TALLINN UNIVERSITY OF TECHNOLOGY
School of Business and Governance
Tallinn Law School

Maria Tolppa

Standard of Proof in Attribution of Internationally Wrongful Cyber Operations

Master's Thesis
Law, Estonian Public and Private Law

Supervisor: Agnes Kasper, PhD

Tallinn 2018

I declare that I have compiled the paper independently
and all works, important standpoints and data by other authors
have been properly referenced and the same paper
has not been previously been presented for grading.
The document length is 26455 words from the introduction to the end of conclusion.

Maria Tolppa ……
(signature, date)
Student code: 152698HAJM
Student e-mail address: maria.tolppa@gmail.com

Supervisor: Agnes Kasper, PhD
The paper conforms to requirements in force

……
(signature, date)

Chairman of the Defence Committee:
Permitted to the defence
……
(name, signature, date)

TABLE OF CONTENTS

ABSTRACT

In 2013 the United Nations Group of Governmental Experts agreed that international law applies to cyberspace and states should practice responsible behavior while using information and communications technologies and restrain themselves from applying it in a contradiction with set principles. This legally not binding agreement has been adopted by states and international organizations and often included in national cybersecurity strategies and is widely accepted. Despite the seeming consensus, increase in state sponsored cyber operations raises the issue of attribution and possible state responsibility for unlawful conduct.

The main aim of the thesis was to analyze if the international law has set unified principles for standard of proof which is required to achieve in order to attribute unlawful conduct to a state. In order to answer the question, the author analyzed standards applied by the International Court of Justice and international tribunals in cases of state responsibility and compared the applied standards with state conduct when states have made the initial attribution for the unlawful cyber operations against another state.

The results of the analysis allowed to come to a conclusion, that international standard of proof does not necessarily exist – there are different standards applied by the court and tribunals. However, when it comes to state attribution, the standard applied is generally lower and in cases even lacking. This raises the question is the standard of proof for attribution of unlawful cyber operations moving towards standard that is and will be considerably lower than in other areas of law.

Keywords: standard of proof, state responsibility, unlawful cyber operations, attribution.

INTRODUCTION

"Security is never absolute; at the end of the day
it's about tolerating and managing real risks"
Marina Kaljurand

Today cyber is no longer something new and peculiar. Although it remains peculiar the issue of tolerating and managing risks is integral part of reassuring security and has become a central issue in both law and policy making. During the course of approximately fifty years since the preliminary predecessor of internet – a system called ARPANet - was invented by IT-technicians and state representatives and put into use without much of security considerations in mind, it was a first step towards the beginning for worldwide reliance on information and communications technology.[1]

The vast development of technology and continuous growth of state use of ICTs in their day to day activities, which in practice includes providing social services to those in need, managing and controlling state infrastructure and organize either state wide or local government level elections, and as well as military command and control functions, storing and maintaining sensitive data, collecting or processing intelligence and conducting remote operations. These are only few examples that present a new and steadily expanding area of vulnerabilities, that alongside with capacity building measures, developing sufficient defence (and in recent years states have shown initiative for publicly discussing offence) capabilities must be sustained in a legally assertive international environment that provides conviction for states, that the international obligations and codes of conduct are followed. This is accompanied by a reasonable expectation that in a case of a breach sufficient attribution is feasible.

Today the issue of attribution for malicious use of ICTs against another state, that constitutes a internationally wrongful act – whether it be equivalent to illegal intervention, intrusion, threat to use force or beyond – is an ambiguous one. It might be said that the ambiguity is tightly related to complexity of ensuring cybersecurity as ICTs can be used for terroristic, criminal or political

[1] Long, G. (1994). Who Are You: Identity and Anonymity in Cyberspace. - *University of Pittsburgh Law Review*, vol 55, issue 4, 1180.

purposes and ergo need a improved policy with a[2]. This fine line of already grey and inconclusive area is continuously being exploited to achieve political or in more serious cases even military goals which hints for a need of international consensus on how states should conduct themselves in cyberspace or in other words while using ICTs.

Our dependence on technology is increasing vulnerability of states. Government, military, judiciary, hospitals, banks, enterprises and universities are only few areas that rely on effectiveness of ICTs and safety of its networks, and as it has in several occasion been established that a simple human error can be the key component to carry out a successful operation - most well-known example would be the Stuxnet hack in 2010 when its main target Iranian nuclear power plant was infiltrated through nuclear scientists' own laptops and memory sticks which was widely attributed to the United States and Israel[3].

In several occasions Russia has been claimed to carry out cyber operations with the objective to influence political tensions – 2007 large scale DDoS attack against Estonian websites, 2014 intrusion in White House and State Department unclassified computer systems or 2015 Ukraine power grid intrusion, which resulted in loss of power for several hours across regional power distribution plants. Russian government denied all allegations, but the timing and context of the lengthy period of cyber operation and some evidence linked to servers locating in Russia gave rise to suspicions that it could have been Russian state sponsored operation.[4] And more recently the Democratic National Committee (DNC) hack in 2016 which resulted in exfiltration and release of documents that many claim have interfered with presidential elections later that year.[5] Many US state officials claim that it was Russia behind the cyber operation because an operation such as this could only be authorized high ranking officials and the target and sensitivity of it indicate state support.[6]

---

[2] Danca, D. (2015). Cyber Diplomacy – A New Component of Foreign Policy. - *Journal of Law and Administrative Sciences*, vol 3, p 91.
[3] Singer, P. W. (2015). Stuxnet and Its Hidden Lessons on the Ethichs of Cyberweapons. - *Case Western Reserve Journal of International Law*, volume 47, issue 1, p 82.
[4] Olivier, M. (2012). Cyber Warfare: The Frontline of 21st Century Conflict. - *LBJ Journal of Public Affairs*, vol 20, p 26 - 29.
[5] Davis, J., *et al*. (2017). *Stateless Attribution. Toward International Accountability in Cyberspace*. Accessible: https://cyber-peace.org/wp-content/uploads/2017/10/RAND_RR2081.pdf, 25 February 2018.
[6] Director of National Intelligence. (2017). *Worldwide Threat Assessment of the US Intelligence Community*. Accessible: https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf, 25 February 2018.

Besides Russia, recently China have gained attention as a hazard to international cyber security mainly due high number of cyber sophisticated operations uncovered to be emanating from China. There are claims that the Chinese have in several occasions targeted U.S – for example, a data theft from U.S. government and military servers in 2002 or an operation carried out by People's Liberation Army (often associated with Chinese government) against Pentagon which compromised its unclassified systems. In addition, China have often been regarded as a state that carries out operations that could be classified as corporate espionage.[7]

There have been several controversial instances, that if conclusively proven to have been a result of a cyber operations, could present the dangers states must challenge in the near future. One would be the 2008 pipeline explosion in Turkey which in 2014 was claimed to have been caused by cyber intrusion into its control system network.[8] Later evidence were presented that this could have not been the case, however, this is often similar in state attribution and goes to show importance of quality of evidence.

There have been lengthy and extensive discussions on how international law applies to cyber operations, mostly in the context of jus ad bellum and jus in bello principle and applicability of UN Charter article 2(4) and 51 and as well as state responsibility for internationally wrongful acts, which has resulted in general understanding that cyber operations in their capacity do fall under the scope of those international norms and are attributable to states. As the International Court of Justice (ICJ) noted in its 1996 Nuclear Weapons Advisory Opinion that law of armed conflict applies to "any use of force, regardless of the weapons employed"[9]. In 2011 United Nations Group of Governmental Experts (UN GGE or GGE), which among others, included representatives from five permanent Security Council member states, came to an agreement that international law and UN Charter in particular is applicable to use of ICTs, and since then most states and international organizations have adopted and further analyzed the agreement. In addition, under the auspice of NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) international law experts have taken on board the approach of the UN GGE and analyzed how international law could be applied by publishing extensive research reports - Tallinn Manual 1.0 and Tallinn Manual 2.0.

[7] Olivier (2012), *supra nota* 4, p 30.
[8] Hellman, H. (2015). Acknowledging the Threat: Securing United States Pipeline Scada System. - *Energy Law Journal*, vol 36, issue 1, p 165.
[9] Legality of the Threat or Use of Nuclear Weapons, p 22, ICJ 2996.

Right of the injured state, deriving from the International Law Committee's Draft Articles on State Responsibility for Internationally Wrongful Acts, to countermeasures is in strong correlation that the other state is responsible for the internationally wrongful act which according to the article 4 of the Draft Articles can only be in a case when the act itself is attributable to the said state and it constitutes a breach of international obligation[10]. The attribution and issue of evidence remains the centre question in cases of attribution of internationally wrongful cyber operation.

Therefore, based on the assertion that international law applies to state use of ICTs, the author raises a hypothesis that application of international law presupposes that there is an international standard of proof.

Although, previously mentioned manuals and reports of the UN GGE, which were adopted by the general assembly, are not legally binding, the assumption that cyberspace falls under the scope of international law is widely accepted. As it is established that state conduct in cyberspace is governed by international norms, the misconduct and international responsibility from it must fall in line with norms that enact state responsibility for unlawful cyber operations. Therefore, the author raises following research questions:

1. **What is international standard of proof and how it applies to state attribution?**
2. **How does it apply to attributing cyber operations?**

The thesis is composed of three chapters – first the author analyses procedural norms for state responsibility for its internationally wrongful acts and norms applicable to attribution. In addition to regulation, the author gives an overview of case law on how international norms have developed. Since the attribution of cyber operations is closely associated with the issue of whether a state is liable for a breach of internationally wrongful act, the author will examine the state responsibility in the context of cyberspace and obligations originating from it.

Often the term of "cyber-attack" is understood and used by media in its most broad sense including every kind of malicious activity whether it be intrusion, interference or an attack that may constitute to a use of force or armed attack. Term "attack" is a legal term of art and therefore, in

[10] International Law Commission. (2001). *Draft Articles on Responsibility of States for Internationally Wrongful Acts with Commentaries*, p 40. Accessible: http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf, 3 March 2018.

the end of the first chapter, the author gives an overview what often is understood under cyber operation.

In the second chapter the author analyses what is the standard of proof and rules of evidence according the ICJ and international tribunals and how it has been applied by analysis of case law. Secondly, the author examines how states engage in cyber operations during peacetimes. This allows to conclude, if there are any coinciding elements to standards of proof.

In the third chapter the author analyses the results of case analysis from the point of view of possible developing international norms for standard of proof for attribution of internationally wrongful cyber operation and how evidentiary rules are in accordance with practices of attribution.

The case law analysis in chapter one and two is chosen by what the ILC have chosen to base their work upon, that resulted in the Draft Articles and including case law that the Tallinn Manual 2.0 expert based their analysis upon.

Due to the limited capacity of the thesis the author will not analyze differences between cyber operations that do and do not succeed the threshold of use of force and uses the general term cyber operation.

In order to conduct the analysis qualitative and deductive methodologies alongside with empirical methodology. In instances the analogous interpretation will be applied.

1. PROCEDURE FOR ESTABLISHING STATE RESPONSIBILITY IN INTERNATIONAL LAW

1.1. State responsibility in international law

Cyber operations have become increasingly common in recent years. Capable of shutting down nuclear centrifuges, air defence systems, and electrical grids means they pose a serious threat to international security. It can be concluded that while the law of war provides useful guidelines for addressing some of the most dangerous forms of cyber operations, it ultimately addresses only a small section of cyber operations, therefore "cyber warfare" is only one element of a much larger problem. One unanticipated challenge is how to address operations that have little or no direct physical consequences, but nonetheless cause real harm. This could be one of the reason why no state so far has claimed that a cyber operation constitutes an armed attack giving rise to a right of self-defence under article 51 of the UN Charter.

The rise in frequency of operations also creates a more pressing need for a comprehensive legal framework for a state conduct which is not governed by the law of war.[11] There is vast amount of academic writings on the matter and the lacking of international jurisprudence has conditioned a situation that theoretical analysis has rather large influence alongside with state practice on understanding how international law governs cyberspace.[12] Following the author will analyse the lex lata for procedural norms state responsibility for internationally wrongful acts and attribution for them.

Relevance to have the ability to accurately attribute cyber operations, both legally and technically, is increasing due to growing international tensions and issues related to national defence and security interests. Today there is no agreed standard or practice on how states should approach attribution of unlawful use of ICT. Attribution from a legal aspect is tightly intertwined with responsibilities and whether it was breached and therefore requires analysis how norms of responsibility of states for internationally wrongful acts apply to state conduct in cyberspace.

[11] Hathaway, O., *et al*. (2012). The Law of Cyber-Attack. - *California Law Review*, vol 100, issue 4, p 840.
[12] Payne, C., Finlay, L. (2017). Addressing Obstacles to Cyber-Attribution: A Model Based on State Response to Cyber-Attack. - *George Washington International Law Review*, vol 49, issue 3, p 536.

Draft articles of the ILC[13] are a normative framework deriving from principles set by international case law, initially aimed at injured aliens but later broadened to states as well.[14] First two articles establish that internationally wrongful act entails state responsibility and act is wrongful when it is attributable to a state and constitutes a breach of international obligation owed to injured state[15]. The responsibility of a state does not necessarily require activity from a guilty state. Scope of the article also includes passivity – for example, in a case where a state fails to fill its due diligence obligation.[16] As the Court stated "the obligations of states is to employ all means reasonably available to them to prevent injurious activity"[17]. Same applies in case of cyber – since due diligence derives from principle of sovereignty, states should consider it carefully in their conduct.[18]

Examples include Phosphates in Morocco case[19], the Corfu Channel case[20], Nicaragua case[21], United States Diplomatic and Consular Staff in Tehran[22] where the court established either international responsibility between states, responsibility for failure to attempt to prevent a disaster or responsibility for conduct of the contras[23] or to what extent acts may be regarded as imputable to a state. The similar issue arose in the Genocide Convention case. Determining responsibility of Serbia for genocide, the ICJ deliberated if perpetrators qualified de jure or de facto state agents. By applying the effective control standard, it came to a judgement that due to autonomy on some levels the actions of non-state actors can not be attributed to Serbia.[24]

[13] United Nations resolution no 56/83 of 22 January 2002 on Responsibility of states for internationally wrongful acts. Accessible: https://www.ilsa.org/jessup/jessup11/basicmats/StateResponsibility.pdf. 3 March 2018.
[14] Hessbruegge, J. (2004). The Historical Development of the Doctrines of Attribution and Due Diligence in International Law. - *N.Y.U. Journal of International Law and Politics*, vol 36, issue 2 & 3, p 269.
[15]International Law Commission (2001), *supra nota* 10, p 32.
[16] Hessbruegge (2004), *supra nota* 14, p 268.
[17] Liu, I. (2017). State Responsibility and Cyberattacks: Defining Due Diligence Obligations. - *The Indonesias Journal of International & Comparative Law*, vol 4, issue 2, p 196.
[18] Schmitt, M. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. - *Cambridge University Press*, p 31.
[19] Phosphates in Morocco, no 71, p 22, ICJ 1938.
[20] The Corfu Channel Case, p 23, ICJ 1949.
[21] Military and Paramilitary Activities in and against Nicaragua, p 115, ICJ 1986.
[22] Case Concerning United States Diplomatic and Consular Staff in Tehran, p 30, ICJ 1980.
[23] Cassesse, A. (2007). The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgement on Genocide in Bosnia. - *The European Journal of International Law*, vol 18, issue 4, p 652. The Contras were Nicaraguan rebel group whos acts were attributed to the United States by Nicaragua and that acted during 1980 – 1990.
[24] Nielsen, E. (2010). State Responsibility for Terrorist Groups. – *U.C. Davis Journal of International Law & Policy*, vol 17, issue 1, p 162.

Despite the nature of customary rule, it is important keep in mind the principle of lex specialis derogat legi generali in cases where a cyber operation reaches the threshold of armed attack, then law of armed conflict applies. [25]

International law bears obligations states must comply with conducting activities in cyberspace. Based on reports of the UN GGE those obligations, inter alia include respecting the principle of state sovereignty, human rights and fundamental freedoms, meeting international obligations regarding internationally wrongful acts attributable to them, prohibition on using proxies to commit those acts and reassure that their territories are not used by non-state actors for unlawful use of ICTs[26]. Also states should not knowingly conduct nor support ICT activity contrary to its obligation under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public[27].

In conclusion, measures taken by the UN to supplement international norms with considerations of cyberspace, may possess significant meaning in the future while addressing applicability of countermeasures. Based on the Draft Articles the process entails that internationally wrongful act has been committed, it is attributable to a state, it constitutes a breach of international obligation and nothing precludes its wrongfulness.

1.2. Attribution in international law

Attribution is the most compelling question when it comes to countermeasures or proceedings in international court or tribunal. General understanding is that it must take place in the framework of the ILC Draft Articles. The court or injured state must come to a certain degree of legal confirmation, that internationally wrongful act, which had a harmful effect, was indeed carried out by the accused party. It is complicated when said act is carried out by a non-state actor – this requires establishing a connection between the accused and a state. Attribution of such cyber operations is more elaborate due to its transborder element and obligation to prove connection

[25] Schmitt (2017), *supra nota* 18, p 80.
[26] United Nations document no 68/98 of 24 June 2013 from the Group of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security, p 8. Accessible: https://ccdcoe.org/sites/default/files/documents/UN-130624-GGEReport2013_0.pdf, 5 March 2018.
[27] United Nations document no 70/174 of 22 July 2015 from the Group of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security, p 8. Accessible: http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174, 5 March 2018.

between a state and non-state actor, who similar to states may possess capabilities to launch cyber operations with crippling effects. In most cases responding to such cyber operation is not permitted, unless they fill exact conditions. Today it is widely regarded that responding to cyber operations is possible, if it constitutes at least use of force under article 2(4) of the UN Charter, an armed attack under article 51 or internationally wrongful act.

Even the most noteworthy operations, which have caused stream of speculations, often went without ramifications. For instance, although the Stuxnet operation cost Iran highly, its officials never issued a public attribution for the incident, which in media was speculated to have been carried out by United States and Israel.[28] Russian expert was part of the 2015 UN GGE team and alongside with rest affirmed commitment to not allow or support ICT activity to be carried out which damages critical infrastructure, nor use it in political or military purposes. Yet, more often than not it is Russia claimed to launch cyber operations against critical infrastructure, but dismisses any statements of attribution and counters it with demand for "hard evidence".[29]

State in essence is an legal entity with legitimate powers to act according to its capacity under international law. The "will" of the state is carried out by its representatives.[30] Which is why, in the context of state responsibility, a question comes about – when a person is considered as "acting on behalf of the state" and what constitutes "act of the state".[31]

Generally only acts of "organs of government" or people or groups of people who are under "direction, instigation or control" of it are attributable[32]. This raises the issue of attribution of actions of non-state actors to a state. ICJ have in several cases approached the matter – conduct is attributable even if carried out in ultra vires[33][34] or conduct of an organ, even independent from executive, is attributable to a state[35].

[28] Mačák, K. (2016). Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors. - *Oxford, Journal of Conflict & Security Law*, vol 21, issue 3, p 409.
[29] Pernik, P. (2018). *Responding to „the Most Destructive and Costly Cyberattack in History"*. Accessible: https://www.icds.ee/blog/article/responding-to-the-most-destructive-and-costly-cyberattack-in-history/, 5 March 2018.
[30] Certain Questions Relating to Settlers of German Origin in the Territory Ceded by Germany to Poland, p 22, PCIJ Advisory Opinions 1923.
[31] International Law Commission (2001)*, supra nota 10*, p 35.
[32] *Ibid*, p 38.
[33] *Ibid.*
[34] Armed Activities on the Territory of the Congo (*Democratic Republic of the Congo v Uganda)*, p 78, ICJ 2005.
[35] Difference Relating to Immunity From Legal Process of a Special Rapporteur of the Commission on Human Rights, ICJ Advisory Opinion 1999

The Doctrine of Attribution of international law consists of eight articles divided into three groups. Articles 4 to 7 determine the rules of attribution for actions conducted by either state organs or its agents, articles 8 to 11 deal with additional cases where conduct, not that of a state organ or entity, is nonetheless attributed to the state in international law, articles of 9 to 11 deal with cases where the conduct of entities that are not state organs or entities are attributed to a state in absence of either official authorities, in case of conduct of insurrectional movements and conduct which is not attributable to a state but is nonetheless adopted by the state.[36]

ICJ have in many occasions addressed the issue, who is a state organ in the context of international law. It can be "officer of person in authority presenting his government"[37] or "ruler belonging to legislative, executive or judicial department of government"[38]. In cyber context an IT technician of the Estonian Defence League's Cyber Unit would suffice and his conduct might be attributable to Estonia[39]. As in previous cases the non-state actor issue have been analyzed in length – if state actors and thus state is responsible for genocide or if conduct of non-state actors who did carry it out is attributable to the state. [40]

In cases a private entity may possess some public authority, for example, through procurement by government – through such capacity, conduct of said entity can be attributed as well, if it acts in the scope of its powers[41]. This could be the case when a charity foundation is under control of state.[42] Considering the case law, in cyber context, it could be cyber security entity who provides defence services to government[43]. Also, conduct of someone placed under disposal of another state, can be attributed to receiving state. Albeit with some reservations because the articles do not define the meaning of "under disposal". It is clear that if this organ has autonomy in some level, this norm would not suffice.

[36] International Law Commission (2010), *supra nota* 10, p 49 – 53.
[37] *Ibid*.
[38] Claim of the Salvador Commercial Company, p 477, Reports of International Arbitral Awards 1902.
[39] Schmitt (2018), *supra nota* 28, p 87.
[40] Tsagourias, N. (2012). Cyber Attacks, Self-Defence and the Problem of Attribution. – *Journal of Conflict and Security Law*, vol 17, issue 2, p 236.
[41] de Stefano, C. (2017). Adel A Hamadi Al Tamimi v Sultanate of Oman: Attributing to Sovereigns the Conduct of State-Owned Enterprises: Towards Corcumvention of the Accountability of States Under International Investment Law. – *Oxford University Press*, vol 32, issue 2, p 271.
[42] International Law Commissin (2010), *supra nota* 10, p 43.
[43] Schmitt (2017), *supra nota* 18, p 89.

