UNIVERSITY OF TARTU

SCHOOL OF LAW

Department of Public Law

Anna-Džessika Bogatšova

THE USE OF COUNTERMEASURES IN RESPONSE TO MALICIOUS CYBER OPERATIONS

Master´s Thesis

Supervisor

Ph.D. Anna-Maria Osula

Tallinn

2020

TABLE OF CONTENTS

INTRODUCTION

Cyberspace is a domain, which with the expansion of technological development and information has caused society to be greatly dependent on it.[1] While people are getting online and society's reliance on computer networks grows, the vulnerability to attacks against States and civilians infrastructures increases,[2] accentuating the need of an adequate legal framework for cyberspace. Cyberspace is widely used to conduct of malicious cyber operations[3] due to the low cost of entry, abundance of legal challenges such as ambiguity of rights and responsibilities, and lack of attribution, which makes cyberspace an attractive area for all malicious State and non-State actors. Such actors often disguise their identity, seek to access information, undermine or damage systems, and attempt to gain a financial, political, or strategic advantage.[4]

Several established legal scholars have published articles on how States can respond to malicious cyber operations based on the law of self-defense,[5] deriving from the Article 51 of the United Nations Charter (hereinafter referred to as UN Charter) that allows States to respond forcefully to an armed attack.[6] However, there are no cyber operations that have crossed the armed attack threshold yet, whereas cyber operations that fall below the threshold are utilized every day.[7] Bearing in mind that no comprehensive treaty exists to specifically regulate international cyber operations, some non-binding rules have merged in State practice[8] and States have accepted them in multilateral statements.[9] The question arises of how international

[1] M. N. Schmitt, *et al*. Tallinn Manual 2.0 On The International Law Applicable to Cyber Operations. Cambridge University Press 2017. T. H. Ilves. Foreword.
[2] North Atlantic Treaty Organisation. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation. Lisbon 19.11.2010, para. 12.
[3] The employment of cyber capabilities to achieve objectives in or *via* cyberspace. See M. N. Schmitt. Tallinn Manual 2.0, *op. cit.*, Glossary, p. 564.
[4] J. A. Shamsi, *et al*. Attribution in Cyberspace: Techniques and Legal Implications. – 9 Security and Communication Networks 2016 (15), p. 2888.
[5] See M. N. Schmitt. Peacetime Cyber Responses and Wartime Cyber Operations under International Law: An Analytical Vade Mecum. - 8 Harvard National Security Journal 2017; M. C. Waxman. Cyber-Attacks and the Use of Force: Back to the Future of Article 2 (4). - 36 Yale Journal of International Law 2011; M. P. Llorens. The Challenges of the Use of Force in Cyberspace. – 17 Anuaria Maxicano de Dercho Internacional 2017; D. R. Priyanka. "Use of Force" and "Armed Attack" Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response. – 50 Texas International Law Journal 2015 (2).
[6] The Charter of the United Nations. San Francisco 26.06.1945, e.i.f. 24.10.1945, Art. 51.
[7] See Symantec Corporation. 24 Internet Security Threat Report 2019; K. Geers *et al*. World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks. - FireEye Inc. 2013.
[8] B. J. Egan. International Law and Stability in Cyberspace. - 35 Berkeley Journal of International Law 2017 (1), pp. 179-180.
[9] UN Doc. A/70/174. Report of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security 2015, para. 28 (e); G7 Declaration on Responsible States Behavior in Cyberspace, Lucca 11.04.201. Accessible at: https:// www.mofa.go.jp/files/000246367.pdf. (01.03.2020).

law applies in cyberspace in order to identify the proper legal framework for responding to the malicious cyber operations that are less serious in character than armed attack.[10]

Bearing in mind that harmful cyber operations tend to remain below the threshold of armed attack, victim-States can respond to malicious cyber operations and hold actors accountable by relying on countermeasures.[11] Countermeasures are actions taken by a victim-State in response to a violation by another State to persuade the latter to comply with its international obligations.[12] Although countermeasures are in principle legally available for usage by the victim-States, it is up to a debate whether countermeasures are used in practice when responding to malicious cyber operations. It should be also noted that countermeasures are the right of the victim-State, whereas availability of and conditions for collective countermeasures is controversial[13]; however, the coordinated use of responses by regional allies is emerging.[14] Furthermore, the harsh conditions associated with the application of countermeasures, such as the need to notify the other State and minimize collateral damage, can be seen as a stumbling stone for the use of countermeasures by victim-States.[15]

Another difficult question concerning countermeasures in cyberspace and international law is attribution of a malicious cyber operation to an actor.[16] The identification of actors is a tough challenge, as cyberspace has an open architecture, new protocols can be easily developed, and different spoofing techniques are used. Even if the origin of a malicious cyber operation is identified, the establishment of an actual attacker behind it, in most cases, as described in this thesis, is impossible, leading to the situation when capabilities of States to respond to the malicious cyber operations are limited.[17]

[10] K. Kaska (ed). Trends in International Law for Cyberspace. - NATO Cooperative Cyber Defence Centre of Excellence May 2019, para. 1.
[11] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.*, Rule 20.
[12] International Law Commission. Draft Articles on Responsibility of States for Internationally Wrongful Acts. November 2011, Supplement no. 10 (A/56/10), Art. 22.
[13] President of Republic of Estonia Kersti Kaljulaid. President of the Republic at the opening of CyCon 2019, 29.05.2019. Accessible at: https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html (03.03.2020); See J. Kosseff. Collective Countermeasures in Cyberspace. - 10 Notre Dame Journal of international & Comparative Law 2020 (1), pp. 18-34.
[14] Council of the European Union. Council Conclusion on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") – adoption 9916/17. Brussels 07.06.2017.
[15] Articles on State Responsibility, *op. cit*., Arts. 49–54.
[16] See J. Carr. Responsible Attribution: A Prerequisite for Accountability. – The NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Paper no. 6. 2014.
[17] M. N. Schmitt. An Analytical Vade Mecum 2017, *op. cit*., p. 249.

If a harmful cyber operation is attributed to a State, one should ask whether it violates an international legal obligation. If the attribution and breach of an international legal obligation is identified, it is possible to establish possible countermeasures for victim-State to respond. While the purpose of the countermeasures is to cause the responsible State to discontinue the harmful cyber activities,[18] the question remains as to whether the State may respond to harmful cyber operations that are not attributed to a State. In this case, there is the capacity of the State to respond to malicious cyber operations by referring to the obligation of due diligence. According to this principle, States have the obligation to ensure that cyber operations that may have serious implications for other States are not conducted from their territory.[19]

For the purposes of this thesis the State to which the obligation is owed is known as the "injured State" or "victim-State" and the "responsible State" is a State breaching the international obligation. The State from where the harmful cyber operation is launched is known as the "host-State". The term "cyber operation" or "malicious cyber operation" or "harmful cyber operation" are used instead of "cyber attack" to avoid the confusion between cyber actions that may or may not qualify as an armed attack crossing a threshold. The term "operation" has no relation to the military nature in this thesis. The author refers to the term "International Group of Experts" as the Tallinn Manual 2 authors.

The primary research problem discussed in this thesis is that due to the problem of attribution and the difficulties in the interpretation of scope and limits of international law in cyberspace, as well as due to the States' strategic reasons, States do not openly resort to countermeasures and very seldom publicly discuss the allegations.

The purpose of this thesis is to analyse the challenges for a victim-State regarding the deployment of countermeasures in the context of malicious cyber operations conducted against it. The thesis discusses the conditions for the applicability of countermeasures that may justify a victim-State outside of an armed conflict (peacetime) to respond to harmful cyber operations that are not serious enough to resort to self-defense under the United Nations Charter.

The primary research questions are:

- Under which conditions can the victim-State use countermeasures in response to malicious cyber operations conducted by State/s and/or non-State actor/s?

[18] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.*, pp. 125-130.
[19] M. N. Schmitt. An Analytical Vade Mecum 2017, *op. cit*., p. 249.

- How have victim-States responded in practice to significant malicious cyber operations? This question will be addressed in Chapter 2 in terms of five selected case studies.
- What developments would support victim-States' deployment of countermeasures in cyberspace?

The hypothesis of the study is that States strategical considerations do not support the practical application of countermeasures legal regime governing cyberspace by the victim-States.

The study consists of three parts. The first chapter explores how and when States may employ countermeasures in response to harmful cyber operations that do not qualify as armed attacks and does not address the issues of where the armed attack threshold lies. The concepts of attribution, breach of legal obligation, requirements and limitations in cyberspace under international law will be described. The first chapter also analyses the conditions for due diligence measures that should be taken by host-State, when victim-State requests the host-State to take appropriate measures to end the harmful cyber operation. Additionally, the author will briefly examine the extent to which a plea of necessity may be invoked in order to justify the use of immediate defensive measures against harmful cyber operations that may have an effect on other States.

The second chapter analyses five malicious cyber operations that were carried out between States. The case studies include cyber operation against the United States private sector companies such as Google (hereinafter referred to as the Operation Aurora); the cyber operation against Iran's main fuel enrichment facility (hereinafter referred to as the Stuxnet case); the stealing of data and destruction of computers of Sony Pictures Entertainment (hereinafter referred to as the Sony Pictures Entertainment case); the stealing of data of the Office of Personnel Management (hereinafter referred to as the OPM case); and global cyber operation WannaCry. The scope of the second chapter is limited to malicious cyber operations that caused significant damage in the physical world or to governmental assets in cyber infrastructure, such as altering data in the attacked networks, or leaking of large amounts of governmental data. This chapter focuses on the responses and reactions of victim-States in order to examine whether they have referred to their rights under international law and on the alleged responsible State obligations under international law. The case studies' selection criteria is more deeply explained in the beginning of the second chapter.

The third chapter analyses the outcomes derived from the second chapter to explore challenges in the usage of countermeasures by the victim-States and provide an analytical framework in order to answer the research questions of the thesis. The author will conclude whether due to the lack of precise international legal framework governing cyberspace or the limited State practice in implementing legitimate responses to malicious cyber operations, it is hard to precisely assess future impacts of legal framework in cyberspace concerning countermeasures.

As the existing inadequacy of the States to use the legal framework to deal effectively with the malicious cyber operations below the armed attack threshold, the possible solutions examined in this thesis are significant for both the academic and research communities in understanding the countermeasures and open up opportunities for further research.

The primary sources used in this thesis are the monographs Tallinn Manual 1.0[20] and Tallinn Manual 2.0[21]. These monographs provide a series of draft rules that reflect possible interpretations of how international law is applied in cyberspace. Even though these rules are non-binding as such, these are the mainframe books that provide the opinions of a group of international experts who discuss the interpretation of international law in cyberspace. Furthermore, they are viewed as an academic work, which can be considered as a subsidiary source of the law.[22] However, it is important to note that Tallinn Manuals do not officially represent any States' position on international law, nor State's domestic law. The thesis is also supported by numerous legal and newspaper articles, such as official statements by governmental agencies, press releases, analyses of cybersecurity companies, to show that the problem is real and timely, and that solutions are needed.

Analytical legal method is mainly used in this thesis. Literature that is relevant to the research questions was collected by searching in the catalogues of scientific publications. The collected material was used to summarize the relevant aspects about the examined field in order to provide theoretical basis for further research. Comparative method is used in the second and third chapters to analyse the data provided in the second chapter in order to provide an analytical framework and answers to the research questions.

[20] M. N. Schmitt, *et al*. Tallinn Manual On The International Law Applicable To Cyber Warfare Cambridge University Press 2013.
[21] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.*
[22] N. Jupillat. Armed Attacks in Cyberspace: The Unseen Threat to Peace and Security That Redefines the Law and State Responsibility. - 92 University of Detroit Mercy Law Review 2015 (2), pp. 115-116.

The case studies examined in Chapter 2 rely on publicly available materials such as official publications issued by governmental agencies, press releases, analyses of cybersecurity companies and press reports with the unofficial allegations. Due to the lack of public transparency in reporting on cyber operations and limited attribution cases, the author firstly conducted research to identify the harmful cyber operation that can meet the purpose and scope of the thesis. The author compared the lists of two depositories – the Center for Strategic and International Studies[23] (hereinafter referred to as CSIS) and the US Council on Foreign Relations' Cyber Operations Tracker (hereinafter referred to as CFR),[24] and selected five case studies based on the criteria discussed in the beginning of Chapter 2.

I am deeply thankful to my family for all the support they have offered me and for giving me an opportunity to continue my studies. I would like to express sincere gratitude to my supervisor Anna-Maria Osula who guided me throughout the process of writing the thesis.

The keywords for this thesis include: international law, countermeasures, cyberspace, State responses and cyber operation.

[23] Significant Cyber Incidents Since 2006. The Center for Strategic & International Studies. Accessible at: https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity (15.02.2020).

[24] Cyber Operations Tracker. The United States Council on Foreign Relations. Accessible at: https://www.cfr.org/interactive/cyber-operations (15.02.2020).

I. COUNTERMEASURES

1.1. Countermeasures defined and differentiated

The countermeasures stand for the actions or omissions by one State (victim-State), directed to another State (responsible State) that would be otherwise unlawful, that are conducted by the former State in order to compel the latter to desist in its actions or omissions that are considered to be internationally wrongful.[25] The employment of countermeasures in response to the international wrongful act by a State is permitted under the customary international law and the United Nations resolution adopted by the General Assembly on the Responsibility of States for International Wrongful Acts (hereinafter referred to as the Articles on State Responsibility) on 28 January 2002.[26] Notwithstanding, that the Articles on State Responsibility are not a treaty and therefore are not binding for the States, they are nowadays characterized as authoritative, reflecting the customary international law. The International Court of Justice (hereinafter referred to as ICJ) has confirmed the principle of State responsibility, and has recognized countermeasures on many occasions.[27] This remedial measure comprising from the law of State responsibility can be cyber or non-cyber in nature that extends to the cyber space activities.[28] Customary international law of State responsibility extends to the cyberspace activities.[29] However it should be noted, that there is a disagreement among States on the interpretation of applicability of international law principles to cyber operations.[30]

The countermeasures should be differentiated from retorsions, as countermeasures involve actions that would be otherwise unlawful, and retorsion acts are lawful, but unfriendly.[31] The State actions that overcome the purpose, means, the scope of execution, legal rights and duties are strictly restricted when applying the countermeasures.[32] A State has a right to take any measures necessary with regards to cyber infrastructure on its territory, unless the action would

[25] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.*, Rule 20, note 1.
[26] Articles on State Responsibility, *op. cit*.
[27] See Corfu Channel case (United Kingdom v. Albania), Judgment, International Court of Justice 1949, p. 23.; Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Judgment, ICJ 1896, para. 249; Gabčíkovo-Nagymaros Project (Hungary v. Slovkia), Judgment, ICJ 1997, paras. 82-83.
[28] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.*, Rule 20, note 1.
[29] Tallinn Manual 2, Chapter 4, Section 1, note 4.
[30] A. Väljataga. Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly. - The NATO Cooperative Cyber Defence Centre of Excellence 01.09.2017. Accessible at: https://ccdcoe.org/incyder-articles/back-to-square-one-the-fifth-un-gge-fails-to-submit-a-conclusive-report-at-the-un-general-assembly/ (21.02.2020).
[31] Articles on State Responsibility, *op. cit*., Part 3, Chapter II, para. 3 of commentary; See T. Giegerich. Retorsion. - 8 Max Planck Encyclopedia of International Law 2012.
[32] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.*, Rule 20, note 5; Rules 21-23.

be unlawful by a rule of international law.[33] The object of a countermeasure must be a State, a non-State actor cannot be the target of an injured State, unless the harmful cyber operation is attributable to a State[34], as discussed in the section 1.2.2.

Countermeasures must be distinguished from the sanctions imposed by the United Nations Security Council under the Chapter VII of the United Nations Charter, as they constitute to be lawful. As provided in Article 41 of the UN Charter, interruption of economic relations and other means of communication means may be lawfully implied to establish the existence of any threat to the peace, act of aggression or breach of the peace.[35] When the Security Council makes a resolution authorizing the interference to the State's cyber infrastructure, such activity would be lawful and thus would not be constituted as a countermeasure. Additionally, even if the targeted State's sovereignty would be violated when applying the actions deriving from the UN Security Council resolution, the activity would still be lawful under international law and will not qualify as a countermeasure.[36]

Further relevant distinction is the difference between the countermeasures and the plea of necessity. The measures deriving from the plea of necessity may be applied when the State confronts with the situation that poses grave and imminent peril to an essential interest to safeguard the interests of a State. Those wrongful acts and imposed measures may be cyber and non-cyber in nature.[37] For instance, the plea of necessity in cyber context is relevant when the cyber operations threaten the operation of the critical infrastructure of a State.[38]

The option of resorting to countermeasures provides a State with the right to respond to malicious cyber operations from another State that fall below the threshold for triggering a right to self-defense. Bearing in mind, that in order to use countermeasures the actor or the State from where a harmful cyber operation originates should be identified, whereas the plea of necessity is a means that may be used if attribution is not possible. Under Article 25 of the Articles on State Responsibility, necessity is a circumstance for precluding the wrongfulness of an act that would otherwise breach international law.[39] It is a very rare case where a State can protect a

[33] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.*, Rule 2, note 1.
[34] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.*, Rule 20, note 6-7.
[35] UN Charter, *op. cit.*, Art 39 and 41.
[36] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.*, Rule 20, note 11.
[37] Articles on State Responsibility, *op. cit.*, Art. 25(1)(a). See Gabčíkovo-Nagymaros Project 1997, *op. cit.*, para. 51, 55; Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, ICJ 2004, para. 140.
[38] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.*, Rule 26.
[39] Articles on State Responsibility, *op. cit.*, Art 25.

substantial interest from a serious and imminent threat in only one way. As mentioned in the Tallinn Manual, the plea of necessity can be used when the exact nature and origin of a cyber operation is unclear. A State that has faced the situation that endangers its essential interests may temporarily shut down certain cyber infrastructures, even if it will affect the infrastructures of another State.[40] The notion of the possible justification of counter-hacking in cases of necessity is also considered.[41]

Even though a plea of necessity is a possible tool to respond to the harmful cyber operations when the attacker is not identified, this measure does have strict limitations. The essential interests of a victim-State must be at stake and a potential harm must be severe.[42] The necessity cannot be invoked if the international obligation precludes the invocation of necessity or a State has contributed to this situation.[43] Furthermore, State may not seriously undermine an essential interest of the State or the international community.[44] In Gabčikovo-Nagymaros Project case the ICJ illustrated that the necessity can be used only in exceptional circumstances and State cannot be the only judge to decide whether conditions have been met.[45] According to the Article 26 of the Articles on State Responsibility the necessity cannot preclude the wrongfulness of any act of a State which is not in accordance with the peremptory norms of international law.[46] Taking into consideration the mentioned above limitations, the plea of necessity is a last resort that could be applied, thus in practice is less evident to be invoked.

[40] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.*, Rule 26, note 11.
[41] *Ibid.*, note 11-12.
[42] Articles on State Responsibility, *op. cit*., Art 25 (1)(a). See M. N. Schmitt. Tallinn Manual 2.0, *op. cit.*, Rule 26, note 4.
[43] Articles on State Responsibility, *op. cit*., Art 25 (2).
[44] *Ibid.*, Art 25 (1)(b).
[45] Gabčíkovo-Nagymaros Project 1997, *op. cit*., paras. 51-52.
[46] Articles on State Responsibility, *op. cit*., Art 26.

1.2. Conditions for countermeasures

Based on customary international law of State responsibility, countermeasures can be employed in response to an internationally wrongful act, having two components to be considered: breach of an international obligation owed to another State, and attribution of the wrongful act to a State.[47]

1.2.1. Breach of international legal obligation

There is an internationally wrongful act of a responsible State, when action or omission constitutes a breach of an international obligation to the injured State.[48] This concept of internationally wrongful act is governed by international law and does not extend to the internal domestic law.[49] Violation of the primary rules establishing international obligations entails State responsibility. For instance, the primary rule is the prohibition to use the force under Article 2 (4) of the UN Charter.[50] The breach may consist of a violation of either customary international law or a State's treaty obligations. For example, in case of an aircraft of one State that conducts harmful operations in the national airspace of another State is in breach with the customary law and it is in violation with a treaty.[51]

There are certain circumstances that preclude the wrongfulness of a State's cyber acts or omissions. Chapter V of the Articles on State responsibility gives a list of considerations precluding wrongfulness.[52] For instance, a consent given by a State to a certain cyber operation or to certain assets of cyber infrastructure precludes the wrongfulness of the action, unless it exceeds the limits of the consent.[53] Moreover, self-defense that has been authorized by the UN Security Council, force majeure, distress and necessity preclude the wrongfulness of an act or omission.[54] Qualification of an act as a countermeasure, under the Article 22 on State Responsibility, precludes the wrongfulness of an act, meaning that a countermeasure is not constituted as an internationally wrongful act, thus countermeasures may not be taken in

[47] Articles on State Responsibility, *op. cit*., Art. 2 (a)(b).
[48] *Ibid.*, Art. 2 (b).
[49] *Ibid.*, Art. 3.
[50] UN Charter, *op. cit.*, Art. 2 (4).
[51] Convention on International Civil Aviation. Chicago 07.12.1944, e.i.f. 04.04.1947, Art. 1.; United Nations Convention on the Law of the Sea. Montego Bay 10.12.1982, e.i.f. 16.11.1994, Arts. 17, 19, Art. 2(2).
[52] Articles on State Responsibility, *op. cit*., Chapter 5.
[53] *Ibid.*, Art. 20.
[54] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.*, Rule 19.

response to legitimate countermeasures.[55] It should be noted, that States practice and opinio juris interpret the international law, as well as consider which cyber operation constitutes a breach of international law.

a) Sovereignty

There is currently debate as to whether respect for the sovereignty of another State is the primary rule that imposes a legal obligation, or whether it is simply a legal principle from which primary rules, such as prohibitions on intervention and the use of force, derive.[56] On the one hand, it is argued that there is a support in State practice and opinion juris for sovereignty as a rule of international law, the violation of which results in international legal responsibility.[57] On the other hand, some scholars present their approach that sovereignty is a principle.[58] However, neither of the disputed approaches, whether sovereignty is a rule or principle, is universally accepted and is faced with a relative inanity of public State practice.[59] The author uses in this thesis the principle of sovereignty as a general principle from which a number of principles and rules of conventional and customary international law derive.

