MYKOLAS ROMERIS UNIVERSITY

FACULTY OF LAW

INSTITUTE OF INTERNATIONAL AND EUROPEAN UNION LAW

SERGII KARASOV

INTERNATIONAL LAW PROGRAMME

COLLECTIVE SELF-DEFENSE IN THE NATO FRAMEWORK AGAINST CYBERATTACKS AND MODERN INTERNATIONAL LAW

Master thesis

Supervisor –
Professor
Dr.
Justinas Žilinskas

Vilnius, 2018

TABLE OF CONTENTS

LIST OF ABBREVIATION

ACT Allied Command Transformation

CERT Computer Emergency Response Team

CDMA Cyber Defense Management Authority

CI Critical Infrastructure

CII Critical Information Infrastructure

CEI Critical Energy Infrastructure

CEIP Critical Energy Infrastructure Protection

CIA Central Intelligence Agency

DoD U.S. Department of Defense of United States

DoS Denial-of-service

DDoS Distributed Denial of Service

DRC Democratic Republic of Congo

ICT Information and Communications Technologies

ICTY International Criminal Tribunal for the former Yugoslavia

IOC International Olympic Committee

IP Internet Protocol

ICS Industrial Control Systems

FRY Federal Republic of Yugoslavia

FSB Federal Security Service of Russia

GRU Military Intelligence of Russia

ICJ International Court of Justice

UN Charter United Nations Charter

UN Security Council United Nations Security Council

NATO North Atlantic Treaty Organization

NATO Treaty North Atlantic Washington Treaty

NAC North Atlantic Council

NCA National Command Authority of US

NATO CCD COE NATO Cooperative Cyber Defense Centre of Excellence

NATO HQ NATO headquarters

NCI Agency NATO Communications and Information Agency

SCADA Supervisory Control and Data Acquisition

SVR Foreign Intelligence Service

UES United Energy System

WADA World Anti-Doping Agency

Special thanks to Dr. Justinas Žilinskas, Mr. Vytautas Butrimas,
Dr. Tadas Jakštas for their helpful comments and inputs
and to Maj. Rimantas Šikas, Dr. Olesia Tragniuk,
my parents for their support during studies.

INTRODUCTION

In recent years, cyber security has become one of the most actively discussed topics of international law, not only because domestic and inter-State cyber security incidents have grown in number and severity, but also because of the realisation that the technical peculiarities of cyberspace create new and unique legal problems that previously have not been encountered.[1]

Several states have in fact been the object of cyberattacks of which other states were suspected. In 2007, a three-week Distributed Denial of Service (DDoS) attack targeted Estonia.[2] Cyber operations also hit, among others, Azerbaijan, Kyrgyzstan, Lithuania, Montenegro, South Korea, Switzerland, Taiwan, the United Kingdom, and the United States. In September 2010, a computer worm, dubbed Stuxnet, had attacked Iran's industrial infrastructure.[3] In December 2015, Ukraine faced a major escalation in the seriousness of cyberattacks on Critical Energy Infrastructure (CEI).[4]

Taking into account that the cyber threats and attacks are becoming more common, sophisticated and damaging, it is very important that such actions are countered with a strong commitment to existing international law and the values that it represents. The right to collective self-defense in the case of cyberattacks becomes relevant and necessary for research in international law.

---

[1] Katharina Ziolkowski, *Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy* (Tallinn, Estonia: NATO CCD COE Publications, 2013), 621.

[2] "Cited from: For the facts of the case, see Eneken Tikk, Kadri Kaska, and Liis Vihul, International Cyber Incidents. Legal Considerations (CCDCOE, 2010), 18 http://www.ccdcoe.org/publications/books/legalconsiderations.pdf", Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 4.

[3] "Cited from: For a comprehensive technical analysis of Stuxnet, see Symantec's Nicolas Falliere, Liam O Murchu, and Eric Chien, W32.Stuxnet Dossier, version 1.4, February 2011, <http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf. Iran claims that its uranium enrichment programme is for purely civilian purposes", Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 6.

[4] "The first case of a successful cyberattack on energy objects has been registered in Ukraine" Ukrainian National News, accessed, 2018, May 3, http://www.unn.com.ua/uk/news/1552689-minenergovugillya-pershiy-u-sviti-vipadok-vdaloyi-kiberataki-na-obyekti-energetiki-zareyestrovano-v-ukrayini

It should be noted that, the International Court of Justice (ICJ) has stated that Article 51 of the United Nations Charter (UN Charter), regarding self-defense respectively, apply to "*any use of force, regardless of the weapons employed"*.[5]

Article 51 of the UN Charter contemplates not only individual but also collective self-defense.[6] Collective self-defense is submitted to the same conditions as individual self-defense.[7]

One way of exercising collective self-defense is through a military alliance established to that purpose. The most significant collective self-defense international organization today is North Atlantic Treaty Organization (NATO) as source of stability in world and the transatlantic framework for strong collective defense.[8]

The fundamental cyber defense responsibility of NATO is to defend its own networks, and that assistance to Allies in accordance with the spirit of solidarity.[9]

In the Wales Summit Declaration on 5 September 2014, NATO recognized that international law, including international humanitarian law and the UN Charter, applies in cyberspace. A decision as to when a cyberattack would lead to the invocation of Article 5 would be taken by the North Atlantic Council (NAC) on a case-by-case basis.[10]

Two years later, in the Warsaw Summit Declaration on 9 July 2016, Alliance reaffirmed NATO's defensive mandate, and recognized cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea.[11]

---

[5] Nuclear Weapons advisory opinion: Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 ICJ 226 (8 July), para. 39, http://www.icj-cij.org/files/case-related/95/095-19960708-ADV-01-00-EN.pdf

[6] Article 51, United Nations Charter, 26 June 1945, http://www.un.org/en/sections/un-charter/chapter-vii/index.html

[7] Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 92.

[8] The North Atlantic Treaty, Washington D.C., 4 April 1949, https://www.nato.int/cps/en/natohq/official_texts_17120.htm

[9] Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, North Atlantic Council, para 72, 5 September 2014, https://www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=en

[10] Ibid.

[11] Warsaw Summit Communiqué issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, North Atlantic Council, para 70, 8-9 July 2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en

Despite all the measures taken by NATO there is still no concurrence between the international community and scholars on the threshold upon which a cyber (armed) attack triggers collective self-defense.[12] In addition, there are legal problems directly related to technical issues concerning the problems of attribution and identification of the attacker, anticipatory self-defense an imminent armed attack by cyber means, self-defense against cyberattacks by non-state actors, necessity and proportionality of the reaction, the standard of evidence for the exercise of self-defense against cyberattacks.

There is no more guidance on criteria for cyberattacks to reach the required threshold of the Article 5 of the NATO Treaty. The NAC might face a challenge to take decisions due to differ views of 29 sovereign NATO allies. Similarly, member States might also have different views on the threshold of "self-defense" in the context of cyberattacks.[13]

The envisaged disagreement on the threshold of "self-defense" in cases of cyberattacks, lack of institutionalized structures of NATO forces during cyberattacks and real defense plans in place could have an adverse effect on NATO's ability to swiftly respond to a cyberattack. There is a significant risk in waiting until such a cyberattack occurs to decide whether the criteria are met to trigger the application of Article 5 of the NATO Treaty.[14]

The problematic aspects raised in the research

The Master thesis concentrates on a problem of the correspondence of collective self-defense in the NATO framework against cyberattacks in the modern international law. In NATO, there is no guidance on criteria for cyberattacks to reach the required threshold and procedure available with regard to Article 5 of the NATO Treaty. The problematic aspects of the legal nature of the Article 5 of the NATO Treaty and the Article 51 of the UN Charter in light of collective self-defense in the NATO framework against cyberattacks is critically analysed to define it is applicable in the modern international law.

The aim of the research

[12] Enrico Benedetto Cossidente, " Legal Aspects of Cyber and Cyber-Related Issues Affecting NATO ", *NATO Legal Gazette* 61, 35 (2014): 14, http://www.act.nato.int/images/stories/media/doclibrary/legal_gazette_35.pdf

[13] Florentine J.M. de Boer, " Examining the Threshold of "Armed Attack" in light of Collective Self-Defence against Cyber Attacks: NATO's Enhanced Cyber Defence Policy", *NATO Legal Gazette* 61, 35 (2014): 35, http://www.act.nato.int/images/stories/media/doclibrary/legal_gazette_35.pdf

[14] Ibid. p. 36.

The aim of this research is to examine whether and when collective self-defense clauses of Article 5 of the NATO Treaty and the Article 51 of the UN Charter are applicable in the case of cyber security threat.

The objectives of the research

- To analyse the main elements of "Armed Attack" as cyberattack in light Article 5 of the NATO Treaty and the Article 51 of the UN Charter and define scale and effects of "Armed Attack" as cyberattack and anticipatory self-defense against an imminent armed attack by cyber means;
- To research the main requirements of collective self-defense against cyberattacks such as necessity, proportionality, immediacy, request of the victim state for collective self-defense and the duty to report the self-defense measures to the UN Security Council;
- To analyse the standard of evidence required for the exercise of collective self-defense against cyberattacks and the main problems of attribution and identification of the attacker;
- To examine collective self-defense against cyberattacks by non-state actors and the role of the third states in the territory where a cyberattack occurred in the identification of attacker;
- To research whether Member State of NATO could reach agreement invoked of Article 5 of the NATO Treaty in the case of "Armed Attack" as cyberattack.

Relevance of the final thesis

There is a specific need to explore legal problems related to collective self-defense in the NATO framework against cyberattacks. After the Wales and Warsaw Summits there is no existing case-law and practical application Article 5 of the NATO Treaty. NATO's readiness will be adversely affected in the absence of clear legal foundation of Article 5 in cyber domain. In other words, the response to the raised legal question is needed to enhance NATO's ability to collectively respond to growing cyberattacks.