The most relevant issue of attribution in the cyber context surrounds article 8. Often evaded subject during state discussions, that states are more vigorously developing cyber-offence capabilities, the other side of this troublesome issue is utilization of non-state actors in state sponsored cyber operations. It is more common for states to use apparently independent hackers or group of hackers as intermediary to carry out cyber operations which correlates with the difficulty of attribution and credibility of it, especially if and when a group conducts their actions with linkage to a state[44]. There have been cases enlightening the problem. In 2017 a Canadian hacker pleaded guilty for conspiring with Russians[45] and in 2016 a Syrian national who pleaded guilty for allegations that he "conspired to receive extortion proceeds and conspired to unlawfully access computers" [46][47].

The main principle of the article 8 is that states do not escape legal responsibility for internationally wrongful acts by perpetrating them through proxies. [48] It is widely accepted and applied by courts and tribunals - "if persons (…) were in such relation to German authorities (…) that Germnay must be held responsible" [49] or "insurgents were acting under orders from Filipino Republic"[50].

The relevance of non-state actor issue must be acknowledged in the cyber context, often such groups possess higher skill-set to carry out invasive operations[51]. Regarding attribution of conduct of non-state actors, ICJ have developed well-known standards in order to establish the connection - the effective control standard where the court required that state is "effectively in control of the contras" [52], that it "devised strategy and directed their tactics" [53] and the contras were in "complete

[44] Maurer, T. (2018) *Here's How Hostile States are Hiding Behind „Independent" Hackers. Carnegie Endowment for International Peace.* Accessible: https://carnegieendowment.org/2018/02/01/here-s-how-hostile-states-are-hiding-behind-independent-hackers-pub-75424, 8 April 2018.
[45] Department of Justice of the United States. (2017). Canadian Hacker Who Conspired With and Aided Russioan FSB Officers Pleads Guilty. Accessible: https://www.justice.gov/opa/pr/canadian-hacker-who-conspired-and-aided-russian-fsb-officers-pleads-guilty, 8 April 2018.
[46] Chung, E. (2014). *Syrian Electronic Army Hackers: Who are they and why are they targeting the media*. The group is suspected to act since 2011 when the Syrian civil war began and which supports the administration of president Bashar al-Assad and attacks often media organisations. Accessible: http://www.cbc.ca/news/technology/syrian-electronic-army-hackers-who-are-they-and-why-are-they-targeting-the-media-1.2852694. 8 April 2018.
[47] Department of Justice of the United States. (2016) *Syrian Electronic Army Hacker Pleads Guilty*. Accessible: https://www.justice.gov/opa/pr/syrian-electronic-army-hacker-pleads-guilty, 9 April 2018.
[48] Banks, W. (2017). State Responsibility and Attribution of Cyber Intrusions after Tallinn 2.0. - *Texas Law Review*, vol 95, issue 7, p 1496.
[49] Leigh Valley Railroad Company, Agency of Canadian Car and Doundry Company, Limited, and Various Underwriters (United States) v Germany (Sabotage Cases), p 84, Reports of International Arbitral Awards 1930.
[50] D. Earnshaw and Others (Great Britain) v United States (Zafiro case), p 160, Reports of International Arbitral Awards 1925.
[51] Schmitt, M. (2013). Classification of Cyber Conflict. – *Journal of Conflict and Security Law*, vol 17, issue 2, p 253.
[52] Shackelford, S. (2010). State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem. – *Georgetown Journal of International Law*, vol 42, issue 4, p 201.
[53] Military and Paramilitary Activities in and Against Nicaragua, *supra nota* 21, p 11.

dependence on the state" [54] and the overall control standard where it "sufficed that group as whole must be under the overall control of the state" [55]. Overall control standard broadens the scope of possibilities which incurs state responsibility.[56] However ICJ set a standard, that when it comes to genocide, more strict approach is required. [5758] From the case law, it has resulted that control, direction or instruction may among other things include "direct connections, financing for example, include indirect support such as support in planning malicious activity".[59]

In conclusion, the Draft Articles on Responsibility of States for Internationally Wrongful Acts is a regulatory framework within which the attribution process takes place. In order to apply countermeasures for internationally wrongful act, the obligatory parts of the attribution must be satisfied with sufficient evidence which meet the requirement of standard of proof. The issue of attribution of cyber operation with its new difficulties requires elements from several applied standards due to the fact that states often use proxies to carry out different kinds of cyber operations. In opinion of the author it serves two purposes – first, the obvious one is to evade responsibility and second, those groups often have people with higher skill-set. Since the use of proxies offer plausible deniability the process of evidence gathering and attribution must adapt because plausible deniability can not mean exemption of responsibility.

1.3. Cyber operations in international law

As it was established that attribution of a cyber operation is combined by both technical, legal and political procedures which are often complicated by decision-making on a various levels – which technical evidence could be produced as evidence for it, possible repercussions and proportionate response. As it states countermeasures must, as reflected in Article 51 of the Articles of State Responsibility, be proportionate, that is "commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question"[60]. However, the countermeasures could only be taken in order to influence the responsible state to halt its unlawful

[54] *Ibid*, p 52.
[55] Prosecutor v Duško Tadić, p 49, ICTY 1999.
[56] Payne, C., Finlay, L (2017)*, supra nota* 12, p 557.
[57] Application of the Convention on the Prevention and Punishment of the Crime of Genocide (*Bosnia and Herzegovina v Serbia and Montenegro*), p 164, ICJ 2008.
[58] Cassesse (2007), *supra nota* 23, p 651 and 653.
[59] Cassesse (2007), *supra nota* , p 657.
[60] Schmitt (2017), *supra nota* 18, p 127.

conduct and if necessary make reparations. In order to reach a legitimate attribution it is necessary to consider the legal meaning of a cyber operation, since the term does not have a legal definition in international law and varies in both intensity and impact and unquestionably will influence the injured state response. It is important to understand that the term "attack" is a term of art and albeit often used in public, does not entail only the meaning of use of force or an armed attacks.

According to the international law experts the cyber operations must fill the box for set of conditions. A state can respond to cyber operation if it constitutes a use of force under UN Charter article 2(4)[61] which enacts that all members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the UN, an armed attack under article 51 that says that nothing in the UN Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against members of the UN or an internationally wrongful act.[62] So in order for a cyber operation, in its broadest meaning, to be qualified as an "attack" it needs to at least cross the threshold of armed attack. Michael Schmitt, in addition to participating in the production of Tallinn Manual group, have analyzed the term separately and comes to a conclusion that the term can most logically be viewed from the perspectives of jus ad bellum and jus in bello principle. He states that "combining the two principles and their source – UN Charter articles 51 and 2(4) – a state may use force without violating article 2(4) when it is the victim of an armed attack and adds that self-defence requires no ex ante authorization from the UN Security Council and states alone enjoy the right of self-defence".[63] He admits that repeating question in the cyber context is, if data gets damaged or destroyed, but it does not bring such harm with it to qualify as an armed attack, what would be appropriate response. Such conduct can not be seen as armed attack mainly because that would mean unreasonably lowering the threshold for forceful response.[64]

According to the experts of Tallinn Manual 2.0 a cyber-attack is a "cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to property"[65]. The manual pulls the meaning of it from Additional Protocol I article

[61] Ühinenud Rahvaste Organisatsiooni põhikiri ning Rahvusvahelise Kohtu statuut. RT II 1996, 24, 95.
[62] Pernik (2018)., *supra nota* 29.
[63] Schmitt, M. (2012). „Attack" as a Term of Art in International Law: The Cyber Operations Context. - *NATO CCD COE Publications*, p 285.
[64] *Ibid*, 288.
[65] Schmitt (2017), *supra nota* 18, p 415.

49(1) which enacts that attack means acts of violence against the adversary, whether in offence or defence[66].

Adding to that, the manual addresses cyber operations which themselves do not constitute as an attack, but could be integral part of an operation that itself constitutes as an armed attack[67]. This interpretation of the article of the Additional Protocol holds a key significance in a case of hybrid warfare which may consist of traditional forms of conflict and is supplemented by state-sponsored terrorism or crime. Similar to state on state cyber operation, the main problem of attribution remains with hybrid war where cyber operations or attacks are deployed and its connection to the state. However, in case of combined attack, for instance a cyber interference and armed conflict reaching the attribution, could tend to be leaning towards the possible motivation of the cyber operation[68]. Whatever the reason, if cyber operation is one part of an operation that qualifies as an attack the law of armed conflict is applicable[69]. One practical example of such an operation would be what today is often referred as information warfare conducted in cyberspace. "Information warfare can be defined through its three main functions: gaining, protecting and disturbing information", which are actions that could be motivated by manipulating information that could effectively influence a rival and change its behavior[70]. One example is Russian aggression towards Ukraine which has prompted some observers remark that it is engaging in hybrid warfare which includes knowingly spreading false information among public or regarding the activities and intentions of particular organizations and engaging in general disinformation campaigns.[71] Same goes to other cyber operations – for example DDoS attacks or defacement of government websites - that often accompany military conflict between states – often activities and operations that wall under the scope of use of force that often remain unchallenged.

Yet some view cyber operations as an attack while "states utilize computers and information technology as the primary mechanisms to detrimentally impact the interests of another state". Conclusively, ICTs are seen as a weapon. On occasions, attempted definitions include kinetic

[66] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I), of 8 June 1977.
[67] Schmitt (2017), *supra nota* 18, p 419.
[68] Brenner, S. (2007). At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare. 2007. - *Journal of Criminal Law & Criminoligy*, vol 97, issue 2, p 423.
[69] Schmitt (2017), *supra nota* 18, p 419.
[70] Swiatkowska, J. (2017). Central and Eastern European Countries Under Cyberthreats. - *Polish Political Science Yearbook*, vol 46, issue 1, p 32.
[71] Lanoszka, A. (2016). Russian hybrid warfare and extended deterrence in Eastern-Europe. – *The Royal Institute of International Affairs*, vol 92, issue 1, p 188.

attacks towards ICT infrastructure but author of the article suggests to limit the scope of the definition with uniqueness of cyberspace.[72]

Other authors say that "scenarios of the meaning of cyber-attack range from a virus that scrambles financial records or incapacitates the stock market, to a false message that causes a nuclear reactor to shut off or a dam to open, to a blackout of the air traffic control system that results in airplane crashes – and anticipate severe and widespread economic or physical damage"[73]. According to Richard Clarke, a security expert for the Government of the United States, cyber war includes "actions by a nation-state to penetrate another nation's computer or networks for the purposes causing damage or disruption"[74] or Michael Hayden, who used to be a director of NSA and CIA, sees cyber-war as a "deliberate attempt to disable or destroy another country's computer networks"[75]. The article brings forth the main problems of those definitions – first one limits cyber attacks to nation states, which, must be considered in the context of the term of attack, and the second is too wide and includes crime and terrorism under one definition.[76]

U.S. Department of Defence has adopted the term "information operation" in its Dictionary of Military and Associated terms which is described as an "integrated employment, during military operations, of information-related capabilities with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own" [77] It also includes the term of "offensive cyberspace operations" which means "cyberspace operations intended to project power by the application of force in or through cyberspace"[78].

NATO in its Glossary of Terms and Definitions define "computer network attack" as "action taken to disrupt, deny, degrade or destroy information resident in a computer and/or computer network, or the computer and/or computer network itself. A computer network attack is a type of cyber attack" [79]. In case of the NATO approach it does conclude that the computer network attack is a type of cyber-attack by giving away that there are additional types but does not offer definitions

[72] Payne, C., Finlay, L (2017)*., supra nota* 12, p 537.
[73] Hathaway, O., *et al* (2012)*, supra nota* 11, p 823.
[74] *Ibid.*
[75] *Ibid.*
[76] *Ibid*.
[77] Department of Defence. (2010) *Dictionary of Military and Associated Terms*. Accessible: https://fas.org/irp/doddir/dod/jp1_02.pdf, 13 March 2018.
[78] *Ibid.*
[79] NATO. (2014). *Glossary of Terms and Definitions*. Accessible: http://wcnjk.wp.mil.pl/plik/file/N_20130808_AAP6EN.pdf, 13 March 2018.

to any other types of cyber-attacks. Another author have viewed cyber-attack as a "use of deliberate actions and operations to alter, disrupt, deceive, degrade, or destroy adversary systems and networks or the information and/or programs resident in or transiting these systems or networks"[80]. This approach is fairly similar to the interpretation of the U.S. government with a broader approach which includes possible programs that could be altered without compromising whole network.

Experts have in general taken on board the notion that cyber-attack is a type of cyber operation that is accompanied by previously stated effects. Some authors have taken on board a contrary approach by not defining the term itself but by analyzing the consequences of a cyber operation. By adopting a "result test" some states use it as a way to determine whether cyber information operation constitute a use of force or an armed attack. Such a test attempts to compare the cause and effect of traditional "attacks" to cyber operations.[81] This approach consistent with how the Tallinn Manual states that a cyber operation constitutes as a cyber-attack in its relation to the effects that are caused. More specifically, consequences are the key element in consideration if the violation threshold have succeeded.[82] However the downside of such assessment does not count attacks that are carried out but due to different circumstances does not reach its goal and effect.

Joint Chiefs of Staff of U.S. Cyber Command's lexicon for military use in cyber operations defines cyber-attack as "a hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions. The intended effects of cyber-attack are not necessarily limited to the targeted computer systems or data themselves. A cyber-attack may use intermediate delivery vehicles including peripheral devices, electronic transmitters, embedded code, or human operators. The activation or effect of a cyber-attack may be widely separated temporally and geographically from the delivery"[83]. With their definition they replace the use of "CNA" and "offensive cyberspace operation" where the action meets use of force levels or is specifically intended to disrupt, deny, degrade, manipulate, and/or destroy adversary computer system or data.[84] Main issue with this definition according to

[80] Lin, H. (2010). Offensive Cyber Operations and the Use of Force. - *Journal of National Security Law & Policy*, vol 4, issue 1, p 63.
[81] Solis, D. (2014). Cyber Warfare. - *Military Law Review*, p 12.
[82] Schmitt (2017), *supra nota* 18, p 415.
[83] US Department of Defence. *Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands and Directors of the Joint Staff Directorates – Joint Terminology for Cyberspace Operations*. Accessible: http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf, 15 March 2018.
[84] *Ibid.*

Hathaway is it narrows the possible cyber-attacks to be carried out only against critical cyber systems[85], completely excluding infrastructure or other possible military targets. To counter deficiencies of possible proposed definitions Hathaway proposed that "a cyber-attack consists of any action taken to undermine the function of a computer network for a political or national security purpose"[86] – with it she applies objective-based approach taken by the U.S. government, but adds a "purpose" requirement with which she very simply distinguishes cyber-attacks from cyber-crime without exhaustive discussion on the state and non-state actor issue on the matter.[87]

In conclusion, in several cases there have been successful attempts to give a legal definition to cyber-attack. Most commonly it stands out that cyber-attack is understood in the context of UN Charter articles 2(4) and 51 which immediately binds it state usage and usually with military context. The author believes that proposals by Tallinn Manual 2.0 and Hathaway are sufficient in pursuing to cover not only military aspect of the term but tries to "cast a wider net", however in order to develop a unilaterally agreeable approach to legal terms used in relation to cyberspace is most successful when done on a multilateral level

[85] Hathaway, O., *et al* (2012)*, supra nota* 11, p 824.
[86] *Ibid.*
[87] *Ibid,*p 831.

2. STANDARD OF PROOF IN STATE ATTRIBUTION OF UNLAWFUL CYBER OPERATIONS

2.1. Standard of Proof Applied by International Court of Justice and International Tribunals

2.1.1. International Court of Justice

Standard of proof varies greatly in diverse areas of international law. Similarly on a national level the international dispute settlement in civil and proceedings of criminal cases apply separate standard for evidence that the resolutions or verdicts of international tribunals and courts are based upon.

The United Nations has 193 member states who with joining the UN has adopted the UN Charter in its entirety[88]. The UN Charter article 92 enacts that the International Court of Justice shall be the principal judicial organ of the United Nations.[89] Article 93(1) enacts that all members of the United Nations are ipso facto parties to the Statute of the International Court of Justice.[90] The statute of the International Court of Justice article 36(1) states that the jurisdiction of the Court comprises all cases which the parties refer to it and all matters specially provided for in the UN Charter or in treaties and conventions in force. The following article 36(2) enact that jurisdiction of the Court include legal disputes concerning the interpretation of a treaty, any questions of international law, the existence of any fact which, if established, would constitute a breach of an international obligation. And finally as the article 38(1) enacts that court shall apply international conventions, whether general or particular, establishing rules expressly recognized by the contesting states, international custom, as evidence of a general practice accepted as law, the general principles of law recognized by civilized nations and as well as judicial decisions and the teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law.[91] Alike national courts, the ICJ has the role of developing international case law which in the past have played a key role in establishing widely accepted principles of attribution. Up to date no state have per se applied to establish whether an internationally wrongful act has been committed or in case of state attribution claimed for

[88] United Nations. Member States. http://www.un.org/en/member-states/index.html, 15 May 2018.
[89] Ühinenud Rahvaste Organisatsiooni põhikiri ning Rahvusvahelise Kohtu statuut. RT II 1996, 24, 95
[90] *Ibid.*
[91] *Ibid.*

reparations[92]. Although the Court has been said to have taken the over sides from both adversarial and the inquisitorial systems, the first authors of the PCIJ rules were on a position that the initial statute is more similar to English system, where parties were free to present their own evidence. Author agrees with opinion that, when the litigants are states, they should be the ones who has the responsibility to produce evidence that supports their claim.[93]

However, according to the ICJ internal rules a party to the dispute may request the court to obtain evidence or the Court can do it by its own initiative if it finds that the standard of proof necessary to reach a judgement has not been met. Article 48 of the Statute of ICJ states that the Court shall make orders for the conduct of the case (…) and make all arrangements connected with the taking of evidence[94]. In principle, there are no highly formalized rules of procedure governing the submission and administration of evidence before the Court, nor are there any restrictions about the what kind of evidence might be produced by parties appearing before the court[95].

In addition the article 57 of the Rules of ICJ say that without prejudice to the production of documents, each party shall communicate to the registrar, in sufficient time before the opening of the oral proceedings, information regarding any evidence which it intends to produce or which it intends to request the Court to obtain[96]. The article 62(1) states that the Court may at any times call upon the parties to produce such evidence or to give such evidence or to give explanations as the Court may consider to be necessary for the elucidation of any aspect of the matters in issue, or may itself seeks other information for this purpose[97]. Article 62(2) enacts that the Court may, if necessary, arrange for attendance of a witness or expert to give evidence in the proceedings.[98] This gives the ICJ relatively wide possibilities to determine the necessary standard of proof for each case.

The concept of an identifiable of quantifiable standard of proof emanates from the common law system, with its "beyond reasonable doubt" in criminal proceedings and the more lenient "by a

[92] The author believes that one reason, even with sufficient evidence of cyber operation being carried out that weighs damage to property, that states have not presented any claims before the Court is lack of will to create a precedent, which may be basis for future claims.
[93] Valencia-Ospina, E. (1999). Evidence before the International Court of Justice.-. *International Law FORUM Du Droit International*, vol 1, issue 4, p 202.
[94] Ühinenud Rahvaste Organisatsiooni põhikiri ning Rahvusvahelise Kohtu statuut. RT II 1996, 24, 95
[95] Tomka, P., Proulx, V. (2016). The Evidentiary Practice of the World Court. - *University of Peace Press*, p 3.
[96] International Court of Justice. (1978). *Rules of Court*. Accessible: http://www.icj-cij.org/en/rules, 15 March 2018.
[97] *Ibid.*
[98] *Ibid.*

preponderance of the evidence" in civil proceedings. The system of ICJ appears to reflect the civil law system, in court must be convinced, without reference to a specific standard. The only guidance offered by the Statute with respect to the standard of proof is article 53, which provides that in the case of a party's failure to appear or defend its case, the Court may rule in favor of the other party, but only after it has satisfied itself that it has jurisdiction, and "that the claim is well founded in fact of law"[99]. International jurisprudence "has always avoided a rigid rule regarding the amount of proof necessary to support the judgement"[100]. When it comes to cyberspace, one of its main advantages is that it offers malicious actors a possibility to keep their anonymity and if necessary even to spoof state's identity. Strong disagreement exists whether international law imposes on victim states a duty to meet a standard of proof prior to exercising self-defense. Some international lawyers argue that, prior to taking action, a responding state must achieve a requisite degree of certainty as to attribution akin to meeting an evidentiary standard in litigation as part of the law of state responsibility.[101]

As there in no unilateral standard of proof developed for the attribution of internationally wrongful act, the Court and international tribunals have to assess each dispute by case-by-case approach. This has resulted in different standards set for the threshold of evidence and quality of them. The rule of thumb for evidentiary matters before the Court is flexibility. In short, in deciding the cases submitted to it, the overarching objective of the Court is to obtain all relevant evidence pertaining to both facts and law that may assist it in ruling on issues of substance, as opposed to providing a judicial outcome grounded primarily on technical and/or procedural rationales.[102]

In general, the ICJ do not apply the same high standard as does the ICC where the article 66(3) of Statute of Rome enacts that in order to convict the accused, the Court must be convinced of the guilt of the accused beyond reasonable doubt[103] and since in practice state responsibility does not require such high threshold the author will not add ICC applied standard in its analysis.

