyber espionage alone does not cause or aim at causing alterations, damage or sabotage, it can provide the necessary information for later use of force, for example an armed attack or other military operations. The author Lin writes that it may from a technical standpoint be very difficult to distinguish between a cyber attack and a cyber exploitation (for example in the form of cyber espionage), because both begin with taking advantage of a vulnerability in the targeted system.[101] Factors that could convert cyber espionage into a cyber attack are for example immediacy, directness and invasiveness. The immediacy factor is

---

[98] There are exceptions to this principle, of which some are relevant to cyber espionage, for example, the argument that cyber espionage is justified in cases of self-defence (cf. Art 51 of the UN Charter and Art 21 of the Draft Articles). Another example is if a state provides assistance upon the request or with the consent of the legitimate government of another state. See also: V Lowe, *International Law* (1st edn Oxford University Press, Oxford 2007) 104 and P Kunig, 'Intervention, Prohibiton of', Max Planck Encyclopedia of Public International Law <http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1434> accessed 24 April 2014.

[99] Cf. the previous discussion in section 2.4.1.

[100] D Fleck, 'Individual and State Responsibility for Intelligence Gathering' (2006-2007) 28 Mich J Int'l L 678, 691-692.

[101] H S. Lin, 'Offensive Cyber Operations and the Use of Force' (2010) J Nat'l Sec L & Pol'y 63, 78.

important because the shorter the time period between the espionage and the attack, the harder it is to tell the two acts apart. The directness factor examines the causality between the espionage and the attack. The more direct the connection, the harder it is to tell the two acts apart. The third factor concerns invasiveness. An act undertaken in order to enable cyber espionage can have different levels of invasiveness. For example, disabling cyber security mechanisms in order to monitor computer screens will be unlikely to be categorized as use of force. However, a military aircraft serving as a platform for cyber espionage penetrates national airspace of another state without authorization involves an increased risk of qualifying as use of force.[102] The above factors are not exhaustive, and other factors may also be relevant.[103]

Above, the main arguments of cyber espionage falling under Art 2(4) of the UN Charter were presented. The following text will argue that the counterarguments carry more weight, holding that cyber espionage does not fall under the said article. Firstly, the Charter does not formally define 'use of force', but based on historical precedents, states appear to agree that a variety of unfriendly actions including espionage do not reach the threshold of use of force.[104] The generally accepted interpretation of Art 2(4) holds that only interventions that produce physical damage are regarded as an unlawful use of force.[105] Secondly, although cyber espionage may include an element of force, it does not inherently do so.

The recent revelations by the Snowden documents on US espionage on institutions within the EU, and its tapping of German Reich Chancellor Merkel's personal cell

---

[102] This example is borrowed from TM page 50.
[103] In a joint communication to the European Parliament, the European Council and other EU organs write that a 'particularly' serious cyber incident or attack could constitute sufficient ground for a member state to invoke the EU Solidarity Clause (Article 222 of the Treaty on the Functioning of the EU). Invoking the solidarity clause might be farfetched in cases of cyber espionage, but at least potentially, an act of cyber espionage could be considered to amount to a cyber incident of such gravity that the victim EU member state might invoke the solidarity clause.
[104] H S. Lin, 'Offensive Cyber Operations and the Use of Force' (2010) J Nat'l Sec L & Pol'y 63, 71.
[105] R Buchan, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' (2012) 17 J C & S L 211, 212.

phone[106] is a clear example of espionage that with the greatest of likelihoods is limited to an intrusion and will not result in a physical attack (by the US) on the (European) targets of the espionage. Regarding the argument about Art 2(4) extending the definition of use of force beyond the physical, it appears to have merits, but the causal chain between the espionage and the political or economic force must be solid for it to be valid.[107]

Furthermore, Art 31(1) of the Vienna Convention on the Law of Treaties (VCLT)[108] requires that before a term can be given its conventional meaning, this meaning must be verified against the broader principles of the treaty. A treaty term cannot be given its conventional meaning if that meaning defeats or undermines the objective of the treaty. The main objective of the UN is in the preamble of the UN Charter[109] described as to maintain international peace and security by locating the use of armed force within the collective security system (as opposed to being located on a member state-level), to prevent 'the scourge of war' and that armed force should only be used if in the common interest.[110] This UN objective to maintain peace means that the curtailing of its member states to use armed force indicates that the term force in Art 2(4) should be interpreted to include only armed force.

Now that it is concluded that Art 2(4) should be interpreted to include only armed force, it must be assessed whether cyber espionage can constitute such force. In international legal doctrine, particularly on the subject of cyberwar, the effect-based approach to questions of what actions are included in armed force is most common. Accordingly, the author Dinstein explains that cyber attacks must

---

[106] SPIEGEL Staff, 'Embassy Espionage: The NSA's Secret Spy Hub in Berlin' *Der Spiegel International* (Hamburg 27 October 2013) <http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html> accessed 2 May 2014.

[107] Cf. Y Dinstein, *War, Aggression and Self*-Defence, (5th edn Cambridge University Press, Cambridge 2011) 88.

[108] VCLT Art 31(1) 'A treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose'.

[109] According to Art 31(2) VCLT, the preamble of a treaty can be used to discern the purposes and objectives of a treaty.