Scientific novelty of the selected topic

Literature review has shown that the issue is poorly investigated by scientists within the framework of NATO. However, the general legal problems related to cyber operations and the use of force in international law is considered. One of the most comprehensive analysis had been

made by Michael N. Schmitt[15] and Marco Roscini[16] who analysed the provision of self-defense in the case cyberattacks according with international law. Nevertheless, the issue still remains to be very controversial as some authors like Katharina Ziolkowski[17] and Florentine J.M. de Boer[18] have an opposite views on some aspects so that comprehensive analysis needs to made. The topic of master thesis also is very actual and new within the framework of NATO, because there are not any researches related applicability Article 5 of the NATO Treaty within NATO specificity what makes master thesis is original in the context of other researches.

Significance of the Final Thesis

The results of the research could be considered by NATO' headquarters (NATO HQ), NAC, Allied Command Transformation (ACT), NATO Communications and Information Agency (NCI Agency), NATO accredited Centres of Excellence, in particularly NATO CCD COE, military legal advisers to the command of NATO allies and partner countries.

Moreover, conclusions and recommendations of this research could to be important to other scholars who are involved in researching problems of collective self-defense in the NATO framework against cyberattacks and modern international law. This master thesis could be a basis for more specific scientific findings, especially to research questions related to legal grounds of NATO' reaction on the cyber domain in the case when cyberattacks on NATO allies do not reach the level of threshold "Armed Attack" that happens very often.

Research methods

The following methods were used in order to achieve the aim of the Master thesis:

Communicative method, (Philosophical method). Communicative method used to understand details of interaction of subjects responsible for create of legal documents (UN Charter, NATO Treaty) and relevant court decisions related to self-defense.

Method of logics, (General scientific method). Method of logics is used for analysis and synthesis, induction and deduction, climbing from abstract to concrete. Method is used in

[15] Michael N. Schmitt, Professor of Public International Law at the University of Exeter, Michael N. Schmitt with the International Groups at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE).

[16] Marco Roscini, Professor of International Law at the University of Westminster in London .

[17] Dr Katharina Ziolkowski, Senior Analyst, NATO CCD COE.

[18] Florentine J.M. de Boer, former a Legal Fellow at NATO SCHOOL Oberammergau.

conjunction while applying other utilized methods to raise assumptions, assess whether they could be confirmed or denied.

Historical (chronological) method, (General scientific method). Historical method was used to research legal development institute of self-defense after adopted UN Charter and NATO Treaty.

System method, (General scientific method). System method used to research collective-self-defense with determine the functions of each of its elements, the interconnection of element with other elements of the same system. Method is used to clarify the main features of judicial practice, legal documents and publications of legal scholars related to collective self-defense.

Formal legal method, (Own methods of law). Formal legal method was used to logical processing and interpretation of legal norms Article 5 of NATO Treaty and Article 51 of the UN Charter and finding out the will of the legislator expressed in the text of the treaties.

Comparative method, **(Own methods of law).** Comparative method was used to compare the opinions of different authors regarding the same subjects and issues. Also, method was used to compare legal nature of cyber strategies of different Member States of NATO to understand prospects for adoption decision by NAC in the case cyberattack one or more of them.

Thesis structure

The thesis consists of introduction, 4 chapters that are divided into subchapters, conclusion, recommendations and the list of bibliography.

Chapter 1 will provide analyse the main elements of "Armed Attack" as cyberattack in light Article 5 of the NATO Treaty and the Article 51 of the UN Charter (actions, consequences, intentions, motives, objects and subjects of cyberattacks).

Chapter 2 will research the nature of the scale and effects required for an act to be characterized as an armed attack as cyberattack necessarily exceed those qualifying the act as a use of force. It is necessary to focus on the nature of an action's consequences of "Armed Attack" as cyberattack for understanding scale and effects within meaning Nicaragua Judgment. Moreover, it will be research anticipatory self-defense against an imminent armed attack by cyber means.

Chapter 3 will research the main requirements of collective self-defense NATO against cyberattacks such as necessity, proportionality, immediacy, request of the victim state for

collective self-defense and the duty to report the self-defense measures to the UN Security Council. Chapter will focus on challenges which can arise on practice.

Chapter 4 will research the standard of evidence required for the exercise of collective self-defense against cyberattacks and the main problems of attribution, identification of the attacker, and collective self-defense against cyberattacks by non-state actors.

Defense Statement

NATO should detail Wales Summit Declaration on 5 September 2014 and Warsaw Summit Declaration on 9 July 2016 related Article 5 of the NATO Treaty in the case of "Armed Attack" as cyberattack through create of the new regional legal instrument that could clearly regulate the use of collective self-defense against the cyberattacks on the Alliance. International law has complexities for application in cyberspace.

1. THE MAIN ELEMENTS OF "ARMED ATTACK" AS CYBERATTACK IN LIGHT ARTICLE 5 OF THE NATO TREATY AND THE ARTICLE 51 OF THE UN CHARTER

There are two recognized exceptions to the international law prohibition of the use of force: the exercise of the right of self-defense and actions implementing a United Nations Security Council resolution under Chapter VII of the United Nations Charter.[19]

Collective self-defense expressed in Article 5 of NATO Treaty is a well-known fundamental principle of NATO: *"(...) an armed attack against one or more of them in Europe or North America shall be considered an attack against them all (...)".*[20] If the NAC decides to activate Article 5, NATO member countries will assist the attacked State in whatever manner they deem necessary. In its turn, NATO exercises of the right collective self-defense recognized by Article 51 of UN Charter.[21] According to Article 51 of the United Nations Charter, *"nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations (...)".*[22] This Article recognizes and reflects the customary law right of self-defense.[23]

Thus, NATO member states have the right to collective self-defense in the event of an "Armed Attack" against them. This requirement applies not only to a defensive reaction with traditional weapons, but also to one with cyber means to the extent that it amounts to a use of force under Article 2(4) of UN Charter[24].

Unfortunately, neither the text of Article 5 of NATO Treaty nor Article 51 of the UN Charter contain an explanation of the threshold required for an armed attack to have occurred,

---

[19] Article 51, Chapter United Nations Charter VII, 26 June 1945, http://www.un.org/en/sections/un-charter/chapter-vii/index.html

[20] Article 5, The North Atlantic Treaty, Washington D.C., 4 April 1949, https://www.nato.int/cps/en/natohq/official_texts_17120.htm

[21] Article 51, United Nations Charter, 26 June 1945, http://www.un.org/en/sections/un-charter/chapter-vii/index.html

[22] Ibid.

[23] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (UK: Cambridge University Press, 2017), 339.

[24] Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, North Atlantic Council, para 72, 5 September 2014, https://www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=en

thus there is no clear definition available.[25] The purpose of this chapter is to research the nature of the "Armed Attack" as a cyberattack. The author of the master thesis offers a structure of analysis that will be included: actions, consequences, intentions, objects and subjects of cyberattacks.

1.1 Actions

In Nicaragua judgment, ICJ acknowledged that a definition of "Armed Attack" does not exist in the UN Charter and is not part of treaty law.[26] If it is apparent that an "Armed Attack" implies the use of arms, ICJ made clear that Article 51 applies to *"any use of force, regardless of the weapons employed"*.[27] The fact that cyber operations do not employ kinetic weapons does not necessarily mean they are not "armed".[28] The use of any device, or number of devices, which results in a considerable severe consequences must therefore be deemed to fulfill the conditions of an "Armed Attack". This conclusion is supported by the Security Council of United Nations (SC UN) reaffirmation of the right to self-defense in relation to the 11 September 2001 attacks on the United States, where the "weapons" employed were hijacked airplanes.[29]

However, Benatar[30] and Woltag[31] suggested that traditionally the definition of the term "armed attack" as laid down in Article 51 would have involved a notion of kinetic force. Such an approach has been almost unanimously rejected in the academic literature dealing with cyberattacks.[32]

Michael N. Schmitt was considering that cyberattacks did not fit neatly into the notion of an attack that was "armed" in the kinetic sense. Cyberattacks seemed distant from the concept of

[25] Enrico Benedetto Cossidente, " Legal Aspects of Cyber and Cyber-Related Issues Affecting NATO ", *NATO Legal Gazette* 61, 35 (2014): 30, http://www.act.nato.int/images/stories/media/doclibrary/legal_gazette_35.pdf

[26] Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America), 27 June 1986, para. 176, http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

[27] Nuclear Weapons advisory opinion: Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 ICJ 226 (8 July), para. 39, http://www.icj-cij.org/files/case-related/95/095-19960708-ADV-01-00-EN.pdf

[28] Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 71.

[29] "Cited from: See SC Res 1368 (12 September 2001) and SC Res 1373 (28 September 2001), Ibid. p. 6.

[30] Benatar, "The Use of Cyber Force: Need for Legal Justification?", *Goettingen Journal of International Law, 1,* (2009): 375, 389.

[31] Woltag, "Cyber Warfare, in Wolfrum (ed.)", *Max Planck Encyclopaedia of Public International Law*, Oxford, (2010): para 8.

[32] Katharina Ziolkowski, *Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy* (Tallinn, Estonia: NATO CCD COE Publications, 2013), 622.