---

[99] Law Teacher. (2013). Rules of evidence before the international court of justice. Accessible: https://www.lawteacher.net/free-law-essays/international-law/rules-of-evidence-before-the-international-court-of-justice-international-law-essay.php#citethis, 15 March 2018.
[100] Foster, C. (2010). Burden of Proof in International Courts and Tribunals. - *Australian Year Book of International Law*, vol 29, p 34.
[101] Osula, A-M., Rõigas, H. (2016). International Cyber Norms. Legal, Policy & Industry Perspectives. *NATO CCD COE Publications,* p 55.
[102] United Nations. (2014). *Meeting coverage*. Accessible: https://www.un.org/press/en/2014/gal3490.doc.htm, 15 March 2018.
[103] Rahvusvahelise Kriminaalkohtu Rooma statuut. RT II 2002, 2, 5.

The Corfu Channel Case (United Kingdom v Albania) is noteworthy from two aspects – first, as it appears, the Court applies separate standards of proof upon the parties to the dispute and subsequently separate evidentiary quality. It was submitted to the Court to determine whether "Albania was responsible under international law for the explosion (…) in Albanian waters and for the damage and loss of human life which resulted from them and is there any duty to pay compensation"[104]. In this case the Court states that a charge of such "exceptional gravity against a state would require a degree of certainty" when addressing a statement by a witness on behalf of the UK[105]. The Court continues that "even in so far as these facts are established, they lead to no firm conclusions"[106] and the "proof may be drawn from inferences of fact, provided that they leave no room for reasonable doubt"[107].

An important principle established with the Corfu Channel case which most certainly rise in case of states' obligation not to allow malicious use of ICTs in its territory and attribution of it – a rule agreed by the UN GGE and analyzed in length in Tallinn Manual 2.0. The Court states that it cannot be concluded from the "mere fact of the control exercised by a state over its territory and waters that that state necessarily knew; or ought to have known, of any unlawful act perpetrated therein, nor yet that it necessarily knew, or should have known the authors"[108]. That does not however, incur immediate responsibility or should alter the burden of proof on the other party. Following the court establishes an important principle by stating that "by reason of exclusive control, the other state, the victim of a breach of international law, is often unable to furnish direct proof of acts giving rise to responsibility. Such a state should be allowed a more liberal recourse to interferences of fact and circumstantial evidence. This indirect evidence is admitted in all systems of law, and its use is recognized by international decisions. It must be regarded as of special weight when it is based on a series of facts linked together and leading logically to a single conclusion" [109]. The Court with this statement offers a concrete leniency towards standard of proof in relation to the issue of collecting evidence in a situation where it may not be enabled nor possible.

[104] The Corfu Channel case, *supra nota* 20, p 12.
[105] *Ibid*, p 17.
[106] *Ibid.*
[107] *Ibid*, p 18.
[108] *Ibid*.
[109] *Ibid*.

However, some scholars have found that although in the Corfu Channel case the Court allowed more tolerant option regarding presenting evidence, the standard of proof in an international court or tribunal should not be lowered simply because it is difficult to reach. The standard offers assurances against untrue attribution, which is a particularly serious problem in the cyber context.[110] The very same is relevant to attribution of cyber operations due to the fact that very often the operations vary by their intensity and impact. Other than that, the evidence collecting is often complicated since the aim of the cyber operation or cyber-attack usually is to conceal the perpetrator which in the future proceedings may require analogous approach when considering whether a cyber operation was in fact internationally wrongful act.

On a side-note, the one principle that the Court based its decision om regarding responsibility of Albania, derives from the PCIJ Lotus case where the Court stated that "the first and foremost restrictions imposed by international law upon a state is that (…) it may not exercise its power in any form in the territory of another state"[111]. Put in a cyber context, in some cases a mere conduct of a cyber operation against non-state actors might violate the sovereignty of another state. According to Michael Schmitt example of violation of the principle would be when cyber operation by public authority of one state targets a private entity of another, that may provoke responsibility of the state based on violation of sovereignty. [112] As it was previously mentioned, according to the UN GGE cyber operations are not beyond the reach of sovereignty and neither do ICT infrastructure[113] which means if a cyber operation breaches the sovereignty of another state it is prohibited by international law and may constitute to a internationally wrongful act. According to the Tallinn Manual if an agent of a state uses USB flash drive to introduce malware into cyber infrastructure located in another state, a violation of sovereignty has taken place[114]. This means that most cyber operations which aims to plant malware to injured state's computer system violates state sovereignty, including 2008 attack against U.S. Department of Defence today know as Operation Buckshot Yankee, when its systems were compromised due to one official inserting a USB stick into his military provided computer.[115] This raises the issue of phising e-mails – does

[110] Roscini, M. (2015). Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations. - *Texas International Law Journal*, vol 50, issue 2 - 3, p 251.
[111] The Case of the S.S. „Lotus", p 18, PCIJ 1927.
[112] Schmitt, M., Watts, S. (2016). Beyond State-Centrism: International Law and Non-State Actors in Cyberspace. - *Journal of Conflict & Security Law*, vol 21, issue 3, p 598.
[113] UN GGE report of 2013*, supra nota* 33.
[114] Schmitt (2017), *supra nota* 18, p 19.
[115] Mudrinich, E. (2012). Cyber 3.0: The Department of Defence Strategy for Opening in Cyberspace and the Attribution Problem. - *The Air Force Law Review*, vol 68, p 198.

sending one with the aim to breach the integrity of a computer system or does the malware need to be activated in order it to constitute a breach as such.

The authors of Tallinn Manual 1.0 have written that state practice provides sufficient evidence that ICT infrastructure falls under the scope of principle of sovereignty. This implies corresponding due diligence duties.[116] Due diligence consists of sub-duties such as adopting necessary regulations, carrying out investigations and complying with international cooperation. The key issue here is the "should have known" and "must have known" principles which possess lower and higher standards of proof respectively.[117] Once again in the Corfu Channel case the Court held Albania liable for harm to the UK, even though there was no direct evidence that Albania knew of the harm. In this case the Court concluded that given the circumstances, Albania must have known about the emplacement of the mines that caused the harm.[118]

During the Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States) the Court uses the term "satisfy itself" which implies that the Court "must attain the same degree of certainty as in any other case that the claim of the party appearing is sound in law, and, so far as the nature of the case permits, that the facts on which it is based are supported by convincing evidence."[119] The Court continues with that for the purpose of deciding whether the claim is well founded in law, the principle jura novit curia[120] signifies that the Court does not have to reach its decision only based on arguments given by the parties and therefore can reach its judgement without one party present.[121] This was the Courts approach to the standard of proof in a position where the United States ceased to participate in the proceedings after the Court declared that the dispute do fall under the scope of its jurisdiction.

The Court also hints for a sufficiency of evidence where it explains, if the Court were to "conclude in the present case, for example, that the evidence was not sufficient for a finding that the United States had used force against Nicaragua, the question of justification on the grounds of self-defense

[116] Jensen, E. (2015). Cyber Sovereignty: The Way Ahead. - *Texas International Law Journal*, vol 50, issue 2-3, p 297.
[117] *Ibid*, p 298.
[118] The Corfu Channel case, *supra nota* 20, p 19 - 20
[119] Military and Paramilitary Activities in and against Nicaragua*, supra nota* 21, p 14.
[120] Mantakou, A. The Misadventures of the Principle Jura Novit Curia in International Arbitration - A Practitioner's Approach.- *Hellenic Institute of International and Foreign Law*, p 488. „Thus, based on the Jura Novit Curia principle, the Judge ort he Court, has the power and the duty to base its decision or rely upon rules, law provisions, legal theories, case law or general principles of the applicable law not advanced by the parties during the procedure." Accessible: http://www.hiifl.gr/wp-content/uploads/MANTAKOUjuranovitcuria.pdf, 17 March 2018.
[121] Military and Paramilitary Activities in and against Nicaragua*, supra nota* 21, p 14.

would not arise, and there would be no possibility of El Salvador being "affected" by the decision."[122]

In addition, the Court can give some weight as an evidence to a public knowledge[123] but it has to be in accordance with rest of the evidence but it certainly must be in accordance with the main facts and circumstances of the case[124]. In the cyber context the credibility of attribution is in great correlation with depiction of it in public, especially in cases where the effects of a cyber operations are mainly suffered by either private entities, including civilians or critical infrastructure. One example of this would be the NotPetya ransomware attack. Although the political response to it has been relatively minimal – six democratic countries have attributed NotPetya cyber-attack to Russia, however, public attribution is a strong signal that the West is not going to tolerate increasing recklessness forever[125] and public has a vital role here to play.

The Court continues with how testimonies are handled in a case. It states that "testimonies, that do not declare a statement of fact, but a mere expression of opinion as to the probability or otherwise of the existence of such facts, not directly known to the witness, may be highly subjective and cannot take the place of evidence. However, it may, in conjunction with other material, assist the Court in determining a question of fact, but is not proof itself"[126]. This principle was already established with the Corfu Channel case, where the court stated that witness statements should be regarded as allegations[127].

And finally, when applying the effective control test in order to determine whether the United States did preside level of that control over the contras the Court stated that there is no clear evidence of the control being established in order to determine that the contras acted on behalf of the U.S.[128] The Nicaragua judgement is today perceived as embodying a rather strict standard for attribution, which played vital role in drafting of article 8 of the Draft Articles under professor James Crawford[129].

[122] *Ibid*, p 27.
[123] *Ibid,* p 30.
[124] *Ibid*, p 31.
[125] Pernik (2018)*, supra nota* 29.
[126] Military and Paramilitary Activities in and against Nicaragua*, supra nota* 21, p 32.
[127] The Corfu Channel case, supra nota 20, p 16.
[128] Military and Paramilitary Activities in and against Nicaragua*, supra nota* 21, p 52.
[129] Mačák (2016), *supra nota* 28, p 413.

However, there is another meaningful principle that derived from the Nicaragua judgement related to evidence and standard of proof which, in the future, may play an important role in the cyber context as well. The Court stated that one of the main challenges in the Nicaragua case was to determine which of the presented facts were significant to the case[130]. In the the said situation the principle emanating from article 53 of the ICJ statute played an important role which in addition to previously analyzed articles sets an additional standard for evaluating evidence and thus setting another standard of proof. The article states that "if one party does not appear before the Court it has the right, if requested by the other party, to solve the dispute in their favor. The article continues that the court has to satisfy itself (…) that the claim is well founded in fact and law".[131] Thus the Court must determine if the claim brought before them is valid to be assessed which brings forth the issue of quality and quantity of evidence. That in case of attribution might be rather challenging to obtain due to the vast possibilities of anonymity an attacker might conceal themselves behind to – this might be the case where the Court in their future assessment may ponder on state practice of public attribution.

In the Case Concerning United States Diplomatic and Consular Staff in Tehran (United States of America v Iran) the Court, in order to establish, whether the militants acted on behalf of Iran, stated that the "information before the Court does not, however, suffice to establish with the requisite certainty the existence at that time of such a link between the militants and any competent organ of the state".[132]

Following on with the Case Concerning Oil Platforms (Islamic Republic of Iran v United States of America) where the dispute concerned an attack and destruction of offshore oil production complexes which belonged to Iranian Oil Company, by warships belonging to the United States[133]. Similar to the Nicaragua case the Court again points to the satisfaction of the Court[134]. The Court sums up that for the present purposes, the Court has simply "to determine whether the United States has demonstrated that it was the victim of an armed attack by Iran such as to justify it using armed force in self-defense; and the burden of proof of the facts showing the existence of such an attack rests on the United States. The Court does not have to attribute responsibility for firing the missile that struck the Sea Isle City, on the basis of a balance of evidence, either to Iran or to Iraq;

[130] Military and Paramilitary Activities in and against Nicaragua*, supra nota* 21, p 29.
[131] Ühinenud Rahvaste Organisatsiooni põhikiri ning Rahvusvahelise Kohtu statuut. RT II 1996, 24, 95.
[132] Case Concerning United States Diplomatic and Consular Staff in Tehran*, supra nota* 22, p 30.
[133] Oil Platforms (*Islamic Republic of Iran v United States of America*), p 45, ICJ 2003.
[134] *Ibid*, p 22.

if at the end of the day the evidence available is insufficient to establish that the missile was fired by Iran, then the necessary burden of proof has not been discharged by the United States".[135] The Court settles that it can not attribute responsibility if evidence presented to it are insufficient and says that albeit the evidence is highly suggestive, it is not conclusive.[136]. The Oil Platform case has prompted an important discussion over anticipatory self-defense and if the degree and nature of the evidence needed to make the determination that an attack is imminent. This is just as critical issue in the cyber security – if there is possibility for a anticipatory move to deter imminence which could be based on either human intelligence, technical intelligence or signals intelligence. [137]

For the Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda) the Court states that "it has not only the task of deciding which of presented materials must be considered relevant, but also the duty to determine which of them have probative value with regard to alleged facts"[138]. The Court continues with that it has to make its clear assessment of their "weight, reliability and value"[139]. Regarding applied standard in its decision-making the Court says that it will "embark upon its task by determining whether it has indeed been proved to its satisfaction that Uganda invaded DRC" (…)[140] and it "must establish relevant facts it regards as having been convincingly established by evidence"[141]. However, as a resolution the Court convincing evidence that Ugandan forces were present are lacking[142] and finds that evidence are weighty and convincing[143]. In this case the continuous standard was set as the presented evidence must be weighty and convincing.

In a Land, Island and Maritime Frontier Dispute (El Salvador/Honduras and Nicaragua intervening) which concerned a delimitation of the frontier line in the six sectors not delimited by the 1980 General Treaty of Peace and to determine the legal situation of the islands in the Gulf of Fonseca and the maritime spaces within and outside it[144]. When the Court is discussing placenames mentioned, which Honduras is applying to be attached certain points, the Court states that it has

[135] *Ibid*, p 32.
[136] *Ibid*, p 38.
[137] Kehler, R., Lin, H., Sulmeyer, M. (2017). Rules of Engagement for Cyberspace Operations: a View From the USA. - *Journal of Cybersecurity*, vol 3, issue 1, p 73.
[138] Armed Activities on the Territory of the Congo (*Democratic Republic of the Congo v Uganda*), p 36, ICJ 2005.
[139] *Ibid*.
[140] *Ibid*, p 37.
[141] *Ibid*, p 41.
[142] *Ibid*, p 45.
[143] *Ibid*, p 56.
[144] Land, Island and Maritime Frontier Dispute (*El Salvador/Honduras: Nicaragua intervening)*, p 13, ICJ 1992.

not provided any evidence justifying it. It continues that "it considers, on a balance of probabilities, there being no great abundance of evidence either way (…)"[145].

In the Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro) the Court establishes when it comes to charges that bears exceptional gravity must be substantiated by evidence that is fully conclusive. The parties to the dispute argued on the matter of standard of proof where the applicant found that "the matter is not one of criminal law" and applicable standard is the balance of evidence or the balance of probabilities. The respondent however pointed to gravity of the issue and therefore the standard required is proper degree of certainty.[146] The Court agreed with the respondent and that it requires that it be "fully convinced that allegations made in the proceedings, that the crime of genocide or the other acts enumerated in Article III have been committed, have been clearly established. The same standard applies to the proof of attribution for such acts".[147]

2.1.2. International tribunals

The former substitute judge on the Iran-U.S. Claims Tribunal Charles Brower said in his article that often tribunals prefer not to adopt clear-cut rules of evidence in order to be able to accept variety of evidence that can be evaluated by their "relevance, credibility and weight".[148] He continues to explain that although parties to the dispute have the authority to put forward any evidence they find relevant to support their claims, eventually it is prerogative of the tribunal to assess which of the presented evidence suffice and retain the right of discretion to determine otherwise[149].

Beyond the ICJ there are several international tribunals that have developed international case law. For example, article 1 of the statute of the ICTY states that "the International Tribunal shall have the power to prosecute persons responsible for serious violations of international humanitarian law committed in the territory of the former Yugoslavia since 1991 in accordance with the provisions

[145] *Ibid*, p 159.
[146] *Ibid*, p 90.
[147] *Ibid*.
[148] Brower, C. N. (1994). Evidence before international tribunals: The need for some standard rules. *International Lawyer,* p 48.
[149] *Ibid.*, p 52.

of the present statute."[150] In order to execute its tasks it must reach its judgements based on article 15 which allows the tribunal to adopt rules of procedure and evidence and puts an obligation upon states to assist with production of evidence if necessary according to the article 29 of the statute[151]. This means that the tribunal has the right to gather evidence if necessary in order to reach required threshold for sufficient evidence. The referred rules of procedure indicate the standard of proof applied by the ICTY. According to the rule 87(A) "a finding of guilt may be reached only when a majority of the Trial Chamber is satisfied that guilt has been proven beyond reasonable doubt."[152] The same goes for the International Criminal Tribunal of Rwanda (ICTR)[153]. This indicates that the standard of proof in cases assessed by those tribunals is similar to the one adopted by the ICC. However the rule 89(B) sets an exception from the "beyond reasonable doubt" standard. It states that "in cases not otherwise provided in rules of evidence section, a chamber shall apply rules of evidence which will best favor a fair determination of the matter before it and are consonant with the spirit of the statute and the general principles of law."[154] This offers the tribunal necessary leniency when assessing presented evidence because as it resulted in the Tadić and Nicaragua case the state responsibility issue in the attribution context does not in all situations need assessed based on the principle of criminal liability. The same applies to the ICTR since their procedural normative framework under UN is similar with the ICTY. As already previously mentioned the "beyond reasonable doubt" evidentiary standard does not suffice in state attribution of cyber operations. This mainly due to the principle already emphasized previously – simple use of proxies should not offer a possibility to evade responsibility however, that does not suggest however that attribution should be made lacking evidence.

The standard of proof in the Tadić case could be found in several statements that pass the "beyond reasonable doubt". Although the tribunal mostly refers that presented evidence must allow conclusion of beyond reasonable doubt, there are some instances where it presents some leniency to it. For example, when the tribunal discusses whether or not armed forces could be considered de facto organs or state agents of the FRY it stated that "there is, in short, no evidence on which this Trial Chamber may confidently conclude that the armed forces of the RS and the RS as a

[150] United Nations. (2009). Updated Statute of the International Criminal Tribunal for the Former Yugoslavia. Accessible: http://www.icty.org/x/file/Legal%20Library/Statute/statute_sept09_en.pdf, 29 April 2018.
[151] *Ibid.*
[152] United Nations. (2015). Rules of Procedure and Evidence for the International Criminal Tribunal for the Former Yugoslavia. Accessible: http://www.icty.org/x/file/Legal%20Library/Rules_procedure_evidence/IT032Rev50_en.pdf, 16 April 2018.
[153] United Nations. (1995). Rules of Procedure and Evidence for the International Criminal Tribunal for Rwanda. Accessible: http://unictr.unmict.org/sites/unictr.org/files/legal-library/150513-rpe-en-fr.pdf, 16 April 2018.
[154] *Ibid.*

whole, were anything more than allies, albeit highly dependent allies, of the Government of the FRY."[155] Therefore evidence presented to the tribunal should allow members of it to reach a confident conclusions. However judge McDonal in his dissenting opinion found that "evidence supports a finding beyond reasonable doubt that the VRS acted as an agent of the FRY."[156]

The Eritrea-Ethiopia Claims Commission also found that there was "clear evidence" that events in the vicinity of Badme were minor incidents and did not reach the magnitude of an armed attack. The judgement of the commission results that the it requires "clear and convincing evidence"[157]. In the Iran – United States Claims Tribunal has affirmed, "in order to attribute an act to the state, it is necessary to identify with reasonable certainty the actor and their association with the state"[158].

However, state responsibility attribution issues are not only discussed in the context of criminal liability. In the case of Air Service Agreement (United States of America v France) when appropriate countermeasures according to the article 22 of ILC Draft Articles were under discussion, the tribunal admitted that deciding, whether a measure was proportionate, is not always simple and could in general be done by approximation. The tribunal continues to explain that parties to the dispute have failed to present "evidence that would be sufficient to affirm or reject the existence of proportionality in these terms, and the tribunal must be satisfied with a very approximate appreciation."[159]

In the International Fisheries Company v United Mexican States case the U.S. company claimed damages from Mexican Government for cancellation of an order. The tribunal states in several occasions that it requires "proof of convincing evidence".[160] When there was a state responsibility issue under discussion the tribunal reiterated that "denial of justice resulting from improper judicial procedure is not the only ground of diplomatic interposition. (…) moreover, from a practical standpoint, much can be said in favor of the view that denial of justice, broadly speaking, may properly be regarded as the general ground of diplomatic intervention. In other words, that on the

[155] United Nations. (1997). Tadić case: the verdict. Accessible: http://www.icty.org/en/press/tadic-case-verdict, 1 May 2018.
[156] *Ibid.*
[157] Eritrea-Ethiopia Claims Commission – Partial Award: Prisoners of war – Eritrea's Claim, p 71, Reports of International Arbitral Award 2003.
[158] International Law Commission (2001), *supra nota* 10, p 39.
[159] Air Service Agreement of 27 March 1946 between the United States of America and France, p 443, Reports of International Arbitral Awards 1978.
[160] International Fisheries Company (U.S.A.) v.United Mexican States, p 736, Reports of International Arbitral Awards 1931.

basis of convincing evidence of a pronounced degree of improper governmental administration on the part of the legislative, executive or judicial branch of the Government, one nation may properly call another to account."[161]

In the Island of Palmas case (Netherlands v United States of America) where the main question included the problem of differences in respecting sovereignty over the Island of Palmas, the standard was set rather concretely. The arbitrator states that "it is for the arbitrator to decide both whether allegations do or – as being within the knowledge of the tribunal – do not need evidence in support and whether the evidence produced is sufficient or not (…). This liberty is essential to him, for he must be able to satisfy himself on those point which are necessary to the legal construction upon which he feels bound to base his judgement. He must consider the totality of the allegations and evidence laid before him by the parties, either motu propio or at his request and decide what allegations are to be considered as sufficiently substantiated."[162] Therefore the standard of proof in this case is bilateral – first, the arbitrator must ascertain that presented evidence is sufficient in their totality to endorse claims and second, evidence presented must satisfy the arbitrator for him to formulate legal conclusions.