The breach of an international legal obligation and specifically internationally wrongful act is connected to the principle of sovereignty that grants States with rights and obligations.[60] Sovereignty affords States to conduct activities on their territory without the interference by another States. The principle of sovereignty applies in cyberspace.[61] Malicious cyber operations that inflict physical damage or injury launched against cyber infrastructure situated on another State's territory amount to a breach of latter State's sovereignty.[62]

The territorial sovereignty means that a State has an exclusive right to exercise its powers and enforce jurisdiction over its territory, including the territorial sea, air space, and vessels and aircrafts registered under its flag.[63] A State must refrain from exercising its authority on the

[55] Articles on State Responsibility, *op. cit*., Art. 22.
[56] G. P. Corn, R. Taylor. Sovereignty in the Age of Cyber, *op. cit.*; M. N. Schmitt, L. Vihul. Sovereignty in Cyberspace: Lex Lata Vel Non?. – 111 American Journal of International Law 2017.
[57] See M. N. Schmitt, L. Vihul. Respect for Sovereignty in Cyberspace. - 95 Texas Law Review 2017 (7).
[58] G. P. Corn, R. Taylor. Sovereignty in the Age of Cyber. - 111 American Journal of International Law 2017.
[59] E. T. Jensen. The Tallinn Manual 2.0: Highlights and Insights. – 48 Georgetown Journal of International Law 2017, pp. 735, 743.
[60] Island of Palmas (Neth. v. U.S.), 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928); M. N. Schmitt. Tallinn Manual 2.0, *op. cit.,* Rules 1-5, 35 and 37.
[61] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.*, Rule 1.
[62] *Ibid.*, Rule 6 on sovereignty and Rule 1 and accompanying commentary.
[63] United Nations Convention on the Law of the Sea, *op. cit.,* Arts. 95-96.

territory of the other States.[64] In regards to cyberspace, knowing that cyber infrastructure consists of physical tools, as well as cyberspace users are operating from the particular jurisdiction, States remain sovereign within this area and over cyber activities exercised therein.[65] The principle of sovereignty grants States with the right to control not only the aspects of physical cyber tools, but also to promote and employ necessary legislation concerning the cyberspace and security issues connected to it.[66] A State has a right to regulate cyber activities on its own territory, for example restrict specific content to be uploaded online or block access to violent content on social media. Such enforcement mechanisms should comply with the human rights obligations and rights.[67] External sovereignty of a State entitling to independently formulate foreign policies and enter into the international arrangements regarding the cyberspace regimes.[68]

According to the Tallinn Manual a computer network operation on cyber infrastructure of another State will constitute as a violation of sovereignty if the caused damage or injury will be at certain level.[69] The question of where lies the line between unlawful cyber operations and those activities in cyberspace that do not constitute as harmful, raises. If a State injures another State or a group of States, the victim-State(s) may invoke the international responsibility of the responsible State and demand reparations, which can be made in the form of restitution, compensation or satisfaction.[70]

Emplacement of malware into a cyber-system of another States, destruction of data and hacking seem to overpass the principle of sovereignty, whereas monitoring activities that constitute espionage are not. In regards to the peacetime espionage while using cyberspace, the mere fact that cyber operation was interpreted as an act of an espionage, it does not signify the violation of a States sovereignty. Rather, the underlying acts of espionage and operation must be examined.[71]

[64] Island of Palmas (United States v. Netherlands), Award, Permanent Court of Arbitration 04.04.1928, p. 838.
[65] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.*, Rule 2 and 3.
[66] *Ibid.*, Rule 2 (6).
[67] *Ibid.*, Rules 35, 37. See Australian Human Rights Commission. Background paper: Human rights in Cyberspace, September 2013. Accessible at: www.humanrights.gov.au/sites/default/files/document/publication/human_rights_cyberspace.pdf (15.01.2020).
[68] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.*, Rule 3, note 2.
[69] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.*, Rule 1, note 6.
[70] Articles on State Responsibility, *op. cit.*, Arts. 30,31,34-37,42,48 (1).
[71] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.*, Rule 32.

The mere collection of intelligence does not itself violate the international law, the exception is specifically protected data of individuals, facilities or documents under international law norms.[72] However, it is up to a legal debate whether malicious cyber activities that only cause very limited damage or no damage, or are routed through the cyber infrastructure of the State will not constitute as a violation of international law.[73]

A State may give a consent to another State to conduct cyber operation that would otherwise constitute as a violation of a State sovereignty. For example, if a State does not have the technical capability to end harmful activities that are conducted from its territory, therefore violating the due diligence obligation, a State in question may request an assistance of another State. In this manner, supporting State would not violate the sovereignty of another State.[74]

b) Prohibition of intervention

The International Court of Justice in Nicaragua judgment held that principle of sovereignty is closely linked with the principle of non-intervention.[75] The principle of non-intervention derives from the principle of sovereign equality of States, prohibiting States to intervene directly or indirectly in internal and external matters of s State.[76] Cyber operations that violate another State's principle of non-intervention and are targeted to force State's government in theirs internal and external affairs, do qualify as internationally wrongful activities.[77] However, the prohibition of intervention is applied restrictively in cyberspace, as non-intervention principle generally requires more than just interference.[78]

The principle of non-intervention, being a customary international law,[79] requires the intervention to be coercive, involving matters on which every State, according to the principle of State sovereignty, can decide freely on its domestic affairs.[80] Notwithstanding, the mere coercion does not suffice to qualify a breach of the prohibition of intervention. The coercive

[72] K. Ziolkowski. Peacetime Cyber Espionage – New Tendencies in Public International Law. - Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy. NATO Cooperative Cyber Defence Centre of Excellence 2013, pp. 431–442; Art. 27 of the Vienna Convention on Diplomatic Relations on specific prohibition against espionage. Vienna 19.04.1961, e.i.f. 24.04.1964.
[73] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.*, Rule 1, 4.
[74] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.*, Rule 19.
[75] Nicaragua case, *op. cit.*, Para. 212.
[76] *Ibid.*, Para. 205. Corfu Channel case 1949, *op. cit.*, at 35.
[77] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.*, Rules 43-45, Rule 66.
[78] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.*, Rule 66, note 3.
[79] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.*, Rule 66, note 1. UN GGE 2015 Report paras 25,28 (b).
[80] R. Jennings, A. Watts (ed.). Oppenheim's International Law 9th ed. 2008, p. 428; P. Kunig. Prohibition of Intervention. Max Planck Encyclopedia of Public International Law 2008.

must influence the outcomes or conduct of a target State.[81] For instance, suppling monetary funds to guerrilla forces in another country, as well as manipulation of public opinion on elections, can be amounted to an unlawful intervention.[82] The distinction between coercive and non-coercive cyber operations has no clear conditions under international law. However, it is generally agreed, that a use of force by one State against another is always coercive, thus constitutes as unlawful intervention. Malicious cyber activities that fall under the armed attack threshold fail to qualify as unlawful interventions, as such operations tend to target private companies and do not affect matters that are dominantly reserved to a State.[83] It is argued that State sponsored harmful cyber operation tend to remain more sophisticated and dangerous than cyber interferences committed by non-State actors.[84]

c) Due diligence principle

States are obliged under the international law and the law of State responsibility to maintain control over conducted activities on their territory.[85] International Group of Experts in Tallinn Manual acknowledged that State must not knowingly allow cyber infrastructure to be used in ways that could unlawfully affect other States.[86] In case of a harmful cyber operations that are launched by non-State actors, States are especially required to use their best possible efforts to comply with the obligation.[87]

Countermeasures may not only be used by a victim-State in response to malicious cyber operations conducted by States, but also, as appropriate, in a situation where another State is in breach of its international due diligence obligations by knowingly allowing the use of its territory for cyber activities that contravene the rights of other States by non-State actors.[88] Although the cyber operation itself is not committed by State, it is responsible for its failure to stop them.

[81] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.,* Rule 66, 19.
[82] Nicaragua case, *op. cit.,* Paras. 205, 228.
[83] Nicaragua case, *op. cit.,* Para. 202; United Nations General Assembly Resolution A/RES/2625 (XXV). Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations 24.10.1970; United Nations General Assembly Resolution 2131 (XX) of 21.12.1965, Para. 2; M. N. Schmitt. Tallinn Manual 2.0, *op. cit.,* p. 45.
[84] B. Barrett. Facebook Now Warns Users of State-Sponsored Attacks. WIRED, 09.10.2015. Accessible at: http://www.wired.com/2015/10/facebook-now-warns-users-of-state-sponsored-attacks (04.03.2020).
[85] Corfu Channel case 1949, *op. cit.,* at 22; See United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran), ICJ 1980, paras. 67–68.
[86] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.,* Rule 6.
[87] J. Crawford. The International Law Commission's Articles On State Responsibility: Introduction, Text and Commentaries. United Kingdom: Cambridge University Press 2002, p. 140.
[88] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.,* Rule 6.

The due diligence principle derived from the principle of sovereignty[89] of States and reflects the general principle of international law.[90] It has been reaffirmed by the International Court of Justice in its Corfu Judgment that each State has an obligation not to use its territory knowingly for acts contrary to the rights of other States[91] and Tehran case, that affirmed that States are bound to take appropriate measures in order to protect other States from non-State actors from the territory of responsible State.[92] International treaties also support this principle, for example the Declaration on Measures to Eliminate Terrorism[93] and the Declaration on the Strengthening of International Security, stipulating that States should refrain from organizing, assisting or participating in terrorist acts in territories of other States, or from acquiescing in or encouraging activities within their territories directed towards the commission of such acts.[94]

The due diligence principle applies in cyber context unless State practice or opinio juris excludes it.[95] This principles involves at least three parties: victim-State; responsible State under due diligence principle and third party as an actor launching cyber operation. It applies to private persons, States, non-State actors or groups, corporations, and encompasses any cyber infrastructure on the territory of the responsible State.[96] State is in breach of its due diligence obligation if it (1) is aware of a malicious cyber operation conducted from its territory, the cyber operation (2) is contrary to the rights of another State, and (3) it does not take practical measures to prevent it.[97] Each circumstance of this principle acts as a reasonable limitation on the potential responsibility of the State.

Knowledge is the first decisive element of due diligence. The International Court of Justice in the Hostages case, brought Iran to justice by concluding that the Iranian authorities were fully aware of the urgent need for action and had the means at their disposal to perform their obligations, as well as completely failed to comply with these obligations.[98] States cannot nonetheless have an absolute knowledge of all things happening on their territory. The International Court of Justice in Corfu case stated that it could not be inferred from the mere

[89] *Ibid.,* Rule 1.
[90] See Island of Palmas case, *op. cit.,* p. 839.
[91] Corfu Channel case 1949, *op. cit.,* Rep 4, 22.
[92] See United States Diplomatic and Consular Staff in Tehran, *op. cit.*
[93]Measures to Eliminate International Terrorism. UN General Assembly Resolution 49/60, 09.12.1994.
[94] Declaration on the Strengthening of International Security. UN General Assembly Resolution 2734 (XXV), 16.12.19170.
[95] M. N. Schmitt. In Defence of Due Diligence in Cyberspace. – 125 Yale Law Journal Forum 2015 (68), p. 73.
[96] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.,* Rule 6, notes 7, 8.
[97] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.,* Rule 5, note 9.
[98] United States Diplomatic and Consular Staff in Tehran 1980, *op. cit.,* para. 68.

fact of a State exercising control over its territory, that that State necessarily knew or ought to have known what had been committed.[99] The European Court of Human Rights, in Osman v. United Kingdom, also found that the unpredictability of human behaviour and the prompt choices to be made in terms of priorities and resources should be interpreted in such a way as not to impose a disproportionate burden on the government.[100]

The problem arises when determining the standard of proof in order to show that a State knew that malicious cyber operation was conducted on its territory. Due to the fact that States exercise exclusive territorial control within their territory, the victim-State of a breach of international law obligation could be unable to provide direct evidence of the facts to demonstrate the existence of knowledge.[101] The International Court of Justice, in its Corfu judgment, stated that a more liberal use of interference with facts and circumstantial evidence should be permitted, and that evidence may be based on facts, provided that they leave no room for reasonable doubt.[102]

In that case the ICJ found that one of the indications of Albanian's knowledge of events was the fact that Albania, after the reported events affecting the United Kingdom, did not inquire into the event nor proceeded to judicial investigation. It is known that the Albanian Government did not notify the presence of mines in its waters when it should have known, while the Greek Government appointed a Commission to investigate the events, the Albanian Government did not take such a decision and did not initiate a judicial investigation into a case that was then under the authority of the sovereign of the territory.[103]

The knowledge element can be satisfied with both actual and constructive knowledge.[104] As it may be difficult to establish the actual knowledge of the State about a cyber operation conducted on its territory, a constructive knowledge standard ensures that a due diligence approach will not be completely redundant.[105] Under this notion, a State should be aware of

[99] Corfu Channel case 1949, *op. cit.*, p. 18.
[100] Osman v. United Kingdom, Judgment, ECHR 28.10.1998, para. 116.
[101] Corfu Channel case 1949, *op. cit.*, p. 18.
[102] K. Del Mar. The International Court of Justice and Standards of Proof. - K. Bannelier, T. Christakis and S. Heathcote (eds), The ICJ and the Evolution of International Law: The Enduring Impact of the Corfu Channel Case 2012, pp. 98-123.
[103] Corfu Channel case 1949, *op. cit.*, pp. 19-20; M. N. Schmitt. Tallinn Manual 2.0, *op. cit.*, Rule 5, note 11.
[104] JR. Crook. Use of Force and Arms Control: State Department Legal Adviser Addresses International Law in Cyberspace. – 107 American Journal of International Law 2013 (1), pp. 243, 247; R. Geiβ, H. Lahmann. Freedom and Security in Cyberspace: Shifting the Focus away from Military Responses towards Non-Forcible Countermeasures and Collective Threat-Prevention. – K. Ziolowski. Peacetime Regime for State Activities in Cyberspace, p. 623; M. N. Schmitt. Tallinn Manual 2.0, *op. cit.*, Rule 6, note 37, 39.
[105] Corfu Channel case 1949, *op. cit.*, p. 22.

everything that is conducted on its territory and could be detected in the course of normal events".[106] For example, a State's knowledge would be more likely to be attributed to the common or easily detectable use of malware.[107] Moreover, a State would be more likely to be aware of the use of its state's cyber infrastructure than of the use of private infrastructure on its territory.[108]

While it is undeniable that the due diligence principle applies automatically in cases where States have actual knowledge of cyber actions, the question should be asked whether it should also be applied where States should have known of a particular situation. The Tallinn Manual provides an indecisive conclusion on this issue, stating that the International Group of Experts could not reach a consensus because this rule applies if the State concerned only had constructive "should have known" knowledge.[109]

In Corfu case the International Court of Justice stated that a State in whose territory an act contrary to international law was committed may be asked to provide an explanation and cannot avoid such a request by merely replying that it is not aware of the circumstances of the act and its authors. A State may, up to a certain point, be obliged to provide information on its use of the media and investigations available to it.[110] It is directly related to the duties related to the exclusive control exercised by States over their territory. The European Court of Human Rights (ECtHR) or the Human Rights Committee has consistently adopted the idea of constructive knowledge as part of States positive human rights obligations.[111]

The questions arise on what measures the State must take to be able to know whether there are illegal cyber acts hostile to third States conducted on their territory. The due diligence principle includes an obligation for States to monitor cyber activities on their territory, it implies not only obligation to respond, but also to prevent. The International Court of Justice held that due diligence implies that States should exercise administrative control applicable to all operators in its territory in order to protect the rights of the other party.[112]

---

[106] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.,* Rule 6, note 42. See K. Bannelier-Christakis. Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?. - 14 Baltic Yearbook of International Law 2014, p. 30.
[107] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.,* Rule 6, note 40.
[108] *Ibid.,* Rule 6, note 41.
[109] *Ibid.,* Rule 6, note 41.
[110] Corfu Channel case 1949, *op. cit.,* p. 18.
[111] Osman v. United Kingdom, *op. cit.,* para. 116. See Paul and Audrey Edwards v. United Kingdom, Judgment, ECtHR 14.03.2002, para. 55.
[112] Pulp Mills on the River Uruguay (Argentina v. Uruguay), Judgment, ICJ 20.04.2010, para. 197.

According to the French White Paper on Defence and National Security, the importance of fighting against harmful cyber activities calls for developing intelligence activity and the corresponding technical expertise in cyberspace area. These measures should allow to identify the origin of attacks (attribution) and assess the offensive capabilities of potential adversaries. Identification and offensive action capabilities are essential to implementing a possible and appropriate response to malicious cyber attacks.[113]

It should be recalled, nonetheless, that the duty of due diligence can only authorise acts compatible with international law. In the Genocide case the ICJ warned that each State may act only within the limits permitted by international law.[114] The ECtHR also emphasized that the police must exercise their powers to combat and prevent crime in a way that fully respects due process and other safeguards that legally limit the scope of their activities to investigate crimes and bring offenders to justice.[115]

It is clear that the "knew or ought to have known" criterion cannot legitimize violations of international human rights or other norms. The Resolution on the Right to Privacy in the Digital Age, adopted by the UN General Assembly in December 2013, is a good example of what States should respect in this area. This resolution invites States to respect and protect the right to privacy, including in the context of digital communication; to take measures to put an end to violations of those rights and to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies with their obligations under international human rights law; as well as to review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law.[116]

[113] French White Paper: Defence and National Security. France 2013, p. 71. See Information Systems Defence and Security France's Strategy. - French Network and Information Security Agency 2011, p. 15.
[114] Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, ICJ 11.07.1996, para. 430.
[115] Osman v. United Kingdom, *op. cit.*, para. 116.
[116] United Nations General Assembly Resolution A/Res/68/167. The Right to Privacy in the Digital Age, 18.12.2013.

The third element, on enforceable measures, provides that States are obliged to intervene in a cyber operation only when they have the capacity to do so and only when appropriate in the circumstances. This element provides States with the greatest protection against the imposition of undefined liability.[117] The feasibility of measures for a State will depend on the technical, intellectual and financial resources at its disposal.[118] Thus, States will not violate international law for failing to prevent very complex cyber operations that they cannot control.[119]

[117] M. N. Schmitt. In Defence of Due Diligence in Cyberspace, *op. cit.*, pp. 74–75.
[118] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.,* Rule 7, note 16.
[119] *Ibid.,* Rule 7, note 17.