"armed." Traditional weapons were not employed, they did not require the supporting elements typically associated with military assaults and, most importantly, their direct destructive effect did not result from a release of kinetic force.[33]

Actions of cyberattacks can be described by five major groups which vary according to the objectives pursued by the attacker of the system:

- Corruption of information – when data on a system or communications channel suffers improper modification;
- Denial-of-service (DoS) – when access to the system is denied for authorized users;
- Disclosure of information – when critical information is disclosed to unauthorized persons or systems;
- Theft of resources – when system resources are used by unauthorized entities;
- Physical destruction – when physical harm or destruction is achieved through the use of Industrial Control Systems (ICS).[34]

Cyberattacks have several stages: reconnaissance to identify the target's vulnerabilities, developing "weaponized" code, breaking in, delivering the software "payload", and then "triggering" it – all without being detected. The most harmful cyberattacks – those like Stuxnet that cause physical damage – are still a high art of which only a few nations are capable.[35]

The International Group of Experts at the invitation of NATO CCD COE (Hereinafter-Group of Experts) determined that a cyberattack can reach the threshold of "armed attack" if the effects caused are equivalent to the effects of (traditional) kinetic attacks.[36]

---

[33] Michael N. Schmitt, "Attack" as a Term of Art in International Law: The Cyber Operations Context", 2012 *4th International Conference on Cyber Conflict*, Tallinn (2012): 287, https://www.ccdcoe.org/publications/2012proceedings/5_2_Schmitt_AttackAsATermOfArt.pdf

[34] Limba T.; Plėta T.; Agafonov K.; Damkus M.,. "Cyber security management model for critical infrastructure", *Entrepreneurship and Sustainability Issues* 4(4), (2017): 561, http://dx.doi.org/10.9770/jesi.2017.4.4(12)

[35] James A. Lewis, "The Role of Offensive Cyber Operations in NATO's Collective Defence, *The Tallinn Papers*, NATO CCD COE, Publication on Strategic Cyber Security, (2015): 8, 9, https://ccdcoe.org/sites/default/files/multimedia/pdf/TP_08_2015_0.pdf

[36] " Cited from: Schmitt (n 13) 54-56; See also Robin Geib and Henning Lahman, "Freedom and Security in Cyberspace: Shifting the Focus away from Military Responses towards Non-Forcible Countermeasures and Collective Threat-Prevention" in Katharina Ziolkowski (ed), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy (NATO Cooperative Cyber Defence Centre of Excellence 2013) 622 n 3." Enrico Benedetto Cossidente, " Legal Aspects of Cyber and Cyber-Related Issues Affecting NATO ", *NATO Legal Gazette* 61, 35 (2014): 14, http://www.act.nato.int/images/stories/media/doclibrary/legal_gazette_35.pdf

Nothing in Article 5 of NATO Treaty and Article 51 of UN Charter or customary international law specifically excludes a particular type of weapon or weapons system.[37]

According to Nuclear Weapons advisory opinion of ICJ, the choice of means of attack is immaterial to the issue of whether an operation qualifies as an armed attack.[38] Moreover, the position is consistent with State practice.[39] For example, it is universally accepted that chemical, biological, and radiological attacks of the requisite scale and effects to constitute armed attacks trigger the right of self-defense. This is so, despite their non-kinetic nature, because the ensuing consequences can include serious suffering or death. Identical reasoning would apply to cyber operations.[40]

As noted by ICJ, not every use of force rises to the level of an armed attack.[41] The scale and effects 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 a State entitled to respond using force in self-defense.[42] It noted the need to "distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms", but provided no further guidance in this regard.[43] Confirmation by the Court of the inherently forcible nature of such attacks is conceptually valuable nonetheless.[44]

An important issue is whether a State may exercise the right of self-defense in response to a series of cyber incidents that individually fall below the threshold of an armed attack. Group of Experts agreed that the determinative factor is whether the same originator (or originators acting

---

[37] Cyber Warfare, No 77, AIV / No 22, CAVV December (2011): 21, https://aiv-advies.nl/download/da5c7827-87f5-451a-a7fe-0aacb8d302c3.pdf

[38] Nuclear Weapons advisory opinion: Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 ICJ 226 (8 July), para. 39, http://www.icj-cij.org/files/case-related/95/095-19960708-ADV-01-00-EN.pdf

[39] Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, North Atlantic Council, para 72, 5 September 2014, https://www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=en

[40] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (UK: Cambridge University Press, 2017), 340.

[41] Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America), 27 June 1986, para. 191, http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

[42] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (UK: Cambridge University Press, 2017), 341.

[43] Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America), 27 June 1986, para. 191, http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

[44] James A Green, *The International Court of Justice and Self-Defence in International Law* (Oxford and Portland, Oregon, 2009), 32.

in concert) has carried out smaller-scale incidents that are related and that taken together meet the requisite scale and effects.[45]

It is thus conceivable that a series of pin-prick attacks could be collectively seen as an armed attack if the attacks are sufficiently related and the consequences sufficiently grave. The same logic applies to cyber operations as well.[46]

An example might be a cyberattack on the electricity grid: attacking an individual transformer or even a power plant might cause physical damage that would constitute force but might not be sufficiently grave as to be an armed attack. However, a series of similar attacks carried out simultaneously on several transformers or power plants might very well collectively cross the threshold of an armed attack.[47]

In the Nicaragua judgment, ICJ distinguished between an "armed attack" and a "mere frontier incident".[48] In this regard, ICJ has subsequently indicated that: *"an attack on a single military platform or installation might qualify as an armed attack"*.[49]

Unfortunately, the Court failed to set forth criteria against which to judge a particular action or incident, an omission for which it has been roundly criticized.[50]

Thus, after analyzing actions as one of the elements of an "Armed Attack" as cyberattack, it becomes clear that more necessary and appropriate to focus on the nature of an action's consequences of "Armed Attack" as cyberattack for understanding scale and effects within meaning Nicaragua Judgment (para. 195).

---

[45] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (UK: Cambridge University Press, 2017), 342.

[46] Janne Valo, Cyber Attacks and the Use Force in Internationa law, (Master thesis, University of Helsinki, 2014), 53, https://helda.helsinki.fi/bitstream/handle/10138/42701/Cyber%20Attacks%20and%20the%20Use%20of%20Force%20in%20International%20Law.pdf?sequence=2

[47] Ibid.

[48] Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America), 27 June 1986, para. 195, http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

[49] Case concerning oil platforms (Islamic republic of Iran v. United States of America), 12 December 1996, para. 57, 61, http://www.icj-cij.org/files/case-related/90/090-19961212-JUD-01-00-EN.pdf

[50] Michael N. Schmitt, "Attack" as a Term of Art in International Law: The Cyber Operations Context, 2012 4th International Conference on Cyber Conflict, Tallinn, (2012): 288, https://www.ccdcoe.org/publications/2012proceedings/5_2_Schmitt_AttackAsATermOfArt.pdf

1.2 Consequences

1.2.1 First approach: consequences with injury, death, damage, or destruction

In the analysis and literal interpretation of Articles 5 of NATO Treaty and Article 51 of the UN Charter it becomes clear that these norms do not foresee consequences in terms of content. However, take in account opinion of ICJ[51] that the scale and effects required for an act to be characterized as an armed attack, it should be focus on such elements of "Armed Attack" as consequences.

If a cyberattack leads to a significant number of fatalities or causes substantial physical damage or destruction to vital infrastructure, military platforms or installations or civil property, it could certainly be qualified as an 'armed attack' within the meaning of article 51 of the UN Charter. The fact that such an attack has not yet taken place does not mean it could not in the foreseeable future. A digital attack against information systems linked to vital infrastructure, military installations and platforms for weapons systems or vital services, such as the emergency services or air traffic control systems, could breach the threshold of an armed attack if it causes significant loss of life or physical destruction.[52]

Consequently, neither the attacks on Estonia in 2007 nor those on Georgia in 2008 fall within the definition of armed attack. Those attacks did not cause any human or material damage and the disruption that they did cause was contained and was manageable. The view that they did not amount to armed attack is also supported by the fact that in the case of Estonia Article 5 of NATO Treaty which provides for collective self-defense action if a Member State has been attacked was not invoked but the whole incident was mainly treated under the criminal law.[53]

The case of cyberattacks that do not result in injury, death, damage, or destruction, but that otherwise have extensive negative effects, remains unsettled. Some of Group of Experts took the

[51] Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America), 27 June 1986, para. 195, http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

[52] Cyber Warfare, No 77, AIV / No 22, CAVV December (2011): 21, https://aiv-advies.nl/download/da5c7827-87f5-451a-a7fe-0aacb8d302c3.pdf

[53] (Cited from: NATO Parliamentary Assembly, Annual Session 2009, Committee Report 173 DSCFC 09 E bis- 'NATO and Cyber Defence', para 58–61, http://www.nato-pa.int/default.asp?SHORTCUT¼17824), Nicholas Tsagourias, "Cyberattacks, self-defense and the problem of attribution", *Journal of Conflict & Security Law,* Oxford University Press, (2012): 232, https://poseidon01.ssrn.com/delivery.php?ID=770086120101089003117080103078105102097019000017052006005002004125003114010120025098011033116011014051125088013102084076093102119041046028050091103091108113012096030052077045008070095095024011092084096088087071111086096016123019084104026025002087083097&EXT=pdf

position that harm to persons or physical damage to property is a condition precedent to the characterization of an incident as an armed attack.[54]

1.2.2 Second approach: consequences without injury, death, damage, or destruction

From opinion of Benedetto, the first approach leaves out cyberattacks that have serious consequences without actually causing physical damage, destruction, injury or death. Consider for example a cyberattack that targets the financial system of a State or other critical infrastructure, such as Supervisory Control and Data Acquisition (SCADA)[55] networks, severely affecting the functioning of a State or even causing a State to be paralyzed. He noted that: *"it appears disproportionate that these cyberattacks would not reach the threshold of armed attack, while their effects may be more severe, long-lasting and on a greater scale than other effects caused by traditional armed attacks".*[56]

For example in the Oil Platforms case, the ICJ mentioned that *"the mining of a single military vessel might be sufficient to bring into play the 'inherent right of self-defense' (...)".*[57]

Others experts took the view that it is not the nature (injurious or destructive) of the consequences that matters,[58] but rather the extent of the ensuing effects.[59] Roscini suggested that in order for a cyberattack to amount to an armed attack, it has to be a use of force first, such an operation that causes or is reasonably likely to cause extrinsic physical damage to persons or

[54] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (UK: Cambridge University Press, 2017), 342.