It is apparent that the ICJ at some point has to weigh in on the cyber issue. When briefly considering pending cases there is 2017 Ukraine application against Russia concerning application of the International Convention for the Suppression of the Financing of Terrorism and of the International Convention of the Elimination of All Forms of Racial Discrimination.[163] With its application the representatives of Ukraine pleads for court's temporary order protect people of Ukraine. Although the main claim concerns the issue of supporting terrorism and racial discrimination, it raises the issue how Russian Federation committed concerted campaign of illegal interventions against Ukraine causing numerous violations of international law, which includes "support for terrorism and acts of racial discrimination, as well as propaganda, subversion, intimidation, political corruption, and cyber-attacks three years ago".[164]

[161] *Ibid.*, p 712.
[162] Island of Palmas case (Netherlands, USA), p 841, Reports of International Arbitral Awards 1928.
[163] Application of the International Convention for the Suppression of the Financing of Terrorism of the International Convention on the Elimination of All Forms of Racial Discrimination (*Ukraine v Russian Federation*), ICJ 2017.
[164] *Ibid.* The Ukraine invokes ICJ jurisdiction under the Terrorism Financing Convention to hold Russia to account for its role financing of terror, Ukraine claims under CERD to ask Russia to keep its commitment not to discriminate on grounds of race and ethnicity while occupying Crimea and apply provisional measures until court's judgement.

The ICJ judge Trindade with his dissenting opinion for the Case Obligations Concerning Negotiations Relating to Cessations of the Nuclear Arms Race and to Nuclear Disarmament (Marshall Island v United Kingdom) admits the risk cyber operations have to assuring safety of management of nuclear weapons. He states that as long as nuclear weapons exist, there remains a possibility of a nuclear weapon explosion. The risk of "accidental, mistaken, unauthorized or intentional use of nuclear weapons are evident due to the vulnerability of nuclear command and control networks to human error and cyber-attack (…)."[165]

To sum up the findings from chapter two, it can be said that the standard of proof applied by the ICJ and by many of the international tribunals, in its proceedings for state attribution of internationally wrongful acts, have adopted more lenient threshold similar to which is applied in national civil proceedings. Although the standard often varies in terminology – well founded in fact and law, offers a degree of certainty or a firm conclusion, leave no room for reasonable doubt, satisfy itself, convincing evidence, sufficiency of evidence, clarity of evidence, balance of evidence, weighty and convincing evidence, evidence that offer reasonable certainty, proof of convincing evidence, balance of probabilities, proper degree of certainty and often regarded standard of preponderance of evidence – it does aim at a similar point what has been considered when reaching a judgement on a either state responsibility for conduct of a state agent or conduct of a non-state actor that can be determined as conduct attributable to that state and tends to align with a proof by a preponderance of the evidence. It is evident by the case analysis that the standard of proof varies depending on what is the subject of the dispute and in what stage the proceedings are. This is the principle that the states and the court must consider in their attribution of cyber operations.

James Green in his analysis came to similar conclusion, that "in general, international law does not have a clear benchmark against which the persuasiveness or reliability of evidence may be gauged for the purposes of attributing responsibility or assessing legal claim."[166] He finds in his assessment, which supports the analysis of the author, that there are some standards that have surfaced through different proceedings – total of four different ones. The first one would be "prima facie" standard – according to Green "this represents a test of very low degree with regards to the assessment of evidence, it simply requires that the evidence produced is indicative of the

[165] Dissenting Opinion of Judge Cancado Trindade, p 78, ICJ 2016.
[166] Green, J. (2009). Fluctuating Evidentiary Standards for Self-Defence in the International Court of Justice. – *International and Comparative Law Quarterly*, vol 58, issue 1, p 165

proportion claimed."[167] The second is what was already previously established by the ICJ judge as well – the preponderance of evidence, or balance of probabilities – in this case, the evidence presented must be more convincing than ones that are presented against it.[168] According to Green the third one is "clear and convincing" standard – this one requires for a party "to convince the judge that it is substantially more likely than not that the factual claims that have been made are true"[169] And the forth one is the "beyond reasonable doubt" standard which in case of cyber operations have not yet been applied.

Judge Higgins in her separate opinion on the Oil Platforms case emphasized that more severe accusations require higher confidence in the evidence presented. She states an important principle – ICJ should take a more transparent approach what kind of standard of proof it needs for establishment of which facts, even if it concerns cases that do not possess elements of criminal proceedings.[170] The severity of the matter of the dispute, based on the case law analysis, in addition shows, that in some cases the standard of proof may be lower when the matter is of passive activity of a state or in other words if it fails to fill its international obligations (for example the Corfu Channel case) and higher when a state has caused damage, harm or injury with by a activity (for example Nicaragua case).

The author however, agrees with statement made by the ICJ in the Corfu Channel case where it allows more lenient standard of proof by raising the merit of presented circumstantial evidence when conclusive evidence may not be enabled nor possible to obtain. In addition, the author is in the position that states during their global or regional discussions on development of cyber norms should take more broadly on board the principle that plausible deniability due to the fact that proxy groups have been deployed can not offer concealment from responsibility. This standpoint is supported by both work of the UN GGE and experts of the Tallinn Manual 2.0 and as well as by the practice of ICJ and international tribunals. When to take that into consideration it can be said that there is not a one level international standard of proof but the ICJ and international tribunals have set a certain threshold for the capacity of evidence in cases where the issue does not necessarily include threats of or uses of force or breaches beyond that.

[167] *Ibid*., p 166
[168] *Ibid*., 167
[169] *Ibid.*
[170] Separate Opinion of Judge Higgins on the Corfu Channel case, p 77, ICJ 1998.

2.2.State Conduct During Peacetimes and Standard of Proof

From previous, it can be said that the attribution can be two leveled where the initial process of attribution is carried out by an injured state. The injured state, while making its assessment based on evidence at hand and deliberating on appropriate response, it must approach from principles set by international law – among those proportionality and necessity – to reach a sufficient standard of responsibility for said acts to be proven to have been committed by a guilty state. However, while states put forward their claims outside the courtroom, the issue of standard of proof varies even more and the set standards are not always communicated to the public to support the actions of the injures state or applied countermeasures.

The UN GGE briefly discussed the issue that it may not be enough to attribute a cyber operation to another state if the injured state has an indication that an activity was either coming from or was discharged from another state's territory or the activity was linked to ICT infrastructure belonging to that state. They emphasized that such allegations should be substantiated, which indicates towards the disclosure of evidence.[171] The experts of Tallinn Manual 2.0 agreed that such an approach is reasonable and may contribute in averting unnecessary political tensions, but on the other hand find that "insufficient state practice and opinio juris (in great part because cyber capabilities are in most cases highly classified) exist to conclude that there is an established basis under international law for such obligation. They acknowledged, however, that a few states have taken the position that there is a legal obligation to disclose evidence on which attribution is based whenever taking actions in response to cyber operations that purportedly constitute an internationally wrongful act."[172] Following the author analyses the state conduct in cyberspace during peacetimes, based on which evidence state attribution have been carried out and how they coincide with practice of ICJ and international tribunals.

Although the attribution and evidence related problems outside the courtroom are key issues from cyber perspective, there are similar concerns in areas different from cyber which goes to show that the question of attribution and finding relevant evidence to support is far from only in cyber context. One of the most contradictory examples would be the Salisbury case where a nerve agent was used on a former Russian agent and his daughter. The main explanation released to the public related to attributing the attack to Russia is that since the nerve agent used on the victims was

[171] UN GGE 2015 report, *supra nota* 33, p 13.
[172] Schmitt (2017), *supra nota* 18, p 83.

initially developed in Russia, it is highly likely that Russia was behind it and emphasizing that violation of the UK sovereignty was assaulted by Russia and therefore chemical weapons convention and international law obligation was breached.[173] France, Germany and the U.S. joined with an explanation that it was highly likely that Russia was behind the attack and shared its assessment that there is no plausible alternative explanation[174] and with them joins Foreign Affairs Council comprised by foreign ministers of EU by admitting that this is a breach of international law[175]. Countermeasures applied included several EU and NATO member states and as well as third countries to expell Russian diplomats or imposed restrictive sanctions on Russia or its citizens[176]. The communication to the public regarding evidence at hand were rather limited. Weeks later the media reports that the research center conducting the analysis failed to confirm that the poison was created in Russia, this was explained by British officials that those inconclusive results were only a mere part of intelligence based evidence that allowed such conclusions. Prime minister May explained to public that Russia still is capable to produce said nerve agent and brought the attention to Russia's previous alleged practice of state-sponsored assassinations[177]. This certainly gives rise to several questions, including whether the attribution is done correctly and are the evidence sufficient. Understandably in order to not disclose methodology for evidence collecting the public and private attribution vary but question of have the sufficient standard of proof have been achieved?[178]

International law professor Marco Roscini in his article, when analyzing Matthew Waxman's work on "The Use of Force Against States that Might Have Weapons of Mass Destruction", references Waxman's position "that previously applied thresholds for evidence has been working well,

[173] Walker, P. (2018). *UK, US, Germany and France unite to condemn spy attack*. Accessible: https://www.theguardian.com/uk-news/2018/mar/15/salisbury-poisoning-uk-us-germany-and-france-issue-joint-statement, 21 March 2018.
[174] Hughes, L., Bond, D., Peel, M. (2018). *US, Germany and France blame Russia for nerve agent attack*. Accessible: https://www.ft.com/content/81edb2ee-284b-11e8-b27e-cc62a39d57a0, 21 March 2018.
[175] Council of the European Union. (2018). *Statement by the Foreign Affairs Council on Salisbury attack*. Accessible: http://www.consilium.europa.eu/en/press/press-releases/2018/03/19/statement-by-the-foreign-affairs-council-on-the-salisbury-attack/, 21 March 2018.
[176] Ferris-Rotman, A. (2018). *Expelled from Russia, U.S. diplomats bid a wistful farewell*. Accessible: https://www.washingtonpost.com/news/worldviews/wp/2018/04/08/expelled-from-russia-u-s-diplomats-bid-a-wistful-farewell/?noredirect=on&utm_term=.a78f1261a407, 1 May 2018.
[177] Morris, S., Bannock, C. (2018). *Salisbury attack: what has the UK said and what evidence does it have?* Accessible: https://www.theguardian.com/uk-news/2018/apr/04/salisbury-attack-what-has-the-uk-said-and-what-evidence-does-it-have, 1 May 2018.
[178] On a sidenote the author wants to explain that although the attribution issues in Salisbury case are in somewhat similar to those met in attribution of unlawful cyber operations the issue at hand is very different. In the salisbury case the instrument to carry out an illegal attack – Novichok nerve agent – is prohibited according to the Chemical Weapons Convention which both Russia and the UK are members of. Today there is no ICT instrument that is prohibited Under International law or treaty.

however that is the case in the world of conventional threats, but mainly because states' capabilities could be evaluated with rather high certainty", nonetheless "the required degree of certainty about capability ought to vary with certainty about intent"[179]. Roscini adds a valid comparison that when seen in cyber context, if the possibility that another state is able and willing to apply cyber means is more probable then the evidentiary threshold should be lower as well[180]. This is an element that coincides with some of the ICJ's applied standards.

Since this section of the thesis analyses attribution and standard of proof during peacetimes, the analysis does not include cyber operations conducted during an armed conflict.

2.2.1. Estonia 2007

The first case the author analyses is the 2007 cyber operations that targeted Estonia. During may Estonia was targeted by large-scale cyber intrusion operations. As the history shows in spring of 2007 tensions between Russia and Estonia began to rise when Estonian Government decided to move the statue called "Pronkssõdur" which set off riots that lasted for about two days. The riots however were followed DDoS attacks that targeted both government websites as well as private companies that lasted in total approximately up to three weeks.

According to a study carried out by NATO CCD CoE researchers Eneken Tikk, Kadri Kaska and Liis Vihul the attacks had two main phases – the "emotional response" and "main attack" which itself included four different waves an attack. The initial phase the intrusions were rather simple. According to the study, several Russian-language web-forums calls and instructions were posted on to and how carry out DDoS attacks against Estonian websites. That was followed by "malformed web queries" which indicates more detailed measures in order to carry out the cyber operation. The second phase continued with dispersing instructions via web-forums which initiated possible hackers to carry out said operations at a set date and time. The sophistication of the second phase of attacks could be found in that the attacks "showed remarkable intensification and precision in concentration, which indicated the use of botnets."[181] With the second wave, which was expected to take place in 9th of May due to a Russian national holiday, the biggest

[179] Roscini, M. (2015). Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations. – *Texas International Law Journal*, p 250 referenced in Waxman (Waxman, M. The Use of Force Against that Might Have Weapons of Mass Destruction, MICH. J. INT'L. L. 1, 2-3 2009).
[180] *Ibid.*
[181] Eneken Tikk, Kadri Kaska, Liis Vihul. (2010). International Cyber Incidents – Legal Considerations. - *NATO CCD CoE Publications*, p 18 – 20.

targets were banking websites. The third wave of coordinated attacks according to Estonian CERT team included more than 85 thousand botnets all over the world and the final wave of operations continued in that matter and eventually died off.[182]

When analyzing what types of intrusions were used the research states that DDoS attacks against specific government websites, as well as private enterprises. The authors call that the attackers chose some "critical information infrastructure targets"[183], which indicates selective decision-making. The second phase of attacks according to the research "confirmed by log analysis, involved coordination and recourses unavailable to ad hoc regular citizen protest. It had features of central command and control and required both financial and intellectual resources."[184] During the analysis it was discovered that some of the attackers IP addresses were identified as Russian, in some instances those IP addresses belonged to Russian state institutions. The counterargument was that those were simple spoofs. However, another indication of planned strategy is that "the attackers had purposefully moved botnet C&C servers to less friendly or less advanced jurisdictions"[185] and including some regions that are not internationally reckognized – Moldovan region Transdniester. There were some who proclaimed to have carried out the large-scale intrusions – including commissar of youth movement Nashi, an IT student[186] and even an assistant to the Duma member.[187]

In order to determine an attacker behind the intrusions, Estonia presented an application to Russia based on article 3 of the Agreement on Mutual Legal Assistance between Estonia and Russia to provide assistance with specific questions presented with the application. However, Russia refused the request with an explanation that requested assistance is not regulated with the agreement.[188] When the state prosecutor explained that reasons for refusal are not sound and have previously cooperated with Estonian state institutions on similar ground, the refusal stood out for another reason as well. Namely, in order to resolve the situation of restoring normal functioning of networks, follow how the situation develops and expertise on technical support, Estonia required

[182] *Ibid.*
[183] *Ibid.*
[184] *Ibid.*, p 23
[185] *Ibid.*, p 28
[186] Arthur, C. (2008). *That cyberwarfare by Russia on Estonia? It was one kid.. in Estonia.* Dmitri Galushkevich who was later fined for defacement of the Reform Party website. Accessible: https://www.theguardian.com/technology/blog/2008/jan/25/thatcyberwarfarebyrussiaon, 2 May 2018.
[187] Eneken Tikk, Kadri Kaska, Liis Vihul (2010), *supra nota* 201, p 23.
[188] Pau, A. (2007). Venemaa keeldus koostööst küberrünnakute uurimisel. Accessible: http://epl.delfi.ee/news/eesti/venemaa-keeldus-koostoost-kuberrunnakute-uurimisel?id=51093368, 3 May 2018.

assistance from several countries and institutions, who did come to Estonia's aid. Estonian CERT was assisted by Israeli, Slovenian, Finnish German counterparts, NATO CERT teams and EU ENISA team.[189]

Although up to date no official state attribution has not been made, government representatives have in occasions taken the position that Russia was behind the attacks based on the political situations and selected targets. For example, former foreign minister was quick to attribute the attacks on Russia[190] and he took a similar stance during Council of Europe meeting as well[191]. The Estonian Foreign Ministry did attribute the intrusions on Russian state officials as well. The Foreign Ministry's publication states that Estonian government blames and confirms that it was Russia who carried out the attacks.[192] Similar standpoints have been published by foreign media.[193] There are additional publications that allege that Estonian government believes that enough evidence have been produced to determine the attribution for the cyber operation on Russia.[194]

As it was already previously established, state attribution is not only legal matter and is influenced by state policy. The operations against Estonia being as one of the first large-scale operation that hindered even the emergency response capabilities[195] it is understandable that Estonia was not quick to stoutly confirm Russia's guilt based on indirect evidence. However, the author is on the position that given how state attribution practices have changed, it might not be the case today with the same indirect and in some case contradictory evidence – there could be sufficient indirect evidence (with a reference to the Corfu Case) at present to be able to carry out the attribution.

[189]Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. – *Journal of Strategic Security,* vol 4, no 2, p 54.
[190] Herzog, S. (2017). Ten Years after the Estonian Cyberattacks. - *Georgetown Journal of International Affairs*, vol XVII, no III, p 69.
[191] Ministry of Foreign Affaris of the Republic of Estonia. (2007). *Address by Minister of Foreign Affairs of Estonia Urmas Paet.* Accessible: http://vm.ee/en/news/address-minister-foreign-affairs-estonia-urmas-paet, 3 May 2018.
[192] Ministry of Foreign Affaris of the Republic of Estonia. (2007). *Cyber Attacks Hit Estonia*. Accessable: http://vm.ee/sites/default/files/content-editors/web-static/115/cyber_attacks.pdf, 3 May 2018.
[193] Lowe, C. (2009). *Kremlin loyalist says launched Estonia cyber-attacks*. Accessible: https://www.reuters.com/article/us-russia-estonia-cyberspace-idUSTRE52B4D820090312, 3 May 2018.
[194] Keizer, G. (2010). *Estonia blamed Russia for backing 2007 cyberattacks, says leaked cable.* Accessible: https://www.computerworld.com/article/2511704/vertical-it/estonia-blamed-russia-for-backing-2007-cyberattacks--says-leaked-cable.html, 3 May 2018.
[195] Eneken Tikk, Kadri Kaska, Liis Vihul (2010), *supra nota* 201, p 21.

2.2.2. Banks of United States 2012

In beginning of September 2012 ten major United States banks suffered from DDoS intrusions which eventually result in huge losses of millions of dollars.[196] Among the suffered banks were Bank of America, JPMorgan Chase, Wells Fargo, U.S. Bank and PNC Bank. Co-founder of CrowdStrike stated "that banks get hit by cyber-attackers all the time but this time, they were outgunned. The volume of traffic sent is unprecedented. In order to carry out the cyber-attacks, the attackers got hold of thousands of high-powered application servers and pointed them all at the targeted banks."[197]

The researchers and analysts quickly understood that operation on such level required months of preparations and could not be carried out simply a group of hackers. Short after the Islamist group called Izz ad-Din al-Qassam Cyber Fighters publicly stated that they were responsible for the DDoS campaign which the group called "Operation Ababil" whose claim was soon after many stakeholders began to doubt if the group was involved in the cyber operation.[198] The Washington Post writes "that according to U.S. intelligence and other officials, Iran recently has mounted a series of disruptive computer attacks against major U.S. banks and other companies in apparent retaliation for Western economic sanctions aimed at halting its nuclear program."[199] The Chairman of the Homeland Security and Governmental Affairs Committee Joseph Lieberman came out with a statement that "he does not believe these were just hackers who were skilled enough to cause disruption of the websites. He thinks this was done by Iran and the Quds Force, which has its own developing cyberattack capability."[200]

Former official in the State and Commerce Departments and a computer expert at the Center for Strategic and International Studies James A. Lewis was certain that Iran is the responsible culprit

[196] Johnson, A. (2016). Cybersecurity for Financial Institutions: The Integral Role of Information Sharing in Cyber Attack Mitigation. – *North Caroline Banking Institute*, vol 20, p 285.
[197] Goldman, D. (2012). *Major banks hit with biggest cyberattacks in history.* Accessible: http://money.cnn.com/2012/09/27/technology/bank-cyberattacks/index.html, 3 May 2018.
[198] *Ibid.*
[199] Nakashima, E. (2012*). Iran blamed for cyberattacks on U.S. banks and companies*. Accessible: https://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html?utm_term=.879211c50f3a, 4 May 2018.
[200]

in this matter and that there is no doubt about that in the U.S. Government however, there was no evidence presented to the public to substantiate their claims.[201]

In media there were claims made by "people familiar with the situation" that "Iranian hackers have repeatedly attacked" different American banks. These sources, who requested anonymity, continued to state that there are evidence that suggests that the operations are carried out to retaliate economic sanctions against Iran.[202]

The operation resulted in seven men accused of "working on behalf of Iran's government and the Islamic Revolutionary Guard. However, those named, live in Iran and the Iranian government is not expected to extradite them." In addition to the banks it is believed that the men carried out an operation to infiltrate Bowman Avenue Dam – a critical infrastructure target that was an alarming development in the matter.[203]

The "Operation Ababil" attribution in public have presented few to no evidence therefore evaluation whether the attribution is based on sufficient or any other standard of proof is impossible. There is no source of intelligence named and presented and the U.S. officials have not made public how the members of the group carrying out DDoS operation against banks are connected to Iranian government.