1.2.2. Attribution to a State

The degree of direction and control by a State was set forth by the International Court of Justice on the Nicaragua case, when Court held that in order the United States to bear legal responsibility, it has to be proven that the States exercised effective control over military and paramilitary operations in which alleged violations occurred.[120] The other ICJ judgment, Genocide case[121], distinguished the standards set forth by Nicaragua case and Tadić case, when the International Criminal Tribunal for the Former Yugoslavia with the relationship between States and non-State actors with respect to the armed conflict in Bosnia – Herzegovina.[122] In Genocide judgment, the ICJ affirmed that the effective control is for the purpose of attribution in the law of State responsibility.[123] Countermeasures may be used by the victim-State, when individual or a group conducting the cyber operation is under effective control and direction of a State.[124] In Nicaragua case, the ICJ pointed out that the general control over forces with a high degree of dependence on them, is not an effective control.[125]

Countermeasures may be applied only when internationally wrongful act is attributable to a State under the law of State responsibility.[126] In case of a harmful cyber operation conducted under the armed attack threshold, it is supposed that countermeasures are a possible way to bring the cyber operation in question to a halt. However, the initiation of countermeasures may in practice be hindered, as it is very complicated to ascertain who is responsible for the harmful cyber operation, in other words to attribute the activity to an responsible actor.[127] The lack of knowledge of the identity of a responsible actor makes it difficult for the victim-State to determine the proper countermeasures and the purpose of the activities is unsubstantiated.[128] The difficulties that are connected to the attribution raise the question of the appropriate standard of proof. For instance, what level of certainty must victim-State have to prove that harmful cyber operation originated form the responsible State, how much evidence is required

[120] Nicaragua case, *op. cit.*
[121] Application of the Convention on the Prevention and Punishment of the Crime of Genocide, *op. cit.*, paras. 403–405.
[122] Prosecutor v. Tadić, Case No. IT-94-1-A, Appeals Chamber Judgement 15.07.1999, International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia since 1991, paras. 117, 131–140, 145.
[123] Application of the Convention on the Prevention and Punishment of the Crime of Genocide, *op. cit.*, paras. 403–405.
[124] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.*, Rule 17.
[125] Nicaragua case, *op. cit.*, para. 115.
[126] Articles on State Responsibility, *op. cit*., Art. 2 (a).
[127] See Nicaragua case, *op. cit.*, para. 115.
[128] S. W. Brenner. At Light Speed: Attribution and Response to Cybercrime/ Terrorism/Warfare. - 97 Journal of Criminal Law and Criminology 2007 (2), pp. 405–415.

to initiate the countermeasures. Does the mere allegation of a possibility is enough, or there should be clear and convincing evidence?[129]

The Tallinn Manual provides that if cyber operation originated from the governmental cyber infrastructure of a State, is not enough condition to attribute the activity to that State, it is simply an indication that the State is associated with the operation.[130] For instance, if a non-State actor attempts to spoof the origin of malicious cyber operation, that is usually the case, then a State that is believed to be responsible for the harmful cyber operation should be given the opportunity to disprove that assumption. This is the case when botnets use so called "zombie" computers in different countries to mount distributed denial of service (DDoS) attacks. In 2013, North Korean cyber operation in order to shut down South Korean banking and media systems, allegedly employed more than thousand IP addresses in multiple countries.[131]

Under Article 8 of the international rules on State responsibility and based on the International Court of Justice case law, there is an attribution to a State when the wrongful acts was committed by an individual or a group, and if the latter acted on the instructions of, or under the control or direction of a State.[132] It should be noted, that there is no requirement that the activities should be governmental in character.

The easiest case when activity is attributable to a State, is when military or intelligence agencies conduct the malicious operation.[133] However, when individual or entity does not qualify as a State organ, but they are empowered by internal law to exercise specific element of a governmental agency, the actions committed by them would be also attributable to a State.[134] The example could be the Computer Emergency Response Team (CERT) that has a right to collect cyber data on behalf of governmental intelligence agencies.[135] Under Article 6 on State responsibility, if a State organ is at the disposal of another State in order to exercise actions, the

[129] R. Geiβ, H. Lahmann. Freedom and Security in Cyberspace: Shifting the Focus away from Military Responses towards Non-Forcible Countermeasures and Collective Threat-Prevention 2013, *op. cit.*, p. 624–625. See J. Lobel. The Use of Force to Respond to Terrorist Attacks: The Bombing of Sudan and Afghanistan. - 24 The Yale Journal of International Law 1999, p. 547.
[130] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.,* Rules 15 and 16 and accompanying notes.
[131] Y. Lee. South Korea Says North Korea Behind Computer Crash in March. Global News 10.04.2013. Accessible at: https://globalnews.ca/news/468054/skorea-says-nkorea-behind-computer-crash-in-march/ (07.02.2020).
[132] Articles on State Responsibility, *op. cit*., Art. 8.; Nicaragua case, *op. cit.,* para. 115.
[133] Articles on State Responsibility, *op. cit*., Art. 4(1).
[134] *Ibid.,* Art. 5.
[135] See RFC 2350 Description for CERT-EE. Accessible at: https://www.ria.ee/sites/default/files/content-editors/CERT/cert-ee_rfc2350.pdf (06.03.2020).

conduct of the organ will be attributable to the latter State.[136] In the case of operations of either State bodies or entities authorized to carry out elements of State power, the State is responsible for actions that go beyond the scope of the powers granted by the State, or that are contrary to the instructions. For instance, if a member of the CERT carries out illegal activities in violation of orders, the host-State is responsible for any breach of obligations to other States.[137]

Companies that are owned by a State, such as information technology companies, cannot hold the State responsible for the wrongful conduct of the company solely due to the State ownership.[138] Nevertheless, if the operation is conducted under the effective direction and control of a State, or the company bears governmental functions, the wrongful activities will be attributable to the State, thus the injured State can employ appropriate countermeasures against the responsible State.[139]

The case of an activity conducted by individual or group of individuals that was under the direction or control of a State[140] can be the situation when State enters into a contract with the individuals to implement the exploit and manages the process. If those individuals will conduct harmful cyber operations against the host-State, the responsible State would be directing State. However, in this case, their conduct is attributable to the State only if it directs or controls a particular operation that is an integral part of that operation.[141]

The State's accidental relationship with cyber operations is not a basis for liability and the attribution. For example, cyber operations against Estonia and Georgia in 2007 and 2008, respectively, were not, at least on the basis of the evidence available, subject to Russian control to justify misappropriation and therefore countermeasures by these countries against Russia.[142] However, the countermeasures would have been justified under the due diligence principle. These situations are likely to grow in numbers, as the ability of individuals to conduct malicious

[136] J. Crawford. The International Law Commission's Articles On State Responsibility: Introduction, Text and Commentaries, *op. cit*., p. 145.
[137] Articles on State Responsibility, *op. cit*., Art. 7.
[138] J. Crawford. The International Law Commission's Articles On State Responsibility: Introduction, Text and Commentaries, *op. cit*., p. 112.
[139] M. N. Schmitt. Cyber Activities and the Law of Countermeasures. - K. Ziolowski (ed). Peacetime Regime for State Activities in Cyberspace NATO CCD COE Publication Tallinn 2013, p. 673.
[140] Articles on State Responsibility, *op. cit*., Art. 8.
[141] J. Crawford. The International Law Commission's Articles On State Responsibility: Introduction, Text and Commentaries, *op. cit*., p. 110.
[142] Eneken Tikk *et al*. International Cyber Incidents: Legal Considerations. - NATO CCD COE Publication Tallinn 2010, pp. 14-31 and 66-89.

cyber operations against States is increasing and the difficulty to attribute those actions to a State is an impediment.

Attribution based on direction and control does not extend to the situations when State organs or organs exercising governmental functions act ultra vires, exceeding the authorities granted by the State.[143] If a State instructs a group not to attack another country's critical cyber infrastructure, and the group does so nevertheless, the group's actions will not serve as a basis for taking countermeasures against the host-State.

If a State fails to take feasible measures to terminate malicious cyber operations taking place from its territory, the State is violating the due diligence obligation, and thus this omission constitutes an internationally wrongful act. When an injured State endeavors countermeasures, the requirement of proportionality, discussed below, must be taken into account, not solely the gravity and consequences will be considered, but rather the countermeasures will be generated to compel the responsible State to exercise control over cyber infrastructure on its territory.[144]

Geography is not relevant to the issues of attribution, as State or non-State actors can conduct cyber operations from the territory of another country that is controlled by another State. The determining factor is the level of direction and control, not the location of the activities. For an example, a non-State actor on the territory of one State is under direction and control of another State, integrating the cyber infrastructure located in multiple States, and using the botnet to employ harmful cyber operation against the victim-State.

On June 19, 2017, the Council of the European Union adopted the Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities, also known as Cyber Diplomacy Toolbox, that interestingly observed that not all measures of a diplomatic response require attribution to a State or a non-State actor.[145] The toolbox reminded that attribution remains a sovereign political decision based on intelligence sources and must be established in accordance with international law on State responsibility.

[143] J. Crawford. The International Law Commission's Articles On State Responsibility: Introduction, Text and Commentaries, *op. cit*., p. 113.
[144] M. N. Schmitt. Cyber Activities and the Law of Countermeasures 2013, p. 669.
[145] Cyber Diplomatic Toolbox, *op. cit.*

On May 17, 2019, the Council of the European Union adopted Council Decision 2019/797[146] and Council Regulation (EU) 2019/796[147] concerning restrictive measures against cyber operation that evolved from the conclusions of the Cyber Diplomacy Toolbox. Base on the regulation in question, the measures as sanctions can be directed only against natural or legal persons different from a State. Therefore, States remain outside of the scope of the sanction regime. The European Union is on the opinion that attribution of a cyber operation to a State should remain sovereign political decision of every Member State and should be assessed case by case.

[146] Council of the European Union. Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber–attacks threatening the Union or its Member States. Brussels: 17.05.2019.
[147] Council of the European Union. Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber–attacks threatening the Union or its Member States. Brussels: 17.05.2019.

1.3. Countermeasures' requirements and limitations

Countermeasures may be conducted only by an injured State with the purpose to induce a responsible State to comply with its international obligations.[148] Retaliation and retribution cannot be the purpose of countermeasures. Thus, when a State is willing to use countermeasures, the risk of escalation and genuine effort of resolving the dispute must be taken into account. It was agreed by the International Group of Experts that countermeasures in response to cyber operation cannot be taken or suspended, if the internationally wrongful operation has ceased or is proceed in a court or tribunal.[149]

The use of collective countermeasures remains unresolved aspect of international law.[150] Tallinn Manual Rule 24 provides that only a victim-State may engage in countermeasures, however the accompanying commentary suggest disagreement on the collective countermeasures in cyberspace.[151] Collective countermeasures are argued to allow States other than the victim-States to resort to countermeasures in response to malicious cyber operations.[152] However, such argumentation was not welcomed by the International Law Commission and States in the Sixth Committee, due to the danger of allowing a large group of State the intervene in other States internal affairs and possible negative effects on international peace and security under UN Charter.[153]

On May 31, 2019, the president of Estonia, Kersti Kaljulaid, made a speech on annual Cyber Conference of NATO Cooperative Cyber Defence Centre of Excellence, stressing the importance of collective countermeasures.[154] Estonia was the first State to publicly address this issue. It can be seen that international legal community does not endorse the use of collective countermeasures, as there are strong grounds to criticize the possible abuse of such actions.[155] Nevertheless, if collective countermeasures could be enacted with significant limitations, such

[148] Articles on State Responsibility, *op. cit*., Art. 49 (1); M. N. Schmitt. Tallinn Manual 2.0, *op. cit.*, Rule 21.
[149] Articles on State Responsibility, *op. cit*., Arts. 49 (2), 52 (2)(3). M. N. Schmitt. Tallinn Manual 2.0, *op. cit.*, Rule 21, note 14.
[150] M. N. Schmitt. Estonia Speaks Out on Key Rules for Cyberspace. Just Security 10.06.2019. Accessible at: https://www.justsecurity.org/64490/estonia-speaks-out-on-key-rules-for-cyberspace/ (18.02.2020).
[151] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.*, Rule 24.
[152] J. Crawford. Third Report on State Responsibility. Doc. A/CN.4/507 and Add. 1-4, 04.08.2000, paras. 105-106.
[153] J. Crawford. Third Report on State Responsibility, *op. cit*., para. 405.; L-A. Sicilianos. Countermeasures in Response to Grave Violations of Obligations Owed to the International Community. - J. Crawford *et al*. (eds.), The Law of International Responsibility, Oxford: Oxford University Press 2010, pp. 1137-1148.
[154] President of Republic of Estonia Kersti Kaljulaid. President of the Republic at the opening of CyCon 2019, 29.05.2019, *op. cit*.
[155] J. Kosseff. Collective Countermeasures in Cyberspace 2020, *op. cit*., 29-32.

as proportionality, the quantity of the potential persistent malicious cyber actors could be minimized.[156]

The requirement that derives from the purpose of countermeasures is that a State that intends to apply countermeasures must notify the responsible State that it has decided to take countermeasures and offer to negotiate.[157] In the Gabčikovo-Nagymaros case, the Court also held that the injured State must call upon the responsible State to cease the malicious act or to make reparation for it.[158] It should be noted that it is reasonable to submit both notices simultaneously. The mentioned conditions are particularly essential in the case of cyber operations, as the responsible attacker can be spoofed or the host-State may not be aware of the malicious cyber operations. In the situation of harmful cyber operations that may rapidly lead to severe consequences, the injured State may take urgent countermeasures if it is necessary to preserve its rights.[159]

When State has the right to use countermeasures against the unlawful activities in cyberspace, the countermeasures must be proportionate and set a fair balance between the act of violation of international law and the measures taken by the injured State.[160] As stated in Article 51 on State responsibility, a countermeasure should be commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the relevant rights.[161] If a countermeasure is not proportionate to the injury, the measure amounts to reprisal or punishment, thus is violating the purpose of countermeasures. The question of what measure is considered to be proportionate raises.

There are two approaches to measure the proportionality of a countermeasure.[162] The first approach is to measure the proportionality of a countermeasure against the gravity of the violation that the injured State suffered from. This approach allows for de-escalation and is the most favorable among others.[163] The second is that the measure must be commensurate with the injury suffered and take into account the gravity of the internationally wrongful act and the

[156] J. Kosseff. Collective Countermeasures in Cyberspace 2020, *op. cit.*, pp. 29-32.
[157] Articles on State Responsibility, *op. cit*., Art 52 (1); M. N. Schmitt. Tallinn Manual 2.0, *op. cit.,* Rule 21, note 10; See Air Services Agreement of 27 March 1946 between the United States of America and France. Reports of Arbitral Award 09.12.1978, paras. 85-87.
[158] Gabčíkovo-Nagymaros Project, *op. cit*., para. 84.
[159] Articles on State Responsibility, *op. cit*., Art 52 (2)
[160] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.,* Rule 23.
[161] Articles on State Responsibility, *op. cit*., Art 51.
[162] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.,* Rule 9, note 7.
[163] T. M. Franck. On Proportionality of Countermeasures in International Law. - 102 American Journal of International Law 2008 (4), p. 763.

rights involved[164], that is supported by the Gabčikovo-Nagymaros Project.[165] It is important to mention, that the approaches must be measured on a case by case basis taking into account all relevant elements.

When the gravity of a countermeasure crosses the line of proportionality, the targeted State may consider the countermeasure as reprisal, therefore wrongfulness is not precluded. Countermeasure is disproportionate to the harm caused, when the mere intention of such intensity and scale is sufficient to persuade the responsible State to refrain from its internationally wrongful conduct. The countermeasures can be executed by employing other that cyber means, however in practice it is more evident, that victim-State will response to the harmful cyber operation through the cyber infrastructure. Notwithstanding, for example the US response to the Sony attacks exemplifies that a State may decide to respond by the non-cyber means, such as pressure to terminate bilateral agreements.[166]

The proportionality of countermeasures and proportionality of jus ad bellum must be differentiated. Jus ad bellum proportionality is applicable in the situations when State has a right to defend itself against the armed attacks and prohibits the conduction of an attack when collateral damage will be excessive in relation to the prospective military advantage. [167] On the contrary, under proportionality of countermeasures in cyberspace, State measures the damage compared to the injury done.

It is very challenging to determine the degree of injury that a countermeasure will likely cause. States should exercise due diligence when they use countermeasures, as the actions must be proportionate to the injury suffered and a possible countermeasure. Due to the various factors that arise with the severity of the suffered harm, time limits, the cyber infrastructure capabilities of the victim-State, each countermeasure in question must be determined case by case.

[164] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.,* Rule 9, note 7.
[165] Gabčíkovo-Nagymaros Project, *op. cit*., para. 85. See N. D. White, A. Abass. Countermeasures and Sanctions. - M.D. Evans (ed.), International Law, New York: Oxford University Press 2010, pp. 539–540.
[166] D. Carr. How the Hacking at Sony over 'The Interview' Became a Horror Movie. - The New York Times, 21.12.2014. Accessible at: www.nytimes.com/2014/12/22/business/media/hacking-at-sony-over-the-interview-reveals-hollywoods-failings-too.html (26.02.2020). See Update on Sony Investigation. FBI National Press Office. 19.12.2014. Accessible at: www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation (26.02.2020).
[167] Nicaragua case, *op. cit.*, paras. 176, 194; Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, ICJ 08.07.1996, para. 4; Oil Platforms (Islamic Republic of Iran v. United States of America), Judgment, ICJ 06.11.2003, paras. 43, 73–74, 76.

For instance, when a State fails to exercise its due diligence obligation by taking appropriate measures to terminate the malicious cyber operation conducted from its territory, the injured State must be very cautious when exercising countermeasures under the State's omission. Assuming the non-State actor that is not attributable to a State conduct harmful cyber operation on the territory of one State against the other State, causing damages throughout the country. The host-State of a non-State actor did not take enough measures to terminate the harmful operation, while it had the reasonable opportunity. The proportionality of countermeasures will be evaluated based on failure to take necessary and appropriate measures, not the injury that was caused by the non-State actor's cyber operation.[168]

Proportionality does not require a victim-State to violate the same obligation that the responsible State violated. The principle of reciprocity does not apply to the countermeasures in cyberspace. However, the injured State should bear in mind that the obligation of proportionality is likely not to be violated, if countermeasure used is correspondent.[169] In addition, there is no obligation that a countermeasure should be numerical in kind with the internationally wrongful act. The victim-State can respond in number of cyber countermeasures that work together as a way to compel the responsible State to desist.

Countermeasures may not affect fundamental human rights, violate a peremptory norms, or amount to reprisals.[170] The Article 50(1) on State Responsibility stipulates obligations that cannot be breached.[171] The fundamental obligations, such as the prohibition of genocide, slavery, crimes against humanity and torture, racial discrimination[172], as well as human rights that cannot be derogated during the national emergency or armed conflicts[173], put necessary limitations on the use of countermeasures. It is forbidden to violate diplomatic and consular inviolability.[174] For instance, State cannot launch an attack as countermeasure against the embassy's cyber system to demand the other State to terminate the internationally wrongful act.

The limitations on countermeasures that may consist of actions that can rise to the level of an armed attack and amount to use of force are not discussed in this paper. Nevertheless, it is

[168] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.,* Rule 23, notes 11-12.
[169] J. Crawford. The International Law Commission's Articles On State Responsibility: Introduction, Text and Commentaries, *op. cit*., pp. 285–295.
[170] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.,* Rule 22.
[171] Articles on State Responsibility, *op. cit*., Art. 51 (1).
[172] Articles on State Responsibility, *op. cit*., Art. 26 (5) of commentary; Art. 40 paras. 4-5 of commentary.
[173] United Nations General Assembly. International Covetant on Civil and Political Rights. New York City 16.12.1966, e.i.f. 23.03.1976, Art. 4 (2).
[174] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.,* Rules 39, 41.

important to mention, that the obligation to refrain from use of force is a principle limitation on an victim-State when using countermeasures.[175] However, some Experts of the International Group were on the position, that this principle would mean the inability of an injured State to respond to the wrongful use of force that does not reach the armed attack level by using forcible cyber or non-cyber operation. This will limit the victim-State to use proportionate response and respond using countermeasures below the use of force.[176]

An additional potential problem associated with the use of countermeasures in cyberspace relates to the fact that it may be difficult to limit the impact of a countermeasure by a State and not cause unintended harm to the third States. Due to the configuration of cyberspace, there is a risk that when trying to target one particular target, this may simply lead to harm to other targets. This does not mean, however, that countermeasures cannot inadvertently affect non-participating third States.[177]

Therefore, before taking countermeasures in cyberspace, the State must take all possible measures to avoid impacts on third parties and, if this is not possible, to keep the impact on third parties to a minimum. If a State realizes that, by resorting to certain countermeasures, they would spread uncontrolled and harm the systems of uninvolved third States, such countermeasures should be considered unlawful and the international responsibility of the initiating State should be initiated.[178]

Countermeasures should aim at encouraging the State against which they are being taken to comply with its international obligations, measures taken after the commission of harmful cyber operation is terminated are incompatible with the principle of legitimate countermeasures. Exceptions may be made when a State faces a series of incidents rather than a single illegal cyber operation, and it becomes clear that the State is either responsible for these attacks or clearly refraining from fulfilling its obligations to cease harmful cyber activities.[179]

---

[175] Articles on State Responsibility, *op. cit.*, Art. 51 (1). See also M. N. Schmitt. Tallinn Manual 2.0, *op. cit.*, Rule 22, note 11.
[176] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.*, Rule 22, notes 11, 12. See Oil Platform judgment, *op. cit.*, Judge Simma seperate opinion, para. 13.
[177] Articles on State Responsibility, *op. cit*., commentaries, p. 130, para. 5.
[178] R. Geiβ, H. Lahmann. Freedom and Security in Cyberspace: Shifting the Focus away from Military Responses towards Non-Forcible Countermeasures and Collective Threat-Prevention 2013, *op. cit*., pp. 640–641.
[179] *Ibid.*, pp. 638–639.

The relevant limitation is that only States may take countermeasures. Private entities, such as information technology companies, may be able to take effective countermeasures for their own protection, but they may not use them for this purpose, unless they do so at the direction of a State and in order to ensure compliance with an obligation that that State is obliged to take another State under international law.