[110] An exception is found in Art 51 of the UN Charter, which states that States have an inherent right to self-defense, permitting States to use force 'where an armed attack occurs'.

manifest physical damage in order to constitute unlawful use of force. He concludes that the specific means – kinetic or electronic – used to conduct the action does not matter; instead, what matters is whether the final result involves threat or occurrence of violence.[111] The same author also emphasizes that 'espionage per se does not constitute an armed attack'.[112]

4.5.2 The Principle of Non-Intervention

If one state interferes with the domestic or international affairs of another state but to a level that does not reach the threshold of an armed attack or an aggression, international law refers to this act as intervention.[113] The principle is integrated, in the words of the ICJ 'part and parcel', in international law.[114] Because the non-intervention principle traditionally is viewed to be a corollary to a state's sovereign territory, the extent of the prohibition against intervening include the areas conventionally regarded as the physical territory of a state.[115] Although it is an autonomous principle of customary international law it is closely linked to the principle of sovereign equality of all states in customary international law and put down in Art 2(1) and 2(7) of the UN Charter.[116]

The principle prohibits all acts that are intended 'to coerce another state in order to obtain from it the subordination of the exercise of its sovereign rights and to secure from it advantages of any kind'.[117] In the *Nicaragua case* the ICJ writes that an intervention is prohibited if it has:

> [B]earing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which

---

[111] Y Dinstein, *War, Aggression and Self-Defence*, (5th edn Cambridge University Press, Cambridge 2011) 88.
[112] Y Dinstein, 'Computer Network Attacks and Self-Defense' (2002) 76 Int'l L Stud. Ser. US Naval War College 99, 105.
[113] M E. O'Connell, 'Cyber Security Without Cyber War' (2012) 17 J Con & Sec L 187, 202.
[114] *Ibid* 202.
[115] Cf. R Buchan, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' (2012) J Con & Sec L Vol 17, 211, 223.
[116] The UN is itself obliged to respect it because of what is stated in Art 2(7) of the UN Charter.
[117] UN General Assembly, Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, UN Doc A/RES/25/265 (24 October 1970).

> must remain free ones. The element of coercion, which defines, and indeed forms the very essence of, prohibited intervention, is particularly obvious in the case of an intervention which uses force, either in the direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State.[118]

In the above citation from the *Nicaragua case*, the Court writes that the element of coercion forms the essence of the non-intervention principle. According to Oppenheim's International Law, the interference 'must be forcible or dictatorial, or otherwise coercive, in effect depriving the state intervened against of control over the matter in question. Interference pure and simple is not intervention'.[119] However, it remains uncertain to what extent acts other than the use of force, are or should be prohibited.[120] In Arts 4-5 of the Budapest Convention on Cybercrime (BCC), it is clear that interference as described by the convention is also not applicable to cyber espionage. These articles describe data and system interference as encompassing the 'damaging, deletion, deterioration, alteration or suppression of computer data' and the 'hindering /…/ of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data'. This definition may thus apply to cyber attacks. In contrast, cyber espionage merely utilizes access and sometimes interception without compromising data, in contrast to interference, which, according to the BCC, alters and consequently affects data. If one views intervention only from the strict perspective, the discussion would end here with a conclusion of cyber espionage not being an unlawful intervention according to international law. However, the non-intervention principle may also be viewed against the backdrop of the rights that a state enjoys through its sovereignty and territorial jurisdiction.

---

[118] *Case Concerning the Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America)* (Merits) [1986] ICJ Rep 14, para 205.
[119] L Oppenheim, R Jennings & A Watts (eds) *Oppenheim's International Law: Peace* (9th edn Harlow, Longman, 1992) 432.
[120] M Wood, 'Non-Intervention (Non-Interference in Domestic Affairs)', The Princeton Encyclopedia of Self-Determination <http://pesd.princeton.edu/?q=node/258> accessed 23 April 2014.

4.5.3 The Coercive Element – A Strict Interpretation of the Principle

There are different sources that emphasize the coercive element of intervention or interference. For example, in the *Nicaragua case* the Court notes that 'intervention is wrongful when it uses methods of coercion'; in consequence, cyber espionage that lacks a coercive element would not violate the non-intervention principle.[121] In an article specifically about the principle of non-intervention, the authors Jamnejad and Wood emphasize the element of coercion as the essence of the principle.[122] Another, more traditional approach, is the notion of 'dictatorial interference', applied in order to determine unlawful interventions.[123] Regardless of which interpretation that is used in this matter, it is clear that the intrusion that cyber espionage constitutes can be seen neither as coercion nor dictatorial interference in the target state. It is another matter that the information obtained through an act of cyber espionage might later on be used for coercive purposes.

4.5.4 Non-Intervention, Sovereignty and Territorial Jurisdiction Combined – A Wide Interpretation

The above arguments have indicated that cyber espionage does not constitute unlawful intervention. There are, however, sources that put less or no weight on the coercive element, and consequently provide a different interpretation of the principle than the ICJ's in the *Nicaragua case*. A wider interpretation of non-intervention is possible, where the concepts of sovereignty and territorial jurisdiction are included, and leads to the conclusion that cyber espionage may be unlawful. The author Wright's description of a state's right to sovereign dominion (see section 4.4.1) can also be applied onto an assessment of the ill- or legality of an act of intervention. Doing this results in an assessment based not on the presence of coercive intention or effect, but on the object and character of an intervention. This approach can therefore possibly lead to cyber espionage constituting an unlawful intervention.