2.2.3. Sony Pictures 2014

Sony Corporation of America is the entertainment branch of the Japanese owned Sony Corporation. Fellow at the Center on National Security and the Law Claire Sullivan analyses the Sony hack in her article where she finds that when the intrusion was discovered in November 2014 it followed more unusual pattern than such intrusions usually do – with a goal to gain profit. It did not per se aim credit card or baking information. The character of the intrusion seemed to be more

[201] Perlroth, N., Hardy, Q. (2013). *Bank Hacking Was the Work of Iranians, Officials Say.* Accessible: https://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html, 4 May 2018.
[202] Finkle, J., Rothacker R. (2012). *Cyber attacks on Wall Street bank straced to Iran.* Accessible: https://www.theglobeandmail.com/globe-investor/cyber-attacks-on-wall-street-banks-traced-to-iran/article4559639/, 4 May 2018.
[203] Volz, D., Finkle, J. (2016). *U.S. indicts Iranians for hackng dozens of banks, New York dam*. Accessible: https://www.reuters.com/article/us-usa-iran-cyber/u-s-indicts-iranians-for-hacking-dozens-of-banks-new-york-dam-idUSKCN0WQ1JF, 5 May 2018.

ideological rather than personal financial gain, therefore the damage resulted was wider than such hacks usually bring about.[204]

As it was unfolding, the main target of the cyber operations were its employees. Studio co-chiefs said that "a large amount of confidential Sony Pictures Entertainment data has been stolen by cyber-attackers, including personnel information and business documents."[205] The stolen data included "in addition to usernames, passwords and sensitive information about its network architecture, a host of documents exposing personal information about employees. The leaked documents include a list of employee salaries and bonuses, social security numbers and birth dates, HR employee performance reviews, criminal background checks and termination records, correspondence about employee medical conditions, passport and visa information for Hollywood stars and crew who worked on Sony films, and internal email spools and among other things, it includes the script for an unreleased pilot by Vince Gilligan as well as full copies of several Sony films, most of which have not been released in theatres yet".[206]

The evidence analyzed during the investigation was vastly different. On December 19 the FBI declared that "as a result of our investigation, and close collaboration with other U.S. government departments and agencies, the FBI now has enough information to conclude that the North Korean government is responsible for these actions (…)".[207] Later, the same was confirmed by president Barack Obama who stated that "we will respond proportionately and in a space, time and manner that we choose."[208]

What their attribution was based upon? As the FBI did admit that they are not able to disclose sensitive sources and methods of how the connection between the hack and North Korea was made, they did admit that it was based on mainly three key findings. The FBI said that "the wiper malware used by attackers revealed links to other malware that the FBI knows North Korean actors previously developed; the FBI found a significant overlap between the infrastructure used by

[204] Sullivan, C. (2016). The 2014 Sony Hack and the Role of International Law. - *Journal of National Security Law & Policy*, vol 8, issue 3, p 437.
[205] Grover, R., Hosenball, M., Finle J. *Sony Suffered The Most Devastating Hack of A Major US Company Ever*. Accessible: http://www.businessinsider.com/the-size-and-scope-of-the-sony-hack-is-incredible-2014-12, 5 May 2018.
[206] Zetter, K. (2014). *Sony got hacked hard: what we know and don't know so far*. Accessible: https://www.wired.com/2014/12/Sony-hack-what-we-know, 5 May 2018.
[207] Federal Bureau of Investigations. (2014). Update on Sony Investigation. Accessible: https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation, 5 May 2018.
[208] Lee, D. (2014). *Sony hack: Obama vows response as FBI blames North Korea*. Accessible: http://www.bbc.com/news/world-us-canada-30555997, 5 May 2018.

Sony's attackers, and malicious infrastructure used in previous attacks that tie to North Korea. For example, the FBI discovered that several internet protocol addresses associated with known North Korean infrastructure communicated with IP addresses that were hardcoded into the data deletion malware used in this attack. And thirdly the tools used in the SPE attack have similarities to a cyber-attack in march of last year against South Korean banks and media outlets, which was carried out by North Korea".[209] In addition to South Korea the "wipe-out" function was found in malware associated with the Bangladesh bank intrusion and was linked to malware found in the Sony hack as well. The Bangladesh government accused different actors but in 2016 private sector investigators took a note that "at least three actors had compromised the Central Bank, one of whom used malware associated with the Lazarus group" and in 2017 the U.S. intelligence confirmed and suggested that North Korea was involved however no concrete evidence was provided.[210] The Novetta report added that "the FBI concluded that (…) malware used in the attack was linked to other malware attributed to North Korea – specifically, code, snippets, encryption algorithms, data deletion method, and compromised infrastructure used during the attack."[211]

The then FBI director James Comey while explaining the FBI's decision on attribution added that "sometimes the Guadians of Peace – the hacking group that took responsibility for the Sony breach – got sloppy as they were sending e-mails threatening Sony employees and posting online various statements." He continued with that "the hackers either forgot or had technical issues with covering their tracks. During those times, the FBI could see that the IP addresses being used were coming from those exclusively used by the North Koreans."[212]

In January 2015 president Obama declared the Sony intrusion as a national emergency which was followed by him signing executive order in order to impose additional sanctions on North Korea – mainly economic or financial on those who are believed to be responsible for the Sony operation.[213] Sullivan in her analysis took a position that the Sony hack breached U.S. sovereignty, and that it did constitute as an internationally wrongful act under the draft articles and as well as "can be categorized as an intervention in the state's political, economic, social and cultural system,

[209] Chabrow, E., Schwartz, M. (2014). *FBI Attributes Sony Hack to North Korea*. Accessible: https://www.bankinfosecurity.com/fbi-attributes-sony-hack-to-north-korea-a-7703, 6 May 2018.
[210] Davis, J., *et al*. (2017), *supra nota* 5, p 11.
[211] Novetta. *Operation Blockbuster. Unravelling the Long Thread od the Sony Attack*. Accessible: https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf, 6 May 2018.
[212] Roman, J. (2015). FBI Defends *Sony Hack Attribution*. Accessible: https://www.bankinfosecurity.com/sony-a-7762, 6 May 2018.
[213] Sullivan (2016), *supra nota* 221, p 467.

and the formulation of foreign policy."[214] However, the author can not agree with her standpoint that "the hack also involved at least the threat of force and arguably, although not in familiar form, an attack to armed level which entitled the United States to invoke the right to anticipatory self-defence.[215] As the right to self-defence is regulated in in the UN Charter article 51 which enacts that "nothing in the present charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations (…)".[216] The UN Charter establishes a presumption for a state to apply self-defence – which is an armed attack. In order for a conduct to qualify as an armed attack is dependent on its scale and effect. The Tallinn Manual 2.0 experts have rather resolutely stated that "the scale and effect required for an act to be characterized as an armed attack necessarily exceed those qualifying the act as a use of force. Only in the event that the use of force reaches the threshold of an armed attack is the state entitled to respond using force in self-defence".[217] They however did admit that the case of a cyber operation that "do no result in injury, death, damage or destruction, but otherwise have extensive negative effects, remains unsettled.[218] However, they clearly do not see right to self-defence in cases that are below of threshold of an armed attack, that however, do not preclude the United States' right for apply countermeasures. This standpoint is supported Michael Schmitt in his article that analyses the Sony hack and where he states "that the cyber operation against Sony involved the release of sensitive information and the destruction of data. Albeit highly disruptive and costly, such effects are not at the level most experts would consider an armed attack."[219]

Another question with the Sony hack is that are the applied countermeasures in accord with both principles of international law and the UN GGE set principle that such decision should be substantiated. Schmitt in his analysis of the Sony hack dismisses the possibility of it being either armed attack, use of force or unlawful intervention. However, he does not preclude that the operation could have been a violation of the United States' sovereignty and if Bureau 121 was responsible for carrying out the operation and their conduct did result in the damage that the Sony hack resulted in, then that would exactly be the case according to article 4 of the ILC, if they were non-state actors then additionally article 8 and 11 would apply.[220]

---

[214] *Ibid.*
[215] *Ibid.*
[216] Ühinenud Rahvaste Organisatsiooni põhikiri ning Rahvusvahelise Kohtu statuut. RT II 1996, 24, 95.
[217] Schmitt (2017), *supra nota* 18, p 341.
[218] *Ibid.*, p 342.
[219] Schmitt, M. (2014). *International Law and Cyber Attacks: Sony v. North Korea.* Accessible: https://www.justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea/, 6 May 2018.
[220] *Ibid*.

2.2.4. WannaCry 2017

The WannaCry ransomware operation in may 2017 was one of the first big intrusions that demonstrated how cybersecurity is not simply a state matter to ensure and how both private and public companies have an important role to perform. The intrusion presented how weak spots does not rise from one simple misgiving but includes multiple elements, among other things "software companies who fail to provide updates or no longer service vulnerabilities, affected companies that have slow patch cycles, secret services that stockpile vulnerabilities, and states that do not force essential service providers (like healthcare companies) to ensure that their systems are stable and secure"[221].

The Guardian wrote that "malicious software has hit Britain's National Health Service, some of Spain's largest companies, as well as computers across Russia, the Ukraine and Taiwan, leading to PCs and data being locked up and held for ransom. The ransomware uses a vulnerability first revealed to the public as part of a leaked stash of NSA-related documents in order to infect Windows PCs and encrypt their contents, before demanding payments of hundreds of dollars for the key to encrypt files."[222] The main concern here was that the malware intruded networks of UK hospitals which compromised both hospitals' and patients' data and as well as hinder medical service availability.

Professor John Chung in his article confirms that although such ransomware intrusions are not something new, this one drew attention due to the fact that it targeted governments and companies all over the world and among them were "sophisticated institutions at the heart of critical infrastructure" [223] which may indicate a central coordination. The result of the WannaCry ransomware case was estimated to result in global financial and economic losses total of up to 4 billion dollars and affected a up to 300 thousand computers from 150 countries[224].

---

[221] Kettemann, M. (2017). Ensuring Cybersecurity Through International Law, 2017. *Revista Espanola de Derecho Internacional,* vol 69, issue 2, p 282.
[222] Hern, A., Gibbs, S. *What is WannaCry ransomware and why is it attacking global computers?* Accessible: https://www.theguardian.com/technology/2017/may/12/nhs-ransomware-cyber-attack-what-is-wanacrypt0r-20, 6 May 2018.
[223] Chung, J. (2018). Critical Infrastructure, Cybersecurity, and Market Failure. - *Oregon Law* Review, vol 96, issue 2, p 444.
[224] TrendMicro. (2018). 2017 Annual Security Roundup: The Paradox of Cyberthreats. Accessible: https://documents.trendmicro.com/assets/rpt/rpt-2017-Annual-Security-Roundup-The-Paradox-of-Cyberthreats.pdf, 6 May 2018.

Research and investigation began to point towards North Korea. The Wired reported that malware code used indicated to a program that has previously been applied by Lazarus group which is believed to be operating under the control of North Korean administration. The Kaspersky researcher Costin Raiudid admit that there is possibility that the "repetition of the code could be false flag but it is rather improbable".[225] The same is verified by Symantec.[226] In addition, SecureWorks analysis suggest link with North Korea's Lazarus group by finding piece of code which have been previously used in cyber operations which have reached a conclusion that Lazarus group was involved.[227] Allegedly the Lazarus group "is thought to be responsible for the 2014 Sony hack and the 81 million USD cyber heist at the Bangladeshi Central Bank from 2016 and is closely affiliated with, or even identified as, the North Korean "Bureau 121".[228]

Rather immediately the UK's National Cyber Security Centre (NCSC) reportedly attributed the operation to North Korea. The NCSC conducted separate investigation that resulted in a discovery of a linkage between the operation and North Korea. The centre however, did not confirm nor deny the reports.[229] In addition, the NSA had reached similar results. It is stated that "the NSA believes with a moderate confidence that the ransomware came from hackers sponsored by North Korea's spy agency". The evidence allegedly is based on IP addresses that have been traced back to North Korean agency.[230]

About half a year later U.S. attributed the global intrusion to North Korea. White House homeland security adviser Tom Bossert gave a press conference, where he stated that "after careful investigation, the United States is publicly attributing the massive WannaCry cyberattack to North Korea. We do not make this allegation lightly. We do so with evidence, and we do so with partners. Other governments and private companies agree. The United Kingdom, Australia, Canada, New Zealand, and Japan have seen our analysis, and they join us in denouncing North Korea for

[225] Greenberg, A. (2017) *The WannaCry Ransomware Has a Link To Suspected North Korean Hackers*. Accessible: https://www.wired.com/2017/05/wannacry-ransomware-link-suspected-north-korean-hackers/, 6 May 2018.
[226] Symantec Security Response. (2017). *What you need to know about the WannaCry Ransomware*. Accessible: https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack, 6 May 2018.
[227] Hern, A., MacAskill, E. (2017). *WannaCry ransomware attack „linked to North Korea"*. Accessible: https://www.theguardian.com/technology/2017/jun/16/wannacry-ransomware-attack-linked-north-korea-lazarus-group, 6 May 2018.
[228] Minárik, T., Peterson, R., Naagel, M. (2017). *WannaCry Campaign: Potential State Involvement Could Have Serious Consequences.* Accessible: https://ccdcoe.org/wannacry-campaign-potential-state-involvement-could-have-serious-consequences.html, 6 May 2018.
[229] Hern, A., MacAskill, E (2017), *supra nota* 243.
[230] Kastrenakes, J. *The NSA reportedly believes North Corea was responsible for WannaCry ransomware attacks*. Accessible: https://www.theverge.com/2017/6/14/15805346/wannacry-north-korea-linked-by-nsa, 6 May 2018.

WannaCry."[231] The UK joined with the attribution – the Foreign Office said that "Britain's National Cyber Security Centre had assessed it was highly likely that North Korea's Lazarus hacking group was behind the one of the most significant cyber attacks to hit the UK in terms of scale of disruption."[232] Prime Minister of Australia stated that "the Australian government condemns North Korea's use of WannaCry ransomware to attack businesses and public institutions around the world (…). Based on advice from our intelligence agencies, and through consultation with our allies, we confirm that North Korea carried out the WannaCry ransomware campaign." [233] Without mentioning North Korea the Chief of Communications Security Establishment of Canada Greta Bossenmaier added that "assessment of their allies is consistent with our analysis. The Government of Canada strongly opposes the use of cyberspace for reckless and destructive criminal activities. Using malware such as WannaCry to extort ransoms and disrupt services is unacceptable, whether conducted by an individual or a nation state."[234] New Zealand took similar approach when the Director General of the Government of Communications Security Bureau Andrew Hampton said that "cyber threat analysis from range of sources, including the United States and the United Kingdom, attributes WannaCry to North Korean cyber threat actors" and added that "they support the actions of our cyber security partners in calling out this sort of reckless and malicious cyber activity."[235]

The attribution by state officials is substantiated by previously mentioned private companies and is largely based on the Sony hack attribution. The Just Security web-site reports that "this may be sufficient given the accusation against North Korea by the private sector, end even the UK government, over the las few months. But it does little to set an example or establish an evidentiary best practice for states to follow in attributing future cyberattacks to states or state-sponsored actors. It is especially unlikely to satisfy states that pushed for a statement in 2015 UN GGE report that "accusations of organizing and implementing wrongful acts brought against states should be

[231] Sharp, A., Tweed, D., Olorunnipa, T. *U.S. Says North Korea Was Behind WannaCry Cyberattack.* Accessible: https://www.bloomberg.com/news/articles/2017-12-19/u-s-blames-north-korea-for-cowardly-wannacry-cyberattack, 6 May 2018.
[232] Sandle, P. Britain joins *U.S. in blaming North Korea for „WannaCry" attack.* Accessible: https://www.reuters.com/article/us-usa-cyber-northkorea-britain/britain-joins-u-s-in-blaming-north-korea-for-wannacry-attack-idUSKBN1ED1SK, 6 May 2018.
[233] Prime Minister of Australia. (2017). *Media release.* Accessible: https://www.pm.gov.au/media/attributing-wannacry-ramsomware-north-korea, 6 May 2018.
[234] Communications Security Establishment. *CSE statement on the Attribution of WannaCry Malware.* Accessible: https://www.cse-cst.gc.ca/en/media/2017-12-19, 6 May 2018.
[235] Government Communications Security Bureau. (2017). *New Zealand concerned North Korean cyber aktivity.* Accessible: https://www.gcsb.govt.nz/news/media-release-new-zealand-concerned-at-north-korean-cyber-activity/, 6 May 2018.

substantiated.""[236]Gregory Elich who is on Board of Directors of the Jasenovac Research Institute adds that "it was considered a particulary damning piece of evidence that some of the tools used in an early variant of WannaCry share characteristics with those deployed in the cyberattack of Sony. (…) If attribution of the Sony hack to North Korea does not hold, then linkage based tool usage falls apart."[237]

When states took the position that WannaCry was conducted by North Korean authorities or under their direct orders, none of the states took the position that the WannaCry operation itself was a breach of international law. This could explain that why no additional countermeasures besides the public attribution was applied and mainly stayed at the "name and shame" approach. However, the standard of proof relied upon was higher but namely due to private companies whose research and analysis on evidence was able to make the connection to the said group. It is clear that the process of attribution was similar to the one Sony hack however there is far less substantiated evidence disclosed to the public.

2.2.5. NotPetya 2017

Soon after the WannaCry ransomware attack it was followed by another one which was dubbed NotPetya and targeted different companies in Europe, Middle East and the United States, among them banks, airline companies and, similar to WannaCry, hospitals as well.[238] It is believed that the attack was initially found in Ukraine, where "government, banks, state power utility and Kiev's airport and metro system were all affected. The radiation monitoring system at Chernobyl was taken offline, forcing employees to use hand-held counters to measure levels at the former nuclear plant's exclusion zone."[239] Reportedly in Ukraine initially more that 12 thousand computers were compromised and then it spread to 64 countries, among them Germany, Russia, United States and Belgium.[240]

---

[236] Eichensehr, K. (2017) *Three Questions on the WannaCry Attribution to North Korea*. Accessible: https://www.justsecurity.org/49889/questions-wannacry-attribution-north-korea/, 6 May 2018.
[237] Elich, G. (2018). *The WannaCry Cyberattack: What the Evidence Says and Why the Trump Administration Blames North Korea*. Accessible: https://www.counterpunch.org/2018/01/03/the-wannacry-cyberattack-what-the-evidence-says-and-why-the-trump-administration-blames-north-korea/, 6 May 2018.
[238] The Verge. (2017). *Petya ransomware: everything we know about the massive cyberattack*. Accesible: https://www.theverge.com/2017/6/28/15888094/petya-ransomware-attack-news-virus, 6 May 2018.
[239] Henley, J., Solon, O. (2017). *„Petya" ransomware attack strikes companies across Europe and US*. Accessible: https://www.theguardian.com/world/2017/jun/27/petya-ransomware-attack-strikes-companies-across-europe, 6 May 2018.
[240] Microsoft Secure. *New ransomware, old techniques: Petya adds worm capabilities*. Accessible: https://cloudblogs.microsoft.com/microsoftsecure/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/?source=mmpc, 6 May 2018.

The US CERT analyzed the how the NotPetya propagated itself through networks. They found that it applied Mimikatz and EternalBlue[241] exploit tools to target unpatched systems." In addition, the team established that the initial infected software was a Ukrainian accounting software and is believed to be the "delivery mechanism". [242]

The initial response to the matter was that there is another ransomware intrusion at hand, however, due to the fact that often, after the payment of ransomware the victim did not receive their files began a discussion on how this is "definitely not designed to make money" but "to spread fast and cause damage, using plausibly deniable cover of ransomware". If looked more closely the functioning of the malware it was believed "that if this was meant to generate revenue, this payment pipeline was possibly the worst of all options" and "in contrast to the payment infrastructure, the malware's infection techniques were described as well-written, using a number of different methods to ensure maximum damage to the networks it penetrates."[243]

The malware instructs payments to be made to an address that is hardcoded into software and in order to retrieve your files and documents the victim in addition to the payment had to receive a individual password or key which was 60-characters long and each case sensitive. After that in order to prove that the victim has done so he or she was expected to send a confirmation email to an Posteo email address which after the breakout was immediately closed. This meant for the victims that even if they pay the ransom and act according to the instructions, they were still not able to decrypt their documents because they could not send the final confirmation email.[244]

NATO CCD CoE researchers believed that this new distribution of malware has a similar aim as WannaCry did with higher level of difficulty for attribution. They suspected that a state is behind the NotPetya operation. [245] The researchers agreed that the fact that the ransomware system was

[241] Newman, L. *The Leaked NSA Spy Tool That Hacked the World.* Accessible: https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/, 6 May 2018.
[242] United States Computer Emergency Readiness Team. *Petya Ransomware.* Accessible: https://www.us-cert.gov/ncas/alerts/TA17-181A, 6 May 2018.
[243] Hern, A. (2017). *Ransomware attack „not designed to make money", researchers claim.* Accessible: https://www.theguardian.com/technology/2017/jun/28/notpetya-ransomware-attack-ukraine-russia, 6 May 2018.
[244] *Ibid.*
[245] Blumbergs, B., *et al.* (2017). *NotPetya and WannaCry Call for a Joint Response from International Community*. Accessible: https://ccdcoe.org/notpetya-and-wannacry-call-joint-response-international-community.html, 6 May 2018.

built rather inadequately collecting ransom was not its main goal and probably the operation as a whole do not succeed to collect the amount it actually costs.[246]

Since the main damage was done in Ukraine, where the malware began to spread, the Ukrainian authorities began to come to similar conclusions that it was a state responsible for the spreading and damage done by the malware. The Guardian writes that "Ukraine has suggested Russia may have been behind the attack, which struck on the eve of Ukraine's constitution day, which celebrates the country's split from the Soviet Union."[247]

In the beginning of July 2017 the Ukrainian law enforcement officials in the country stated that "it took control of software company MeDoc's systems. It is suspected by security experts that a malicious software update was installed on the firm's devices and then sent out to clients and that since the company knew about its security issues and didn't do anything about it they will for this neglect, face criminal responsibility."[248] The case for the fact that the malware began spreading through MeDoc's servers is confirmed by several private researchers such as Microsoft[249] or ESET[250].