The limitations and requirements make it difficult for a State to take the necessary countermeasures against harmful cyber operation, the pressure on injured State limit the use of countermeasures. Malicious cyber operations are often unexpected and can cause significant damage to critical infrastructure of the State, it is therefore important to clearly define the conditions under which an injured State must assume responsibility and take the countermeasures necessary to preserve its rights. As long as above mentioned countermeasures conditions are fulfilled and the requirements and limitations are complied with, countermeasures are legitimate to be used.

II. THE CASE STUDIES

2.1. Case selection criteria

Every day hundreds cyber operations take place in cyberspace. The majority of these cyber operations do not fall under the interest of the present thesis, as the thesis focuses on malicious cyber operations carried out by States. The five case studies examined below involve malicious cyber operations that arguably originated from States or State-sponsored actors (i.e. State attribution can be established) and were directed against the victim-State/s official databases, infrastructure and governmental departments. For the purpose of this thesis, the case studies are limited to cyber operations that caused significant monetary losses, threatened critical infrastructure or national security, had potential to cause loss of life and damage to physical property or involved a large scale data-leaks exposing personal information of users. The pre-existing international conflicts and political motives of the States will not be discussed in the case studies.

The case studies examined below rely on publicly available material such as official publication issued by governmental agencies, press releases, analyses of cybersecurity companies and press reports with the unofficial allegations. Due to the lack of public transparency in reporting on cyber operations and limited attribution cases, the author firstly conducted research to identify the harmful cyber operation that can meet the purpose and scope of the thesis. The author compared the lists of two depositories, the CSIS[180] and the CFR[181], and selected five harmful cyber operation based on the following criteria:

1) Cyber operations are alleged to have been initiated or conducted under the effective control of a State;
2) Cyber operations have caused significant damage to physical world or to governmental assets, such as altering data in the attacked networks and / or leaking of large amount of governmental data;
3) Cyber operations have been publicly discussed and commonly considered as major cyber operations;
4) Cyber operations have not constituted a malicious cyber operation to gain solely financial profit;

[180] Significant Cyber Incidents Since 2006, CSIS, *op. cit.*
[181] Cyber Operations Tracker, CFR, *op. cit.*

5) Cyber operations may have generated the response of the victim-State, such as response acts or official statements.

The selected cases must meet at least first four criteria out of the five criteria listed above. Three of the cases examined below relate to cyber operations against the United Stated, and were selected due to the availability of information about cyber operations against the United States and its relative openness of governmental officials to discuss cyber operations and responses. The three case studies in relation to the United States include: cyber operation against US private sector companies such as Google (Operation Aurora); the accessing and leaking of data of the Office of Personnel Management (OPM); and the accessing and leaking of data and destruction of computers of Sony Pictures Entertainment. Other case studies discussed below include the cyber operation against Iran's main fuel enrichment facility and particularly destructive global cyber operation WannaCry.

This chapter defines the time frame of events in each individual case, the damage suffered, the targets, the attribution of responsibility and the response of the affected State(s). The author focuses on the illegality of the cyber operations under discussion and countermeasures used by victim-States under international law governing cyberspace. However, it should be noted, that not a single State had taken responsibility for the harmful cyber operation as discussed below in the case studies. The author focuses on the responses and reactions of victim-States in order to examine whether States have referred to their rights under international law and on the alleged responsible State obligations under international law, such as for example due diligence. The analysis of the cases will be provided in Chapter 3.

2.2. Malicious cyber operations

2.2.1. Operation Aurora case

On January 12, 2010, Google announced in its official blog, that it has been subject to a sophisticated malicious cyber operation originating from China, which led to the theft of intellectual property.[182] According to the blog, the purpose of the attack was to access the e-mail accounts of Chinese human rights activists. However, only two Gmail accounts were accessed, and the e-mails contents were not exposed, except for information such as the date when account was created. Google also discovered that accounts of Gmail users in the United States, China, and Europe who are human rights advocates have been regularly accessed by third parties, but not specifically through the Google attack.[183] The same day after Google's announcement, Adobe announced that their corporate systems has also been hacked.[184] The same cyber operation was conducted against 30 more companies, in the areas of Internet, technology, finance, media, and chemical, as Yahoo, Dow Chemical and Symantec.[185]

This operation is known as "Operation Aurora" due to the fact that attackers utilized the Aurora Trojan horse program named directly from the unique lines of the malware code.[186] The Operation Aurora was initiated with spear phishing, in other words by sending a tailored e-mail from a trusted sender to induce the targeted individual to open the e-email. These e-mails contained links to a malicious web site based out of Taiwan that when clicked, initiated a certain series of events. The attackers took advantage of Internet Explorer web browser vulnerability, often called as a "zero-day exploit", that allowed to download a second piece of malware.[187] When the malware was installed, it set up a connection back out allowing the attacker to access the targeted systems.[188] It should be noted, that identifying such weaknesses requires a highly

[182] D. Drummond. A new approach to China. Google Official Blog, 12.01.2010. Accessible at: https://googleblog.blogspot.com/2010/01/new-approach-to-china.html (28.01.2020).
[183] *Ibid.*
[184] P. Prasad. Adobe Investigates Corporate Network Security Issue. Adobe Featured Blogs, 12.01.2010. Accessible at: https://www.blogs.adobe.com/conversations/2010/01/adobe_investigates_corporate_n.html (29.01.2020).
[185] K. J. Higgins. More victims of Chinese hacking attacks come forward. Dark Reading, 14.01.2010. Accessible at: https://www.darkreading.com/attacks-breaches/more-victims-of-chinese-hacking-attacks-come-forward/d/d-id/1132773 (29.01.2020). See K. Zetter. Google Hackers Targeted Source Code of More than 30 Companies. WIRED, 01.13.10. Accessible at: https://www.wired.com/2010/01/google-hack-attack/ (01.02.2020).
[186] J. Stewart. Operation Aurora: Clues in the Code. SecureWorks, 19.01.2010. Accessible at: https://www.secureworks.com/blog/research-20913 (01.02.2020).
[187] V. Phatak. Vulnerabilities, Exploits & Payloads, Oh My!. NSS Labs Blogspot, 12.03.2010. Accessible at: http://nsslabs.blogspot.com/2010/03/vulnerabilities-exploits-payloads-and.html (02.02.2020).
[188] McAfee Labs and McAfee Foundstone Professional Service. Protecting Your Critical Assets: Lessons Learned from Operation Aurora. White Paper 2010. Accessible at: https://www.wired.com/images_blogs/threatlevel/2010/03/operationaurora_wp_0310_fnl.pdf (02.02.2020).

skillful endeavor, which can be assumed to be possessed by the larger organizations or governmental authorities.

The Operation Aurora was a high-profile cyber operation against Google and the Symantec securities linked the attacks to the Chinese hacker group Hidden Lynx, indicating that the Operation Aurora was initiated with the full knowledge or under control of the Chinese government.[189] Chinese IP addresses were detected as primary servers in the attacks, as well as programming codes were written using Chinese code and tools.[190] The security expert Brian Krebs also linked the Operation Aurora to the Chinese government.[191] On February 19, 2010 the New York Times reporters published an article saying that experts believe that the attacks originated from two Chinese schools - Shanghai Jiaotong University and the Lanxiang Vocational School in the Shandong province.[192] The Chinese authorities, along with the universities, have denied any wrongdoing. Lanxiang Vocational School officially stated that investigations did not find any trace the attacks originated from their school. Rong Lanxiang, the founder of the Lanxiang School made a public statement claiming that the New York Time report is merely a fabrication.[193]

On January 21, 2010, the United States Secretary of State Hillary Clinton in her speech on Internet freedom called upon China to initiate a transparent investigation on the attack on Google.[194] China Foreign Ministry spokesman Ma Zhaoxu responded to the accusations by claiming that Chinese companies have also been hacked, adding that foreign companies need to adhere to laws and regulations of China and bear corresponding social responsibilities.[195] However, spokesman did not indicate that China will investigate the Google attacks. Another Foreign Ministry spokesman, Jiang Yu, responding to allegations that Chinese hackers were

[189] W. Howlett IV. The Rise of China's Hacking Culture: Defining Chinese Hackers. – California State University – San Bernardino 2016, p. 125.

[190] J. Stewart. Operation Aurora: Clues in the Code, *op. cit*.

[191] B. Krebs. New Clues Draw Stronger Chinese Ties to 'Aurora' Attacks. Krebs on Security, 20.01.2010. Accessible at: http://krebsonsecurity.com/2010/01/new-clues-suggest-stronger-chinese-role-in-aurora-attacks/ (03.02.2020).

[192] J. Markoff, D. Barboza. Two Chinese Schools Said to Be Tied to Online Attacks. New York Times, 19.02.2010. Accessible at: https://www.nytimes.com/2010/02/19/technology/19china.html (03.02.2020). See J. T. Areddy People's Republic of Hacking. The Wall Street Journal, 18.02.2010. Accessible at: http://www.wsj.com/articles/SB10001424052748704140104575057490343183 78 (03.02.2020).

[193] S. Beach. People's Republic of Hacking (Updated). China Digital Times, 20.02.2010. Accessible at: http://chinadigitaltimes.net/2010/02/chinese-school-denies-cyber-attack-on-google/ (03.02.2020).

[194] H. R. Clinton. Remarks on Internet Freedom, 21.01.2010. Accessible at: https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm (03.02.2020).

[195] CIOL Bureau. China Says Google, Foreign Firms Must Respect Laws. CIOL, 19.01.2010. Accessible at: https://www.ciol.com/china-google-foreign-firms-respect-laws/ (04.02.2020). See China Rebuts US Accusation of Hacker Attacks. China Daily, 31.10.2011. Accessible at: https://www.chinadaily.com.cn/china/2011-10/31/content_14011089.htm (04.02.2020).

responsible for the January 2010 Google attack, said Chinese law prohibits all forms of hacking and that the Internet is open in China.[196] Chinese officials have also questioned the Report to Congress on Foreign Economic Collection and Industrial Espionage[197], made by the Office of the National Counterintelligence Executive, arguing that the report is unprofessional and no comprehensive investigation was carried out. Finally, other officials refer the fact that most of the world's botnets are controlled from servers in the United States, hinting that Washington needed to clean up its own cybersecurity before accusing other countries of being responsible for the malicious cyber operations.[198]

Google entered the Chinese market with www.google.cn in 2006 and surrendered under strict regime of China's Internet censorship. However, after cyber operations in December 2009, Google reassessed its business in the country, which led to the relocation of Google servers for google.cn to Hong Kong in order to escape China's Internet filtering policy.[199] Cyber operations on Google that originated in China are argued to be part of a broader political strategy of China and pushed Google to withdraw from the Chinese market.[200] The Operation Aurora was not the first nor last cyber operation on private and government actors, assumed to be initiated by China. On June 1, 2011, Google announced that hackers based in China, Jinan, had compromised the personal email accounts of hundreds of top United States officials, military personnel and journalists.[201] The Operation Aurora is an example of how cyber operations can impact a tremendously large group of people, empowering the actors to conduct a subsequent cyber operation.

[196] H. Miguel, J. Markoff. Google Alerted Activists of Attacks. New York Times, 15.01.2010.
[197] Office of the National Counterintelligence Executive. Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011.
[198] Chines hacking: Impack on human Rights and Commercial Rule of Law. US Government Publishing Office. Hearing before the Congressional-executive Commission on China 113 Congress, 25.06.2013. Accessible at: https://www.govinfo.gov/content/pkg/CHRG-113hhrg81855/html/CHRG-113hhrg81855.htm (05.02.2020).
[199] D. Drummond. A new approach to China: an update. Google Official Blog, 22.03.2010. Accessible at: https://googleblog.blogspot.com/2010/03/new-approach-to-china-update.html (05.02.2020).
[200] C. A. Eunjung, E. Nakashima. Google Attack Part of Vast Campaign; Targets Are of Strategic Importance to China, Where Scheme Is Thought to Originate. The Washington Post, 14.01.2010.
[201] E. Grosse. Ensuring your information is safe online. Google Official Blog, 01.06.2011. Accessible at: https://googleblog.blogspot.com/2011/06/ensuring-your-information-is-safe.html (05.02.2020).

2.2.2. Stuxnet case

The Iran's main fuel enrichment facility Natanz and its uranium centrifuges began failing in the 2009, but it took nearly a year before the Natanz inspectors learned about this.[202] Around one thousand of Iran's six thousand centrifuges were destroyed over the course of this year.[203] In July 2010, a Belarus' computer security company VirusBlockAda researched Iran's computers troubleshoots and found out that the virus, later become known as the Stuxnet, used a "zero-day exploit".[204] The vulnerability allowed the Stuxnet virus to spread from one computer to anther through USB stick[205], that had a malware to infect Iran's nuclear facilities and destroy centrifuges by manipulating rotor speed and pressure levels inside the centrifuges.[206] The primary goal was to cause failures to the industrial facilities (equipment). If the Stuxnet was simply a gimmick, the adjustment of the frequencies would not be probably necessary. The Stuxnet virus was specifically designed to cause disruption slowly and gradually, and included a function that manipulated Iran's sensors to pretend that the manipulated functions worked as normal, which made a quick detection less likely to happen.[207] The Stuxnet virus was even called as the world's first digital weapon[208], causing physical damage to critical infrastructure.

In November 2010, President Ahmadinejad confirmed the presence of malware that affected the Natanz centrifuges.[209] The general secretary of Iran's Supreme National Security Council, also admitted that the incident had occurred,[210] however neither the President nor the general secretary have elaborated on the effects the Stuxnet virus inflicted.

Security scientist Ralph Langer claimed that the Stuxnet required tremendous amount of intelligence about the Natanz systems, which limits the list of possible attackers who would

---

[202] Stuxnet Analysis. European Union Agency for Network and Information Security (ENISA). Accessible at: http://www.enisa.europa.eu/media/press-releases/stuxnet-analysis (07.02.2020).
[203] E. Nakashima, J. Warrick. Stuxnet was the Work of U.S. and Israeli Experts, Officials Say. The Washington Post, 02.06.2012. Accessible at: http://www.washingtonpost.com/world/national-security/stuxnet-was-work-ofus-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html (07.02.2020).
[204] O. Kupreev, S. Ulasen. Trojan-Spy.0485 and Malware-Cryptor.Win32.Inject.gen.2 Review. VirusBlockAda 2010. See K. Zetter. How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History. Wired, 11.07.2011. Accessible at: http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet (07.02.2020).
[205] K. Zetter. How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History, *op. cit.*
[206] R. Langner. To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators tried to Achieve. The Langner Group 2013. Accessible at: https://www.langner.com/to-kill-a-centrifuge/ (08.02.2020).
[207] *Ibid.*
[208] K. Zetter. Countdown To Zero Day: Stuxnet And The Launch Of The World's First Digital Weapon 2015.
[209] E. T. Ahmandinejad. Iran's nuclear program hit by sabotage. The Washington Post, 29.11.2010. Accessible at: http://www.washingtonpost.com/wp-dun/content/article/2010/11/29/AR2010112903468.html (08.02.2020).
[210] D. Bednarz, E. Follath. Iran's chief nuclear negotiator: we have to be constantly on guard. Spiegel Online, 18.01.2011.

have the intelligence and resources to develop such advanced persistent cyber operation.[211] The allegations that the Stuxnet could have been initiated by a joint USA and Israel effort have a simple explanation, considering the facts that Iran was most affected by the malware, the USA and Israel have a very strong military capabilities and Israel was threatened by Iran's nuclear program.[212] It is important to note, that neither the USA nor Israel has denied the accusations that of involvement in the Stuxnet case.

The Russian, Chinese or German origin of the Stuxnet can be also considered. Russia being the only supplier of fuel for Iran, could have economically benefit from the Iran's problem, as well as China could have prevented the Iran's nuclear proliferation. Germany was also mentioned as a possible creator of the Stuxnet, due to the deep knowledge of systems built by Siemens, being a German company, that were used in the Natanz facility and contained one of five zero-day exploits that allowed the worm access to the infected systems.[213] The fact that the Stuxnet code had five zero-day exploits, which would have been worth millions to private hackers in terms of its resale value, again implied that there was serious power behind the attack, almost guaranteeing that such an attack came from a State with means to employ such cyber operation. Moreover, the information alone was nearly dispositive, since few States had the motivation and the means to target Iran's nuclear centrifuges.[214]

Finally, the analysis written one year before the Stuxnet coming to the light in July 2009 by Dan Williams, provided that director of the United States Cyber Consequences Unit, Scott Borg, said that Israel can be assumed to have advanced cyber capabilities with the possibility to control or crash uranium enrichment plants. Furthermore, as a way to access the computers, Scott Borg proposed the infected USB stick as a tool.[215]

[211] R. Langner. To Kill a Centrifuge, *op. cit.*
[212] W. J. Broad, J. Markoff, D. E. Sanger. Israeli Test On Worm Called Crucial In Iran Nuclear Delay. The New York Times, 15.01.2011. Accessible at: https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=2&hp=&pagewanted=print (08.02.2020).
[213] Stuxnet Facts Report: A Technical and Strategic Analysis. LTC Marco De Facto. NATO CCD COE 2012, pp. 26-30.
[214] L. Bilge, T. Dumitras. Before We Knew It: An Empirical Study Of Zero-Day Attacks In The Real World. Procedings of the 2012 ACM Conference on Computer and Communications Security 2012.
[215] D. Williams. Analysis-wary of naked force, Israelis eye cyberwar on Iran. Reuters, 7.07.2009. Accessible at: https://www.reuters.com/article/idUSLV83872 (08.02.2020).

2.2.3. Sony Pictures Entertainment case

On November 24, 2014, attackers, calling themselves the "Guardians of Peace", raided the computer network of Sony Pictures Entertainment - on every employee's screen at Sony Pictures headquarters in California flashed a red skull.[216] The attackers downloaded more than one hundred terabytes of Sony Pictures' data, including unreleased movies, internal communications, scripts, and leaked thousands of confidential documents online while erasing them from the Sony Pictures' systems.[217] The attack affected more than 3000 computers and 800 servers.[218]

The attackers are known for threatening to release more documents of Sony Pictures, unless Sony Pictures cancels the release of *The Interview*, the Sony Pictures' political-comedy film on North Korea leader Kim Jong Un.[219] As a result of those threatening's, the comedy film was not released[220], as well as many theaters refused to screen the film.[221] However, the cancellations were made after the attacks have caused tens of millions of dollars in damage, including the destruction of Sony Pictures' information systems, damage to thousands of computers, loss of millions of dollars in revenue and the leakage of trade secrets.[222]

On December 19, 2014, the Federal Bureau of Investigation (hereinafter referred to as the FBI) declared that it has information to link the Sony Pictures' attack code, infrastructure, and overall design to have been carried out by North Korea.[223] On the same day, the United States, unprecedentedly, officially condemned the government of North Korea for the cyber operation

---

[216] A. Peterson. The Sony Pictures Hack, Explained. The Washington Post, 18.12.2014. Accessible at: http://www.washingtonpost.com/news/the-switch/wp/2014/12/18/thesony-pictures-hack-explained (10.02.2020).
[217] D. Robb. Sony Hack: A timeline. Deadline, 22.12.2014. Accessible at: http://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interview-north-korea-1201325501 (10.02.2020). See P. Elkind. Sony Pictures: Inside the Hack of the Century: Part I. Fortune, 25.06.2015. Accessible at: http://fortune.com/sony-hack-part-1 (10.02.2020).
[218] S. Kroft. The Attack on Sony. CBS News, 12.04.2015. Accessible at: http://www.cbsnews.com/news/north-korean-cyberattack-on-sony-60-minutes (10.02.2020).
[219] C. Shoard. Sony Hack: The Plot To Kill The Interview – a Timeline So Far, The Guardian, 18.12.2014. Accessible at: http://www.theguardian.com/film/2014/dec/18/sony-hack-the-interview-timeline (10.02.2020).
[220] A. Peterson. The Sony Pictures Hack, Explained, *op.cit.*
[221] L. Brinded. The Interview Tipped to Cost Sony Pictures $200m Following Hack and Cancellation. International Business Times, 18.12.2014. Accessible at: http://www.ibtimes.co.uk/interview-tipped-cost-sony-pictures-200m-total-following-hack-cancellation-1480157 (10.02.2020).
[222] A. Hess. Inside the Sony Hack. Slate, 22.11.2015. Accessible at: http://www.slate.com/articles/technology/users/2015/11/sony_employees_on_the_hack_one_year_later.html (11.02.2020). See L. Brinded. The Interview Tipped to Cost Sony Pictures $200m Following Hack and Cancellation, *op.cit.*; L. Richwine. Cyber Attack Could Cost Sony Studio as Much as $100 Million. Reuters, 09.12.2014. Accessible at: http://www.reuters.com/article/us-sony-cybersecurity-costs-idUSKBN0JN2L020141209 (11.02.2020).
[223] Update on Sony Investigation. FBI National Press Office, *op.cit.*

targeting Sony Pictures.[224] The observers recognized that the United States' response was a main example of a State officially accusing another of a malicious cyber operation.[225] In a special year-end press release, President Obama said that the United States would respond proportionally in the manner of its choosing.[226] Since then, international legal and technology experts have been actively discussing the attribution of the Sony attack whether to North Korea or not.[227] Director James Comey announced with the high confidence that the attack came from North Korea,[228] and the NSA Director Michael Rogers also said that he was confident that this was North Korea.[229] Some experts however noted, that United States action could set a dangerous precedent.[230]

The North Korean Ministry of Foreign Affairs issued a statement, prior to the release of *The Interview*, declaring that North Korea would take a "*decisive and merciless countermeasure*" if Sony Pictures released the film.[231] Thus, it may be assumed, that Sony Pictures officials were aware that North Korea could take measures to reach their political goals. The FBI representatives also noted similarities of Sony Pictures attack with the DarkSeoul attack, a previous malicious cyber operation launched by North Korea against South Korean banks. They also found evidence that the malware was created on computers with Korean language settings and the data revealed traces of an Internet attack that also pointed to North Korea.[232]

[224] J. Kerry. Secretary of State. Condemning Cyber-Attacks by North Korea. Press Release, 19.12.2014. Accessible at: https://2009-2017.state.gov/secretary/remarks/2014/12/235444.htm (11.02.2020).
[225] H. Lin. Learning from the Attack Against Sony. Lawfare, 23.01.2015. Accessible at: http://www.lawfareblog.com/learning-attack-against-sony (11.02.2020).
[226] Remarks by the President in Year-End Press Conference. The White House, 19.12.2014. Accessible at: http://www.whitehouse.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference (12.02.2020).
[227] K. Zetter. Critics Say New Evidence Linking North Korea to the Sony Hack Is Still Flimsy. Wired, 08.01.2015. Accessible at: http://www.wired.com/2015/01/critics-say-new-north-korea-evidence-sony-still-flimsy (11.02.2020).
[228] P. Elkind. Inside the Hack of the Century: Part III. Fortune, 27.06.2015. Accessible at: http://fortune.com/sony-hack-final-part (12.02.2020).
[229] S. Frizell. NSA Director on Sony Hack: 'The Entire World is Watching'. Time, 08.01.2015. Accessible at: http://time.com/3660757/nsa-michael-rogers-sony-hack (12.02.2020).
[230] R. M. Lee. The Feds Got the Sony Hack Right, but the Way They're Framing It Is Dangerous. Wired, 10.01.2015. Accessible at: http://www.wired.com/2015/01/feds-got-sony-hack-right-way-theyre-framing-dangerous (12.02.2020).
[231] M. Cieply, B. Barnes. Sony Cyberattack, First a Nuisance, Swiftly Grew Into a Firestorm. New York Times, 30.12.2014. Accessible at: https://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html (13.02.2020).
[232] P. Elkind. Inside the Hack of the Century: Part III, *op. cit.*

On December 24, 2014, the Internet in North Korea was shut down for around nine hours and the connection was interrupted for the next two days. This disruption of the Internet connection is supposed to be a covert reaction to a Sony Pictures Entertainment operation.[233]

On January 2, 2015, the United States declared the imposition of new sanctions to North Korea as a response for destructive economical efforts on the United States company and the limitation of free expression of artists and other individuals.[234] The sanctions were imposed on three entities and ten individuals who had connections with the North Korea government, which included the seizure of property held in the United States.[235] There is no publicly available information on the evidence explaining why especially these ten individuals and three entities were sanctioned.