[55] Supervisory Control and Data Acquisition (SCADA) systems that are used to monitor and control features in the industrial sector and energy transit infrastructure. The security of the SCADA system consists of four major elements: real-time monitoring, detection of anomalies, impact analysis and mitigation strategies.
Limba T.; Plėta T.; Agafonov K.; Damkus M.,. "Cyber security management model for critical infrastructure", *Entrepreneurship and Sustainability Issues* 4(4), (2017): 561, http://dx.doi.org/10.9770/jesi.2017.4.4(12)

[56] Enrico Benedetto Cossidente, " Legal Aspects of Cyber and Cyber-Related Issues Affecting NATO ", *NATO Legal Gazette* 61, 35 (2014): 32, http://www.act.nato.int/images/stories/media/doclibrary/legal_gazette_35.pdf

[57] Case concerning oil platforms (Islamic republic of Iran v. United States of America), 12 December 1996, para. 72, http://www.icj-cij.org/files/case-related/90/090-19961212-JUD-01-00-EN.pdf

[58] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (UK: Cambridge University Press, 2017), 342.

[59] Advisory Council on International Affairs, Cyber Warfare, No. 77, AIV / No 22, CAVV, at 21 (December 2011) (stating the implied approval by the Netherlands of the position that: 'if there are no actual or potential fatalities, casualties or physical damage', a cyber operation targeting 'essential functions of the state could conceivably be qualified as an "armed attack" . . . if it could or did lead to serious disruption of the functioning of the state or serious and long-lasting consequences for the stability of the state.'), https://aiv-advies.nl/download/da5c7827-87f5-451a-a7fe-0aacb8d302c3.pdf

property or severe disruption of critical infrastructures, in spite of a contrary opinion.[60] Dinstein has suggested some examples of cyberattacks serious enough to amount to "Armed Attacks" without extrinsic physical damage to persons or property.[61] (it will be discussed in further detail in subchapter 1.2.4). As argued Shmitt, the law's qualitative focus on the type of harm may yield somewhat to a quantitative analysis such that a cyberattack causing serious consequences, such as severe economic effects or significant disruption of societal functions, may be characterized as armed attack even if it does not cause death, injury, damage or destruction. Time will tell.[62]

NATO member countries such as the United States and the Netherlands indicate what the criteria could be for a cyberattack without physical consequences to constitute an "armed attack".[63] (it will be revealed in subchapter 1.2.4).

Thus, it is obvious that cyberattacks as "Armed Attack" can be with consequences such as physical damage, destruction, injury or death and without consequences, if it significantly affects the performance of State functions in various sectors of security, defense, economy and society.

1.3 Intentions and motives

While analyzing the main elements of an "Armed Attack" as cyberattack, it is important to pay attention to meaning of intentions and motives.

There are two types of degree of guilt of "Armed Attack" as cyberattack, such as intentional and accidental (negligence).

1.3.1 Intentional "Armed Attack" as cyberattack

In international law, there is a clear example of jurisprudence of ICJ regarding the existence of such an element as intentions of "Armed Attacks". In the case concerning oil platforms (Islamic republic of Iran v. United States of America), court emphasized that it had not been established that the mine which struck *the Bridgeton* had been laid with the specific intention of harming that ship or other US vessels. That is, it had not been established that the

---

[60] Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 71.

[61] "Cited from: Dinstein, 'Computer Network Attacks', p 105", Ibid p. 73.

[62] Michael N. Schmitt, "Attack" as a Term of Art in International Law: The Cyber Operations Context," (2012) *4th International Conference on Cyber Conflict*, Tallinn, (2012): 288-289, https://www.ccdcoe.org/publications/2012proceedings/5_2_Schmitt_AttackAsATermOfArt.pdf

[63] Florentine J.M. de Boer, " Examining the Threshold of "Armed Attack" in light of Collective Self-Defence against Cyber Attacks: NATO's Enhanced Cyber Defence Policy", *NATO Legal Gazette* 61, 35 (2014): 33, http://www.act.nato.int/images/stories/media/doclibrary/legal_gazette_35.pdf

incidents were aimed at the USA (as opposed to Iraq). The Court apparently decided that harm by a mine or a missile constitutes "*an armed attack on a third state during a conflict between two other states only if the attack was specifically aimed at that third state".*[64] This is a brief and rather obscure discussion of a difficult issue; the Court does not go into any greater detail as to the element of intent apparently required by the notion of armed attack in this particular context or as to the general significance (if any) of its approach.[65]

However, the US State Department Legal Adviser was very critical of the Court's judgment on this point.[66] He claimed that the need to prove a specific intent would undermine international peace and security; a requirement of specific intent would encourage intentionally indiscriminate attacks, since no victim would have the right to defend against them. And it is not clear whether the Court was trying to establish a general requirement for all armed attacks or whether its brief statements on the intent requirement should be limited to the particular and unusual facts of the case where there was US involvement in a conflict between two other states.[67]

Group of Experts was divided over the issue of whether the effects in question must have been intended. For instance, consider the example of cyber espionage by one State against another that unexpectedly results in significant damage to the latter's cyber infrastructure. Some of the Experts were unwilling to characterize the operation as an armed attack because the consequences are unintended, although they acknowledged that measures could be taken to counteract the negative effects of the operation (e.g., the plea of necessity). [68]

The majority of Group of Experts was of the view that *intention is irrelevant* in qualifying an operation as an armed attack and that only the scale and effects matter. However, any response thereto would have to comport with the necessity and proportionality criteria (it will be discussed in further detail in chapter 2); the former would prove a significant hurdle in this respect. All the Experts agreed that: "*the lawfulness of the response would be determined by the*

[64] Christine Gray, *International Law and the Use of Force, Third Edition* (UK: Oxford University Press, 2008), 145-146.

[65] Ibid.

[66] "Cited from: Taft, 'Self-Defense and the Oil Platforms Decision', 29 Yale Journal of International law (2004) 295", Ibid.

[67] "Cited from: ICJ Reports (2003) 161 para 62–4", Ibid.

[68] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (UK: Cambridge University Press, 2017), 343.

reasonableness of the State's assessment as to whether an armed attack was underway against it".[69]

For example, a cyber armed attack by one State (A) against another (B) may have bleed-over effects in a third State (C). The majority of Group of Experts supported the view that if those effects meet the scale and effects criteria for an armed attack, State C is also entitled to resort to the use of force in self-defense, so long as the defensive action complies with the necessity and proportionality criteria. Furthermore, for them, even if the cyber operations against State B had not qualified as an armed attack, this would not preclude the bleed-over effects from amounting to an armed attack against State C. The remaining Experts would not characterize the operation as an armed attack absent an intent to create such effects.[70]

The author of the thesis can not agree with the opinion of Group of Experts, because the fundamental factor of intentions during an "Armed Attack" was determined by the practice of the ICJ in Oil Platforms Case. In each case, NATO will need to determine the degree of intent of the armed attack as a cyberattack on the Alliance. This will be unacceptable if the right to collective self-defense will be used against another State which did not intend to cause damage to allies.

1.3.2 Accidental (negligence) "Armed Attack" as cyberattack

When the damage caused to a certain state or its nationals is however not intended (a situation that is particularly likely in the cyber context),[71] it is doubtful that self-defense can be invoked by the accidental victim, for two reasons. First, as an armed attack is nothing else than a form of aggression, it requires *animus aggressionis*. Indeed, according to the ICJ, an armed attack must be carried out "with the specific intention of harming".[72]

[69] Ibid. p. 344.

[70] Ibid.

[71] "Cited from: As Schmitt notes, 'the attacker, because of automatic routing mechanisms, may not be able to control, or even accurately predict, the cyber pathway to the target', which increases the risk of unintended consequences (Schmitt, 'Computer Network Attack: The Normative Software', p 56")", Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 76.

[72] "Cited from: Case concerning oil platforms (Islamic republic of Iran v. United States of America), 12 December 1996, http://www.icj-cij.org/files/case-related/90/090-19961212-JUD-01-00-EN.pdf", Ibid, 77.

Secondly, if the armed attack by state A against state B also produces unintended harmful consequences on property, persons or systems in state C, a reaction in self-defense by state C would not be necessary, as state A will probably stop the attack on C.[73]

The problem is more complicated if state A attacks B posing as state C by spoofing or manipulating transmission data to appear as if they originated from state C. In this case, state C appears to attack state B, which might take actions in self-defense against an unaware state C. But even in this case, the reaction in self-defense may not be necessary if the misunderstanding is cleared up.[74]

Thus, it should be noted that, the fact that a cyber operation has been launched from, or has been routed through, the governmental cyber infrastructure of a state is not per se sufficient evidence that the state is responsible for the operation.[75] The author of the thesis believe that in every case it is necessary to carefully use all possible instruments (technical, expert, diplomatic, legal) to determine the degree of intent to carry out an armed attack as a cyberattack against the Alliance. The main goal is to avoid violating the sovereign rights of other States that are not involved in cyberattacks.

1.3.3 Motives of "Armed Attack" as cyberattack

In fact, motives of "Armed Attack" as cyberattack could be different. It is necessary to emphasize the main motives of such an "Armed Attack" as cyberattack is to weaken the fulfillment of the State of its main functions in various spheres of activity such as economy, energy, transport, financial sector, life support of the population and others (critical infrastructure - CI), destabilize the situation, affect the functionality of the armed forces and state authorities, as well as create "favorable conditions" for conducting other cyberattacks and even kinetic attacks on states.

While some Group of Experts took the position that attacks solely motivated by purely private interests would not trigger the right of self-defense, others were of the view that motives are irrelevant. This issue is likely to be resolved through State practice.[76]

[73] "Cited from: Schmitt, 'Cyber Operations in International Law', 165", Ibid.

[74] Ibid.

[75] Ibid.

[76] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (UK: Cambridge University Press, 2017), 346.

The author of the thesis believes that NATO will be considering the nature of the "Armed Attack" as cyberattacks where the motives will not have the decisive significance for the application of Article 5 of the NATO treaty. However, such motives can be evaluated by the ICJ, for example, during the review of cases concerning the application of Article 5 of the NATO Treaty and Article 51 of the UN Charter afterwards.