---

[121] *Case Concerning the Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America)* (Merits) [1986] ICJ Rep 14, para 205.
[122] M Jamnejad, M Wood, 'The Principle of Non-Intervention' (2009) 22 Leiden J Int'l L 345, 348.
[123] L Oppenheim, R Jennings & A Watts (eds) *Oppenheim's International Law: Peace* (9th edn Harlow, Longman, 1992) 432.

In section 4.5 it was concluded that Arts 4-5 of the BCC, on data and system interference, were not applicable to cyber espionage. However, Arts 2-3 of the BCC, on illegal access and illegal interception lack a prerequisite of a coercive element, and can be therefore applied to the intrusive element of cyber espionage activities. This is because the intrusive component of cyber espionage is essentially an unauthorized access into protected data and cyber espionage aims at intercepting data that is directed elsewhere or meant for others than the intruders. According to Art 2, the access to the whole or any part of a computer system without right 'shall be criminalized in the Parties' domestic systems of law'. Furthermore, the offence activity in Art 2 is described as infringing on security measures, such as an encrypted server, in order to obtain computer data. This article is therefore analogously[124] applicable on cyber espionage, as the act of intrusion of cyber espionage also is made without rights, and the access is the result of the cyber intrusion infringing on security measures. Similarly, according to Art 3, the interception without right, made by technical means, of non-public transmission of computer data should also be a criminal offence in the domestic law systems of the convention's parties. This article is therefore also analogously applicable to cyber espionage; cyber espionage is conducted without right, with technical means, onto non-public transmissions of computer data, making cyber espionage intrusions a criminal offence in the domestic laws of the convention's parties.

4.6 SUMMARY

This chapter concluded that cyber espionage entails an intrusive element, which violates the principles of sovereignty and territorial jurisdiction. Because a server located within a state's territory is under that state's territorial jurisdiction, an unauthorized intrusion into that server and the data stored on it is in violation of the rights that the state enjoys under the principles of sovereignty and territorial jurisdiction.

---

[124] An analogy is applied because the BCC is not directly applicable to inter-state relationships, the convention states that the parties of the convention shall have domestic legislation in accordance with the convention.

Furthermore, it was concluded that cyber espionage does not fall within the scope of Art 2(4) of the UN Charter and the prohibition of use of force, because cyber espionage does not per se include the use of force and in essence does not consist of use of force. Therefore, another customary principle of international law was examined, the principle of non-intervention. When the meaning of this principle is examined, the word 'intervention' is described to prohibit coercion or dictatorial interference in the internal matters of a state by a foreign state. According to this strict interpretation, the intrusive element of cyber espionage is not an intrusion in the sense of the principle as it lacks the coercive or dictatorial element. Nevertheless, it was found that by applying a wider perspective where the non-intervention principle is combined with the principles of sovereignty and territorial jurisdiction, cyber espionage could indeed be viewed as unlawful intervention.

5 SUMMARY AND CONCLUSIONS

5.1 ANSWERING THE QUESTION

This essay has aimed at providing clarification and explanation of the developing subject of cyber intrusions, specifically, intrusions in the form of cyber espionage and its relation to international law. The outset was to determine if extraterritorial cyber intrusions in the form of cyber espionage by states constitute illegal intrusion into the sovereignty of the state intruded upon.

Cyber espionage was found to differ from conventional espionage, not in its essence, but in its mode of action and field of operation. From the perpetrator's point of view, a significant advantage of cyber espionage is that it is geographically independent, but this simultaneously raises questions related to the legality of its intrusions upon other states' data. However, before a conclusion could be drawn on the putative legality or illegality of cyber espionage, it was concluded that only specific activities related to espionage, but not espionage as such, are prohibited under international law.

When addressing the question if cyber espionage could constitute an intrusion into the sovereignty of another state, it was found that for this to be the case, the sovereign territory of states must include also the virtual space through which

cyber espionage is conducted. Under the provision that the data intruded upon are physically stored on servers located within the target state, the targeted state has sovereignty and territorial jurisdiction over the data present on those servers.

Cyber espionage has bearings on several principles and aspects of international law. In legal discussions on cyber intrusions a commonly mentioned principle is the prohibition of use of force according to Art 2(4) of the UN Charter. However, it was concluded that espionage falls below the threshold of prohibited use of force. This is due to the fact that although cyber espionage might lead to consequences that include elements of (armed) force, it neither inherently nor in essence does so. Furthermore, Art 2(4) is an effects-based prohibition, which is in contrast to the aim of cyber espionage to operate covertly. Since cyber espionage fails to reach the threshold of prohibited use of force, it is relevant to examine whether it is unlawful under the principle of non-intervention. The word intervention can be interpreted strictly, leading to prohibition only of interference that is coercive or dictatorial. However, through the analogous application of case-law, doctrine and conventions it was found that cyber espionage can indeed be unlawful in that it involves an intrusion into the jurisdiction and sovereignty of the targeted state. A wider interpretation of the principle of non-intervention, where less weight is put on the coerciveness of the purported interference, but more on interference in internal matters of the targeted state, also leads to the conclusion that cyber espionage is unlawful under international law. Therefore, the answer to whether extraterritorial cyber intrusions through cyberspace by a state into protected data located and belonging to another state, referred to as cyber espionage, can constitute unlawful intrusion under international law into the sovereignty of the state intruded upon, is yes.