[233] C. Strohm. North Korea Web Outage Response to Sony Hack, Lawmaker Says. Bloomberg Politics, 17.03.2015. Accessible at: https://www.bloomberg.com/politics/articles/2015-03-17/north-korea-web-outage-was-response-tosony-hack-lawmaker-says (13.02.2020).

[234] White House Press Release. Statement by the Press Secretary on the Executive Order Entitled "Imposing Additional Sanctions with Respect to North Korea", The White House, 02.01.2015. Accessible at: https://obamawhitehouse.archives.gov/the-press-office/2015/01/02/statement-press-secretary-executive-order-entitled-imposing-additional-s (13.02.2020).

[235] Sony Cyber-attack: North Korea Faces New US Sanctions. BBC NEWS, 03.01.2015. Accessible at: http://www.bbc.com/news/world-us-canada-30661973 (14.02.2020).

2.2.4. The United States Office of Personnel Management case

The Office of Personnel Management is responsible United States government department for human resources housing a database of identifying information on personnel, including, but not limited to, the security clearances, data of the applicants along with the information on family members and friend.[236] On June 4, 2015, the Office of Personnel Management revealed the cyber intrusion into its systems, that compromised around 4.2 million federal employees.[237] Later in June, the Office of Personnel Management announced that around twenty one million people was affected by a theft of confidential data as a separate cyber incident.[238]

Due to the fact that stolen information was not only sensitive, but could potentially undercover the United States agents and put them at risk, the Office of Personnel Management data breaches were one of the most significant cases in 2015 in the United States.[239] Notwithstanding, in 2014, hackers had also targeted data of thousands of employees of the Office of Personnel Management, looking for the information on top-secret security clearances.[240]

There is no exactly known how the access to the Office of Personnel Management network was gained, it is known that the attackers compromised a junction box with access to virtually the entire Office of Personnel Management network. The attackers were able to install a variant of PlugX malware, which provided a method of exporting data and securely accessing infected systems. There were many security and infrastructure holes, such as the inability to use encryption for sensitive data and the lack of two factor authentication. Once the attackers had

[236] OPM to Notify Employees of Cybersecurity Incident. Office of Personnel Management Press Release, 04.06.2015. Accessible at: https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/ (15.02.2020). See D. Bisson. The OPM breach: Timeline of a Hack. Tripwire, 29.06.2015. Accessible at: https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-opm-breach-timeline-of-a-hack/ (15.02.2020); OPM Announces Steps to Protect Federal Workers and Others from Cyber Threats. Office of Personnel Management Press Release, 09.07.2015. Accessible at: https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats/ (15.02.2020).

[237] D. Bisson. The OPM breach: Timeline of a Hack, *op. cit.*

[238] OPM Announces Steps to Protect Federal Workers and Others from Cyber Threats, *op. cit.*

[239] K. McGettigan. OPM's 2018 - 2022 Strategic Plan. Office of Personnel Management, 12.02.2018. Accessible at: https://www.opm.gov/blogs/Director/2018/2/12/OPMs-2018---2022-Strategic-Plan (15.02.2020). See B. I. Koerner. Inside the Cyberattack That Shocked the US Government. Wired, 23.10.2016. Accessible at: https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/ (15.02.2020).

[240] M. S. Schmidt, *et al*. Chinese Hackers Pursue Key Data on U.S. Workers. The New York Times, 09.07.2014. Accessible at: https://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html (16.02.2020).

the extended credentials, they had all the keys to the system to capture the data.[241] There were also reporting delays, as first signs of a breach appears to have occurred at least two-three year prior to the Office of Personnel Management announcement in June 2015. In June 2014, United States Investigation Services reported interfering to the Office of Personnel Management.[242]

On June 24, 2015, James Clapper, director of National Intelligence, announced at an intelligence conference that China is a main suspect of the malicious cyber operations against the Office of Personnel Management of the United States. However, on the same conference, Michael Rogers, director of the National Security Agency, refused to discuss the possible attribution.[243] It should be noted, that investigating these malicious cyber operations is difficult, not only because of the sensitive nature of the targets and the consequences, but also because the alleged attacker was over time believed to be the advanced permanent threat sponsored by China, with a high level of skills, resources and determination.[244] Furthermore, president Obama considered imposing sanctions against actors who were engaged in that cyber operation.[245]

China called the speculations of its role in the Office of Personnel Management breach irresponsible and unscientific.[246] Moreover, during the annual session of the Unite States - China Strategic & Economic Dialogue, the officials from both countries did not discuss the official outcomes of the mentioned above breaches.[247] However, Chinese authorities later arrested possible hackers who were allegedly connected to the breach of Office of Personnel Management' systems. However, it could be seen as a way to lessen tensions with United

[241] J. Fruhlinger. The OPM hack explained: Bad security practices meet China's Captain America. CSO Online, 06.11.2018. Accessible at: https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html (16.02.2020).
[242] J. Chaffetz, *et al*. The OPM Data Breach: How The Government Jeopardized Our National Security For More Than A Generation. Committee on Oversight and Government Reform,114th Congress 2016, pp. 5–7.
[243] D. Paletta. U.S. Intelligence Chief James Clapper Suggests China Behind OPM Breach. The Wall Street Journal, 25.06.2015. Accssible at: http://www.wsj.com/articles/SB10007111583511843695404581069863170899504 (16.02.2020); D. Welna. In Data Breach, Reluctance to Point the Finger at China. National Public Radio, 02.07.2015. Accessible at: https://www.npr.org/sections/parallels/2015/07/02/419458637/in-data-breach-reluctance-to-point-the-finger-at-china (16.02.2020).
[244] D. Bisson. The OPM breach: Timeline of a Hack, *op. cit.*; J. Fruhlinger. The OPM hack explained, *op. cit.;* See B. I. Koerner. Inside the Cyberattack That Shocked the US Government, *op. cit.*
[245] M. D. Shear, S. Shane. White House Weighs Sanctions After Second Breach of a Computer System. The New York Times, 12.06.2015. Accessible at: https://www.nytimes.com/2015/06/13/us/white-house-weighs-sanctions-aftersecond-breach-of-a-computer-system.html (16.02.2020).
[246] Ministry of Foreign Affairs of the People's Republic of China. Foreign Ministry Spokesperson Hong Lei's Regular Press Conference, 05.06.2015.
[247] U.S. Department of the Treasury. 2015 U.S.-China Strategic and Economic Dialogue U.S. Fact Sheet—Economic Track, 25.06.2015. Accessible at: https://www.treasury.gov/press-center/press-releases/Pages/jl0092.aspx (17.02.2020).

States.[248] The United States were informed about the arrests, but no results on Chinese investigation were published.

The director of the National Counterintelligence and Security Center, William Evanina, observed that the possibility that criminal individuals, rather than a State, has stolen data is highly unlikely, as the stolen data did not leak or any financial profit was not gained. William Evanina argued that government took the data from an intelligence perspective[249], but still he did not publicly attributed responsibility to China.

It is argued, that the United States Office of Personnel Management hack is linked to the Marriott Starwood hotel brand malicious cyber operation[250] and the 2017 Equifax harmful cyber operation,[251] that similarly did not result in an upload of personal data on the dark net. It is believed that all these operations are part of a Chinese operation to collect a huge database, with the intention of using big data collection methods to learn about the United States government officials and intelligence agencies. For example, data on the United Stated officials who are in financial trouble can be used by Chinese intelligence to identify potential targets and to recruit those officials as spies.[252]

---

[248] E. Nakashima. Chinese Government Has Arrested Hackers it Says Breached OPM Database. The Washington Post, 02.12.2015. Accessible at: https://www.washingtonpost.com/world/national-security/chinese-government-has-arrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb_story.html (17.02.2020).

[249] C. Strohm. Hacked OPM Data Hasn't Been Shared or Sold, Top Spy-Catcher Says. Bloomberg, 28.09.2017. Accessible at: https://www.bloomberg.com/news/articles/2017-09-28/hacked-opm-data-hasn-t-been-shared-or-sold-top-spy-catcher-says (17.02.2020).

[250] On November 30, 2018, Marriott International announced that it has been a victim of a malicious cyber operation, leading to the theft of the personal information of 500 million Starwood properties customers. Marriott announced that in the beginning of September 2018, that internal security tool indicated an attempt to access the Starwood guest reservation database by the unknown entity. With the help of external cybersecurity experts, it was discovered that unauthorized access to Starwood's network occurred as early as 2014 and that a third party copied and encrypted customer information and took steps to remove it from Starwood's database. Marriott said the disclosed data included passwords, email addresses, departure and arrival dates and passport details
See C. Bing. Exclusive: Clues in Marriott hack implicate China – sources. Reuters, 06.12.2018. Accessible at: https://www.reuters.com/article/us-marriott-intnl-cyber-china-exclusive/exclusive-clues-in-marriott-hack-implicate-china-sources-idUSKBN1O504D (18.02.2020).
Marriott Announces Starwood Guest Reservation Database Security Incident. Martiott, 30.11.2018. Accessible at: https://news.marriott.com/2018/11/marriott-announces-starwood-guest-reservation-database-security-incident/ (18.02.2020).

[251] On September 7, 2017, Equifax, consumer credit reporting agency, announced that it had been a victim of a malicious cyber operation resulting in a massive data breach - 148 million US citizens' sensitive personal data were compromised including names, dates of birth, Social Security numbers, and driver's license numbers. Moreover, 209 000 credit card numbers were also stolen.
See Equifax Announces Cybersecurity Incident Involving Consumer Information. Equifax Security, 07.09.2017. Accessible at: https://www.equifaxsecurity2017.com/2017/09/07/equifax-announces-cybersecurity-incident-involving-consumer-information/ (08.02.2020). See J. Fruhlinger. Equifax data breach FAQ: what happened, who was affected, was the impact? CSO Online, 12.02.2020. https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html (18.02.2020).

[252] M. S. Chen. China's Data Collection on US Citizens: Implications, Risks, and Solutions. - 15 Journal of Science Policy & Governance 2019 (1), p. 11.

2.2.5. WannaCry case

On May 12, 2017 a ransomware malicious cyber operation, known as the WannaCry, affected more than 200,000 computers in at least 100 countries by encrypting computer files and demanding $300 in crypto currency from users in order to restore access. It was made possible because of the vulnerability in older versions of Microsoft Windows, that has not installed the updated versions.[253] The companies such as Renault, FEDEX and Deutsche Bahn, were affected, as well as thousand computers of the Russian Interior Ministry[254] and twenty-five percent of India's Andhra Pradesh police department network.[255] However, the biggest impact was on the United Kingdom's National Health Service (hereinafter referred to as NHS) affecting at least 80 out if the 236 components of the NHS serving either geographic areas or performing specialized functions, and 603 primary care and other NHS organisations across the United Kingdom. Thousands of operations and appointments were cancelled, the NHS personnel could not access their documents and therefore were unable to update patient records, and thousands of pieces of medical equipment were locked.[256] A Department of Health and Social Care reported that the cost to the NHS during the attack was approximately £19 million, due to the lost output and a further £0.5 million for additional IT support. The report also estimated a further £73 million input on further IT support required to recover data and restore systems.[257]

The United Kingdom's National Cyber Security Centre believed that the Lazarus Group, which has ties to the North Korean government, launched the operation.[258] On December 18, 2017, the Wall Street Journal editorial by Thomas P. Bossert, who was the assistant to the president for homeland security and counterterrorism, announced that the United States attributes the

[253] Report by the Comptroller and Auditor General. Investigation: WannaCry cyber attack and the NHS. National Audit Office, 25.04.2018.
[254] A. E. Kramer. Russia, This Time the Victim of a Cyberattack, Voices Outrage. The New York Times, 14.05.2017. Accessible at: https://www.nytimes.com/2017/05/14/world/europe/russia-cyberattack-wannacry-ransomware.html?smid=tw-nytimesworld&smtyp=cur&_r=0&mtrref=www.bbc.com (20.02.2020).
[255] A. Pradesh. WannaLaugh: Faced with WannaCry attack, AP cops unplug systems and save data. The New Indian Express, 13.05.2017. Accessible at: https://www.newindianexpress.com/states/andhra-pradesh/2017/may/13/wannalaugh-faced-with-wannacry-attack-ap-cops-unplug-systems-and-save-data-1604416.html (20.02.2020).
[256] Report by the Comptroller and Auditor General. Investigation: WannaCry cyber attack and the NHS 2018, *op. cit.*
[257] Cyber Security Policy. Securing cyber resilience in health and care. Progress update October 2018. Department of Health and Social Care. Accessible at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747464/securing-cyber-resilience-in-health-and-care-september-2018-update.pdf (21.02.2020).
[258] G. Corera. NHS cyber-attack was "launched from North Korea". BBC News, 16.06.2017. Accessible at: https://www.bbc.com/news/technology-40297493 (21.02.2020).

WannaCry ransomware malicious cyber operation to North Korea.[259] On December 19, 2017, the British government made public press release, arguing that it is likely that North Korean actors were behind the WannaCry operation, in particular the Lazarus Group.[260] The Canada[261], New Zealand[262], Japan[263] and Microsoft[264] have also come to the same conclusion – North Korea was behind the WannaCry operation. North Korea denied any link with the WannaCry ransomware malicious cyber operation.[265] The attribution of responsibility to North Korea by multiple States is clearly made, however, no act of response has been reported. The United Kingdom security minister called on States to develop a doctrine of deterrence to prevent future harmful cyber operation.[266] Microsoft has also called on States to adopt new Digital Geneva Convention to have clear rules and limitations on such cyber operation whether they violate the international law or are in line with it.[267] However, there is no publicly known official response by any State taken against North Korea. With regard to possible responses, an injured State may take countermeasures in response to another State's malicious cyber operation aimed at ending it or at forcing the responsible State to make reparations. As the WannaCry operation has ended, countermeasures are now available only to compel North Korea to pay reparations, such as a compensation to the injured States. Like countermeasures, the plea of necessity is only available to end harmful cyber-operations, and thus it will no longer be available.

---

[259] T. P. Bossert. It's Official: North Korea Is Behind WannaCry. WSJ, 18.12.2017. Accessible at: https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537?shareToken=st2d38565d59c24132b421a4b03edb68b5&reflink=article_email_share (21.02.2020).

[260] Foreign & Commonwealth Office and Lord Ahmad of Wimbledon. Foreign Office Minister condemns North Korean actor for WannaCry attacks. 19.12.2017. Accessible at: https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks (21.02.2020). See Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea. The White House, 19.12.2017. Accessible at: https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/ (21.02.2020).

[261] G. Bossenmaier. CSE Statement on the Attribution of WannaCry malware. Communications Security Establishment, 19.12.2017. Accessible at: https://www.cse-cst.gc.ca/en/media/2017-12-19 (22.02.2020).

[262] New Zealand concerned at North Korean cyber activity. National Cyber Security Center, 20.12.2017. Accessible at: https://www.ncsc.govt.nz/newsroom/new-zealand-concerned-at-north-korean-cyber-activity/ (22.02.2020).

[263] The U.S. Statement on North Korea's Cyberattacks (Statement by Press Secretary Norio Maruyama). Ministry of Foreign Affairs of Japan, 20.12.2017. Accessible at: https://www.mofa.go.jp/press/release/press4e_001850.html (21.02.2020).

[264] B. Smith. Microsoft ad Facebook disrupt ZINC malware attack to protect customers and the internet from ongoing cyberthreats. Microsoft, 19.12.2017. Accessible at: https://blogs.microsoft.com/on-the-issues/2017/12/19/microsoft-facebook-disrupt-zinc-malware-attack-protect-customers-internet-ongoing-cyberthreats/ (22.02.2020).

[265] M. Nichols. North Korea saya linking cyber attacks to Pyongyang is "ridiculous". Reuters, 19.05.2017. Accessible at: https://www.reuters.com/article/us-cyber-attack-northkorea/north-korea-says-linking-cyber-attacks-to-pyongyang-is-ridiculous-idUSKCN18F1X3 (22.02.2020).

[266] R. Browne. UK Government: North Korea Was Behind the WannaCry Cyber-attack that Crippled Health Service. CNBC, 27.10.2017. Accessible at: https://www.cnbc.com/2017/10/27/uk-north-korea-behind-wannacry-cyberattack-that-crippled-nhs.html (22.02.2020).

[267] B. Smith. The Need for a Digital Geneva Convention. Microsoft Blog, 14.02.2017. Accessible at: https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention (23.02.2020).