1.4 Objects of cyberattacks

The object of a cyber operation is meeting the trans-border and scale and effects requirements may also determine whether it qualifies as an armed attack. If it consists of property or persons within the affected State's territory, whether governmental or private, the action is an armed attack against that State. It must be noted that Group of Experts did not achieve consensus on whether further criteria must be satisfied in order to bring into operation the right of self-defense.[77]

1.4.1 Objects of cyberattacks situated outside the State's territory

It is sometimes unclear in international law whether a cyber operation can qualify as an armed attack if the object of the operation consists of property or citizens situated outside the State's territory. Attacks against non-commercial government facilities or equipment and government personnel certainly qualify as armed attacks so long as the above-mentioned criteria are met. For instance, Group of Experts agreed that: "a cyber operation undertaken by one State to kill another's head of State while abroad would amount to an armed attack. The determination of whether other operations are armed attacks depends on, but is not limited to, such factors as: the extent of damage caused by the operation; whether the property involved is governmental or private in character; the status of the individuals who have been targeted; and whether the operations were politically motivated, that is, conducted against the property or individuals because of their nationality. No bright-line rule exists in such cases. Consider a cyber operation conducted by one State to kill the CEO of another State's State-owned corporation abroad".[78] Opinions among the members of Group of Experts were divided as to whether the operation amounts to an armed attack.[79]

[77] Ibid.

[78] Ibid.

[79] Ibid.

1.4.2 Military and civilian, government and private objects of cyberattacks

In a traditional armed attack, the fact that the target is military or civilian would not make any difference: the state where the target is located would be entitled to self-defense because its territorial integrity has been violated.[80] Hence, Dinstein correctly points out that, if a conventional armed attack against a civilian facility on the territory of the target state would amount to an armed attack even if no member of the armed forces is injured or military property damaged, there is no reason to come to a different conclusion with regard to cyberattacks against civilian systems: *"even if the cyberattack impinges upon a civilian computer system which has no nexus to the military establishment (like a private hospital installation), a devastating impact would vouchsafe the classification of the act as an armed attack"*.[81]

Most critical infrastructure (CI) are not owned by the government, but by the private sector: the governmental or private character of the infrastructure targeted, however, is also not relevant to the determination of the existence of an armed attack against the state, and neither is the fact that the computer system is run by a company possessing the nationality of a third state or that the computer system operated by the victim state is located outside its borders (for instance, in a military base abroad).[82]

Taking into account the experience of previous cyberattacks on state CI facilities, as well as the results of Tabletop Exercise Coherent Resilience (CORE) 2017 in Ukraine[83], the author of the thesis suggests the following structure of the objects of cyberattacks in the light of Article 5 of the NATO treaty. (Table 1)

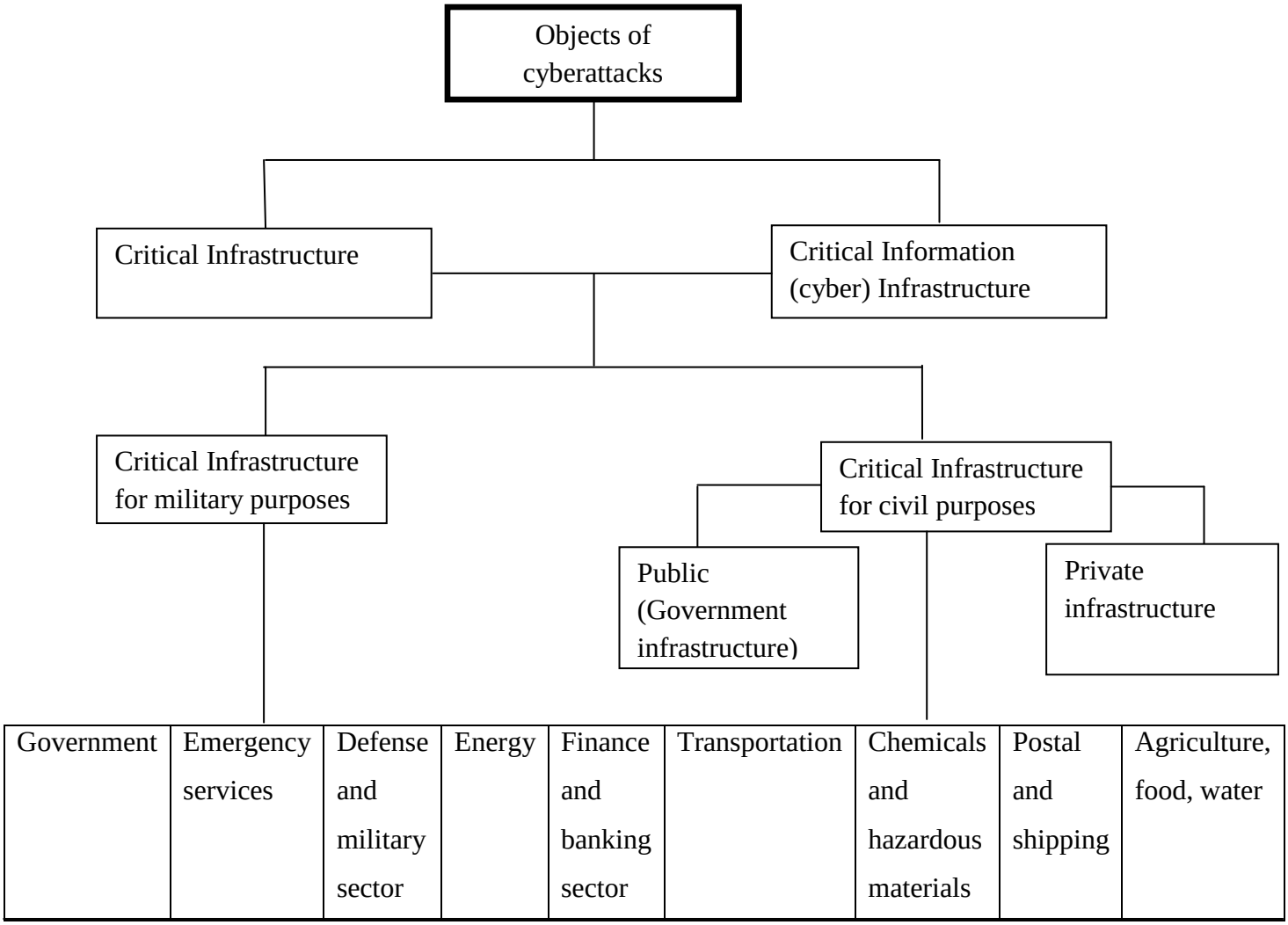
[80] Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 76.

[81] "Cited from: Dinstein, 'Computer Network Attacks', p 106.", Ibid.

[82] Cited from: Dinstein, 'Computer Network Attacks', p 106-7.", Ibid.

[83] Final Evaluation Report, Advanced Training Course on Critical Energy Infrastructure Security with Tabletop Exercise Coherent Resilience (CORE) 2017, NPS EAG, Kyiv, Ukraine.

Table №1: Objects of cyberattacks as "Armed Attack" in light Article 5 of NATO Treaty



From this table it can be concluded that cyberattacks as Armed Attacks can be carried out on CI, and on Critical Information Infrastructure (CII). Such objects can function for both military and civilian purposes. CI for civil purposes can be both in state and private ownership. The types of activities of such objects are important for the exercise of state functions.

1.4.3 Critical Infrastructure and Critical Information Infrastructure

The cyberattacks can be directed at both CI and CII. In modern international law there is no definition of these two concepts. However, NATO countries and partner countries refer to the Critical Infrastructures Protection Act of United States of 2001. This is defined CI as "*system and assets, whether physical or virtual, so vital to the country that the incapacity or destruction*

of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters".[84]

In my opinion, although governments administer only a minority of the Nation`s CI computer systems, *governments at all levels perform essential services that rely on each of the CI sectors. Such sectors related to agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping.*[85]

In turn, when it comes to cyberattacks, in most cases it is conducted on a CII, which is directly connected and is the source of automatic control of critical infrastructure. To date, the most successful such definition is in the strategy for cybersecurity of Lithuania as a NATO member[86], and a partner of NATO, Finland[87].

According to approval of the program for the development of electronic information security (cyber-security) of Lithuania for 2011-2019, *"CII shall mean an electronic communications network, information system or a group of information systems (included all hardware and software that process, store, and communicate information, or any combination of all of these elements, computer systems; control systems (e.g. SCADA); networks, such as the Internet; and cyber services (e.g., managed security services) are part of cyber infrastructure) where an incident that occurs causes or may cause grave damage to national security, national economy or social well-being".* [88] In Finland's Cyber Security Strategy from 2010, *"CII refers to the structures and functions behind the information systems of the vital functions of society which electronically transmit, transfer, receive, store or otherwise process information (data)".*[89]

---

[84] NATO Cooperative Cyber Defence Centre of Excellence, Tallinn , Estonia, accessed 2018 May 3, https://ccdcoe.org/cyber-definitions.html

[85] Ibid.

[86] "National cyber security strategy of Lithuania, Programme for the Development of Electronic Information Security for 2011–2019 (2011)", accessed 2018 May 3, https://ccdcoe.org/cyber-security-strategy-documents.html

[87] "National cyber security strategy Finland's Cyber Security Strategy (2013)", accessed 2018 May 3, https://ccdcoe.org/cyber-security-strategy-documents.html

[88] NATO Cooperative Cyber Defence Centre of Excellence, Tallinn , Estonia, accessed 2018 May 3, https://ccdcoe.org/cyber-definitions.html

[89] Ibid.