5.2 A DISCUSSION ON FURTHER ISSUES

The various opportunities and dangers that cyber espionage present raise questions that go beyond the legal discussion of sovereignty, territoriality, jurisdiction and intervention. The below sections are provided as an outset for further discussion on the impact of cyber espionage.

5.2.1 Can Cyber Espionage Be Lawful Under International Law?

The above reasoning indicates that there are circumstances where cyber espionage activities could be unlawful according to international law. In addition, there are also circumstances that might provide a state conducting cyber espionage with lawful reasons to do so. Briefly, one such circumstance is if the target state gives its valid consent.[125] If governments have relationships involving mutual interest towards e.g., a third party, this might provide grounds for consent. A second circumstance could be in cases of self-defence according to Art 21 of the Draft Articles or Art 51 of the UN Charter. However, as already concluded in section 3.3.1, such a situation would intrinsically be limited to cyber espionage taking place in situations of armed conflict.

5.2.2 The State's Perspective

Since it is likely that a majority, if not all, states are engaged in espionage and also engage in cyber espionage, states should have interest in which rules and regulations that are applicable to these activities. One might claim that states could care less, since espionage, including cyber espionage, are secret and covert operations. However, because espionage is sometimes uncovered, as exemplified by the recent Snowden revelations, states should find it advantageous to be cautious in what espionage activities they conduct, and how. Revelations of espionage can restrain diplomatic relations, as exemplified by reports that Israel was not admitted into the US Visa Waiver Program (which would exempt Israeli citizens from the need for tourist visas into the US and enable them to stay in the country for up to 90 days) because of US intelligence officials who were sceptical due to purported Israeli espionage against the US.[126] Another example is when US espionage against Europe was revealed in 2013, prospects of a transatlantic trade and investment partnership were restrained.[127] These recent examples demonstrate that states should keep in mind that what is secret now, may not always remain so,

---

[125] Draft Articles, Art 20.
[126] R Ahren, 'Foxman slams unfounded US fears of Israeli spying' *Times of Israel*, (Jerusalem 25 April 2014) <http://www.timesofisrael.com/foxman-slams-unfounded-us-fears-of-israeli-spying/> accessed 3 May 2014.
[127] F Heisbourg, 'America's spying has made a European trade deal even harder' *Financial Times* (London 2 July 2013) <http://www.ft.com/intl/cms/s/0/5102c9b6-e31e-11e2-bd8700144feabdc0.html#axzz32k3m7BNY> accessed 3 May 2014.

and apart from the embarrassment of being caught, it can have effects on the level of international and national politics. When it comes to foreign policy, states risk being caught two-faced if a leak would reveal that a government has not acted as it has claimed to. In an article in Foreign Affairs, titled 'The End of Hypocrisy', the authors advise that American foreign policy must take into account that it now acts in an 'age of leaks'.[128] Because governments, just like their citizens, depend on storing information within cyberspace, they are possible victims of leaks both from inside and outside cyber intrusions. The article exemplifies what it calls the two-faced hypocrisy with the war on terror; while the US government pushes foreign governments hard on human rights, it 'claims sweeping exceptions for its own behaviour when it feels its safety is threatened'.[129]

Yet another reason for states to keep in mind how they commit espionage activities is the possibility of cyber espionage merging with activities that are not only prohibited under the principle of non-intervention, but also according to Art 2(4) of the UN Charter. As mentioned in section 4.5.2, cyber espionage does not have to – but can – constitute use of force. An example could be when cyber espionage is conducted by the same organ or unit that would, based primarily on the information obtained by the cyber espionage, perform a physical or a so called cyber attack resulting in or intended to result in physical effects on an extraterritorial target. Other contexts could be if the cyber espionage and the attack take place simultaneously or close in time. In short, one can speculate that in cases where an attack (or other action prohibited under international law) and cyber espionage are intertwined to the extent that they cannot be separated, the cyber espionage activities would merge with the unlawful action and thus, at least indirectly, be prohibited also according to other principles or regulations of international law, for example Art 2(4) of the UN Charter.

Furthermore, this essay's conclusion that cyber espionage intrusions into other states' data are unlawful based on a combination of aspects of sovereignty,

---

[128] H Farrell & M Finnemore, 'The End of Hypocrisy: American Foreign Policy in the Age of Leaks' *Foreign Affairs* (November/December 2013) 22.
[129] *Ibid* 24.

territorial jurisdiction and non-intervention, may be both welcomed and unwanted by states. However, regardless of the unlawfulness under international law, states can, and indeed do, just as in the case of conventional espionage, penalize cyber espionage or intrusions in their respective domestic systems of law. States can of course also criminalize actions committed in connection with espionage activities. Such activities might include illegal weapons proliferation or intrusion on protected data in the form of cyber espionage.