As more links come to show that the APT alleged to be behind NotPetya ransomware intrusions, could be blamed for several other operations that in the past have been linked to Russian state officials, however, neither ESET or Kaspersky who have conducted the research that linked this APT to for Example Ukrainian power grid intrusion, are not willing to state that it is Russia per se behind the operation.[251] However, there are some, for example FireEye's head of global intelligence operations John Watters who said "he is reasonably confident that Russia was behind the attack."[252]

Almost half a year later, states began to join with the assessment carried out by Ukraine that it was Russia behind the intrusion. In February 2018 UK Foreign Office minister Lord Ahmad attributed

[246] *Ibid.*
[247] Hern (2018), *supra nota* 259.
[248] Burgess, M. (2017) Police in Ukraine have seized the servers of the company at the heart of the NotPetya cyberattack. Accessible: http://www.wired.co.uk/article/notpetya-petya-russia-cause, 6 May 2018.
[249] Microsoft Secure (2017), *supra nota* 256.
[250] We Live Security by ESET. (2017). *New WannaCryptor-like ransomware attack hits globally: All you need to know.* Accessible: https://www.welivesecurity.com/2017/06/27/new-ransomware-attack-hits-ukraine/, 6 May 2018.
[251] Cimpanu, C. (2017). *Security Firms Find Thin Lines Connecting NotPetya to Ukraine Power Grid Attacks.* Accessible: https://www.bleepingcomputer.com/news/security/security-firms-find-thin-lines-connecting-notpetya-to-ukraine-power-grid-attacks/, 6 May 2018.
[252] *Ibid.*

the NotPetya cyber attack to Russia by stating that "the UK government judges that the Russian Government, specifically the Russian military, was responsible for NotPetya"[253] Foreign Office's attribution was based on UK's National Cyber Security Centre assessment that "the Russian military was almost certainly responsible for NotPetya cyber attack of June 2017".[254]

Soon the United States followed with a statement released "that in June 2017 the Russian military launched the most destructive and costly cyber-attack in history (…). It was part of the Kremlin's ongoing effort to destabilize Ukraine and demonstrates ever more clearly Russia's involvement in the ongoing conflict. This was also a reckless and indiscriminate cyber-attack that will be met with international consequences."[255] When assessed from international law perspective, the United States have made it clear that this is a violation of international law and that Russia has breached an obligation owed to Ukraine which would allow attribution and applicable countermeasures to be considered.

Many followed the steps of the UK and the United States. Same day the Australian government joined with their allies and released a statement that "the Australian government has joined the governments of the United States and the United Kingdom in condemning Russia's use of NotPetya malware to attack critical infrastructure and businesses in June 2017. Based on advice from Australian intelligence agencies, and through consultation with the United States and United Kingdom, the Australian government has judged that Russian state sponsored actors were responsible for the incident."[256] Canada releases a statement saying that "many of Canada's allies and partners have made statements regarding the malware known as NotPetya. Communications Security Establishment also assesses that actors in Russia were responsible for developing NotPetya. Canada condemns the use of the NotPetya malware to indiscriminately attack critical financial, energy, government, and infrastructure sectors around the world in June 2017."[257] New Zealand joined with others by condemning the operation by saying that "New Zealand supports

[253] Foreign and Commonwealth Office. *Foreign Office Minister condemns Russia for NotPetya attac*ks. Accessible: https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks, 6May 2018.
[254] National Cyber Security Centre. (2018). *Russian military „almost certainly" responsible for destructive 2017 cyber attack.* Accessible: https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack, 6 May 2018.
[255] Statement from the Press Secretary. (2018) Accessible: https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/, 6 May 2018.
[256] Minister of Law Enforcement and Cyber Security. (2018) *Australian Government attribution of the „NotPetya" cyber incident to Russia.* Accessible: http://minister.homeaffairs.gov.au/angustaylor/Pages/notpetya-russia.aspx, 6 May 2018.
[257] Communications Security Establishment. (2018). *CSE Statement on the NotPetya Malware*. Accessible: https://www.cse-cst.gc.ca/en/media/2018-02-15, 6 May 2018.

actions of our cyber security partners in calling out this sort of reckless and malicious cyber activity."[258] Among others, Estonian Foreign Minister have also taken a stance that Estonia condemns Russian cyber operations against Ukraine and calls Russia to responsible behavior in cyberspace. The minister said that operations showed disrespect towards Ukranian sovereignty and caused significant economic damage not only for Ukraine but others who were inflicted by the NotPetya as well.[259]

The European Union Foreign Affair Council without naming any state per se released a statement "that the council is concerned about the increased ability and willingness of third states and non-state actors to pursue their objectives by undertaking malicious cyber activities. (…). The council firmly condemns the malicious use of information and communications technologies, including in WannaCry and NotPetya, which have caused significant damage and economic loss in the EU and beyond."[260]

As NATO CCD CoE researchers emphasized the importance of joint response to operations such as those, perhaps by joint investigation[261], the response to NotPetya has been rather minimal. The United States imposed additional sanctions on "designated five entities and 19 individuals under the Countering America's Adversaries Through Sanctions Act as well as Executive Order 13694 "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities.""[262]

[258] Government Communications Security Bureau. (2018). *New Zealand joins international condemnation of NotPetya cyber.attacks*. Accessible: https://www.gcsb.govt.nz/news/new-zealand-joins-international-condemnation-of-notpetya-cyber-attack/, 6 May 2018.
[259] Õhtuleht. (2018). *Välisminister mõistab hukka Venemaa valitsuse küberründe NotPetya Ukraina vastu.* Acessible: https://www.ohtuleht.ee/858906/valisminister-moistab-hukka-venemaa-valitsuse-kuberrunde-notpetya-ukraina-vastu, 6 May 2018.
[260] Council of the European Union. (2018). *Response to malicious cyber activities: Council adopts conclusions*. Accessible: http://www.consilium.europa.eu/en/press/press-releases/2018/04/16/malicious-cyber-activities-council-adopts-conclusions/, 6 May 2018.
[261] Blumbergs, B., *et al*. (2017), *supra nota* 261.
[262] U.S. Department of Treasury. *Treasury Sanctions Russian Cyber Actor for Interference with the 2016 U.S. Elections and Malicious Cyber-attacks.* Accessible: https://home.treasury.gov/news/press-releases/sm0312, 6 May 2018.

3. PEREMPTORY AND DISPOSITIVE NORMS OF STANDARD OF PROOF

3.1. Case analysis conclusions and results

The international law has set rules and norms for attribution of internationally wrongful act and if the conduct has been carried out by a non-state actor, then the international law has set rules if and when the non-state actors' conduct can be attributed to that state. The international law, mainly draft articles of ILC on state responsibility, do not indicate the certainty which have to be met in order to determine whether the attribution is legitimate, to either apply countermeasures or in more severe cases result in use of force against the adversary or even individual or collective self-defence. The content of standard of proof for attribution of internationally wrongful acts have been left to two instances – international courts and states themselves.

The analysis of the case law of the ICJ and some international tribunals and how states have conducted their attributions bears several differences. Before discussing which are resulted peremptory and dispositive norms that states must and do consider in the attribution process, it is important to understand the difference between public and private attribution. The threshold of evidence presented, based on case analysis, almost never rise to the level that allow conclusively for an injured state to claim that another state is responsible for cyber operation. The ICJ and international tribunals are bind by their statutes and general principles from international law that judgements and verdicts must be substantiated but the states usually are not, especially if the attribution is solely based on classified information. That however does not mean that privately conducted attribution and evidence does not reach the threshold of sufficiency. This approach is supported by some of the case analysis as well and this allows to conclude that the fact that despite the lack of conclusive evidence presented to the public countermeasures are still applied and attributions are carried out allows to presume that the standard of proof threshold is significantly lower than the one applied by the ICJ. This raises concerns on whether such attribution is legitimate, if countermeasures are applied can they themselves constitute an unlawful act and how to reach needed standard in order to be in conformity with international law.

Melissa Hathaway in her article points very suggestively out that although states have reached certain consensus level on how to conduct their activities in cyberspace and have pledged to

practice restraint on misuse of ICTs, the principles are constantly violated. She continues that "all evidence suggest that states are not following their own doctrines of restraint and that each disruptive and destructive attack further destabilizes our future."[263] As it was established by the UN GGE that "a state should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public; states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs; and states should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructure, and other relevant resolutions."[264] Albeit not legally binding, it is important to understand, that among the states who participated in the development of such normative framework were (in the GGE that produced 2015 report) states who have been main parties of attributions based on the case analysis – the United States, the United Kingdom, Estonia, the Russian Federation and in addition major players in the ICT field such as China, France, Germany, Israel, Japan and the Republic of Korea.[265]

Regarding the analysis of possible norms for standard of proof from the state conduct there are some conclusions that can be drawn. There were some examples that can be set perhaps as an example. It seems that more severe cases have had a higher standard of proof in order to attribute it to an adversary and the ones that had less effect or caused no damage had far lower standard – subsequently, in some cases it seemed that no evidence were presented to the public.

In case of Estonian intrusion against its governmental and private companies' websites that coincided with street riots in a politically complex situation. The state officials did not publicly attribute it to Russia, however, since this was the case that was internationally for the first time dubbed as "cyberwar" the author believed it to be necessary to analyse. Despite there were some statements convened to the public it seems that only standard implied was that "there was enough evidence" to attribute it to Russia. The set standard among other evidence included, in the politically tense situation chosen politically significant targets, symbolic meaning behind the time the operation was carried out, the level of coordination determined to be behind the operation, the

[263] Hathaway, M. Getting beyond Norms When Violating the Agreement Becomes Customary Practice. Accessible: https://www.cigionline.org/sites/default/files/documents/Paper%20no.127.pdf, 6 May 2018.
[264] UN GGE report of 2013, *supra nota* 33.
[265] *Ibid.*

level of sources required to carry out such an operation, presence of features of central command and control behind the necessary resources, pinpointing IP addresses, location choice for botnet servers and finally willingness to cooperate.

This standpoint is substantiated by Rain Ottis who in his analysis adds that attacks had a political motivation. Russian state officials took rather hostile positions towards the situation, which was disseminated in through internet. Ottis claims that such discourse could be perceived as encouragement to attackers from Russian political elite. When considering possible evidence he continued that "it is remarkable, however, that neither is there any proof of measures taken by the Russian government to mitigate the situation. The lack of cooperation in the Estonian investigation indicates that the Russian government is not interested in identifying the attackers and is therefore, in essence, protecting them. In other words, hostile rhetoric from the political elite motivated people to attack Estonia while nothing was done to stop the attacks. This silent consent, however, can be interpreted as implicit state support because without fear of retribution the attackers were free to target Estonian systems."[266] He rather quickly dismissed that the cyber operation could be anything else than "Russian information operation against Estonia" .[267] He presented interesting analogy – that this situation is similar to the people's war concept used in China, where "the government motivates people to attack its enemies by any means at their disposal. The digital version provides plausible deniability for the government, while in this case of this event the government can easily protect the attackers by refusing to cooperate with foreign investigators."[268] Research and analyses conducted further down the road since the event took place, it is rather significant that the attribution would have been made and evidence would have sufficed if carried out today. Ottis in his preface argues as well that there is an "abundance of circumstantial evidence" which indicated its linkage to political situation and as it has been already previously established, the circumstantial evidence can be considered as sufficient evidence.

The next analyzed incident - the Operation Ababil – however is a rather contradictory cyber operation that resulted not only in state attribution, but indictment of alleged culprits. The information available does almost nothing to that whether any kind of standard was considered in the attribution process. This brings forth the issue that in certain cases, where perhaps potential financial loss is anticipated, the received intelligence is relied upon instead of "testable and high-

[266] *Ibid.*
[267] *Ibid.*
[268] *Ibid.*

quality evidence."[269] Giving that the attribution presented by U.S. officials was publicized after few weeks, this could easily be the case.

As later seven Iranians were indicted by the U.S. Attorney General, with more substantiated evidence, it seems that the initial attribution might have been correct. However, given that the it was communicated with a statement, which implied that it should simply be trusted without disclosing anything else does not set an acceptable standard for evidence in state attribution – it rather hinders the general aim that claims to the public should be substantiated.

In the opinion of the author, one of the most interesting cases of state attribution would be the Sony hack because there was a lot of contradictory evidence presented both by public officials but as well as private researchers. The FBI's communicated standard was that it had enough information to conclude, which does not seem too far from some ICJ applied standards. The FBI in this case stated three main findings based upon which the attribution stands. Before applying countermeasures the president Obama declared that the state will respond in appropriate manner. According to senior military official the president had "no doubt" that the operation was carried out by North Korea. The FBI director later have stated that "there was other evidence he could not discuss." His statement was later supported by the NSA director Michael Rogers that "after reviewing the classified data he had high confidence that the North had ordered the action."[270]

Albeit the Sony hack, in the sense of public attribution, was conducted far better than some of the previous cyber operations conducted against the United States, however the uncertainty remains. One issue that have been risen in the Sony context is the mistrust towards FBI since the false attribution that Iraq held weapons of mass destruction.[271]

The standard of enough information to conclude in the Sony hack case was substantiated in addition to intelligence sources which were not disclosed public technical information of IP-addresses and as well as how some of the technical evidence was overlapping with evidence from other investigations in which an attribution had made, as well as private investigators research.

[269] Guitton, C. (2017). Inside the Enemy's Computer: Identifying Cyber Attackers. - *Oxford University Press*, p 85 - 92

[270] Sanger, D., Fackler,M. (2015). *N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say*. Accessible: https://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html, 6 May 2018.

[271] Risk Based Security. (2014). *A Breakdown and Analysis of the December, 2014 Sony Hack*. Accessible: https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/

This might be dangerous precedent – especially in the view that malware is not used only by one culprit, it is often sold and applied cyber criminals or other actors. If such conclusions are often drawn without additional information, this may suffice as "sloppy attribution" as Comey described "sloppy hackers". This coincides with false flagging as well - as researchers of the Stateless Attribution article describe "sophisticated adversaries that want to avoid attribution will carefully dedicate resources to deploy false indicators and cast suspicion on other parties"[272].

In the case of WannaCry the initial standard based on which the UK made its attribution is not communicated to the public, besides the comment that NCSC conducted its own investigation but the representatives of the UK government did not comment on the findings, aside the public attribution. Same was done by the NSA. Of course, there might be additional support coming from findings from the Kaspersky and Symantec who both concluded that the WannaCry ransomware is linked with the Lazarus group who are allegedly tied to North Korean administration. Later on, the US attributed the attack with evidence, the UK added the highly likely element, Australia sufficed itself with consistent assessment of analyses. New Zealand and and Canada however mainly agreed with their partners. This would be one of the initial joint responses by states to malicious cyber operation, however, it mainly stayed on the level of "naming and shaming" but in international law communities, including NATO CCD CoE, were discussions about if the attribution have been made, the operation could be treated as violation of sovereignty which would allow more concrete response but it seems that legal options have to be substantiated by policy decisions.

The initial attribution of NotPetya to Russa was made by Ukraine mainly based on political and symbolic context. It later reiterated that it had proof that Russia was behind the operation.[273] Between state attributions, private sector companies conducted their own investigations, which established a link with a Russian based APT. The UK communicated that Russia were almost certainly responsible and the US at least indirectly admitted Russia's violation of international law. Australian government judges that Russian state sponsored actors were responsible, Canada assesses that Russia was responsible.

[272] Davis, J., *et al*. (2017), *supra nota* 5, p 12.
[273] Baraniuk, C. (2017). *Ukraine claims Russia launched NotPetya ransomware attack*. Accessible: https://www.newscientist.com/article/2139647-ukraine-claims-russia-launched-notpetya-ransomware-attack/, 6 May 2018.

Under international law there are several possibilities to counter malicious activity that is attributable to a state, however, there are certain conditions that has to be met – a state can respond to a malicious cyber operation only if it constitutes an armed attack according to the UN Charter article 51, a use of force under article 2(4) or it is an internationally wrongful act according to the Draft Articles of the International Law Committee. Piret Pernik in her article concludes that in instances, ransomware cyber operations could violate state sovereignty.[274] It was previously briefly considered, for example the Sony hack could constitute a violation of the United States sovereignty which in case being attributable to North Korea could give an inherent right for countermeasures.

Today there is no cyber operation that have been attributed under the article 2(4) of the UN Charter but several operations would amount to violation of state sovereignty. However, the attribution must suffice for a state to take actions on countermeasures. The standard of proof that states apply for public attribution varies greatly, in some cases it lacks altogether. Clement Guitton describes in his book that "the argument that the standards are malleable in the case of attribution to state actors follows from two separate opinion, one conceptual and other empirical, about the lack of scrutiny behind attribution cases."[275]

It is apparent from the previous analysis that the standard of proof in state attribution do not amount up to legal evaluation as the ICJ or international tribunals apply. However, there are some similarities that seem to rely on sufficiency of evidence when being communicated to wider public. The author thinks that when it comes to standardized norms for state attribution there is possibility that general principles of the ICJ are adopted by state practice. As a generalization, when comparing the results of the study of state behaviour with findings of James Green in his ICJ standard analysis, states do mostly apply the prima facie standard or the lowest one of ICJ applied standards where the main importance is that statements made are somewhat or proportionally substantiated with evidence presented.

It is understandable that the standard of proof is higher for cases which are higher in complexity and severity, and lower if they are less, however, if seen from the perspective of ICJ such differences in standards are necessary. Still, it is apparent from the case law study of the ICJ and the international tribunals compared to case study of state attribution, that standard of proof for

[274] Pernik (2018), *supra nota* 29.
[275] Guitton (2017), *supra nota* 286, p 85 – 92.

attribution of wrongful cyber operation, at the time is moving towards considerably lower thresholds. The author tends to argue from one point that the lower standard for cyberspace has not always been the case – mainly because when the matter of international law governing cyberspace came under global discussion, the approach has never been that the attribution should be based on lower standard of proof and it was by analogy from different areas of international law how this matter was approached. Nonetheless, despite how the normative framework was approached, in practice states do not generally fully comply with ICJ set rules nor with ILC Draft Article regulation.

3.2. Evidentiary recommendation and standard of proof

When it comes to evidence and cyber operations the types of evidence required to succeed the necessary standard of proof does not necessarily vary from a conventional case – this was eminent from the state attribution case analysis as well. Of course, what may differ is their format. Following, the author suggests some new approaches towards evidentiary rules in cases of cyber attribution that could be incorporated to the issue of standard or proof in the future.

Roscini in his analysis says that generally evidence presented to ICJ includes "documents, statements, testimonies, expert standpoints and digital evidence". Documentary evidence among other things would include "published treaties included in one of the recognized international or national collections of treaty texts; official records of international organizations and of national parliaments; published and unpublished diplomatic correspondence, and communiqués and other miscellaneous materials, including books, maps, plans, charts, accounts, archival material, photographs, films, legal opinions of experts and affidavits and declarations."[276] When an attribution of a unlawful cyber operations is at hand then such documents would in addition include the work done by the UN GGE or experts of Tallinn Manuals and of course national and international cyber-strategies. The issue here is the fact that often key evidence is classified and not to be disclosed to wider public. The author is in opinion of that cyber-strategies, whether regional or national, especially already second and third adaptations may in the future obtain relevant status in development of opinion juris and therefore play a key role in development of normative framework for state conduct, and attribution for deviating from it. Depending on the

[276] Roscini (2015), *supra nota* 132, p 256.

way that international norm development is aimed, it could be expected that perhaps the positions of the UN GGE will be seen as a threshold for responsibility as well.

One possibility for evidence gathering would in the future could as well be fact-finding missions. Roscini in his analysis indicates to the fact-finding mission to Georgia, where the mission draws attention to the fact that cyber-attacks were "one of the particular features of the conflict" which were believed to be carried out in order to hinder effectiveness of Georgian government's decision-making processes[277]. The author believes that such approach to evidence gathering has the potential to be sufficient. Fact-finding missions have previously deployed in order to retrieve evidence in cases of Gaza conflict[278], to Myanmar about the Rohingya persecutions or in Northern Sri Lanka armed conflict[279]. The format of cooperation offers national cyber units of states that already are cooperating in different fronts to further develop it in the area of use of ICTs – for example a G7 countries could develop a format for such cooperation that can be deployed in ad hoc manner.

However, the success of those missions would depend on effective cooperation in the cyber related issues on a international level – for example, between EU and NATO. ICDS researcher Piret Pernik in her policy brief suggested different forms of cooperation for NATO and the EU – in the area of international law she suggests that it is up to these two to "agree which norms and rules of behavior are valid in cyberspace, what triggers the right for digital self-defence and as much as possible create some framework for transparent attribution.[280] Similar suggestion is made by NATO CCD CoE under the discussion of the NotPetya cyber operation. Its researcher Lauri Lindström suggests that, as the sophistication and disruptiveness of malicious cyber operations is constantly increasing, it is time to take closer look at responses that the international community can take, and by that, perhaps it is "an opportunity for victim nations to demonstrate the contrary by launching a special joint investigation."[281]

In addition to such cooperation, different formats of collaborative frameworks are emerging. Only few days ago it was announced that a Transatlantic Commission on Election Integrity was founded

[277] *Independent International Fact-Finding Mission on the Conflict in Georgia*. (2009). Accessible: http://www.mpil.de/files/pdf4/IIFFMCG_Volume_II1.pdf, 6 May 2018.
[278] United Nations. (2009). *United Nations Fact Finding Mission on the Gaza conflict*. Accessible: http://www.ohchr.org/EN/HRBodies/HRC/SpecialSessions/Session9/Pages/FactFindingMission.aspx, 13 May 2018.
[279] United Nations. (2018). *Fact-finding Mission on Myanmar: conrete and overwhelming information points to international crimes.* Accessible: http://www.ohchr.org/EN/HRBodies/HRC/Pages/NewsDetail.aspx?NewsID=22794&LangID=E, 13 May 2018.
[280] Pernik (2018)*, supra nota* 29.
[281] Blumbergs, B., *et al* (2017), *supra nota* 261.

with the participation of Joe Biden, Michael Chertoff and Anders Foght Rasmussen and several representatives from European countries, including our former president Toomas-Hendrik Ilves.[282] There are several bodies similar to this one that are emerging, but it is vital that the work on development of normative framework for ICT use would not get too fragmented and international cooperation can be held by some kind of line.