For a clear understanding of the enemy's real target as CI, the author suggests several examples of cyberattacks on CI, like some situations during crisis (military) stage, which were used during Tabletop Exercise Coherent Resilience (CORE) 2017 in Ukraine: 1) As a result of cyberattacks, three regions have had their power interrupted. A 750 kV high-voltage substation is disconnected from the United Energy System (UES) of Kray; 2) As a result of a cyberattack on the SCADA system of telemechanical control, the system lost the opportunity to receive information.[90]

These examples show that CI is the target of the attacker. Situations were used from real practice. A feature of these examples is that such an infrastructure works in disconnected access to the Internet network. However, working personnel periodically violated the rules of automated control and connected the system SCADA to the Internet.

Thus, the author in this subchapter analyzed the main objects of cyberattacks as an "Armed Attack" in the light of Article 5 of the NATO Treaty. From this it can be understood that there are serious threats to cyberattacks against such objects.

1.5 Subjects of cyberattacks

The main problem in the process of identifying and determining the sources of cyberattack is the subjects of cyberattacks. In general, the process of investigation and determination of the attacker, even in the case of a kinetic attack, takes quite a long time, not to mention cyberattacks. Modern technologies, strategic concepts of non-partners states of NATO use different means (for example hybrid warfare) to avoid responsibility for committing attacks on other states. However, international law has the established legal practice of qualifying the subjects of committing "Armed Attacks" to other states.

1.5.1 State and non-State actors on behalf of a State or under overall control

It is generally accepted that an armed attack can be carried out directly by a state's armed forces or indirectly by armed groups operating under the authority or control of a state. [91]

It is incontrovertible that a cyber operation by organs of a State may so qualify. It is equally indisputable that the actions of non-State actors may sometimes be attributed to a State

[90] Final Evaluation Report, Advanced Training Course on Critical Energy Infrastructure Security with Tabletop Exercise Coherent Resilience (CORE) 2017, NPS EAG, Kyiv, Ukraine.

[91] Cyber Warfare, No 77, AIV / No 22, CAVV December (2011): 20, https://aiv-advies.nl/download/da5c7827-87f5-451a-a7fe-0aacb8d302c3.pdf

for the purpose of finding an armed attack.[92] In the Nicaragua judgment, ICJ stated that: *"an armed attack must be understood as including not merely action by regular forces across an international border, but also 'the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to' (inter alia) an actual armed attack conducted by regular forces, 'or its substantial involvement therein".*[93]

For instance, if a group of private individuals undertakes cyber operations on behalf of one State directed against another State, and those actions reach the requisite scale and effects level, the first State will have committed an armed attack. This same conclusion would apply to cyber operations conducted by a single individual operating on behalf of a State.[94]

There is less agreement on the degree of control a state must exercise over an indirect armed attack. The ICJ's standard is 'effective control', but the International Criminal Tribunal for the former Yugoslavia (ICTY), in its judgment in the Tadic case[95], settled on the slightly broader standard of 'overall control', albeit in the slightly different context of criminal law. Both forms of armed attack are carried out by or under the control of a state.[96]

1.5.2 Non-State actors without involvement by a State

The issue of whether acts of non-State actors can constitute an armed attack absent involvement by a State is controversial. Traditionally, Article 51 of the UN Charter and the customary international law of self-defense were characterised as applicable solely to armed attacks undertaken by one State against another. Violent acts by non-State actors fell within the law enforcement paradigm.

---

[92] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (UK: Cambridge University Press, 2017), 344.

[93] Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America), 27 June 1986, para. 195, http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

[94] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (UK: Cambridge University Press, 2017), 344.

[95] Tadic Case, International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia since 1991, http://www.icty.org/x/cases/tadic/acjug/en/tad-aj990715e.pdf

[96] Cyber Warfare, No 77, AIV / No 22, CAVV December (2011): 22, https://aiv-advies.nl/download/da5c7827-87f5-451a-a7fe-0aacb8d302c3.pdf

However, the international community characterised the 9/11 attacks by Al Qaeda on the United States as an armed attack triggering the inherent right of self-defense.[97]

Article 51 of UN Charter contains no such limitation vis-à-vis armed attacks (although the text does make it clear that only States enjoy the right of self-defense). For its part, the ICJ does not seem to have been prepared to adopt this approach, although it appears that there is a lack of unanimity on the Court in this regard.[98]

A majority of Group of Experts concluded that State practice has established a right of self-defense in the face of cyber operations at the armed attack level by non-State actors acting without the involvement of a State, such as terrorist or rebel groups.[99]

The ICJ has not yet adopted a clear position on this matter. In practice, states and the UN Security Council have recognised since 11 September that an organised group can in principle be the author of an armed attack and that a response to such an attack can be qualified as self-defense. It seems reasonable to assume that the attack should be comparable to one carried out either directly by a state or by an armed group under the control or substantial influence of a state. If this third possibility is accepted, it must be asked against whom or what self-defense should be directed and whether it can take place in the territory of a state not directly involved in the attack.[100]

As noted the Estonian Foreign Intelligence Service's third public report from 2018, Russia has become one of the world's leading players in the field of cyber operations. In addition to Russian, one needs to continue to be attentive to North-Korean and Chinese. Moreover,

[97] "Cited from: The Security Council adopted numerous resolutions recognising the applicability of the right of self-defense. See, e.g., SC Res 1368, UN Doc. S/RES/1368 (12 September 2001); SC Res. 1373, UN Doc. S/RES/1373 (28 September 2001). International organizations such as NATO and many individual States took the same approach. See, e.g., Press Release, NATO, Statement by the North Atlantic Council (12 September 2001); Terrorist Threat to the Americas, Res. 1, Twenty-Fourth Meeting of Consultation of Ministers of Foreign Affairs, Terrorist Threat to the Americas, OAS Doc. RC.24/RES.1/01 (21 September 2001); Brendan Pearson, PM Commits to Mutual Defence, Austl. Fin. Rev., 15 September 2001, at 9.", Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (UK: Cambridge University Press, 2017), 344.

[98] Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory Advisory Opinion of 9 July 2004, http://www.icj-cij.org/files/case-related/131/131-20040709-ADV-01-00-EN.pdf

[99] Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (UK: Cambridge University Press, 2017), 345.

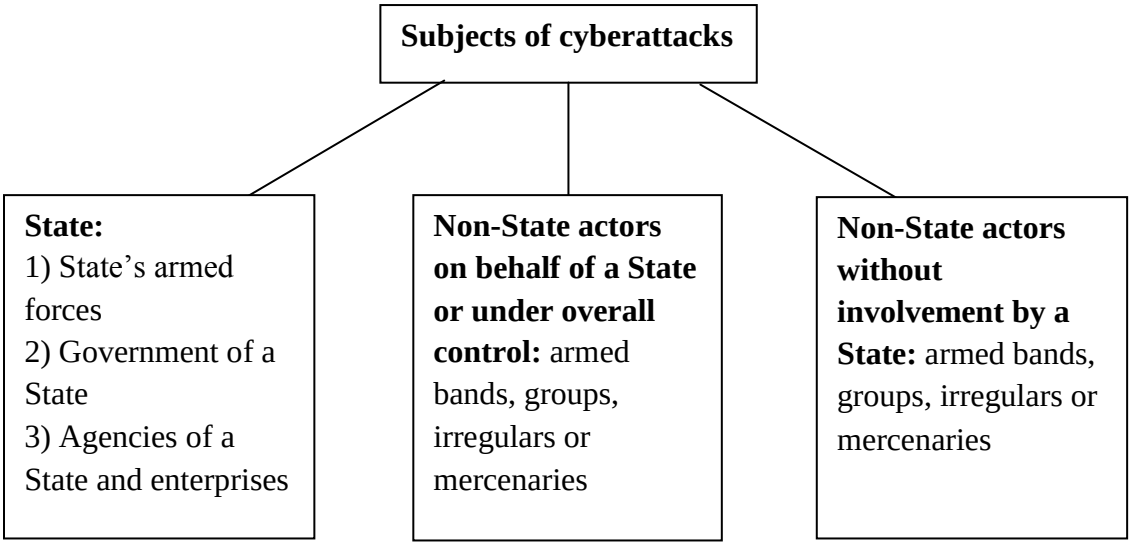
[100] Cyber Warfare, No 77, AIV / No 22, CAVV December (2011): 21, https://aiv-advies.nl/download/da5c7827-87f5-451a-a7fe-0aacb8d302c3.pdf

Russian's policy is implemented by *hackers, internet trolls and cyber criminals* who at first seem to have *no link to any state structures* but who are central to Russian information warfare.[101]

Russian cyber groups – examples include APT28 (Sofacy/Fancy Bear) associated with the military intelligence of Russia (GRU), SNAKE (Turla) tied to the federal security service (FSB), and APT29 (Cozy Bear/The Dukes) associated with the FSB and the foreign intelligence service (SVR) – play the key role in Russia's influence operations toolbox. These are long-term Russian cyber operations with a clear direction based on Russia's interests and objectives. Good examples of the use of these sorts of attacks for political purposes include the GRU cyber operations against the World Anti-Doping Agency (WADA) in September 2016 and against the International Olympic Committee (IOC) in January 2018.[102]

After analyzing all possible subjects of cyberattacks, the author suggests the following table for a clear understanding of such classification. (Table 2)

Table №2: Subjects of cyberattacks as "Armed Attack" in light Article 5 of NATO Treaty



In this chapter, the author of the thesis tried to research the nature of the "Armed Attack" as a cyberattack in the light of Article 5 of the NATO Treaty. Analyzing the structure, it becomes clear that the complexity of the application of this Article in the case of cyberattacks lies in the case of consequences, intentions and determination of the attribution of the subject of such cyberattacks to the State, as to the subject of international law.

[101] International Security and Estonia 2018, Estonian Foreign Intelligence Service's third public report, Estonia, (2018): 54-55, https://www.valisluureamet.ee/pdf/raport-2018-ENG-web.pdf

[102] Ibid.