III. POSSIBLE USE OF COUNTERMEASURES BY VICTIM-STATE

3.1. Attribution of responsibility to a State

When a malicious cyber operation occurs, the victim-State is eager to establish the actor of an operation to respond against the responsible State. However, as it was discussed in the Chapter 1, is it difficult to clearly attribute responsibility for an unlawful malicious cyber operation to a responsible State or non-State actor. Based on the law of State responsibility, States are only responsible for acts attributable to the State that are in breach of international obligation.[268] The case studies show, that despite the increasingly common and destructive nature of State sponsored malicious cyber operations,[269] it is difficult to locate the exact type of unlawfulness for these malicious cyber operations that fall below the armed attack threshold. Scholars have recognized the lack of clear application for low intensity malicious cyber operations and sought solutions[270]. Some have tried to broaden current international legal categories of impermissible conduct to cover these operations.[271] Others argued that a new treaty or legal regime is needed before international law could prohibit low intensity harmful cyber operations.[272]

Bearing in mind, that there is no established body of international law that defines the exact legal criteria and standards of evidence to determine whether cyber operation should be attributed to a State, individual or a group,[273] States are expected to follow standard of reasonableness when attributing State responsibility, but they are not required to provide information on which they relied in determining attribution, thus absolute certainty is not required.[274] There is also no internationally recognized way how victim-States can use legal attribution of cyber operations. Secret intelligence agencies may enable State responsibility to be assigned to a State with full or near-full confidence, but, since national security interests, such as protecting intelligence sources or maintaining the secrecy of technological capabilities, policymakers may refrain from publicly asserting attribution of State responsibility or

[268] Articles on State Responsibility, *op. cit*., Art. 2.
[269] S. Watts. Low-Intensity Cyber Operations and the Principle of Non-Intervention. – J. D. Ohlin *et al*.(eds.). Cyber War: Law And Ethics For Virtual Conflicts 2015, pp. 249-250.
[270] See B. Walton. Duties Owed: Low-Intensity Cyber Attacks and liability for Transboundary Torts in International Law. – 126 The Yale Law Journal 2017 (5).
[271] W.G. Sharp. Sr. Cyberspace and The Use Of Force. Ageis Research Corp 1999, pp. 129-133.
[272] See J. Goldsmith. Cybersecurity Treaties: A Skeptical View. - Hoover Institution, Stanford University 2011, for an analysis of why comprehensive treaty regimes are unlikely in cyberspace.
[273] M. Roscini. Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations. - 50 Texas International Law Journal 2015, p. 233.
[274] Reasonableness means that States should act reasonably when gathering information and provide conclusions under particular circumstances. B. J. Egan. International Law and Stability in Cyberspace, *op. cit.*, p. 177.

indicating its grounds.[275] For example, the United States and the United Kingdom argue that international law does not require a full transparency as a precondition for attributing State responsibility.[276]

The case studies examined in Chapter 2 show the difficulties in attributing State responsibility for harmful cyber operations. In three of five cases no official attribution was made. However, based on investigations conducted by cybersecurity companies, the nationality of actors was suggested; however, this does not endorse any attribution. In the Aurora Operation case and the OPM case, the attribution was assumed to Chinese hackers with the strong indication that operations were State sponsored, however, the assignment of responsibility to government was not officially made. In the Stuxnet case, the presence of malware was confirmed by the Iran's president, but no elaboration on the attribution to any State or non-State actor was presented. It can be argued, that public attribution may have jeopardized the secrecy of intelligence sources and revealed their technological capabilities in relation to those harmful cyber operations. In the same vein, resorting to uncover technological capabilities may expose the technology to actors who could potentially imitate such destructive malwares and use them against their targets.

In two case studies, the findings of an intelligent agencies appear to be sufficient for States to attribute responsibility to North Korea – in Sony Picture Entertainment case and WannaCry case. In Sony Picture Entertainment case the attribution was followed by public sanctions. It can be argued, that covert countermeasures were also made, such as the shutdown of the internet in North Korea.

The WannaCry attribution can be distinguished from other cases examine in Chapter 2, due to the public and official attribution by a group of victim-States. The author is of the opinion, that recent collective attribution in WannaCry case shows that there could be a shift in international community approach to attribution of State responsibility. This may signify the beginning of cooperation between States to develop firstly non-binding norms governing cyberspace, that

[275] M. Roscini. Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations, *op. cit.,* p. 272.
[276] B. J. Egan. International Law and Stability in Cyberspace, *op. cit.,* p. 177; J. Wright. The United Kingdom Attorney General. Cyber and International Law in the 21st Century. London 23.05.2018. Accessible at: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century (01.03.2020); H. H. Koh. US Department of State, Speech delivered at USCYBERCOM Inter-Agency Legal Conference at Fort Meade, Maryland: International Law in Cyberspace, 18.09.2012. Accessible at: http://www.harvardilj.org/wp-content/uploads/2012/12/Koh-Speech-to-Publish1.pdf (01.03.2020).

can lead to the establishment of new international norms on evidence relating to cyberspace. It is possible, that some of these rules will be enshrined in customary international law in the future.

As it is established, in order to lawfully respond with countermeasures, the internationally wrongful act should be attributable to a State under the law of State responsibility.[277] When analysing the case studies, the author encountered the difficulty, that there is no required standard of proof under international law governing cyberspace and that the limits and extent to which information underlying attribution should be transparent are under question. In the Sony Pictures Entertainment case, the United States condemned North Korea for this malicious cyber operation, but did not provide any proof of such attribution.[278] Tallinn Manual did not resolve this question also.

There is legal uncertainty surrounding the attribution process, leading to the remaining of States silence in cyberspace. As a result of such imprecisions in international law in regards to cyberspace, the victim-States often remain ambiguous in relation to their activities and responses in cyberspace, which can be seen as an act of non-disclosure of their vulnerabilities or possible political decisions. Notwithstanding, such cautions approach of non-making public statements or even not acknowledging that a malicious cyber operation has ever been conducted, leads to the exacerbation of using unrecognized operational techniques by both States and non-State actors, such as, for example, proxy looser relationship with a State, when funding is received, but no specific instructions are provided.[279] It may be concluded that this ambiguous approach by States not to resort to public and vigorous attribution of cyber operations implies a failure to attest to State responsibility. It should be noted, that this thesis relies on publicly open materials, meaning that we cannot fully understand the implications and possible responses of States to the harmful cyber operations conducted against them.

[277] Articles on State Responsibility, *op. cit*., Art. 2 (a).
[278] J. Kerry. Secretary of State. Condemning Cyber-Attacks by North Korea, *op. cit*.
[279] T. Maurer. Cyber Mercenaries: The State, Hackers, And Power. Cambridge University Press 2018, pp. 151-152.

3.2.Breach of international legal obligation

Malicious cyber operations that fall under armed attack threshold may violate other rules of international law, such as the sovereignty of a State if the consequences are significant enough.[280] However, many scholars challenge the existence of a concept of prohibition of a violation of sovereignty that applies beyond the prohibition against the use of force and the rule of non-intervention.[281] In particular, a question is raised as to whether international law prohibited cyber operations other than those that reached the scale and effect of the use of force or that involuntarily interfered with the inherent functions of other governments, thereby violating the rule of non-intervention.[282]

The case studies examined in Chapter 2 do not clarify the legal framework of breach of international obligation under international law governing cyberspace. There were diplomatic and law enforcement reactions to the OPM case and relatively strong reaction to the Sony Pictures Entertainment case, which can be seen as a support for a broader application of the sovereignty rule. However, when the United States condemned North Korea for the Sony Pictures Entertainment operation, the secretary vaguely stated that North Korea violated international norms, but without explicitly referring to any violation of international law[283], as well as President Obama called North Korea's harmful cyber operation as an act of cyber vandalism.[284] Thus, it can be concluded, that States remain silent not only in regard to the attribution, but also do not explicitly refer to any infringement of international law governing cyberspace. In WannaCry case, the victim-States also did not explicitly refer to the violation of sovereignty or any other specific rule derived from it. Thus, it is reaffirmed by the case studies that States recognize the existence of a challenges in international law governing cyberspace.

The rule of non-intervention, which is derived from the sovereignty principle, is a part of customary international law under which a State should not intervene in the internal or external affairs of another State.[285] According to the Tallinn Manual coercion is an constructive act

[280] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.,* Rule 4, note 17 and pp. 20-21.
[281] See G. Corn. Tallinn Manual 2.0 – Advancing the Conversation. Just Security, 15.02.2017. Accessible at: https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation (03.03.2020).
[282] E. T. Jensen. The Tallinn Manual 2.0: Highlights and Insights. – 48 Georgetown Journal of International Law 2017, pp. 735, 743.
[283] J. Kerry. Secretary of State. Condemning Cyber-Attacks by North Korea, *op. cit*.
[284] E. Bradner. Obama: North Korea's Hack Not War, But 'Cybervandalism,'. CNN Politics, 24.12.2014. Accessible at: http://www.cnn.com/2014/12/21/politics/obama-north-koreas-hack-not-war-but-cyber-vandalism (04.03.2020).
[285] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.,* Rule 66; Declaration on Principles of International Law concerning Friendly Relations 1970, *op. cit.*

aimed at depriving another State of its freedom of choice, such as forcing that State to involuntarily refrain from any action or act in an involuntary way.[286] The coercion is a prerequisite for the non-intervention rule.[287] However, the non-intervention rule may be breached without the condition of coercion when the act captures essential governmental functions.[288] The case studies examined above do not bring States closer as to whether States accept the non-intervention rule under international law as it is or tend to broaden the rule in question. It can be argued, that out of five case studies the Stuxnet operation can be qualified as a breach of non-intervention principle, because it aimed to prevent a State from taking a particular course of action. Assuming that operation was conducted by a State or States acting jointly, it remained below the threshold of an armed attack, because it caused neither human casualties nor significant long-term damage, nor the disruption of critical infrastructure vital to the functioning of the injured State. The operation may be also described as the use of force, but not in the sense of armed attack, as it reportedly caused material damage and was intrusive enough to consider it a use of force, although Iran underestimated its effect and did not claim that it was a use of force or an armed attack[289], nor any other wrongful act under international law.

In the OPM case, according to the United Stated officials, Michael Rogers and James Clapper, who proposed to take response actions against China, such as economic sanctions[290], leads to the view that this cyber operation was a violation of international law, that may justify to use the response measures. On the other hand, others were on the opinion, that the United States should not take countermeasures, as it was actually an act of espionage.[291] Notwithstanding, the United States did not use countermeasures or challenge China's claim that it had initiated criminal proceedings against private hackers. If the OPM cyber operation is considered as an act of espionage, the operation is not considered as unlawful act.[292] It should be concluded that the United Stated response mostly appears to be only undertaking of necessary steps to improve cybersecurity capabilities.

[286] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.,* Rules 17-18.
[287] Nicaragua case, *op. cit.,* p. 108.
[288] J. D. Ohlin. Did Russian Cyber Interference in the 2016 Election Violate International Law?, - 95 Texas Law Review 2017, p. 1594.
[289] T. D. Gill. Non-intervention in cyber context. - K. Ziolowski (ed). Peacetime Regime for State Activities in Cyberspace NATO CCD COE Publication Tallinn 2013, pp. 235-236. For the alternative view see K. Ziolkowski. Stuxnet - Legal Considerations. NATO CCD COE 2012.
[290] D. E. Sanger. US Decides to Retaliate Against China's Hacking. The New York Times, 31.07.2015. Accessible at: https://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html?mcubz=0 (05.03.2020).
[291] E. Nakashima. Chinese Government Has Arrested Hackers it Says Breached OPM Database, *op. cit.*
[292] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.,* Rule 32, 89.

The OPM case was included to the list of case studies because the operation has a severe disruptive effect on governmental activities and national security, as well as sensitive information of millions individuals was stolen. Such damage cannot be seen as a typical espionage operation, as some of the United States policymakers tend to amount this operation to the breach of international law obligations or even to an armed attack, justifying the response measures.[293] It may be questioned, whether the response of the United States would have been different, it the data had been stolen entirely or could not be restored or even entirely deleted.

The WannaCry operation did not appear to reach the level to constitute as a violation of Article 2 (4) of the UN Charter, as malicious cyber operation affected mostly private companies and did not lead to the major disruption of the national economies. Therefore, the possible self-defense response according to the Article 51 of the UN Charter could not be justified. The WannaCry attack did not fall under the prohibition on intervention into other States' internal or external affairs, as the operation was not coercive aimed at depriving another States' of their freedom of choice. However, this operation can be considered a violation of the sovereignty of certain affected State, for example for the United Kingdoms, as the biggest impact was on the United Kingdom's National Health Service.

Countermeasures cannot only be employed by the victim State in response to malicious cyber activities perpetrated by States, but also, depending on the circumstances, in the situation where another State breaches its due diligence international obligations by knowingly allowing its territory to be used for cyber-activities contrary to the rights of other States committed by private actors. The rule of due diligence imposes positive obligations on States to prevent its territory from being exploited to conduct the operations that can violate the rights of other States in a serious adverse manner.[294] The case studies discussed in the thesis show that States do not rely on the due diligence principle when formulating their statements and demands against the alleged host-State from where the harmful cyber operation was conducted. In the Operation Aurora, Stuxnet and OPM case, the Iran and the United States respectively did not publicly invoke the due diligence against the host-States. In the Sony Pictures Entertainment case the due diligence could have been responded to, since the response was done with the North Korea's denial of direct participation in malicious cyber operation.

[293] I. Tuttle. Cyberdisaster: How the Government Compromised Our Security. National Review, 09.09.2016. Accessible at. http://www.nationalreview.com/article/439869/opm-hack-house-oversight-committee-report (06.03.2020).
[294] M. N. Schmitt. Tallinn Manual 2.0, *op. cit.,* Rule 6.

If we assume, that in WannaCry case North Korea's failed to abide by its due diligence obligation, which obliges States to put an end to ongoing cyber operations from their territory that have serious negative implications for the rights of other States, it could be seen as a possible internationally wrongful act. Under the law of State responsibility, an internationally wrongful act requires not only the breach of one State's obligation towards another State, but also attribution of the primary act to the former. It could seem that a strong consensus has developed that the Lazarus Group conducted the WannaCry operation, however, it is difficult to establish the level of direction or control of Lazarus Group by North Korea, due to the limited public materials. The other reason for the inability to claim the State's responsibility for lack of due diligence is that it is required for the responsible State to have evidence linking the operation to its territory.

The reason for a victim-State not to demand its international legal rights from the host-State, can be a fact, that victim-State will have to depart from its political strategic of silence and present evidence and specific understanding of the due diligence obligations in relation to the cyberspace activities. The lack of availability of information that links harmful cyber operations to the host-Sates makes the due diligence rule largely irrelevant in practice, as such cases would involve direct attribution of State responsibility. The case studies illustrate that rules that deal with due diligence are less relevant to State practice, whether or not States actually support the due diligence principle as it is constituted in international law, because States did not rely on the due diligence principle when formulating their statements and demands against the alleged host-State.

It can be argued, that States remain passive in clarifying a legal regime to deal with harmful cyber operation that fall below the armed attack, as well as States are reluctant to adopt a strong ban on all cross-border malicious cyber operations, because such prohibition may restrict their own cross-border covert intelligence and even harmful cyber operations.[295] If we leave malicious cyber operations that fall under armed attack threshold into the legally unclear category, it will lead to the inability of international law to prevent and repair the damages. If we recognize that the case studies discussed above go beyond mere espionage, as it is claimed for example in the OPM case, it is necessary to define principles of customary international law governing cyberspace.

[295] S. Chesterman. The Spy Who Came in from the Cold War: Intelligence and International Law. - 27 Michigan Journal of International Law 2006 (4), p. 1075.; O. A. Hathaway. The Drawbacks and Dangers of Active Defense. – 6th International Conference on Cyber Conflict. P. Brangetto, et al. (Eds.). NATO CCD COE Publications 2014, p, 49.

3.3. Implications on countermeasures and possible developments

The victim-State may use countermeasures, if the State from which territory the harmful cyber operation was implicated, was directly or indirectly involved in operation in question, for example through a violation of the due diligence principle. If a victim-State cannot show that cyber operation breached international law, then the only way for a victim-State to respond to a responsible State, is to use retorsion, as the act of retorsion do not violate the international law.[296] Recourse to acts of retorsion may reflect the complexity of the choice between conflicting political imperatives of silence, on the one hand, and legal transparency, on the other. Despite its public nature, the use of retorsion, as opposed to countermeasures, does not depend on the adoption of a clear position on the content of international law and the question whether any right of a State has been violated.

In regard to the case studies discussed in the Chapter 2, it is difficult to deduce whether States follow the rules of international law in connection with the application of countermeasures. There is only the Sony Pictures Entertainment case, where the potential resort to countermeasures was used, that allegedly led to the temporary disruption of internet in North Korea.[297] However, there was no public statements on that case to examine the legal position of the United States, whereas the alleged countermeasure did not appear to violate sovereignty of a State or non-interventional rule. It appears that the operation directed against the nuclear industry in Iran was conducted in violation of international law rules, but the silence on the part of the involved States does not allow for an adequate analysis of the way in which States interpret relevant international law terms or how they apply them in cyberspace.

Depending on how existing international law expands, States may lose the right to respond to harmful cyber operations that do not reach the armed attack level or, for example, be empowered to respond with a disproportionate number of counterattacks. However, such measures may not be sustainable, as miscalculations, human errors and different perceptions of damages may lead to responses that will result in even greater destruction and legal consequences than originally anticipated. Nonetheless, the alternative of leaving harmful cyber

[296] G. Corn, E. Jensen. The Technicolor Zone of Cyberspace – Part I. Just Security, 30.05.2018. Accessible at: https://www.justsecurity.org/57217/technicolor-zone-cyberspace-part (15.03.2020).
[297] M. Fackler. North Korea Accuses U.S. of Staging Internet Failure. The New York Times, 27.12.2014. Accessible at: http://www.nytimes.com/2014/12/28/world/asia/north-korea-sony-hacking-the-interview.html (20.03.2020).

operation below the armed attack threshold unaddressed (i.e. due to the political strategies) may also have a negative effect on the international legal order.

It can be concluded, that States' reluctance to publicly assert the countermeasures may indicate that States are not eager to clarify the legislation governing cyberspace or have no interest in notifying the alleged responsible State about the harmful cyber operation and minimizing the collateral damage. The case studies show that there is a gap in regulation of international cyber operations, which is connected with the silent approach of the States and their unwillingness to formulate their official political strategy publicly. Taking into account the case studies examined above, it is clear that States rely to a large extent on political consideration in applying responses to cyber operations. The findings of this thesis provides that the international law principles governing cyberspace and the application in practice are obscure, due to the problem of attribution and the difficulties in the limits of the breaches on international law in cyberspace, that lead to the unfortunate situation where States do not openly resort to countermeasures and even publicly discuss the allegations.

The lack of cooperation between States has exacerbated the time when important decisions must be made regarding the responses in cyberspace. If States would not commit harmful cyber operations and host-States would help victim-States to track down their attackers, States could safely rely on passive protection knowing that attackers who violated the rules of international law would be tracked down and punished in accordance with the host-State's national criminal law. Unfortunately, reality seems to be different. In addition, even if the malicious cyber operation was attributed to a non-State actor/s and a victim-State wanted to respond, it is obliged not to interfere in the internal affairs of other States and to attempt to respond through the criminal laws of the host-State rather than risk to violate the sovereignty of another State. However, the due diligence can be also used to claim the responsibility of a host-State.

The choice not to apply international law is even more evident when the victim-State did not recognize the cyber operation or refrained from trying to attribute the attack to other States, such it was the case with the Stuxnet operation, when Iran's government did not publicly attribute the harmful operation to any State or non-State actor. Thereby States deliberately choose not to contribute to the interpretation of international law in terms of the malicious cyber operations. Notwithstanding, the recent interest shown by many States in the collective attribution of international responsibility for global malicious cyber operation WannaCry, reflects a different conscious decision to facilitate a coordinated open and public response that

could broaden the international law governing cyberspace. It could seem that we are on the stage of development of international law governing cyberspace, where national security considerations advocating the silence and ambiguity may gradually give way to the communicative and normative imperatives of collective action and the application of public diplomacy pressure, which would affect the policies of the States worldwide.[298]

Based on the case studies examined in the second chapter, it can be reaffirmed, that reactions of the victim-States to malicious cyber operations directed against them indicate that existing international law in the eyes of the States are subject to strict enforcement measures. Such an approach may arise from doubts as to the advisability of applying international law in response to harmful cyber operation, bearing in mind the problems of attribution mentioned above.

The possible development that could be adopted by States, is to establish international body for the attribution of responsibility to a State or non-State actors,[299] that would provide a legitimate basis for the usage of countermeasures by the victim-State or collective sanctions against the responsible State. The proposals by the Atlantic Council in 2012 and Microsoft Corporation in 2016[300], indicate the importance of strong multilateral participation of States, as well as strong technical competence. However, such solution could only emerge if States under their free will decide to develop such institution. The limited response of victim-States may also reflect their interest in maintaining legal ambiguity to participate in offensive cyber operations on their part. If such an institution had succeeded in conferring legitimacy, it could have partially resolved many of the difficulties associated with the attribution problem that arise today from the lack of an internationally recognized rules on how international law should be applied in cyberspace.

The case studies illustrate that victim-States focus their responses on detecting and further deterring cybersecurity breaches in order to minimize negative impacts, rather than publicly provide any information that can potentially be used against them. It could be seen, that victim-

[298] D. Efony, *et al*. A Rule book on the shelf? Tallinn Manual 2.0 on Cyberopeations and Subsequent State Practice. -112 The American Society of International Law 2018, p. 649.
[299] See J. Healey, *et al*. Confidence-Building Measures in Cyberspace: A Multistakeholder Approach for Stability and Security. Atlantic Council, Brent Scowcroft Center on International Security. Washington DC, 2012. Accessible at: http://www.atlanticcouncil.org/images/publications/Confidence-Building_Measures_in_Cyberspace.pdf (03.03.2020); S. Charney, *et al*. From Articulation to Implementation: Enabling progress on cybersecurity norms. Microsoft Corporation June 2016. Accessible at: https://mscorpmedia.azureedge.net/mscorpmedia/2016/06/Microsoft-Cybersecurity-Norms_vFinal.pdf (03.03.2020).
[300] Both proposals refer to the International Atomic Energy Agency, being a precedent for an international body that addresses disputes of high technical capabilities and its important value in compliance with the Nuclear Non-Proliferation Treaty.

States do not want to draw attention to the national cybersecurity misleads, that further can put pressure on States to respond. Furthermore, none of the States invoked its rights under specific treaties.