5.2.3 The Right to Privacy

Furthermore, cyber espionage may not only have implications also from the individual citizen's perspective. The growing technical developments make it possible to monitor larger amounts of data, and the perpetrator can do this with a decreasing risk of being traced. It is therefore particularly enticing for certain regimes of more doubtable characters (and perhaps other regimes, too) to seek to use cyber espionage on their own citizens. This would violate the right to privacy in Art 12 of the Universal Declaration of Human Rights, which states that no one should be subjected to arbitrary interference with his or her privacy, family, home or correspondence. The article also states that everyone has the right to protection of the law against such interferences.

5.2.4 Outsourcing Cyber Espionage

If a state is prohibited by its domestic legislation to spy on its own citizens it could outsource the spying that the state is prohibited from conducting to another state. Now, this might create disturbing consequences as nations prevented by their own laws from spying on their own citizens could outsource the job to intelligence agencies of other countries, resulting in for example decreased freedom and privacy for the individual citizen.

In Sweden, the risk of outsourcing cyber espionage has been addressed through the organization of the involved state-actors. The Swedish National Defence Radio Establishment (FRA), the authority for signals intelligence, is prohibited from asking another state's intelligence service to gather signal intelligence that the FRA is itself prohibited from gathering. According to Wallin, spokesperson for the FRA, there is no specific regulation for this prohibition. However, the regulations

of the activities of FRA, set the requirements and boundaries for its intelligence gathering. Based on a broad assessment of these regulations, the FRA is prohibited from gathering such data. In addition, the Swedish Foreign Intelligence Inspectorate (SIUN), monitors the FRA's adherence to relevant regulations.[130] Yet, one might wonder if a prohibition for the state to outsource the gathering of data the states or state actors are prohibited from gathering, should not be more specified than as derived only from a broad assessment.

5.3 FINAL WORD

The structure of sovereign states and the coexistence of national jurisdictions prevail as the foundation of today's world order. The ideals of a cyberspace that is separate from the sovereignty of states and managed by servers and individuals, are more of a 'cyberlibertarian' utopia than a reality. This is because the data that make up cyberspace are stored on servers located within jurisdiction of states, and cyberspace is thus subject to state sovereignty and the pertaining jurisdiction of the state of the server's location.

Cyberspace has given rise to cyber espionage as a new, but rapidly growing, way of conducting espionage. Although it is concluded that extraterritorial intrusions by cyber espionage by states into other state's data are unlawful according to the principles of sovereignty, territorial jurisdiction and a wide interpretation of the principle of non-intervention, many factors remain uncertain regarding determining and defining what exact activities are lawful or unlawful. It is well known that technology tends to develop faster than law, and this is true also with regard to cyber espionage. Although there is much discussion, the actual substance in the forms of treaties, conventions, or even agreements on definitions are perhaps as intangible as cyberspace itself.

---

[130] Email and interview from/with F Wallin, Spokesperson, Swedish National Defence Radio Establishment (*Försvarets radioanstalt*) (23 October 2014 and Stockholm, Sweden 24 October 2014 respectively). See Appendix i.

TABLE OF CASES

PERMANENT COURT OF INTERNATIONAL JUSTICE

The Case of the S.S. 'Lotus' (France v Turkey) (Judgment) [1927] PCIJ Rep Series A No 9

PERMANENT COURT OF ARBITRATION

Islands of Palmas (Netherlands v US) (1928) 2 RIAA 829, 838

INTERNATIONAL COURT OF JUSTICE

North Sea Continental Shelf (Federal Republic of Germany v Denmark; Federal Republic of Germany v Netherlands) (Judgment) [1969] Rep 54

Case Concerning the Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America) (Merits) [1986] Rep 14

Questions of Interpretation and Application of the 1971 Montreal Convention arising from the Aerial Incident at Lockerbie (Libyan Arab Jamahiriya v United Kingdom) (Judgment) [1998] ICJ Rep 3

Questions of Interpretation and Application of the 1971 Montreal Convention arising from the Aerial Incident at Lockerbie (Libyan Arab Jamahiriya v United States of America) (Judgment) [1998] ICJ Rep 3

THE EUROPEAN COURT OF JUSTICE

Joined Cases 89, 104, 114, 116, 117 and 129/85, *Ahlström Osakeyhtiö and Others v Commission* [1994] ECR I-100, Opinion of AG Darmon

SUPREME COURT OF CANADA

R v Hape SCC (CanLII) (2007) 2 SCR 292

DECLARATIONS AND TREATIES

Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) 3 Bevans 1153; hap59 Stat 1031; TS No 993

Statute of the International Court of Justice, 26 June 1945, San Francisco

Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III)

Vienna Convention on Diplomatic Relations (adopted 18 April 1961, entered into force 24 April 1964) 500 UNTS 95

Vienna Convention on Consular Relations (adopted 24 April 1963) 596 UNTS 261

Vienna Convention on the Law of Treaties (adopted 23 May 1969, entered into force 27 January 1980) 1155 UNTS 331

United Nations Convention on the Law of the Sea (adopted 10 December 1982, entered into force 16 November 1994) 1833 UNTS 3