2. THE SCALE AND EFFECTS OF "ARMED ATTACK" AS CYBERATTACK IN LIGHT ARTICLE 5 OF THE NATO TREATY AND ANTICIPATORY SELF-DEFENSE

As it was already determined that not every use of force rises to the level of an armed attack and the scale and effects required for an act to be characterized as an armed attack necessarily exceed those qualifying the act as a use of force. In Nicaragua case, the court did not determine what scales and effects are, and what the consequences for the qualification of an armed attack should be. Especially, when it comes to cyberattacks, many difficulties arise. The author proposes to research nature scale and effects and determine how it should be qualified in practice.

Also, in practice, many questions arise about anticipatory self-defense. In this case, there should be no doubt about the definition of this concept. Since this should not contradict Article 5 of the NATO Treaty.

2.1 Scale

This majority rule mandates that, when a State is to evaluate whether or not another State's act was an armed attack, it is customary to take into account not only the effects of an action but also the scale of the action.[103]

The scale and effects required for an act to be characterised as an armed attack necessarily exceed those qualifying the act as a use of force. The phrase "scale and effects" is drawn from the Nicaragua judgment. In that case, the Court identified scale and effects as the criteria that distinguish actions qualifying as an armed attack from those that do not. It noted the need to 'distinguish the most grave forms of the use of force (those constituting an armed attack)'.[104] As an example of use of force that would not be of the 'scale and effects' to warrant being termed an armed attack the Court mentioned 'a mere frontier' incident.[105] Therefore, the parameters of the scale and effects criteria remain unsettled beyond the indication that they need to be grave.

[103] Priyanka R. Dev, "Use of Force" and "Armed Attack" Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response", *Texas International law Journal,* 50, 2, (2015): 394.

[104] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (UK: Cambridge University Press, 2017), 341.

[105] "Cited from: *Ibid.*, at para. 194. The approach of the ICJ in the *Nicaragua* and *Oil Platforms* cases is discussed and criticized by Moir, *supra* note 14, at 117–140.", David Kretzmer, "The Inherent Right to Self-Defence and Proportionality in *Jus Ad Bellum*," *European Journal of International Law* 24, 1 (2013): 235-282, https://academic.oup.com/ejil/article/24/1/235/438278

This means that "scale and effects" is a pedagogic term that captures the qualitative and quantitative factors to be analyzed when to determine whether a cyber operation qualifies as a use of force.[106]

The demand for the force used to meet a threshold of 'scale and effects', or gravity of harm in order for it to be regarded as an armed attack for the purposes of Article 51 has not been universally accepted.[107]

It is true that the Court, with its consistent statements, have put forward the gravity element as an important factor in determining an armed attack.[108] Thus an armed attack under Article 51 of UN Charter requires *"*a *relatively large scale*, […] *a sufficient gravity*, and […] *a substantial effect"*.[109]

According to rule 11 in the Tallinn Manual, a cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force.[110]

In its turn, Constantinou argued that *an armed attack* is "an act or the beginning of a series of acts of armed force considerable *magnitude and intensity (scale)* which have as their consequences (effects)".[111]

Note that it is both *the scale* and the effects of the use of force that determine the occurrence of an armed attack: a massive DDoS attack (like the one that occurred in Estonia) involving millions of botnets that only disrupts a NCI for a limited amount of time is certainly significant with regard to its scale, but its effects are not.[112]

---

[106] "When do cyber operations amount to use of force and armed attack, and what response will they justify?", accessed 2018 May 3, https://www.duo.uio.no/bitstream/handle/10852/50840/723.pdf?sequence=1

[107] David Kretzmer, "The Inherent Right to Self-Defence and Proportionality in *Jus Ad Bellum*," *European Journal of International Law* 24, 1 (2013): 235-282, https://academic.oup.com/ejil/article/24/1/235/438278

[108] James Green, *The International Court of Justice and Self-Defence in International* Law (Hart Publishing, Oxford 2009), 31.

[109] ÖyküIrmakkesen, The Notion of Armed Attack under the UN Charter and the Notion of International Armed Conflict – Interrelated or Distinct?, Geneva Academy, 2014, http://www.prix-henry-dunant.org/wp-content/uploads/2014_IRMAKKESEN_Paper.pdf

[110] "Cited from: The Tallinn manual, p. 48. ", "When do cyber operations amount to use of force and armed attack, and what response will they justify?", https://www.duo.uio.no/bitstream/handle/10852/50840/723.pdf?sequence=1

[111] Avra Constantinou, *the Right of Self-Defence under Customary International Law and Article 51 of the UN Charter* (Athens and Bruxelles: Ant N Sakkoulas/Bruylant, 2000), pp 63–4.

[112] "Cite from: Duncan Blake and Joseph S Imburgia, "Bloodless Weapons"? The Need to Conduct Legal Reviews of Certain Capabilities and the Implications of Defining Them as "Weapons" ', Air Force Law

The authors of the Chatham House Principles of International Law on Use of Force in Self-Defense take the view that *"[a]n armed attack means any use of armed force, and does not need to cross some threshold of intensity"*.[113] This has also been the view taken by the US.

The scale of "Armed Attack" can be divided into three categories: 1) small-scale of armed attack, when an attack occurs small, but multiple (for example Oil Platform Case); 2) scale of armed attack which can be used by any states without small-scale and large-scale features, 3) large-scale of armed attacks which can be used non-state actors (for example 9/11 case).

It should be noted, that in Nicaragua case, court was talking about "scale and effects" within meaning the sending by a State of armed bands to the territory of another State, if such an operation, because of its *scale and effects*, would have been classified as an armed attack.[114] However, the court did not say anything about kinetic or non-kinetic attacks on other countries, and the application of such a concept in this case. Nicaragua case was determined peculiarities of the application of the right to self-defense in the case of armed bands and groups under the control of other states.

The most significant obstacle in the endeavour is the interpretation of Art. 51 UN Charter presently preferred by the majority of the judges of the ICJ. Hence it is not surprising that some judges challenged the majority view and appended declarations or separate opinions to the Israeli Wall Advisory Opinion[115] (Judges Buergenthal, Higgins, and Kooijmans) and the judgment in the Congo v Uganda case[116] (Judges Kooijmans and Simma).[117]

Judge Simma remarked on that occasion: *"Such a restrictive reading of Article 51 might well have reflected the state, or rather the prevailing interpretation, of the international law on self-defense for a long time. However, in the light of more recent developments not only in State*

Review 66 (2010), p 186", Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 76.

[113] "Cited from: *Chatham House Principles of International Law on Use of Force in Self-Defence,* available at: www.chathamhouse.org.uk/publications/papers/view/-/id/308 (last accessed 3 Feb. 2011), David Kretzmer, "The Inherent Right to Self-Defence and Proportionality in *Jus Ad Bellum*," *European Journal of International Law* 24, 1 (2013): 235-282, https://academic.oup.com/ejil/article/24/1/235/438278

[114] Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America), 27 June 1986, para. 195, http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

[115] Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory Advisory Opinion of 9 July 2004, http://www.icj-cij.org/files/case-related/131/131-20040709-ADV-01-00-EN.pdf

[116] Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda) judgment of 19 December 2005, http://www.icj-cij.org/files/case-related/116/116-20051219-JUD-01-00-EN.pdf

[117] Karl Zemanek, Armed Attack, Oxford Public International Law, (2013), accessed 2018 May 3, http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e241

practice but also with regard to accompanying opiniojuris, it ought urgently to be reconsidered, also by the Court" (Congo v Uganda [Separate Opinion Judge Simma], para. 11).[118]

As a rule, the destructive objective of a cyberattack and scales does often not centre on the direct damage or disruption on the computer or the computer itself, but on the indirect *effects* from the cyberattack.

The definition of *effects* is one of the important parts of the qualification of an "Armed Attack" as cyberattacks against other states.

2.2 Effects

Effects of "Armed Attack" as cyberattack is consequences of the infliction of substantial destruction upon important elements of the target State namely, upon its people, economic and security infrastructure, destruction of aspects of its governmental authority, its political independence, as well as damage to or deprivation of its physical element namely, its territory, and the *"use of force which is aimed at a State's main industrial and economic resources and which results in the substantial impairment of its economy"*.[119]

The effects will usually materialize on the systems or devices controlled by the targeted computer or on the human decision maker that depends on information that the targeted computer or computer system contains or processes. Reports on the Stuxnet attack often refers to the effects on the nuclear facilities, and not necessary the attack on the computer system controlling the centrifuges.[120]

According to Reese Nguyen, the thing that matters are not so much that the effects are indirect, but more importantly, these effects are removed from the actors that caused them. The predicted use of large scale cyberattacks, will not be directed against soldiers, but larger infrastructure facilities that, in serious situation, will have impact on more than soldiers, but also civilians.[121]

---

[118] Ibid.

[119] Avra Constantinou, the Right of Self-Defence under Customary International Law and Article 51 of the UN Charter (Athens and Bruxelles: Ant N Sakkoulas/Bruylant, 2000), pp 63–4.

[120] "When do cyber operations amount to use of force and armed attack, and what response will they justify?", accessed 2018 May, https://www.duo.uio.no/bitstream/handle/10852/50840/723.pdf?sequence=1

[121] "Cited from: Nguyen, (2013), p. 1099", Ibid., 3, https://www.duo.uio.no/bitstream/handle/10852/50840/723.pdf?sequence=1

Cyberattacks can produce multiple effects. *The primary effects* are those on the attacked computer, computer system or network, the deletion, corruption, or alteration of data or software, or system disruption through a DDoS attack or other cyberattacks. *The secondary effects* are those on the infrastructure operated by the attacked system or network (if any), its partial or total destruction or incapacitation. *Tertiary effects* are those on the persons affected by the destruction or incapacitation of the attacked system or infrastructure, for instance those that benefit from the electricity produced by a power plant incapacitated by a cyber operation. Physical damage to property, loss of life and injury to persons, then, are never the primary effects of a cyber operation: damage to physical property can only be a secondary effect, while death or injury of persons can be a tertiary effect of a cyber operation.[122]

By dividing the effects in such way, the unique features of how a cyberattack work out are highlighted.[123]

2.3 Scale and effects with physical damage, destruction, injury, death

In modern international law, there is a debate about the nature of the consequences in the case of cyberattacks, which can reach the level of armed attack.