As it is well known that when it comes to development of ICT capabilities, the private sector is leading the way. In order to apply the capabilities of private companies specializing in cybersecurity or technical and analytical research should be included in the evidentiary processes. Private companies already conduct independent research – this is eminent from case analysis as well, where cybersecurity companies such as ESET, Kaspersky or Symantec or Microsoft have produced technical reports in cases of Wannacry, Sony or NotPetya operations. Roscini in his analysis points out how Project Grey Goose conducted such open source investigations.[283] This opinion is supported by the RAND Corporation study on stateless attribution, which confirms the issue of quality of persuasive attribution. It points out that cyber requires a different approach – especially in evidence gathering and evaluation. Perhaps in case of cyber the evidence gathering process should be more similar to one conducted in criminal forensics.[284]

When it comes to digital evidence Roscini explains that "digital forensics deals with identifying, storing, analyzing, and reporting computer finds, in order to present valid digital evidence that can be submitted in civil or criminal proceedings".[285] On a positive side, in practice there does not seem to be legal difference between digital and physical evidence, but on the other, as it is with all other types of evidence, digital requires interpretation as well and today, more often than not, parties disagree on interpretation.[286] This was confirmed by the state attribution analysis where private researchers analyzing same incident came to completely different result.

He concludes with an opinion that it is doubtful that digital evidence will have conclusive role in cyber attribution because it tends to be "volatile, has a short life span, and is frequently located in foreign countries. Second, the collection of digital evidence can be very time consuming and

[282] Rogin, J. (2018). Former Western leaders join forces to fight Russian meddling. Accessible: https://www.washingtonpost.com/opinions/global-opinions/former-western-leaders-join-forces-to-fight-russian-meddling/2018/05/10/f93dc3c6-5491-11e8-abd8-265bd07a9859_story.html?noredirect=on&utm_term=.5b4549fdfd9e, 15 May 2018.
[283] Roscini (2015), *supra nota* 132, p 260.
[284] Davis, J., *et al* (2017), *supra nota* 5, p 2.
[285] Roscini (2015), *supra nota* 132, p 264.
[286] *Ibid*.

requires the cooperation of the relevant internet service providers, which may be difficult to obtain when the attack originates from other States. Third, although digital evidence may lead to the identification of the computer or computer system from which the cyber operation originates, it does not necessarily identify the individual(s) responsible for the cyber operation (as the computer may have been hijacked, or the IP spoofed). In any case, such digital evidence will say nothing about whether the conduct of those individuals can be attributed to a State under the law of state responsibility."[287] However, it mostly seems that the attributions that the author analyzed did rely on digital evidence – the communication to the public allows this assessment. Most certainly it plays key role alongside with other evidence that is placed in the political context of the situation.

Besides international organizations, there have been suggestions to form a body of researchers that does not have public background and would be comprised only of representatives of non-state actors. This might come in handy since digital evidence is broadly translatable and the idea that body of experts to develop understanding towards evidence analysis for attribution of cyber operations would offer legitimate base for national governments.

The author of the thesis believes that normative framework for cyber operation must come from international law and international cooperation. In 2005 with the Tunis Agenda, which was endorsed by UN members' heads of state at the UN World Summit on the Information Society the states noted that "Internet governance, carried out according to the Geneva principles, is an essential element for a people-centred, inclusive, development-oriented and non-discriminatory Information Society. Furthermore, we commit ourselves to the stability and security of the Internet as a global facility and to ensuring the requisite legitimacy of its governance, based on the full participation of all stakeholders (…)."[288] This puts a commitment upon states that in order to develop normative framework for attribution of cyber operations, it must include private sector, academia and non-governmental organizations. When it comes to international standard of proof it first requires at least some regional understanding and commitment to those principles how a state should carry out their conduct in cyberspace.

[287] *Ibid.*
[288] International Telecommunication Union. (2005). *Tunis Agenda for the Information Society*. Accessable: http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html, 13 May 2018.

CONCLUSION

It can be argued, that international law in its entirety is purposed to legitimize international consensus on matters agreed upon by nation states and give those agreements a legal form that in instances can be reinforced. At different times in the past there have been new areas of law which have required innovative ways of approach by both states and international law experts – one of such could be either outer space or in case of the thesis, the information and communications technology or as referred in most cases – cyberspace. In case of cyber, the main difficulty for formulating a normative framework is the lack of political will to either agree upon extensive legislation or somehow enforce agreed norms on applicability of international law or non-binding regulation on responsible state behaviour in using ICTs.

Despite the lacking agreement on international normative framework, states continue to increasingly rely on use of ICTs and different information networks in new and different areas – for example, states have taken the aim to build network of e-services also known as e-Government. The other side of the constructive use of the development of ICTs is the ambiguous side of unlawful use of cyber operations to meet various intentions, which frequently tend to include attempts to influence either political scene or gain certain leverage through data exfiltration. Nevertheless, that the lex specialis is lacking international law experts have in several years analyzed how cyberspace is governed by existing international law. The research has resulted in several outcomes. Most imperative outcome in the development of international cyber law would be the work of the UN GGE, which established in 2013 that international law does apply to cyber space along with UN Charter, the second certainly would be the Tallinn Manual 1.0 on how international law applies to cyber warfare and Tallinn Manual 2.0 on how international law applies to cyber operations.

Deriving from previous, the aim of the thesis was to analyze, in relation to existing body of international law, does international standard of proof exist when it comes to attribution of internationally wrongful acts. If there are standardized elements of standard of proof, then that would allow more unified approach to state attribution of internationally wrongful cyber operations. In order to substantiate the hypothesis and research questions the author analyzed applied standards of proof by the ICJ and international tribunals in reaching a judgement whether a state was responsible for conduct carried out either state agents themselves or non-state actors whose conduct can be attributed to said state.

The case law analysis was followed by analyzing state conduct during peacetimes, this means that cyber operations such as Georgia and Ukraine intrusions do not fall under the scope of the analysis. The author analyzed six instances of state attribution of wrongful cyber operations in order to determine whether the standards of proof established by the ICJ or the international tribunals have been applied.

To sum up the analysis of the thesis, the author has resulted that there is no such universal international standards of proof that are similarly applied by the ICJ, ICC, ICTY, ICTR and other international tribunals under the auspice of UN or other independent tribunals. There is a possibility to categorize different standards of proof according to different thresholds they require by a claimant in order to satisfy the court which would allow it to reach a judgement. If seen from this angle, there is a possibility to claim that there is a sub-category of standard of proof that is applied to state attribution of internationally wrongful cyber operations, however this has not been substantiated sufficiently yet to claim that this is how international law has approached to standard of proof.

States have taken a similar stance on applying standard of proof when they carry out their attribution. However, it is apparent that states do apply higher standard for public attribution according to the severity of the operation and perhaps lower ones when it is less. The main problem of attribution are the cases where there is no apparent standard applied nor state attributions are sufficed with any evidence to the public. According to the international law, states are not obligated to disclose sensitive information upon which most attributions are based, however as international law experts have explained that it is reasonable when countermeasures are applied.

To sum up the findings of the research, there are some similarities that come forward in both cases of ICJ and state attribution – at the moment, the practice shows that it lies somewhere in between highly likely and enough evidence/information. But probably the most important part to emphasize in relation to international law and state attribution is that the attribution must always be looked at in the current political context – it will either support the attribution made or explains the lack of it. State interest play major role in both development of international law as such and in carrying out evidentiary investigations. The author is on a firm position that for example, if the extensive cyber operations against Estonia would have been carried out today, the attribution could be substantiated based on the evidence that were provided. The political context can be valuable

evidence when it comes to attribution. The research paper on stateless attribution emphasize that "a type of indicator that can assist in an attribution investigation is the political context in which an incident takes place and the relevant motives of capable parties. If a specific actor stands to benefit from an attack for political, economic, or other reason, then this might factor into an attribution judgement. Similarly, the type of target selected and the specialized knowledge required to exploit that target might also serve as relevant political indicators."[289]

The thesis is finalized with suggestive remarks by the author that the states could look towards in the future during discussions of standard of proof, evidentiary investigations and international cooperation. The author's point of view presumes mainly cooperative measures between states, included with private sector entities and representatives of academia. It is vital for all stakeholders to contribute to international norm development on responsible state behavior in cyberspace. Through state practice and leveled expectations this would give rise to development acceptable use of ICTs and therefore valid response if a state deviates from those norms.

[289] Davis, J., *et al* (2017), *supra nota* 5, p 12.

KOKKUVÕTE

TÕENDAMISSTANDARD RAHVUSVAHELISELT ÕIGUSVASTASTE KÜBEROPERATSIOONIDE OMISTAMISEL

Maria Tolppa

Rahvusvaheline õigus oma olemuselt on suunatud tagama, et riikide vahel kokkulepitul on legitiimne alus ja seda on võimalik vajadusel jõustada. Sõltuvalt valdkonnast, on ka varasemalt tekkinud küsimus sellest, kas ja kuidas rahvusvaheline õigus reguleerib valdkonda, milles rahvusvaheline konsensus puudub. Üheks selliseks näiteks võib tuua väliskosmose, mille reguleerimiseks ja kasutamiseks on riigid alla kirjutanud rahvusvahelisele väliskosmose leppele. Täna on riigid taas analoogse küsimuse ees – reguleerimist vajab küberruum. Samas tuleb tõdeda, et küberruumis tegevuse läbiviimisega seoses, on riikide poliitiline valmisolek rahvusvahelise normistiku kokku leppimiseks oluliselt tagasihoidlikum.

Aastal 2013 leppis ÜRO peasekretäri poolt kokku kutsutud valitsuste vaheline ekspertide töörühm kokku, et rahvusvaheline õigus tõepoolest kohaldub riikide poolt informatsiooni ja kommunikatsioonitehnoloogiate kasutamisele, eelkõige rõhutades ÜRO põhikirjast tulenevatele õigustele ja kohustustele. Sellest tulenevalt on NATO CCD COE juures kokku kutsutud rahvusvahelise õiguse töörühm uurinud, kuidas ÜRO valitsuste vahelise ekspertide töörühma kokkulepitu praktikas peaks toimima. Aastal 2013 välja antud mahukas uurimus Tallinn Manual 1.0 selgitab, kuidas rahvusvaheline õigus kohaldub juhtudel, mil küberoperatsioon ületab vähemalt jõu kasutamise lävendi ÜRO põhikirja artikli 2 lõike 4 kohaselt. Kuna reeglina küberoperatsioonid seda lävendit ei ületa, andis uuenenud koosseisus töörühm välja järgmise uurimuse Tallinn Manual 2.0, mis selgitab, kuidas kohaldada rahvusvahelist õigust madalama lävendiga küberoperatsioonidele. Põhjalik uurimus ei täpsusta, milline peab olema tõendamisstandardi lävend selleks, et omistamine oleks legitiimine ja põhjendatud.

Sõltumata rahvusvahelise õiguse suurest üldistatusest küberruumis tegevuse läbiviimisele, riigid siiski jätkuvalt toetuvad üha enam infosüsteemidel põhinevatele avalikele ja erateenustele – üheks selliseks võib pidada arenevat e-riigi kontseptsiooni. Küberruumi praktilise kasutuse levikuga kaasneb selle üha suurem ekspluateerimise oht kolmandate riikide poolt mõjutamaks kas riigisisest

poliitilist keskkonda või saamaks majanduslikku või mõnda muud eelist. Taoliste küberoperatsioonide aina suurenev levik tõstatab paratamatult küsimuse riikide rahvusvahelisest vastutusest tulenevalt rahvusvahelises õiguses eksisteerivatele riigivastutuse normidele.

Eelnevast tulenevalt ja arvestades eeldusega, et rahvusvaheline õigus ja sellest tulenev riigivastutuse regulatsioon kohaldub küberoperatsioonidele, oli käesoleva magistritöö eesmärgiks uurida, kas on olemas rahvusvaheline tõendamisstandard, mida kohaldavad kas rahvusvahelised kohtud või tribunalid. Juhul, kui eksisteerivad ühtsed normid, siis kas neid on võimalik kohaldada ka küberoperatsioonidele, mis on vastuolus rahvusvahelise õiguse riigivastutuse normidega. Küsimust komplitseerib asjaolu, et riigivastutuse normid näevad ette võimaluse, kus riik on vastutav ka sellise teo eest, mille paneb toime isik, kes ei ole riigiametnik rahvusvahelise riigivastutuse normide mõistes. Selleks, et küsimusele vastata, analüüsis autor Rahvusvahelise Kohtu ja rahvusvaheliste tribunalide poolt kohaldatavaid standardeid kohtuasjades, kus on küsimuse all olnud justnimelt isiku tegevuse omistamine riigile ja sellest tulenevalt riigi vastutuse küsimus toimepandu eest. Seejärel analüüsib autor, kuidas on riigid omistamise läbi viinud küberoperatsioonide puhul, millised olid nendel juhtudel kohaldatavad tõendamisstandardid ja kas kohtu/tribunalide ja riikide kohaldatud standardid on omavahel korrelatsioonis.

Analüüsi läbiviimiseks kohaldas autor imperatiivset, kvalitatiivset ja deduktiivset uurimismeetodit, vajadusel ka analoogset tõlgendamist. Kohtulahendid, mida autor analüüsis on lahendid, mille alusel töötati välja rahvusvahelised riigivastutse reeglid ning ositi, millel põhineb Tallinn Manual 2.0 analüüs.

Analüüsi tulemusena väidab autor, et puudub ühtne rahvusvaheline tõendamisstandard, mida kas rahvusvaheline kohus või tribunalid kohaldavad. Tõepoolest, standardid on tihti sarnased, mistõttu on akadeemikuid, kes leiavad, et kuigi ühtne standard puudub, on võimalik neid kategoriseerida ja seetõttu väita, et on olemas teatud alamkategooriad või alamstandardid. Selgub, et ka riigid kohaldavad standardeid erinevalt – mõnel juhul ilmneb, et standard üldse puudub. Põhiprobleem, mis analüüsist ilmneb on asjaolu, et riigid kohaldavad reeglina madalamat tõendamisstandardit, kui seda teevad kohtud. Töö analüüs näitab, et see standard jääb toime pandud suure tõenäosusega ja tõendite/informatsiooni piisavuse vahele. Küll aga tõdevad Tallinn Manual 2.0 eksperdid tulenevalt ÜRO valitsuste vahelise ekspertide töörühma tulemustele tuginedes, et juhul, kui riik rakendab vastumeetmeid, on ta kohustatud omistamist põhjendama. Muu hulgas näitab analüüs ka seda, et riigid liiguvad üha madalama lävendiga standardi suunas juhul, kui tegu on riigivastutuse

normidega vastuolus olevate küberoperatsiooni omistamisega, mis toob omakorda kaasa küsimuse sellest, et kas liiga madal standard paneb ohtu omistamise legitiimsuse ja kvaliteedi.

Töö võib kokku võtta rõhuasetusega sellele, et kuna rahvusvaheline õigus on sisuliselt riikide poliitikate prioriteetsuse tulemus, siis tuleb riikide vahelist poliitilist konteksti arvestada ka nii küberoperatsioonide omistamisel, kui ka selleks tõendite kogumise protsesside läbiviimisel – sellel kontekstil võib olla tõendamisstandardi aspektist kriitiline roll. Oma analüüsi lõpetab autor sellega, et uurib, millised on võimalused ja ettepanekud arendamaks edasi rahvusvahelist õigust omistamise raames ning kuidas saavad riigid läbi praktikate arendada ka ühtsemat lähenemist tõendamisstandardile küberoperatsioonide kontekstis.

LIST OF REFERENCES

Scientific artcles

1. Banks, W. (2017). State Responsibility and Attribution of Cyber Intrusions after Tallinn 2.0. - Texas Law Review, vol 95, issue 7, 1487 – 1514.

2. Brenner, S. (2007). At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare. - Journal of Criminal Law & Criminology, vol 97, issue 2, 379 – 476.

3. Buchan, R. (2012). Cyber-attacks: Unlawful Uses of Force or Prohibited Interventions? - Oxford University Press, vol 17, issue 2, 212 – 227.

4. Cassesse, A. (2007). The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgement on Genocide in Bosnia. - The European Journal of International Law, vol 18, issue 4, 649 – 668.

5. Chung, J. (2018). Critical Infrastructure, Cybersecurity, and Market Failure. - Oregon Law Review, vol 96, issue 2, 441 – 476.

6. Danca, D. (2015). Cyber Diplomacy – A New Component of Foreign Policy. - Journal of Law and Administrative Sciences, vol 3, 91 – 97.

7. de Stefano, C. (2017). Adel A Hamadi Al Tamimi v Sultanate of Oman: Attributing to Sovereigns the Conduct of State-Owned Enterprises: Towards Corcumvention of the Accountability of States Under International Investment Law. – Oxford University Press, vol 32, issue 2, 267 – 274.

8. Foster, C. (2010). Burden of Proof in International Courts and Tribunals. - Australian Year Book of International Law, vol 29, 27 – 86.

9. Green, J. (2009). Fluctuating Evidentiary Standards for Self-Defence in the International Court of Justice. – International and Comparative Law Quarterly, vol 58, issue 1, 163 – 180.

10. Guitton, C. (2017). Inside the Enemy's Computer: Identifying Cyber Attackers. - Oxford University Press, p 85 – 92.

11. Hathaway, O., et al. (2012). The Law of Cyber-Attack. - California Law Review, vol 100, issue 4, 817 – 886.

12. Hellman, H. (2015). Acknowledging the Threat: Securing United States Pipeline Scada System. - Energy Law Journal, vol 36, issue 1, 157 – ii.

13. Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. – Journal of Strategic Security, vol 4, no 2, 49 – 60.

14. Herzog, S. (2017). Ten Years after the Estonian Cyberattacks. - Georgetown Journal of International Affairs, vol XVIII, no III, p 28 – 59.

15. Hessbruegge, J. (2004). The Historical Development of the Doctrines of Attribution and Due Diligence in International Law. - N.Y.U. Journal of International Law and Politics, vol 36, issue 2 & 3, 265 – 306.

16. Jensen, E. (2015). Cyber Sovereignty: The Way Ahead. - Texas International Law Journal, vol 50, issue 2 – 3, 275 – 304.

17. Johnson, A. (2016). Cybersecurity for Financial Institutions: The Integral Role of Information Sharing in Cyber Attack Mitigation. – North Caroline Banking Institute, vol 20, 277 – 310.

18. Kehler, R., Lin, H., Sulmeyer, M. (2017). Rules of Engagement for Cyberspace Operations: a View From the USA. - Journal of Cybersecurity, vol 3, issue 1.

19. Kettemann, M. (2017). Ensuring Cybersecurity Through International Law, 2017. Revista Espanola de Derecho Internacional, vol 69, issue 2, 281 – 290.

20. Lanoszka, A. (2016). Russian hybrid warfare and extended deterrence in Eastern-Europe. – The Royal Institute of International Affairs, vol 92, issue 1, 175 – 195.

21. Lin, H. (2010). Offensive Cyber Operations and the Use of Force. - Journal of National Security Law & Policy, vol 4, issue 1, 63 – 86.

22. Liu, I. (2017). State Responsibility and Cyberattacks: Defining Due Diligence Obligations. - The Indonesias Journal of International & Comparative Law, vol 4, issue 2, 191 – 260.

23. Long, G. (1994). Who Are You: Identity and Anonymity in Cyberspace. - University of Pittsburgh Law Review, vol 55, issue 4, 1177 – 1214.

24. Mačák, K. (2016). Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors. - Oxford, Journal of Conflict & Security Law, vol 21, issue 3, 405 – 428.

25. Mudrinich, E. (2012). Cyber 3.0: The Department of Defence Strategy for Opening in Cyberspace and the Attribution Problem. - The Air Force Law Review, vol 68, 167 – 206.

26. Nielsen, E. (2010). State Responsibility for Terrorist Groups. – U.C. Davis Journal of International Law & Policy, vol 17, issue 1, 151 – 192.

27. Olivier, M. (2012). Cyber Warfare: The Frontline of 21st Century Conflict. - LBJ Journal of Public Affairs, vol 20, 23 – 42.

28. Payne, C., Finlay, L. (2017). Addressing Obstacles to Cyber-Attribution: A Model Based on State Response to Cyber-Attack. - George Washington International Law Review, vol 49, issue 3, 535 – 568.

29. Roscini, M. (2015). Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations. - Texas International Law Journal, vol 50, issue 2 – 3, 233 – 274.

30. Schmitt, M. (2013). Classification of Cyber Conflict. – Journal of Conflict and Security Law, vol 17, issue 2, 245 – 260.

31. Schmitt, M. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. - Cambridge University Press.

32. Schmitt, M., Watts, S. (2016). Beyond State-Centrism: International Law and Non-State Actors in Cyberspace. - Journal of Conflict & Security Law, vol 21, issue 3, 595 – 611.

33. Shackelford, S. (2010). State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem. – Georgetown Journal of International Law, vol 42, issue 4, 971 – 1016.

34. Singer, P. W. (2015). Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons. - Case Western Reserve Journal of International Law, vol 47, issue 1, 79 – 86.

35. Sullivan, C. (2016). The 2014 Sony Hack and the Role of International Law. - Journal of National Security Law & Policy, vol 8, issue 3, 437 – 468.

36. Swiatkowska, J. (2017). Central and Eastern European Countries Under Cyberthreats. - Polish Political Science Yearbook, vol 46, issue 1, 30 – 39.

37. Tsagourias, N. (2012). Cyber Attacks, Self-Defence and the Problem of Attribution. – Journal of Conflict and Security Law, vol 17, issue 2, 229 – 244.

38. Valencia-Ospina, E. (1999). Evidence before the International Court of Justice.-. International Law FORUM Du Droit International, vol 1, issue 4, 202 – 207.

EU and International legislation

39. Rahvusvahelise Kriminaalkohtu Rooma statuut. RT II 2002, 2, 5.

40. Ühinenud Rahvaste Organisatsiooni põhikiri ning Rahvusvahelise Kohtu statuut. RT II 1996, 24, 95.

41. International Law Commission. (2001). Draft Articles on Responsibility of States for Internationally Wrongful Acts with Commentaries

42. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I), of 8 June 1977.