The main conclusions are that there seems to be limited States' support for the interpretation of international law rules in State' practice and it is difficult to establish whether States accept those rules and wish to clarify the application of international law regulating harmful cyber operations. This thesis also shows that States involved in malicious cyber operations discussed in the Chapter 2 seem to have little interest in promoting legal certainty in regulating cyberspace.

Furthermore, the case studies indicate that States tend not to rely publicly and directly on specific rules of international law in connection with harmful cyber operations conducted against them and instead prefer a policy of silence and ambiguity. Some of the victim-States do not recognize that they have been attacked, while most of the victim-States are not prone to attribute responsibility to other States and impose responsibility, as well as most victim-States do not explicitly refer to the right to take countermeasures under international law. Only in Sony Pictures Entertainment case the victim-State openly resorted to response action in regards to the malicious cyber operation.

It should be noted that the challenges identified in the thesis cannot be rectified immediately and possible developments, as the recent collective attribution claims in WannaCry case, may represent a shift in the attitude of States towards the role of international law in cyberspace. This should signify an important step in ensuring stability and order in cyberspace. This shift can ensure greater accountability by strengthening inter-State cooperation in attributing responsibility for malicious cyber operations that fall under the armed attack threshold and develop a coordinated response to harmful cyber operations and impose countermeasures to the responsible States. The growing interest in the use of international law for coordinating and legitimizing inter-State responses to malicious cyber operation may encourage States to develop and adopt international legal instrument governing cyberspace.

CONCLUSION

The purpose of this thesis was to analyse the challenges for a victim-State regarding the deployment of countermeasures in the context of malicious cyber operations conducted against it. The thesis discussed the conditions for the applicability of countermeasures that may justify a victim-State outside of an armed conflict to respond to harmful cyber operations that are not serious enough to resort to self-defense under the United Nations Charter. The main difficulty was that due to the problem of attribution and the difficulties in the interpretation of scope and limits of international law in cyberspace, as well as due to the States' strategic reasons, States do not openly resort to countermeasures and very seldom publicly discuss the allegations.

There were three parts in this thesis that helped to find a solution to the indicated problem. The first one analyzed when and how victim-States may employ countermeasures in response to malicious cyber operations. The study went on to analyse the concepts of attribution, breach of legal obligation and limitations in cyberspace under international law. The second chapter analysed five malicious cyber operation, such as the Operation Aurora, the Stuxnet case, the Sony Pictures Entertainment case, the OPM case and WannaCry operation. This chapter examined whether victim-States have referred to their rights under international law when they encountered malicious cyber operations. In the Chapter 3, the author explored challenges in the usage of countermeasures based on five case studies and provided possible developments and answers to the research questions.

The hypothesis of the study was that States strategical considerations do not support the practical application of countermeasures legal regime governing cyberspace by the victim-States.

The hypothesis of this thesis was confirmed – States tend not to rely publicly and directly on specific rules of international law in connection with harmful cyber operations conducted against them and instead prefer a policy of silence and ambiguity. The case studies examined show that political and strategical considerations of States do not support the practical application countermeasures by the injured States.

The primary research questions were:

- Under which conditions can the victim-State use countermeasures in response to malicious cyber operations conducted by State/s and/or non-State actor/s?

- How have victim-States responded in practice to the significant malicious cyber operations?
- What developments would support victim-States' deployment of countermeasures in cyberspace?

A victim-State targeted by harmful cyber operation that fall below the threshold for triggering a right to self-defence may legitimately attempt to bring the attack to a halt by resorting to proportionate countermeasures and, in some circumstances at least, plea of necessity. However, a number of important uncertainties remain regarding the specific application of the law. Countermeasures are subject to important restrictions. Most significant among these is the limitation of countermeasures to internationally wrongful acts attributable to States. If a victim-State cannot show that cyber operation breached international law and attribute the operation to the responsible State, then the only way for a victim-State to respond to a responsible State is to use retorsion, as the act of retorsion do not violate the international law. Regarding the case studies discussed, it is difficult to deduce whether States follow the rules of international law in connection with the application of countermeasures.

In the case of cyber operations launched by non-State actors, the international wrongfulness of a victim-State's response will not be precluded unless a separate breach by the State to which the victim-State's obligations are owed can be identified, such as due diligence. The case studies examined in this thesis indicate that there is legal uncertainty surrounding the attribution process and legal framework of breach of international obligation under international law governing cyberspace, leading to the remaining of States silence in cyberspace. As a result of such inaccuracies in international law governing cyberspace, victim-States often remain ambiguous about their activities and responses in cyberspace, which may be seen as an act of non-disclosure of their vulnerabilities or possible policy decisions. The attribution of malicious cyber operations to States creates unique legal challenges that have not yet been fully addressed under international law. As a result, in the absence of an effective State responsibility regime, a strong commitment to existing international law and the rule of law may weaken.

The limitation to collective countermeasures restricts the potential effectiveness of countermeasures in question, as in many cases, the victim-State may be unable to respond, but has friendly relations with other States that possess the means, and that would be willing to come to the assistance. Other limitations, such as proportionality and purpose, further temper the scope of the resorting to countermeasures. Proportionality will be measured against the

violation of international obligation, not the severity of the State or non-State actor's malicious cyber operations.

This thesis provided an account of countermeasures and its implications for State responsibility in cyberspace. It is recognized that States should not allow malicious cyber operations to be conducted on their territories that will cause serious negative consequences for other States. The general applicability of due diligence to cyberspace is not disputed. However, the case studies discussed in the thesis show that States do not rely on the due diligence principle when formulating their statements and demands against the alleged host-State from where the harmful cyber operation was conducted.

While examining the second research question of this thesis and taking into account the case studies analysed above, it became clear that there seems to be limited support for the interpretation of international law rules in States' practice and that States rely to a large extent on political consideration in applying responses to cyber operations. The five case studies do not show that States generally accept or rely on the normative categories of international law governing cyberspace to draw meaningful legal distinctions in their reactions to malicious cyber operations.

The findings of this thesis demonstrate that the international law principles governing cyberspace and the application in practice are obscure due to the problem of attribution and the difficulties in the limits of the breaches on international law in cyberspace that lead to the unfortunate situation where States do not openly resort to countermeasures or even publicly discuss the allegations. States' reluctance to publicly assert the countermeasures may indicate that States are not eager to clarify the legislation governing cyberspace or have no interest in notifying the alleged responsible State about the harmful cyber operation and minimizing collateral damage. The case studies illustrate that victim-States focus their responses on detecting and further deterring cybersecurity breaches in order to minimize negative impacts, rather than publicly provide any information that can potentially be used against them.

The author argued that the establishment of an international body for the attribution of responsibility to a State or non-State actor in cyberspace would be an effective mean of ensuring the proper regulation of cyberspace within the framework of international law on State responsibility. It was argued that such development would provide a legitimate basis for the

usage of countermeasures by the victim-State or collective sanctions against the responsible State.

The official reactions and public statements like those following the Sony Pictures Entertainment case enhance transparency and enable public and scholarly debate on the right application of the international law in cyberspace. However, all of the issues are unlikely to be resolved in the near future. The debate on how international law should regulate malicious cyber operation that fall under the threshold of an armed attack is also a debate on how States perceive the international law should regulate such operations, and on such issues it will be difficult to reach the agreement.

This, however, does not mean that no international law regulation of malicious cyber operations is possible or desirable. For example, recent developments following the collective attribution claims in WannaCry case and the speech of Estonian President at CyCon, relating to the need of development of collective countermeasures, may render the international law rules more relevant than before and may generate greater interest in the establishment of an international attribution body to improve collective enforcement capabilities. This shift can ensure greater accountability by strengthening inter-State cooperation in attributing responsibility for malicious cyber operations that fall under the armed attack threshold and develop a coordinated response to harmful cyber operations and impose countermeasures to the responsible States.

ABBREVIATIONS

CERT – Computer emergency response team

CFR – The Council on Foreign Relations

CSIS – Center for Strategic and International Studies

DDoS – Distributed denial of service

ECtHR - The European Court of Human Rights

EU – European Union

ICAO – International Civil Aviation Organization

ICJ – International Court of Justice

NATO – North Atlantic Treaty Organization

UN – United Nations

UN Charter – United Nations Charter

REFERENCES

TREATIES

1. Convention on International Civil Aviation. Chicago: 7.12.1944, e.i.f. 4.04.1947;
2. The Charter of the United Nations. San Francisco 26.06.1945, e.i.f. 24.10.1945;
3. United Nations Convention on the Law of the Sea. Montego Bay 10.12.1982, e.i.f. 16.11.1994;
4. United Nations General Assembly. International Covetant on Civil and Political Rights. New York City 16.12.1966, e.i.f. 23.03.1976;

BOOKS AND ARTICLES

5. Brenner, Susan W. At Light Speed: Attribution and Response to Cybercrime/ Terrorism/Warfare. - 97 Journal of Criminal Law and Criminology 2007 (2);
6. Bilge, Leyla and Dumitras, T. Before We Knew It: An Empirical Study of Zero-Day Attacks In The Real World. Proceedings of the 2012 ACM Conference on Computer and Communications Security 2012;
7. Carr, Jeffrey. Responsible Attribution: A Prerequisite for Accountability. - The NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Paper no. 6. 2014;
8. Chesterman, Simon. The Spy Who Came in from the Cold War: Intelligence and International Law. - 27 Michigan Journal of International Law 2006 (4);
9. Chen, Ming. S. China's Data Collection on US Citizens: Implications, Risks, and Solutions. - 15 Journal of Science Policy & Governance 2019 (1);
10. Corn, Gary P., Taylor, R. Sovereignty in the Age of Cyber. - 111 American Journal of International Law 2017;
11. Crawford, James. The International Law Commission's Articles On State Responsibility: Introduction, Text and Commentaries. United Kingdom: Cambridge University Press 2002;
12. Crawford, James. Third Report on State Responsibility. Doc. A/CN.4/507 and Add. 1-4, 04.08.2000;
13. Crook, John R. Use of Force and Arms Control: State Department Legal Adviser Addresses International Law in Cyberspace. – 107 American Journal of International Law 2013 (1);
14. Egan, Brian J. International Law and Stability in Cyberspace. - 35 Berkeley Journal of International Law 2017 (1);

15. Efony, Dan, et al. A Rule book on the shelf? Tallinn Manual 2.0 on Cyberopeations and Subsequent State Practice. -112 The American Society of International Law 2018;
16. Franck, Thomas M. On Proportionality of Countermeasures in International Law. - 102 American Journal of International Law 2008 (4);
17. Geiβ, Robin and Lahmann, Henning C. Freedom and Security in Cyberspace: Shifting the Focus away from Military Responses towards Non-Forcible Countermeasures and Collective Threat-Prevention. – K. Ziolowski (ed). Peacetime Regime for State Activities in Cyberspace NATO CCD COE Publication Tallinn 2013;
18. Giegerich, Thomas. Retorsion. - 8 Max Planck Encyclopedia of International Law 2012;
19. Goldsmith, Jack. Cybersecurity Treaties: A Skeptical View. - Hoover Institution, Stanford University 2011;
20. Hathaway, Oona A. The Drawbacks and Dangers of Active Defense. – 6th International Conference on Cyber Conflict. P. Brangetto, *et al*. (eds). NATO CCD COE Publications 2014;
21. Howlett, William IV. The Rise of China's Hacking Culture: Defining Chinese Hackers. – California State University – San Bernardino 2016;
22. Jennings, Robert and Watts, Arthur (ed.). Oppenheim's International Law 9th ed. 2008;
23. Jensen, Eric Talbot. The Tallinn Manual 2.0: Highlights and Insights. – 48 Georgetown Journal of International Law 2017;
24. Jupillat, Nicolas. Armed Attacks in Cyberspace: The Unseen Threat to Peace and Security That Redefines the Law and State Responsibility. - 92 University of Detroit Mercy Law Review 2015 (2);
25. Kaska, Kadri (ed). Trends in International Law for Cyberspace. - NATO Cooperative Cyber Defence Centre of Excellence May 2019;
26. Kosseff, Jeff. Collective Countermeasures in Cyberspace. - 10 Notre Dame Journal of international & Comparative Law 2020 (1);
27. Kunig, Philip. Prohibition of Intervention. Max Planck Encyclopedia of Public International Law 2008;
28. Llorens, Maria Pilar. The Challenges of the Use of Force in Cyberspace. – 17 Anuaria Maxicano de Dercho Internacional 2017;
29. Lobel, Jules. The Use of Force to Respond to Terrorist Attacks: The Bombing of Sudan and Afghanistan. - 24 The Yale Journal of International Law 1999;
30. Mar Del, K. The International Court of Justice and Standards of Proof. - K. Bannelier, T. Christakis and S. Heathcote (eds.), The ICJ and the Evolution of International Law: The Enduring Impact of the Corfu Channel Case 2012;

31. Maurer, Tim. Cyber Mercenaries: The State, Hackers, And Power. Cambridge University Press 2018;
32. Ohlin, Jens David. Did Russian Cyber Interference in the 2016 Election Violate International Law?. - 95 Texas Law Review 2017;
33. Priyanka, Dev R. "Use of Force" and "Armed Attack" Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response. – 50 Texas International Law Journal 2015 (2);
34. Roscini, Marco. Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations. - 50 Texas International Law Journal 2015;
35. Schmitt, Michael N. and Vihul, Liis. Respect for Sovereignty in Cyberspace. - 95 Texas Law Review 2017 (7);
36. Schmitt, Michael N. and Vihul, Liis. Sovereignty in Cyberspace: Lex Lata Vel Non?. – 111 American Journal of International Law 2017;
37. Schmitt, Michael N. Cyber Activities and the Law of Countermeasures. - K. Ziolowski (ed). Peacetime Regime for State Activities in Cyberspace NATO CCD COE Publication Tallinn 2013;
38. Schmitt, Michael N. *et al*. Tallinn Manual On The International Law Applicable To Cyber Warfare Cambridge University Press 2013;
39. Schmitt, Michael N. *et al*. Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations. Cambridge University Press 2017;
40. Schmitt, Michael N. In Defence of Due Diligence in Cyberspace. – 125 Yale Law Journal Forum 2015 (68);
41. Schmitt, Michael N. Peacetime Cyber Responses and Wartime Cyber Operations under International Law: An Analytical Vade Mecum. - 8 Harvard National Security Journal 2017;
42. Shamsi, Jawwad. A. *et al*. Attribution in Cyberspace: Techniques and Legal Implications. – 9 Security And Communication Networks 2016 (15);
43. Sharp, Walter Gary. Cyberspace and The Use Of Force. Ageis Research Corp 1999;
44. Sicilianos, Linos-Alexandre. Countermeasures in Response to Grave Violations of Obligations Owed to the International Community. - J. Crawford *et al*. (eds.), The Law of International Responsibility, Oxford: Oxford University Press 2010;
45. Tikk, Eneken *et al*. International Cyber Incidents: Legal Considerations. - NATO CCD COE Publication Tallinn 2010;
46. Väljataga, Ann. Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly. - NATO Cooperative Cyber Defence Centre of

Excellence 01.09.2017. Accessible at: https://ccdcoe.org/incyder-articles/back-to-square-one-the-fifth-un-gge-fails-to-submit-a-conclusive-report-at-the-un-general-assembly/ (21.02.2020);

47. Watts, Sean. Low-Intensity Cyber Operations and the Principle of Non-Intervention. – Jens Daved Ohlin *et al*.(eds.). Cyber War: Law and Ethics For Virtual Conflicts 2015;
48. Waxman, Matthew C. Cyber-Attacks and the Use of Force: Back to the Future of Article 2 (4). - 36 Yale Journal of International Law 2011;
49. White, Nigel D. and Abass, Ademola. Countermeasures and Sanctions. - M.D. Evans (ed.), International Law, New York: Oxford University Press 2010;
50. Zetter, Kim. Countdown to Zero Day: Stuxnet and The Launch Of The World's First Digital Weapon 2015;
51. Ziolkowski, Katharina. Stuxnet - Legal Considerations. - NATO Cooperative Cyber Defence Centre of Excellence 2012;

LIST OF LEGAL ACTS

52. Council of the European Union. Council Conclusion on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") – adoption 9916/17. Brussels 07.06.2017;
53. Council of the European Union. Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber–attacks threatening the Union or its Member States. Brussels 17.05.2019;
54. Council of the European Union. Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber–attacks threatening the Union or its Member States. Brussels 17.05.2019;
55. Declaration on the Strengthening of International Security. UN General Assembly Resolution 2734 (XXV), 16.12.19170;
56. G7 Declaration on Responsible States Behavior in Cyberspace, Lucca 11.04.201. Accessible at: https:// www.mofa.go.jp/files/000246367.pdf;
57. International Law Commission. Draft Articles on Responsibility of States for Internationally Wrongful Acts. November 2011, Supplement no. 10 (A/56/10);
58. Measures to Eliminate International Terrorism. UN General Assembly Resolution 49/60, 09.12.1994;
59. North Atlantic Treaty Organisation. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation. Lisbon 19.11.2010;

60. UN General Assembly. UN Doc. A/70/174. Report of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security 2015;
61. United Nations General Assembly Resolution A/RES/2625 (XXV). Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations 24.10.1970;
62. United Nations General Assembly Resolution A/Res/68/167. The Right to Privacy in the Digital Age, 18.12.2013;
63. United Nations General Assembly Resolution 2131 (XX) of 21.12.1965;

LIST OF JUDICIAL PRACTICE

64. Air Services Agreement of 27 March 1946 between the United States of America and France. Reports of Arbitral Award 09.12.1978;
65. Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, ICJ 11.07.1996;
66. Corfu Channel case (United Kingdom v. Albania), Judgment, International Court of Justice 1949;
67. Gabčíkovo-Nagymaros Project (Hungary v. Slovkia), Judgment, ICJ 1997;
68. Island of Palmas (United States v. Netherlands), Award, Permanent Court of Arbitration 04.04.1928;
69. Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, ICJ 2004;
70. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, ICJ 08.07.1996;
71. Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Judgment, ICJ 1896;
72. Oil Platforms (Islamic Republic of Iran v. United States of America), Judgment, ICJ 06.11.2003;
73. Osman v. United Kingdom, Judgment, ECHR 28.10.1998;
74. Paul and Audrey Edwards v. United Kingdom, Judgment, ECtHR 14.03.2002;
75. Prosecutor v. Tadić, Case No. IT-94-1-A, Appeals Chamber Judgement 15.07.1999, International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia since 1991;
76. Pulp Mills on the River Uruguay (Argentina v. Uruguay), Judgment, ICJ 20.04.2010;

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

NEWS REPORTS AND PRESS RELEASES

78. Ahmandinejad, E. T. Iran's nuclear program hit by sabotage. The Washington Post, 29.11.2010. Accessible at: http://www.washingtonpost.com/wp-dun/content/article/2010/11/29/AR2010112903468.html (08.02.2020);
79. Areddy, James T. People's Republic of Hacking. The Wall Street Journal, 18.02.2010. Accessible at: https://www.wsj.com/articles/SB10001424052748704140104575057490343183782 (03.02.2020);
80. Barrett, Brian. Facebook Now Warns Users of State-Sponsored Attacks. WIRED, 09.10.2015. Accessible at: http://www.wired.com/2015/10/facebook-now-warns-users-of-state-sponsored-attacks (04.03.2020);
81. Beach, Sophie. People's Republic of Hacking (Updated). China Digital Times, 20.02.2010. Accessible at: http://chinadigitaltimes.net/2010/02/chinese-school-denies-cyber-attack-on-google/ (03.02.2020);
82. Bednarz, Dieter, Follath, Erich. Iran's chief nuclear negotiator: we have to be constantly on guard. Spiegel Online, 18.01.2011;
83. Bing, Christopher. Exclusive: Clues in Marriott hack implicate China – sources. Reuters, 06.12.2018. Accessible at: https://www.reuters.com/article/us-marriott-intnl-cyber-china-exclusive/exclusive-clues-in-marriott-hack-implicate-china-sources-idUSKBN1O504D (18.02.2020);
84. Bossert, Thomas P. It's Official: North Korea Is Behind WannaCry. WSJ, 18.12.2017. Accessible at: https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537?shareToken=st2d38565d59c24132b421a4b03edb68b5&reflink=article_email_share (21.02.2020);
85. Bradner, Eric. Obama: North Korea's Hack Not War, But 'Cybervandalism,'. CNN Politics, 24.12.2014. Accessible at: http://www.cnn.com/2014/12/21/politics/obama-north-koreas-hack-not-war-but-cyber-vandalism (04.03.2020);
86. Brinded, Lianna. The Interview Tipped to Cost Sony Pictures $200m Following Hack and Cancellation. International Business Times, 18.12.2014. Accessible at: http://www.ibtimes.co.uk/interview-tipped-cost-sony-pictures-200m-total-following-hack-cancellation-1480157 (10.02.2020);