Convention on Cybercrime (opened for signature 23 November 2001, entered into force 1 July 2004) ETS No 185

Consolidated Version of the Treaty on the Functioning of the European Union (adopted 26 October 2012) OJ C 326/47

UN DOCUMENTS

UN General Assembly, Draft Declaration on Rights and Duties of States, UN Doc A/RES/375 (6 December 1949)

Union of Soviet Socialist Republics, Draft Resolution Concerning Alleged Aggressive Acts by the United States Air Force Against the Soviet Union, UNSC Doc S/4321(23 May 1960, not adopted)

UN General Assembly, Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, UN Doc A/RES/25/265 (24 October 1970)

International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, Supplement No. 10 (A/56/10), chapter IV.E. (November 2001)

UN Secretary General, Group of Governmental Experts 'Developments in the Field of Information and Telecommunications in the Context of International Security' Rep. of the Secretary-General, UN Doc A/66/152 (20 July 2010)

UN General Assembly, Group of Governmental Experts 'Developments in the Field of Information and Telecommunications in the Context of International Security' UN Doc A/65/201(30 July 2010)

UN General Assembly, Group of Governmental Experts, Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc A/68/98 (24 June 2013)

EU SOURCES

Directorate-General for External Policies, Policy Department 'Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action Within the EU' Study, European Parliament 2011

European Commission and High Representative, 'Cybersecurity Strategy of the European Union: An Open Safe and Secure Cyberspace', Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, JOIN(2013)1, 2013

GOVERNMENT PUBLICATIONS

The Executive Office of the President of the United States, *The Comprehensive National Cybersecurity Initiative* (The White House 2010)

US Department of Defense Dictionary of Military Terms, '*Computer Intrusion'* <http://www.dtic.mil/doctrine/dod_dictionary/data/c/11171.html> accessed 14 March 2014

The MI5, '*Cyber Threats*' <https://www.mi5.gov.uk/home/the-threats/cyber.htmlviewed> accessed 12 March 2014

United States Army, '*Establishment of the US Army Cyber Command'* (US Army Cyber Command) <http://www.arcyber.army.mil/history.html> accessed 25 February 2014

Swedish Ministry of Defence, *Försvaret av Sverige – Starkare försvar för en osäker tid*, Ds 2014:20

The White House, '*International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*' (2011)

The Vice Chairman of the Joint Chiefs of Staff '*Joint Terminology for Cyberspace Operations'* Memorandum (US Department of Defense 2010) <http://www.nsciva.org/CyberReferenceLib/201011joint%20Terminology%20for%20Cyberspace%20Operations.pdf> accessed 12 March 2014

Office of the Secretary of Defense '*Military and Security Developments Involving the People's Republic of China'* Annual Report to Congress, (US Department of Defense 2011) <http://www.defense.gov/pubs/pdfs/2011_cmpr_final.pdf> accessed 18 March 2014

The United States, The Office of Public Services, Bureau of Public Affairs, '*President's Statement of May 16'* The Department of State Bulletin, XLII, No. 109 (Washington D.C. 6 June 1960)

The MI5, '*What is Espionage?*' <https://www.mi5.gov.uk/home/the-threats/espionage/what-is-espionage. html> accessed 4 April 2012

ARTICLES

S W. Brenner & A C. Crescenzi, 'State-Sponsored Crime: The Futility of the Economic Espionage Act' (2006) 28 Houston Journal of International Law

R Buchan, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' (2012) 2 Journal of Conflict & Security Law Vol. 17, 211

Y Dinstein, 'Computer Network Attacks and Self-Defense' (2002) 76 International Law Study Series US Naval War College 99

D Fleck, 'Individual and State Responsibility for Intelligence Gathering' (2006-2007) 28 Michigan Journal of International Law 678

C Forcese, 'Spies Without Borders: International Law and Intelligence Collection' (2011) 5 Journal of National Security & Policy 179

M Jamnejad, M Wood, 'The Principle of Non-Intervention' (2009) 22 Leiden Journal of International Law 345

H S. Lin, 'Offensive Cyber Operations and the Use of Force' (2010) Journal of National Security and Policy 63

M E. O'Connell, 'Cyber Security Without Cyber War' (2012) 17 Journal of Conflict & Security Law 187

A J. Radsan, 'The Unresolved Equation of Espionage and International Law' (2006-2007) 28 Michigan Journal of International Law 595

M N. Schmitt, 'Reaction: Cyberspace and International Law: the Penumberal Mist of Uncertainty' (2013) 126 Harvard Law Journal 176

M N. Schmitt, 'The Law of Cyber Warfare: Quo Vadis?' (2014) 25 Stanford Law & Policy Review 269

B J. Theutenberg, 'U 137 – Folkrätt och neutralitetspolitik i tillämpning' (1982) 2 Kungliga Krigsvetenskapsakademins handlingar och tidskrift 112

M C. Waxman, 'Cyber-Attacks and the Use of Force: Back to the Future of Artice 2(4)' (2011) 36 Yale Journal of International Law 421

Q Wright, 'Subversive Intervention' (1960) 54 American Journal of International Law 521