43. United Nations resolution no 56/83 of 22 January 2002 on Responsibility of states for internationally wrongful acts.

44. United Nations document no 68/98 of 24 June 2013 from the Group of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security.

45. United Nations document no 70/174 of 22 July 2015 from the Group of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security.

Other court decisions

PCIJ

46. Certain Questions Relating to Settlers of German Origin in the Territory Ceded by Germany to Poland, PCIJ Advisory Opinions 1923.

47. The Case of the S.S. „Lotus“, CIJ 1927

ICJ

48. Phosphates in Morocco, no 71, ICJ 1938

49. The Corfu Channel Case, ICJ 1949

50. Case Concerning United States Diplomatic and Consular Staff in Tehran, ICJ 1980.

51. Military and Paramilitary Activities in and against Nicaragua, ICJ 1986.

52. Land, Island and Maritime Frontier Dispute (El Salvador/Honduras: Nicaragua intervening), ICJ 1992.

53. Legality of the Threat or Use of Nuclear Weapons, ICJ 1996.

54. Separate Opinion of Judge Higgins on the Corfu Channel case, ICJ 1998.

55. Difference Relating to Immunity From Legal Process of a Special Rapporteur of the Commission on Human Rights, ICJ Advisory Opinion 1999.

56. Oil Platforms (Islamic Republic of Iran v United States of America), ICJ 2003.

57. Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda), ICJ 2005.

58. Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro), ICJ 2008.

59. Dissenting Opinion of Judge Cancado Trindade (Marshall Islands v United Kingdom), ICJ 2016.

Tribunals

60. Claim of the Salvador Commercial Company, Reports of International Arbitral Awards 1902.

61. Earnshaw and Others (Great Britain) v United States (Zafiro case), Reports of International Arbitral Awards 1925.

62. Island of Palmas case (Netherlands, USA), Reports of International Arbitral Awards 1928.

63. Leigh Valley Railroad Company, Agency of Canadian Car and Doundry Company, Limited, and Various Underwriters (United States) v Germany (Sabotage Cases), Reports of International Arbitral Awards 1930.

64. International Fisheries Company (U.S.A.) v.United Mexican States, Reports of International Arbitral Awards 1931.

65. Air Service Agreement of 27 March 1946 between the United States of America and France, Reports of International Arbitral Awards 1978.

66. United Nations. (1997). Tadić case: the verdict. Accessible: http://www.icty.org/en/press/tadic-case-verdict.

67. Eritrea-Ethiopia Claims Commission – Partial Award: Prisoners of war – Eritrea's Claim, Reports of International Arbitral Award 2003.

Other sources

68. Application of the International Convention for the Suppression of the Financing of Terrorism of the International Convention on the Elimination of All Forms of Racial Discrimination (Ukraine v Russian Federation), ICJ 2017.

69. Arthur, C. (2008). That cyberwarfare by Russia on Estonia? It was one kid.. in Estonia. Dmitri Galushkevich who was later fined for defacement of the Reform Party website. Accessible: https://www.theguardian.com/technology/blog/2008/jan/25/thatcyberwarfarebyrussiaon, 2 May 2018.

70. Baraniuk, C. (2017). Ukraine claims Russia launched NotPetya ransomware attack. Accessible: https://www.newscientist.com/article/2139647-ukraine-claims-russia-launched-notpetya-ransomware-attack/, 6 May 2018.

71. Blumbergs, B., et al. (2017). NotPetya and WannaCry Call for a Joint Response from International Community. Accessible: https://ccdcoe.org/notpetya-and-wannacry-call-joint-response-international-community.html, 6 May 2018.

72. Brower, C. N. (1994). Evidence before international tribunals: The need for some standard rules. International Lawyer.

73. Burgess, M. (2017) Police in Ukraine have seized the servers of the company at the heart of the NotPetya cyberattack. Accessible: http://www.wired.co.uk/article/notpetya-petya-russia-cause, 6 May 2018.

74. Chabrow, E., Schwartz, M. (2014). FBI Attributes Sony Hack to North Korea. Accessible: https://www.bankinfosecurity.com/fbi-attributes-sony-hack-to-north-korea-a-7703, 6 May 2018.

75. Chung, E. (2014). Syrian Electronic Army Hackers: Who are they and why are they targeting the media. Accessible: http://www.cbc.ca/news/technology/syrian-electronic-army-hackers-who-are-they-and-why-are-they-targeting-the-media-1.2852694. 8 April 2018.

76. Cimpanu, C. (2017). Security Firms Find Thin Lines Connecting NotPetya to Ukraine Power Grid Attacks. Accessible: https://www.bleepingcomputer.com/news/security/security-firms-find-thin-lines-connecting-notpetya-to-ukraine-power-grid-attacks/, 6 May 2018.

77. Communications Security Establishment. (2018). CSE Statement on the NotPetya Malware. Accessible: https://www.cse-cst.gc.ca/en/media/2018-02-15, 6 May 2018.

78. Communications Security Establishment. CSE statement on the Attribution of WannaCry Malware. Accessible: https://www.cse-cst.gc.ca/en/media/2017-12-19, 6 May 2018.

79. Council of the European Union. (2018). Response to malicious cyber activities: Council adopts conclusions. Accessible: http://www.consilium.europa.eu/en/press/press-releases/2018/04/16/malicious-cyber-activities-council-adopts-conclusions/, 6 May 2018.

80. Council of the European Union. (2018). Statement by the Foreign Affairs Council on Salisbury attack. Accessible: http://www.consilium.europa.eu/en/press/press-releases/2018/03/19/statement-by-the-foreign-affairs-council-on-the-salisbury-attack/, 21 March 2018.

81. Davis, J., et al. (2017). Stateless Attribution. Toward International Accountability in Cyberspace. Accessible: https://cyber-peace.org/wp-content/uploads/2017/10/RAND_RR2081.pdf, 25 February 2018.

82. Department of Defence. (2010) Dictionary of Military and Associated Terms. Accessible: https://fas.org/irp/doddir/dod/jp1_02.pdf, 13 March 2018

83. Department of Justice of the United States. (2016) Syrian Electronic Army Hacker Pleads Guilty. Accessible: https://www.justice.gov/opa/pr/syrian-electronic-army-hacker-pleads-guilty, 9 April 2018.

84. Department of Justice of the United States. Canadian Hacker Who Conspired With and Aided Russioan FSB Officers Pleads Guilty. (2017). Accessible: https://www.justice.gov/opa/pr/canadian-hacker-who-conspired-and-aided-russian-fsb-officers-pleads-guilty, 8 April 2018.

85. Director of National Intelligence. (2017). Worldwide Threat Assessment of the US Intelligence Community. Accessible: https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf, 25 February 2018.

86. Eichensehr, K. (2017) Three Questions on the WannaCry Attribution to North Korea. Accessible: https://www.justsecurity.org/49889/questions-wannacry-attribution-north-korea/, 6 May 2018.

87. Elich, G. (2018). The WannaCry Cyberattack: What the Evidence Says and Why the Trump Administration Blames North Korea. Accessible: https://www.counterpunch.org/2018/01/03/the-wannacry-cyberattack-what-the-evidence-says-and-why-the-trump-administration-blames-north-korea/, 6 May 2018.

88. Eneken Tikk, Kadri Kaska, Liis Vihul. (2010). International Cyber Incidents – Legal Considerations. - NATO CCD CoE Publications.

89. Federal Bureau of Investigations. (2014). Update on Sony Investigation. Accessible: https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation, 5 May 2018.

90. Ferris-Rotman, A. (2018). Expelled from Russia, U.S. diplomats bid a wistful farewell. Accessible: https://www.washingtonpost.com/news/worldviews/wp/2018/04/08/expelled-from-russia-u-s-diplomats-bid-a-wistful-farewell/?noredirect=on&utm_term=.a78f1261a407, 1 May 2018.

91. Finkle, J., Rothacker R. (2012). Cyber attacks on Wall Street bank straced to Iran. Accessible: https://www.theglobeandmail.com/globe-investor/cyber-attacks-on-wall-street-banks-traced-to-iran/article4559639/, 4 May 2018.

92. Foreign and Commonwealth Office. Foreign Office Minister condemns Russia for NotPetya attacks. Accessible: https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks, 6May 2018.

93. Goldman, D. (2012). Major banks hit with biggest cyberattacks in history. Accessible: http://money.cnn.com/2012/09/27/technology/bank-cyberattacks/index.html, 3 May 2018.

94. Government Communications Security Bureau. (2017). New Zealand concerned North Korean cyber aktivity. Accessible: https://www.gcsb.govt.nz/news/media-release-new-zealand-concerned-at-north-korean-cyber-activity/, 6 May 2018.

95. Government Communications Security Bureau. (2018). New Zealand joins international condemnation of NotPetya cyber.attacks. Accessible: https://www.gcsb.govt.nz/news/new-zealand-joins-international-condemnation-of-notpetya-cyber-attack/, 6 May 2018.

96. Greenberg, A. (2017) The WannaCry Ransomware Has a Link To Suspected North Korean Hackers. Accessible: https://www.wired.com/2017/05/wannacry-ransomware-link-suspected-north-korean-hackers/, 6 May 2018.

97. Grover, R., Hosenball, M., Finle J. Sony Suffered The Most Devastating Hack of A Major US Company Ever. Accessible: http://www.businessinsider.com/the-size-and-scope-of-the-sony-hack-is-incredible-2014-12, 5 May 2018.

98. Hathaway, M. Getting beyond Norms When Violating the Agreement Becomes Customary Practice. Accessible: https://www.cigionline.org/sites/default/files/documents/Paper%20no.127.pdf, 6 May 2018.

99. Henley, J., Solon, O. (2017). „Petya“ ransomware attack strikes companies across Europe and US. Accessible: https://www.theguardian.com/world/2017/jun/27/petya-ransomware-attack-strikes-companies-across-europe, 6 May 2018.

100. Hern, A. (2017). Ransomware attack „not designed to make money“, researchers claim. Accessible: https://www.theguardian.com/technology/2017/jun/28/notpetya-ransomware-attack-ukraine-russia, 6 May 2018.

101. Hern, A., Gibbs, S. What is WannaCry ransomware and why is it attacking global computers? Accessible: https://www.theguardian.com/technology/2017/may/12/nhs-ransomware-cyber-attack-what-is-wanacrypt0r-20, 6 May 2018.

102. Hern, A., MacAskill, E. (2017). WannaCry ransomware attack „linked to North Korea". Accessible: https://www.theguardian.com/technology/2017/jun/16/wannacry-ransomware-attack-linked-north-korea-lazarus-group, 6 May 2018.

103. Hughes, L., Bond, D., Peel, M. (2018). US, Germany and France blame Russia for nerve agent attack. Accessible: https://www.ft.com/content/81edb2ee-284b-11e8-b27e-cc62a39d57a0, 21 March 2018.

104. Independent International Fact-Finding Mission on the Conflict in Georgia. (2009). Accessible: http://www.mpil.de/files/pdf4/IIFFMCG_Volume_II1.pdf, 6 May 2018.

105. International Court of Justice. (1978). Rules of Court. Accessible: http://www.icj-cij.org/en/rules, 15 March 2018.

106. International Telecommunication Union. (2005). Tunis Agenda for the Information Society. Accessable: http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html, 13 May 2018.

107. Kastrenakes, J. The NSA reportedly believes North Corea was responsible for WannaCry ransomware attacks. Accessible: https://www.theverge.com/2017/6/14/15805346/wannacry-north-korea-linked-by-nsa, 6 May 2018.

108. Keizer, G. (2010). Estonia blamed Russia for backing 2007 cyberattacks, says leaked cable. Accessible: https://www.computerworld.com/article/2511704/vertical-it/estonia-blamed-russia-for-backing-2007-cyberattacks--says-leaked-cable.html, 3 May 2018.

109. Law Teacher. (2013). Rules of evidence before the international court of justice. Accessible: https://www.lawteacher.net/free-law-essays/international-law/rules-of-evidence-before-the-international-court-of-justice-international-law-essay.php#citethis, 15 March 2018.

110. Lee, D. (2014). Sony hack: Obama vows response as FBI blames North Korea. Accessible: http://www.bbc.com/news/world-us-canada-30555997, 5 May 2018.

111. Lowe, C. (2009). Kremlin loyalist says launched Estonia cyber-attacks. Accessible: https://www.reuters.com/article/us-russia-estonia-cyberspace-idUSTRE52B4D820090312, 3 May 2018.

112. Mantakou, A. The Misadventures of the Principle Jura Novit Curia in International Arbitration - A Practitioner's Approach.- Hellenic Institute of International and Foreign Law. Accessible: http://www.hiifl.gr/wp-content/uploads/MANTAKOUjuranovitcuria.pdf, 17 March 2018.

113. Maurer, T. (2018) Here's How Hostile States are Hiding Behind „Independent" Hackers. Carnegie Endowment for International Peace. Accessible: https://carnegieendowment.org/2018/02/01/here-s-how-hostile-states-are-hiding-behind-independent-hackers-pub-75424, 8 April 2018.

114. Microsoft Secure. New ransomware, old techniques: Petya adds worm capabilities. Accessible: https://cloudblogs.microsoft.com/microsoftsecure/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/?source=mmpc, 6 May 2018.

115. Minárik, T., Peterson, R., Naagel, M. (2017). WannaCry Campaign: Potential State Involvement Could Have Serious Consequences. Accessible: https://ccdcoe.org/wannacry-campaign-potential-state-involvement-could-have-serious-consequences.html, 6 May 2018.

116. Minister of Law Enforcement and Cyber Security. (2018) Australian Government attribution of the „NotPetya" cyber incident to Russia. Accessible: http://minister.homeaffairs.gov.au/angustaylor/Pages/notpetya-russia.aspx, 6 May 2018.

117. Ministry of Foreign Affaris of the Republic of Estonia. (2007). Address by Minister of Foreign Affairs of Estonia Urmas Paet. Accessible: http://vm.ee/en/news/address-minister-foreign-affairs-estonia-urmas-paet, 3 May 2018.

118. Ministry of Foreign Affaris of the Republic of Estonia. (2007). Cyber Attacks Hit Estonia. Accessable: http://vm.ee/sites/default/files/content-editors/web-static/115/cyber_attacks.pdf, 3 May 2018.

119. Morris, S., Bannock, C. (2018). Salisbury attack: what has the UK said and what evidence does it have? Accessible: https://www.theguardian.com/uk-news/2018/apr/04/salisbury-attack-what-has-the-uk-said-and-what-evidence-does-it-have, 1 May 2018.

120. Nakashima, E. (2012). Iran blamed for cyberattacks on U.S. banks and companies. Accessible: https://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html?utm_term=.879211c50f3a, 4 May 2018.

121. National Cyber Security Centre. (2018). Russian military „almost certainly" responsible for destructive 2017 cyber attack. Accessible: https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack, 6 May 2018.

122. NATO. (2014). Glossary of Terms and Definitions. Accessible: http://wcnjk.wp.mil.pl/plik/file/N_20130808_AAP6EN.pdf, 13 March 2018.

123. Newman, L. The Leaked NSA Spy Tool That Hacked the World. Accessible: https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/, 6 May 2018.

124. Novetta. Operation Blockbuster. Unravelling the Long Thread od the Sony Attack. Accessible: https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf, 6 May 2018.

125. Õhtuleht. (2018). Välisminister mõistab hukka Venemaa valitsuse küberründe NotPetya Ukraina vastu. Acessible: https://www.ohtuleht.ee/858906/valisminister-moistab-hukka-venemaa-valitsuse-kuberrunde-notpetya-ukraina-vastu, 6 May 2018.

126. Osula, A-M., Rõigas, H. (2016). International Cyber Norms. Legal, Policy & Industry Perspectives. NATO CCD COE Publications.

127. Ottis, R. (2008). Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective. – NATO Cooperative Cyber Defence Centre of Exellence.

128. Pau, A. (2007). Venemaa keeldus koostööst küberrünnakute uurimisel. Accessible: http://epl.delfi.ee/news/eesti/venemaa-keeldus-koostoost-kuberrunnakute-uurimisel?id=51093368, 3 May 2018.

129. Perlroth, N., Hardy, Q. (2013). Bank Hacking Was the Work of Iranians, Officials Say. Accessible: https://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html, 4 May 2018.

130. Prime Minister of Australia. (2017). Media release. Accessible: https://www.pm.gov.au/media/attributing-wannacry-ramsomware-north-korea, 6 May 2018.

131. Risk Based Security. (2014). A Breakdown and Analysis of the December, 2014 Sony Hack. Accessible: https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/

132. Rogin, J. (2018). Former Western leaders join forces to fight Russian meddling. Accessible: https://www.washingtonpost.com/opinions/global-opinions/former-western-leaders-join-forces-to-fight-russian-meddling/2018/05/10/f93dc3c6-5491-11e8-abd8-265bd07a9859_story.html?noredirect=on&utm_term=.5b4549fdfd9e, 15 May 2018.

133. Roman, J. (2015). FBI Defends Sony Hack Attribution. Accessible: https://www.bankinfosecurity.com/sony-a-7762, 6 May 2018.

134. Sandle, P. Britain joins U.S. in blaming North Korea for „WannaCry“ attack. Accessible: https://www.reuters.com/article/us-usa-cyber-northkorea-britain/britain-joins-u-s-in-blaming-north-korea-for-wannacry-attack-idUSKBN1ED1SK, 6 May 2018.

135. Sanger, D., Fackler,M. (2015). N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say. Accessible: https://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html, 6 May 2018.

136. Schmitt, M. (2012). „Attack“ as a Term of Art in International Law: The Cyber Operations Context. - NATO CCD COE Publications.

137. Schmitt, M. (2014). International Law and Cyber Attacks: Sony v. North Korea. Accessible: https://www.justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea/, 6 May 2018.

138. Sharp, A., Tweed, D., Olorunnipa, T. U.S. Says North Korea Was Behind WannaCry Cyberattack. Accessible: https://www.bloomberg.com/news/articles/2017-12-19/u-s-blames-north-korea-for-cowardly-wannacry-cyberattack, 6 May 2018.

139. Statement from the Press Secretary. (2018) Accessible: https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/, 6 May 2018.

140. Symantec Security Response. (2017). What you need to know about the WannaCry Ransomware. Accessible: https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack, 6 May 2018.

141. The Verge. (2017). Petya ransomware: everything we know about the massive cyberattack. Accesible: https://www.theverge.com/2017/6/28/15888094/petya-ransomware-attack-news-virus, 6 May 2018.

142. Tomka, P., Proulx, V. (2016). The Evidentiary Practice of the World Court. - University of Peace Press.

143. TrendMicro. (2018). 2017 Annual Security Roundup: The Paradox of Cyberthreats. Accessible: https://documents.trendmicro.com/assets/rpt/rpt-2017-Annual-Security-Roundup-The-Paradox-of-Cyberthreats.pdf, 6 May 2018.

144. U.S. Department of Treasury. Treasury Sanctions Russian Cyber Actor for Interference with the 2016 U.S. Elections and Malicious Cyber-attacks. Accessible: https://home.treasury.gov/news/press-releases/sm0312, 6 May 2018.

145. United Nations. (1995). Rules of Procedure and Evidence for the International Criminal Tribunal for Rwanda. Accessible: http://unictr.unmict.org/sites/unictr.org/files/legal-library/150513-rpe-en-fr.pdf, 16 April 2018.

146. United Nations. (2009). United Nations Fact Finding Mission on the Gaza conflict. Accessible: http://www.ohchr.org/EN/HRBodies/HRC/SpecialSessions/Session9/Pages/FactFindingMission.aspx, 13 May 2018.

147. United Nations. (2009). Updated Statute of the International Criminal Tribunal for the Former Yugoslavia. Accessible: http://www.icty.org/x/file/Legal%20Library/Statute/statute_sept09_en.pdf, 29 April 2018.

148. United Nations. (2014). Meeting coverage. Accessible: https://www.un.org/press/en/2014/gal3490.doc.htm, 15 March 2018.

149. United Nations. Member States. http://www.un.org/en/member-states/index.html, 15 May 2018.

150. United Nations. (2015). Rules of Procedure and Evidence for the International Criminal Tribunal for the Former Yugoslavia. Accessible: http://www.icty.org/x/file/Legal%20Library/Rules_procedure_evidence/IT032Rev50_en.pdf, 16 April 2018.

151. United Nations. (2018). Fact-finding Mission on Myanmar: conrete and overwhelming information points to international crimes. Accessible: http://www.ohchr.org/EN/HRBodies/HRC/Pages/NewsDetail.aspx?NewsID=22794&LangID=E, 13 May 2018.

152. United States Computer Emergency Readiness Team. Petya Ransomware. Accessible: https://www.us-cert.gov/ncas/alerts/TA17-181A, 6 May 2018.

153. US Department of Defence. Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands and Directors of the Joint Staff Directorates – Joint Terminology for Cyberspace Operations. Accessible: http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf, 15 March 2018.

154. Volz, D., Finkle, J. (2016). U.S. indicts Iranians for hackng dozens of banks, New York dam. Accessible: https://www.reuters.com/article/us-usa-iran-cyber/u-s-indicts-iranians-for-hacking-dozens-of-banks-new-york-dam-idUSKCN0WQ1JF, 5 May 2018.

155. Walker, P. (2018). UK, US, Germany and France unite to condemn spy attack. Accessible: https://www.theguardian.com/uk-news/2018/mar/15/salisbury-poisoning-uk-us-germany-and-france-issue-joint-statement, 21 March 2018.

156. We Live Security by ESET. (2017). New WannaCryptor-like ransomware attack hits globally: All you need to know. Accessible: https://www.welivesecurity.com/2017/06/27/new-ransomware-attack-hits-ukraine/, 6 May 2018.

157. Zetter, K. (2014). Sony got hacked hard: what we know and don't know so far. Accessible: https://www.wired.com/2014/12/Sony-hack-what-we-know, 5 May 2018.