87. Broad, W. J. *et al*. Israeli Test On Worm Called Crucial In Iran Nuclear Delay. The New York Times, 15.01.2011. Accessible at: https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=2&hp=&pagewanted=print (08.02.2020);
88. Browne, Ryan. UK Government: North Korea Was Behind the WannaCry Cyber-attack that Crippled Health Service. CNBC, 27.10.2017. Accessible at: https://www.cnbc.com/2017/10/27/uk-north-korea-behind-wannacry-cyberattack-that-crippled-nhs.html (22.02.2020);
89. Carr, David. How the Hacking at Sony over 'The Interview' Became a Horror Movie. - The New York Times, 21.12.2014. Accessible at: www.nytimes.com/2014/12/22/business/media/hacking-at-sony-over-the-interview-reveals-hollywoods-failings-too.html (26.02.2020);
90. China Rebuts US Accusation of Hacker Attacks. China Daily, 31.10.2011. Accessible at: https://www.chinadaily.com.cn/china/2011-10/31/content_14011089.htm (04.02.2020);
91. Cieply, Michael and Barnes, Brooks. Sony Cyberattack, First a Nuisance, Swiftly Grew Into a Firestorm. New York Times, 30.12.2014. Accessible at: https://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html (13.02.2020);
92. Clinton, Hilary R. Remarks on Internet Freedom, 21.01.2010. Accessible at: https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm (03.02.2020);
93. Corera, Gordon. NHS cyber-attack was "launched from North Korea". BBC News, 16.06.2017. Accessible at: https://www.bbc.com/news/technology-40297493 (21.02.2020);
94. Elkind, Peter. Inside the Hack of the Century: Part III. Fortune, 27.06.2015. Accessible at: http://fortune.com/sony-hack-final-part (12.02.2020);
95. Elkind, Peter. Sony Pictures: Inside the Hack of the Century: Part I. Fortune, 25.06.2015. Accessible at: http://fortune.com/sony-hack-part-1 (10.02.2020);
96. Eunjung, C. A. and Nakashima, E. Google Attack Part of Vast Campaign; Targets Are of Strategic Importance to China, Where Scheme Is Thought to Originate. The Washington Post, 14.01.2010;
97. Fackler, Martin. North Korea Accuses U.S. of Staging Internet Failure. The New York Times, 27.12.2014. Accessible at: http://www.nytimes.com/2014/12/28/world/asia/north-korea-sony-hacking-the-interview.html (20.03.2020);
98. Frizell, Sam. NSA Director on Sony Hack: 'The Entire World is Watching'. Time, 08.01.2015. Accessible at: http://time.com/3660757/nsa-michael-rogers-sony-hack (12.02.2020);

99. Fruhlinger, Josh. Equifax data breach FAQ: what happened, who was affected, was the impact? CSO Online, 12.02.2020. https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html (18.02.2020);
100. Fruhlinger, Josh. The OPM hack explained: Bad security practices meet China's Captain America. CSO Online, 06.11.2018. Accessible at: https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html (16.02.2020);
101. Hess, Amanda. Inside the Sony Hack. Slate, 22.11.2015. Accessible at: http://www.slate.com/articles/technology/users/2015/11/sony_employees_on_the_hack_one_year_later.html (11.02.2020);
102. Higgins, Kelly Jackson. More victims of Chinese hacking attacks come forward. Dark Reading, 14.01.2010. Accessible at: https://www.darkreading.com/attacks-breaches/more-victims-of-chinese-hacking-attacks-come-forward/d/d-id/1132773 (29.01.2020);
103. Kerry, John. Secretary of State. Condemning Cyber-Attacks by North Korea. Press Release, 19.12.2014. Accessible at: https://2009-2017.state.gov/secretary/remarks/2014/12/235444.htm (11.02.2020);
104. Koh, Harold Hongju. US Department of State, Speech delivered at USCYBERCOM Inter-Agency Legal Conference at Fort Meade, Maryland: International Law in Cyberspace, 18.09.2012. Accessible at: http://www.harvardilj.org/wp-content/uploads/2012/12/Koh-Speech-to-Publish1.pdf (01.03.2020);
105. Koerner, Brendan I. Inside the Cyberattack That Shocked the US Government. Wired, 23.10.2016. Accessible at: https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/ (15.02.2020);
106. Kramer, Andrew E. Russia, This Time the Victim of a Cyberattack, Voices Outrage. The New York Times, 14.05.2017. Accessible at: https://www.nytimes.com/2017/05/14/world/europe/russia-cyberattack-wannacry-ransomware.html?smid=tw-nytimesworld&smtyp=cur&_r=0&mtrref=www.bbc.com (20.02.2020);
107. Kroft, Steve. The Attack on Sony. CBS News, 12.04.2015. Accessible at: http://www.cbsnews.com/news/north-korean-cyberattack-on-sony-60-minutes (10.02.2020);
108. Lee, Robert M. The Feds Got the Sony Hack Right, but the Way They're Framing It Is Dangerous. Wired, 10.01.2015. Accessible at: http://www.wired.com/2015/01/feds-got-sony-hack-right-way-theyre-framing-dangerous (12.02.2020);

109. Lee, Youkyng. South Korea Says North Korea Behind Computer Crash in March. Global News 10.04.2013. Accessible at: https://globalnews.ca/news/468054/skorea-says-nkorea-behind-computer-crash-in-march/ (07.02.2020);

110. Markoff, J. and Barboza, D. Two Chinese Schools Said to Be Tied to Online Attacks. New York Times, 19.02.2010. Accessible at: https://www.nytimes.com/2010/02/19/technology/19china.html (03.02.2020);

111. Marriott Announces Starwood Guest Reservation Database Security Incident. Martiott, 30.11.2018. Accessible at: https://news.marriott.com/2018/11/marriott-announces-starwood-guest-reservation-database-security-incident/ (18.02.2020);

112. Miguel, H. and Markoff, J. Google Alerted Activists of Attacks. New York Times, 15.01.2010;

113. Ministry of Foreign Affairs of the People's Republic of China. Foreign Ministry Spokesperson Hong Lei's Regular Press Conference, 05.06.2015;

114. Nakashima, Ellen and Warrick, J. Stuxnet was the Work of U.S. and Israeli Experts, Officials Say. The Washington Post, 02.06.2012. Accessible at: http://www.washingtonpost.com/world/national-security/stuxnet-was-work-ofus-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html (07.02.2020);

115. Nakashima, Ellen. Chinese Government Has Arrested Hackers it Says Breached OPM Database. The Washington Post, 02.12.2015. Accessible at: https://www.washingtonpost.com/world/national-security/chinese-government-has-arrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb_story.html (17.02.2020);

116. Nichols, Michelle. North Korea saya linking cyber attacks to Pyongyang is "ridiculous". Reuters, 19.05.2017. Accessible at: https://www.reuters.com/article/us-cyber-attack-northkorea/north-korea-says-linking-cyber-attacks-to-pyongyang-is-ridiculous-idUSKCN18F1X3 (22.02.2020);

117. OPM Announces Steps to Protect Federal Workers and Others From Cyber Threats. Office of Personnel Management Press Release, 09.07.2015. Accessible at: https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats/ (15.02.2020);

118. OPM to Notify Employees of Cybersecurity Incident. Office of Personnel Management Press Release, 04.06.2015. Accessible at: https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/ (15.02.2020);

119. Paletta, Damian. U.S. Intelligence Chief James Clapper Suggests China Behind OPM Breach. The Wall Street Journal, 25.06.2015. Accssible at: http://www.wsj.com/articles/SB10007111583511843695404581069863170899504 (16.02.2020);

120. Peterson, Andrea. The Sony Pictures Hack, Explained. The Washington Post, 18.12.2014. Accessible at: http://www.washingtonpost.com/news/the-switch/wp/2014/12/18/thesony-pictures-hack-explained (10.02.2020);

121. Pradesh, Andhra. WannaLaugh: Faced with WannaCry attack, AP cops unplug systems and save data. The New Indian Express, 13.05.2017. Accessible at: https://www.newindianexpress.com/states/andhra-pradesh/2017/may/13/wannalaugh-faced-with-wannacry-attack-ap-cops-unplug-systems-and-save-data-1604416.html (20.02.2020);

122. President of Republic of Estonia Kersti Kaljulaid. President of the Republic at the opening of CyCon 2019, 29.05.2019. Accessible at: https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html (03.03.2020);

123. Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea. The White House, 19.12.2017. Accessible at: https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/ (21.02.2020);

124. Remarks by the President in Year-End Press Conference. The White House, 19.12.2014. Accessible at: http://www.whitehouse.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference (12.02.2020);

125. Richwine, Lisa. Cyber Attack Could Cost Sony Studio as Much as $100 Million. Reuters, 09.12.2014. Accessible at: http://www.reuters.com/article/us-sony-cybersecurity-costs-idUSKBN0JN2L020141209 (11.02.2020);

126. Robb, David. Sony Hack: A timeline. Deadline, 22.12.2014. Accessible at: http://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interview-north-korea-1201325501 (10.02.2020);

127. Sanger, David E. US Decides to Retaliate Against China's Hacking. The New York Times, 31.07.2015. Accessible at: https://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html?mcubz=0 (05.03.2020);

128. Schmidt, Michael S. *et al*. Chinese Hackers Pursue Key Data on U.S. Workers. The New York Times, 09.07.2014. Accessible at:

https://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html (16.02.2020);

129. Shear, Michael D. and Shane, Scott. White House Weighs Sanctions After Second Breach of a Computer System. The New York Times, 12.06.2015. Accessible at: https://www.nytimes.com/2015/06/13/us/white-house-weighs-sanctions-aftersecond-breach-of-a-computer-system.html (16.02.2020);

130. Shoard, Caterina. Sony Hack: The Plot To Kill The Interview – a Timeline So Far, The Guardian, 18.12.2014. Accessible at: http://www.theguardian.com/film/2014/dec/18/sony-hack-the-interview-timeline (10.02.2020);

131. Sony Cyber-attack: North Korea Faces New US Sanctions. BBC NEWS, 03.01.2015. Accessible at: http://www.bbc.com/news/world-us-canada-30661973 (14.02.2020);

132. Strohm, Chris. Hacked OPM Data Hasn't Been Shared or Sold, Top Spy-Catcher Says. Bloomberg, 28.09.2017. Accessible at: https://www.bloomberg.com/news/articles/2017-09-28/hacked-opm-data-hasn-t-been-shared-or-sold-top-spy-catcher-says (17.02.2020);

133. Strohm, Chris. North Korea Web Outage Response to Sony Hack, Lawmaker Says. Bloomberg Politics, 17.03.2015. Accessible at: https://www.bloomberg.com/politics/articles/2015-03-17/north-korea-web-outage-was-response-tosony-hack-lawmaker-says (13.02.2020);

134. The U.S. Statement on North Korea's Cyberattacks (Statement by Press Secretary Norio Maruyama). Ministry of Foreign Affairs of Japan, 20.12.2017. Accessible at: https://www.mofa.go.jp/press/release/press4e_001850.html (21.02.2020);

135. Tuttle, Ian. Cyberdisaster: How the Government Compromised Our Security. National Review, 09.09.2016. Accessible at. http://www.nationalreview.com/article/439869/opm-hack-house-oversight-committee-report (06.03.2020);

136. Welna, David. In Data Breach, Reluctance to Point the Finger at China. National Public Radio, 02.07.2015. Accessible at: https://www.npr.org/sections/parallels/2015/07/02/419458637/in-data-breach-reluctance-to-point-the-finger-at-china (16.02.2020);

137. White House Press Release. Statement by the Press Secretary on the Executive Order Entitled "Imposing Additional Sanctions with Respect to North Korea", The White House, 02.01.2015. Accessible at: https://obamawhitehouse.archives.gov/the-press-office/2015/01/02/statement-press-secretary-executive-order-entitled-imposing-additional-s (13.02.2020);

138. Williams, Dan. Analysis-wary of naked force, Israelis eye cyberwar on Iran. Reuters, 7.07.2009. Accessible at: https://www.reuters.com/article/idUSLV83872 (08.02.2020);

139. Wright, Jeremy. The United Kingdom Attorney General. Cyber and International Law in the 21st Century. London 23.05.2018. Accessible at: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century (01.03.2020);
140. Zetter, Kim. Critics Say New Evidence Linking North Korea to the Sony Hack Is Still Flimsy. Wired, 08.01.2015. Accessible at: http://www.wired.com/2015/01/critics-say-new-north-korea-evidence-sony-still-flimsy (11.02.2020);
141. Zetter, Kim. Google Hackers Targeted Source Code of More than 30 Companies. Wired, 01.13.10. Accessible at: https://www.wired.com/2010/01/google-hack-attack/ (01.02.2020);
142. Zetter, Kim. How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History. Wired, 11.07.2011. Accessible at: http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet (07.02.2020);

OTHER SOURCES

143. Australian Human Rights Commission. Background paper: Human rights in Cyberspace, September 2013. Accessible at: www.humanrights.gov.au/sites/default/files/document/publication/human_rights_cyberspace.pdf (15.01.2020);
144. Bisson, David. The OPM breach: Timeline of a Hack. Tripwire, 29.06.2015. Accessible at: https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-opm-breach-timeline-of-a-hack/ (15.02.2020);
145. Bossenmaier, Greta. CSE Statement on the Attribution of WannaCry malware. Communications Security Establishment, 19.12.2017. Accessible at: https://www.cse-cst.gc.ca/en/media/2017-12-19 (22.02.2020);
146. Chaffetz, Jason, *et al*. The OPM Data Breach: How The Government Jeopardized Our National Security For More Than A Generation. Committee on Oversight and Government Reform,114th Congress 2016;
147. Charney, Scott, et al. From Articulation to Implementation: Enabling progress on cybersecurity norms. Microsoft Corporation June 2016. https://mscorpmedia.azureedge.net/mscorpmedia/2016/06/Microsoft-Cybersecurity-Norms_vFinal.pdf (03.03.2020);
148. Chines hacking: Impack on human Rights and Commercial Rule of Law. US Government Publishing Office. Hearing before the Congressional-executive Commission

on China 113 Congress, 25.06.2013. Accessible at: https://www.govinfo.gov/content/pkg/CHRG-113hhrg81855/html/CHRG-113hhrg81855.htm (05.02.2020);

149. CIOL Bureau. China Says Google, Foreign Firms Must Respect Laws. CIOL, 19.01.2010. Accessible at: https://www.ciol.com/china-google-foreign-firms-respect-laws/ (04.02.2020);
150. Corn, G. and Jensen, E. The Technicolor Zone of Cyberspace – Part I. Just Security, 30.05.2018. Accessible at: https://www.justsecurity.org/57217/technicolor-zone-cyberspace-part (15.03.2020);
151. Corn, G. Tallinn Manual 2.0 – Advancing the Conversation. Just Security, 15.02.2017. Accessible at: https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation (03.03.2020);
152. Cyber Operations Tracker. The United States Council on Foreign Relations. Accessible at: https://www.cfr.org/interactive/cyber-operations (15.02.2020);
153. Cyber Security Policy. Securing cyber resilience in health and care. Progress update October 2018. Department of Health and Social Care. Accessible at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747464/securing-cyber-resilience-in-health-and-care-september-2018-update.pdf (21.02.2020);
154. Drummond, David. A new approach to China: an update. Google Official Blog, 22.03.2010. Accessible at: https://googleblog.blogspot.com/2010/03/new-approach-to-china-update.html (05.02.2020);
155. Drummond, David. A new approach to China. Google Official Blog, 12.01.2010. Accessible at: https://googleblog.blogspot.com/2010/01/new-approach-to-china.html (28.01.2020);
156. Equifax Announces Cybersecurity Incident Involving Consumer Information. Equifax Security, 07.09.2017. Accessible at: https://www.equifaxsecurity2017.com/2017/09/07/equifax-announces-cybersecurity-incident-involving-consumer-information/ (08.02.2020);
157. French White Paper: Defence and National Security. France 2013;
158. Foreign & Commonwealth Office and Lord Ahmad of Wimbledon. Foreign Office Minister condemns North Korean actor for WannaCry attacks. 19.12.2017. Accessible at: https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks (21.02.2020);

159. Geers, Kenneth. *et al*. World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks. - FireEye Inc. 2013;

160. Grosse, Erik. Ensuring your information is safe online. Google Official Blog, 01.06.2011. Accessible at: https://googleblog.blogspot.com/2011/06/ensuring-your-information-is-safe.html (05.02.2020);

161. Healey, Jason. *et al*. Confidence-Building Measures in Cyberspace: A Multistakeholder Approach for Stability and Security. Atlantic Council, Brent Scowcroft Center on International Security. Washington DC, 2012. Accessible at: http://www. atlanticcouncil. org / images / publications / Confidence - Building _ Measures _ in _ Cyberspace . pdf (03.03.2020);

162. Information Systems Defence and Security France's Strategy. - French Network and Information Security Agency 2011;

163. Krebs, Brian. New Clues Draw Stronger Chinese Ties to 'Aurora' Attacks. Krebs on Security, 20.01.2010. Accessible at: http://krebsonsecurity.com/2010/01/new-clues-suggest-stronger-chinese-role-in-aurora-attacks/ (03.02.2020);

164. Kupreev, O. and Ulasen, S. Trojan-Spy.0485 and Malware-Cryptor.Win32.Inject.gen.2 Review. VirusBlockAda 2010;

165. Langner, R. To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators tried to Achieve. The Langner Group 2013. Accessible at: https://www.langner.com/to-kill-a-centrifuge/ (08.02.2020);

166. Lin, Herb. Learning from the Attack Against Sony. Lawfare, 23.01.2015. Accessible at: http://www.lawfareblog.com/learning-attack-against-sony (11.02.2020);

167. McAfee Labs and McAfee Foundstone Professional Service. Protecting Your Critical Assets: Lessons Learned from Operation Aurora. White Paper 2010. Accessible at: https://www.wired.com/images_blogs/threatlevel/2010/03/operationaurora_wp_0310_fnl. pdf (02.02.2020);

168. McGettigan, Kathy. OPM's 2018 - 2022 Strategic Plan. Office of Personnel Management, 12.02.2018. Accessible at: https://www.opm.gov/blogs/Director/2018/2/12/OPMs-2018---2022-Strategic-Plan (15.02.2020);

169. New Zealand concerned at North Korean cyber activity. National Cyber Security Center, 20.12.2017. Accessible at: https://www.ncsc.govt.nz/newsroom/new-zealand-concerned-at-north-korean-cyber-activity/ (22.02.2020);

170. Office of the National Counterintelligence Executive. Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011;
171. Phatak, Vikram. Vulnerabilities, Exploits & Payloads, Oh My!. NSS Labs Blogspot, 12.03.2010. Accessible at: http://nsslabs.blogspot.com/2010/03/vulnerabilities-exploits-payloads-and.html (02.02.2020);
172. Prasad, Pooja. Adobe Investigates Corporate Network Security Issue. Adobe Featured Blogs, 12.01.2010. Accessible at: https://www.blogs.adobe.com/conversations/2010/01/adobe_investigates_corporate_n.html (29.01.2020);
173. Report by the Comptroller and Auditor General. Investigation: WannaCry cyber attack and the NHS. National Audit Office, 25.04.2018;
174. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (a/68/98) 24 June 2013;
175. RFC 2350 Description for CERT-EE. Accessible at: https://www.ria.ee/sites/default/files/content-editors/CERT/cert-ee_rfc2350.pdf (06.03.2020);
176. Schmitt, Michael N. Estonia Speaks Out on Key Rules for Cyberspace. Just Security 10.06.2019. Accessible at: https://www.justsecurity.org/64490/estonia-speaks-out-on-key-rules-for-cyberspace/ (18.02.2020);
177. Significant Cyber Incidents Since 2006. The Center for Strategic & International Studies. Accessible at: https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity (15.02.2020);
178. Smith, Brad. Microsoft ad Facebook disrupt ZINC malware attack to protect customers and the internet from ongoing cyberthreats. Microsoft, 19.12.2017. Accessible at: https://blogs.microsoft.com/on-the-issues/2017/12/19/microsoft-facebook-disrupt-zinc-malware-attack-protect-customers-internet-ongoing-cyberthreats/ (22.02.2020);
179. Smith, Brad. The Need for a Digital Geneva Convention. Microsoft Blog, 14.02.2017. Accessible at: https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention (23.02.2020);
180. Stewart, Joe. Operation Aurora: Clues in the Code. SecureWorks, 19.01.2010. Accessible at: https://www.secureworks.com/blog/research-20913 (01.02.2020);

181. Stuxnet Analysis. European Union Agency for Network and Information Security (ENISA). Accessible at: http://www.enisa.europa.eu/media/press-releases/stuxnet-analysis (07.02.2020);
182. Stuxnet Facts Report: A Technical and Strategic Analysis. LTC Marco De Facto. NATO CCD COE 2012;
183. Symantec Corporation. 24 Internet Security Threat Report 2019;
184. Update on Sony Investigation. FBI National Press Office. 19.12.2014. Accessible at: www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation (26.02.2020);
185. U.S. Department of the Treasury. 2015 U.S.-China Strategic and Economic Dialogue U.S. Fact Sheet—Economic Track, 25.06.2015. Accessible at: https://www.treasury.gov/press-center/press-releases/Pages/jl0092.aspx (17.02.2020).