NEWSPAPERS AND MAGAZINES

R Ahren, 'Foxman slams unfounded US fears of Israeli spying', *Times of Israel*, (Jerusalem 25 April 2014) <http://www.timesofisrael.com/foxman-slams-unfounded-us-fears-of-israeli-spying/> accessed 3 May 2014

J Appelbaum, H Stark, M Rosenbach & J Schindler, 'Berlin Complains: Did US Tap Chancellor Merkel's Mobile Phone?' *Der Spiegel International* (Hamburg 23 October 2013) <http://www.spiegel.de/international/world/merkel-calls-obama-over-suspicions-us-tapped-her-mobile-phone-a-929642.html> accessed 18 April 2014

S Elegant 'Cyberwarfare: The Issue China Won't Touch' *Time Magazine* (New York City 18 Nov 2009) <http://content.time.com/time/world/article/0,8599,1940009,00.html> accessed 4 April 2014

H Farrell & M Finnemore, 'The End of Hypocrisy: American Foreign Policy in the Age of Leaks' *Foreign Affairs* (November/December 2013) 22

M Giles, 'Special report: Cyber-security, Defending the digital frontier' *The Economist* (London 12 July 2014) digital edition for android

S Gorman, 'Annual US Cybercrime Costs Estimated at $100 Billion' *The Wall Street Journal* (New York City 22 July 2013) <http://online.wsj.com/news/articles/SB10001424127887324328904578621880966242990> accessed 3 May 2014

GovInfoSecurity.com, 'Time Line of Major Global Cyber Incidents 2010-2011' *Bank Info Security Magazine* (Princeton 17 March 2011) <http://www.bankinfosecurity.com/articles.php?art_id=3440> accessed 17 March 2014

N Hopkins, 'Stuxnet attack forced Britain to rethink the cyber war' *The Guardian* (London 30 May 2011) <http://www.theguardian.com/politics/2011/may/30/stuxnet-attack-cyber-war-iran> accessed 28 April 2014

F Heisbourg, 'America's spying has made a European trade deal even harder' *Financial Times* (London 2 July 2013) <http://www.ft.com/intl/cms/s/0/5102c9b6-e31e-11e2-bd8700144feabdc0.html#axzz32k3m7BNY> accessed 3 May 2014

J Markoff & D Barboza, '2 China Schools Said to Be Tied to Online Attacks' *The New York Times* (New York City 18 February 2010)

<www.nytimes.com/2010/02/19/technology/19china.html?th&emc=th> accessed 4 April 2014

L Poitras, M Rosenbach & H Stark, 'Codename 'Apalachee': How America Spies on Europe and the UN' *Der Spiegel International* (Hamburg 26 August 2013) <http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html> accessed 30 April 2014

B Schneier, 'There's No Real Diffrence Between Online Espionage and Online Attack' *The Atlantic* (Washington DC 6 March 2014) <http://www.theatlantic.com/technology/archive/2014/03/theres-no-real-difference-between-online-espionage-and-online-attack/284233/> accessed 12 March 2014.

A Segal, 'Chinese Computer Games: Keeping Safe in Cyberspace' *Foreign Affairs* (New York March/April 2012) http://www.foreignaffairs.com/articles/137244/adam-segal/chinese-computer-games accessed 15 March 2014

H Shane, 'The Cyberwar Plan' *National Journal Magazine* (11 November 2009) 15

SPIEGEL Staff, 'Embassy Espionage: The NSA's Secret Spy Hub in Berlin' *Der Spiegel International* (Hamburg 27 October 2013) <http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html> accessed 2 May 2014

Z Wa & F Jing, 'Washington Tries to Shift Spying Blame to China' *China Daily* (Beijing 24 December 2013) <http://www.chinadaily.com.cn/china/2013-12/24/content_17192169.htm> accessed 30 April 2014

P Warren, 'Smash and grab, the hi-tech way' *The Guardian* (London 19 January 2006) <http://www.theguardian.com/politics/2006/jan/19/technology.security> accessed 28 April 2014

DICTIONARIES AND ENCYCLOPEDIAS

P Kunig, 'Intervention, Prohibiton of' Max Planck Encyclopedia of Public International Law <http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1434> accessed 24 April 2014

'Cyberspace, n' Oxford English Dictionary Online (Oxford University Press November 2010)

<http://www.oed.com.ezp.sub.su.se/view/Entry/240849?redirectedFrom=cyberspace&accessed> accessed 14 March 2014

M Wood, 'Non-Intervention (Non-Interference in Domestic Affairs)' The Princeton Encyclopedia of Self-Determination <http://pesd.princeton.edu/?q=node/258> accessed 23 April 2014

WEBSITES

J P. Barlow, 'A Declaration of the Independence of Cyberspace' (1998) <https://projects.eff.org/~barlow/Declaration-Final.html> accessed 3 March 2014

General Services Administration, 'Gov Domain Name Registration Services' (General Services Administration) <https://www.dotgov.gov/portal/web/dotgov> accessed 2 May 2014

Kaspersky Labs and ITU Research, 'Kaspersky Labs and ITU Research Reveals New Advanced Cyber Threat' (Kaspersky Lab 29 May 2012) <http://usa.kaspersky.com/about-us/press-center/press-releases/kaspersky-lab-and-itu-research-reveals-new-advanced-cyber-threa > accessed 25 March 2014

'"Red October" Diplomatic Cyber Attacks Investigation' (SecureList) <http://www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation> accessed 2 April 2014

OTHER SOURCES

C Czosseck, 'State Actors and their Proxies in Cyberspace' in K Ziolkowski (ed), Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy (NATO CCD COE Publication, Tallinn 2013)

J Postel, 'Domain Name System Structure and Delegation' (The Internet Engineering Task Force 1994) Memo <http://tools.ietf.org/html/rfc1591> accessed 2 May 2014

Email from F Wallin, Spokesperson, Swedish National Defence Radio Establishment (*Försvarets radioanstalt*) (23 October 2014)

Interview with F Wallin, Spokesperson, Swedish National Defence Radio Establishment (*Försvarets radioanstalt*) (Stockholm, Sweden 24 October 2014)

Interview with E Wennerström, Head Secretary in the Committee on a strategy on information security (*Regeringens utredning om Strategi och mål för hantering och överföring av information i elektroniska kommunikationsnät och it-system*) Dir 2013:110 (Stockholm, Sweden, 24 November 2014)

BIBLIOGRAPHY

A Aust, *Handbook of International Law* (1st edn Cambridge University Press, 2005)

S W. Brenner, *Cyberthreats and the Decline of the Nation State* (1st edn Routledge, New York 2014)

A Cassese, *International Law* (2nd edn Oxford University Press, Oxford 2004)

T Crowdy, *The Enemy Within: A History of Spies, Spymasters and Espionage* (1st edn Osprey Publishing, Oxford 2006)

Y Dinstein, *War, Aggression and Self-Defence* (5th edn Cambridge University Press, Cambridge 2011)

M D. Evans, *International Law* (3rd edn Oxford University Press, Oxford 2010)

Greenberg, Goodman et al., *Information Warfare and International Law* (National Defense University Press, Washington DC 1998)

M Inazumi, *Universal Jurisdiction in Modern International Law: Expansion of National Jurisdiction for Prosecuting Serious Crimes Under International Law* (1st edn Intersentia, 2005)

G Kerschischnig, *Cyberthreats and International Law* (1st edn Eleven International Publishing, The Netherlands 2012)

V Lowe, *International Law* (1st edn Oxford University Press, Oxford 2007)

M N. Schmitt (Gen. ed.), International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence, M N. Schmitt (ed) *Tallinn Manual on the International Law Applicable to Cyber Warfare* (1st edn Cambridge University Press, Cambridge 2013)

L Oppenheim, H Lauterpacht (ed) *International Law: A Treatise* (8th edn Longmans, Green, and Co., 1955)

L Oppenheim, R Jennings & A Watts (eds) Oppenheim'*s International Law: Peace* (9th edn Harlow, Longman, 1992)

T Ploug, *Ethics in Cyberspace: How Cyberspace May Influence Interpersonal Interaction* (1st edn Springer, 2009)

A Schwabach, *Internet and the Law: Technology, Society, and Compromises* (2nd edn ABC-CLIO, California 2014)

S J. Shackelford, *Managing Cyber Attacks in International Law, Business and Relations: In Search of Cyber Peace* (1st edn Cambridge University Press, 2014)

J P. Trachtman, Global Cyberterrorism, Jurisdiction, and International Organization in M F. Grady & F Parisi (eds), *The Law and Economics of Cybersecurity* (1st edn, Cambridge University Press 2005)

P Wrange, 'Intervention in National and Private Cyberspace and International Law' in Ebbesson, et al.: *International Law and Changing Perceptions of Security* (1st edn Brill | Nijhoff, 2014)

K Ziolkowski, 'Peacetime Cyber Espionage – New Tendencies in Public International Law' in K Ziolkowski (ed), *Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy* (1st edn NATO CCD COE Publication, Tallinn 2013)

Appendix i

Email from F Wallin, Spokesperson, Swedish National Defence Radio Establishment (*Försvarets radioanstalt*) (23 October 2014)

Ella Shoshan <ella.shoshan@gmail.com>

Juridisk fråga

Fredrik Wallin <frewal@fra.se> Fri, Oct 24, 2014 at 9:44 AM
To: Ella Shoshan <ella.shoshan@gmail.com>

Hej!

Det finns ingen paragraf i lagen eller gällande föreskrifter som uttryckligen säger att samarbete med andra länder inte får användas för att kringgå lagstiftningen. Lagstiftningen anger dock inom vilka ramar och förutsättningar som FRA får signalspana, och lagstiftningen ska tillämpas även vid samarbete med andra länder. Att FRA inte genom samarbeten får kringgå lagen framgår således inte specifikt av lagtexten, men följer av lagstiftningen som helhet.

Jag kan tillägga att FRA:s samarbeten med andra länder vid flera tillfällen granskats av de kontrollorgan som granskar vår verksamhet (Siun), bland annat just med avseende på detta.

Mvh

Fredrik Wallin

Ella Shoshan skrev 2014-10-23 14:36:
[Quoted text hidden]

--

Mvh

Fredrik Wallin
Informationsfunktionen FRA

Tel: 08 471 45 48