There is a tendency of fear that only the presence of such consequences of cyberattacks as physical damage, destruction, injury, death will lead to the impossibility of applying the Article 5 of the NATO treaty. In addition, there is criticism of Group of Experts on this issue. Although, according to opinion of the author of the thesis, the position of the experts is well-balanced, due to the fact that to date there is no clear interpretation of Article 51 of the UN Charter and Article 5 of the Treaty of NATO related to cyberattacks.

Group of Experts agreed that any use of force that: *"injures or kills persons or damages or destroys property would satisfy the scale and effects requirement"*.[124] They also agreed that acts of cyber intelligence gathering and cyber theft, as well as cyber operations that involve brief or periodic interruption of non-essential cyber services, do not qualify as armed attacks. The Experts took the view that the law is unclear as to the precise point at which the extent of death,

[122] Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 52-53.

[123] "When do cyber operations amount to use of force and armed attack, and what response will they justify?", accessed 2018 May, https://www.duo.uio.no/bitstream/handle/10852/50840/723.pdf?sequence=1

[124] Michael N. Schmitt, *Tallinn Manual 1.0 on the International Law Applicable to Cyber Warfare* (UK: Cambridge University Press, 2013), 56.

injury, damage, destruction, or suffering caused by a cyber operation fails to qualify as an armed attack.[125]

In the opposite opinion, J.M. de Boer, putted differently position of experts, and was asked *"why not a cyberattack that targets CI and paralyses a State without causing physical damage, destruction injury or death?"*[126] Consequently, from his opinion this leaves room for adversaries to exploit these types of cyberattack and it diminishes the deterrent effect of Article 5 in light of cyberattacks.[127]

However, according to observation of author of thesis, such a position of J.M. de Boer is wrong. Group of Experts just said that the case of actions that *"do not result in injury, death, damage, or destruction, but which otherwise have extensive negative effects, is unsettled".*[128]

Some of the Experts took the position that harm to *persons or physical damage to property* is a condition precedent to the characterization of an incident as an armed attack. Others took the view that it is not the nature (injurious or destructive) of the consequences that matters, but rather the extent of the ensuing effects.[129]

Karl Zemanek pointed that: "the use of any device, or number of devices, which results in a considerable loss of life and/or extensive destruction of property must therefore be deemed to fulfill the conditions of an "armed" attack".[130]

The 2011 AIV/CAVV Report on Cyber Warfare, the jus ad bellum conclusions of which have been endorsed by the Dutch government, states that: *"a cyberattack against a computer or information system as an armed attack if the consequences are comparable to those of an attack with conventional or unconventional weapons. In other words, if a cyberattack leads to a significant number of fatalities or causes substantial physical damage or destruction to vital infrastructure, military platforms or installations or civil property, it could certainly be qualified*

[125] Ibid.

[126] Florentine J.M. de Boer, " Examining the Threshold of "Armed Attack" in light of Collective Self-Defence against Cyber Attacks: NATO's Enhanced Cyber Defence Policy", *NATO Legal Gazette* 61, 35 (2014): 31-32, http://www.act.nato.int/images/stories/media/doclibrary/legal_gazette_35.pdf

[127] Ibid.

[128] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (UK: Cambridge University Press, 2017), 342.

[129] Michael N. Schmitt, *Tallinn Manual 1.0 on the International Law Applicable to Cyber Warfare* (UK: Cambridge University Press, 2013), 56.

[130] "Cited from: Karl Zemanek, 'Armed attack', *Max Planck Encyclopedia of Public International Law* (2012), Vol I, p 599.", Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 71.

as an 'armed attack' within the meaning of article 51 of the UN Charter. A digital attack against information systems linked to vital infrastructure, military installations and platforms for weapons systems or vital services, such as the emergency services or air traffic control systems, could breach the threshold of an armed attack if it causes significant loss of life or physical destruction".[131]

Group of Experts illustrated on example which underlined unsettling this problem about a cyberattack directed against a major international stock exchange that causes the market to crash. Group of Experts was divided over the characterization of such an event. Some of the Experts were unprepared to label it as an armed attack because they were not satisfied that mere financial loss constitutes damage for the purpose of qualifying a cyber operation as an armed attack. Others emphasized the catastrophic effects such a crash would occasion and therefore regarded them as sufficient to characterize the cyberattack as an armed attack.[132]

Consider, for example, the case of a cyber operation targeting a water purification plant. Sickness and death caused by drinking contaminated water are foreseeable and should therefore be taken into account.[133]

Thus, there is no justified position that there is only one threshold for an armed attack as a cyberattack in the modern international law. Until the court determines the extent of the scales and effects for cyberattacks as armed attacks or until NATO develops a unified position on this matter, this question will not be solved in modern international law.

2.4 Scale and effects without such consequences

As it was already defined, the 2011 AIV/CAVV Report on Cyber Warfare, the jus ad bellum conclusions of which have been endorsed by the Dutch government, states that "*a serious, organized cyberattack* on essential functions of the state could conceivably be qualified as an 'armed attack' within the meaning of article 51 of the UN Charter if it *could or did lead to*

[131] Cyber Warfare, No 77, AIV / No 22, CAVV December (2011): 21, https://aiv-advies.nl/download/da5c7827-87f5-451a-a7fe-0aacb8d302c3.pdf

[132] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operation*, (UK: Cambridge University Press, 2017), 343.

[133] Michael N. Schmitt, *Tallinn Manual 1.0 on the International Law Applicable to Cyber Warfare* (UK: Cambridge University Press, 2013), 57.

serious disruption of the functioning of the state or serious and long-lasting consequences for the stability of the state".[134]

In such cases, there must be a disruption of the state and/or society, or a sustained attempt thereto, and not merely an impediment to or delay in the normal performance of tasks for it to be qualified as an armed attack. A disruption of banking transactions or the hindrance of government activity would not qualify as an armed attack. However, a cyberattack that targets the entire financial system or prevents the government from carrying out essential tasks, for example an attack on the entire military communication and command network that makes it impossible to deploy the armed forces, could well be equated with an armed attack.[135]

In a reply to the Report of the UN Secretary General on "Developments in the Field of Information and Telecommunications in the Context of International Security", the United States found that under some circumstances, a disruptive activity in cyberspace could constitute an armed attack. Additionally, an assessment of the U.S. Department of Defense (DoD) explains that, *"there may be a right to use force in self-defense against a single foreign electronic attack in circumstances where significant damage is being done to the attacked system or the data stored in it, when the system is critical to national security or to essential national infrastructures, or when the intruder's conduct or the context of the activity clearly manifests a malicious intent".*[136]

It appears that the developments in the United States and the Netherlands demonstrate support for a lower threshold of "armed attack" since highly disruptive cyberattacks are described as able to constitute an "armed attack".[137] However, the section in the Wales Summit Declaration implies that NATO's Enhanced Cyber Defense Policy adopts the existing threshold

[134] Cyber Warfare, No 77, AIV / No 22, CAVV December (2011): 21, https://aiv-advies.nl/download/da5c7827-87f5-451a-a7fe-0aacb8d302c3.pdf

[135] Ibid.

[136] United States Department of Defense Office of General Counsel, An Assessment of International Legal Issues in Information Operations (May 1999): 18, accessed 2018 May 3, http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf

[137] Florentine J.M. de Boer, " Examining the Threshold of "Armed Attack" in light of Collective Self-Defence against Cyber Attacks: NATO's Enhanced Cyber Defence Policy", *NATO Legal Gazette* 61, 35 (2014): 34, http://www.act.nato.int/images/stories/media/doclibrary/legal_gazette_35.pdf

of "armed attack" from international law as it says that the impact of cyberattacks "could be as harmful to modern societies as a conventional attack".[138]

Dinstein has suggested some examples of cyberattacks serious enough to amount to armed attacks: "fatalities caused by the loss of computer-controlled life-support systems; an extensive power grid outage (electricity blackout) creating considerable deleterious repercussions; a shutdown of computers controlling waterworks and dams, generating thereby floods of inhabited areas; deadly crashes deliberately engineered (e.g., through misinformation fed into aircraft computers)' and 'the wanton instigation of a core-meltdown of a reactor in a nuclear power plant, leading to the release of radioactive materials that can result in countless casualties if the neighbouring areas are densely populated".[139]

Constantinou's definition of the scale and effects standard also includes the effects on the industrial and economic resources of the target state. Indeed, as already noted, it is not only cyber operations causing physical damage that potentially amount to a use of force, but also those that severely incapacitate critical infrastructures so to affect state security: "it is not their physical destruction as such but their unavailability in the sense of not being able to fulfil the purpose for which they have been set that makes an attack on them an armed attack".[140]

As a consequence, a large-scale cyberattack that shuts down CIs such as the financial market for a prolonged time and cripples a state's economy or causes the collapse of the national currency would, if the effects are serious enough, potentially amount to an "armed attack" for the purposes of self-defense.[141]

The White Paper on German Security Policy also seems to suggest, if indirectly, that "military attacks from or on cyberspace" against 'Germany's political and economic structures as well as its critical infrastructure' can be countered "using military means".[142]

---

[138] "Cited from: Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, North Atlantic Council, para 72, 5 September 2014, https://www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=en", Ibid.

[139] "Cited from: Dinstein, 'Computer Network Attacks', p 105.", Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 73.

[140] "Cited from: Tsagourias, 'Cyber Attacks', p 231.", Ibid, 74.

[141] Ibid.

[142] "Cited from: German Federal Ministry of Defence, *White Paper 2006 on German Security Policy and the Future of the Bundeswehr*, 2006, p 17, <http://www.isn.ethz.ch/Digital-Library/Articles/Special-Feature/Detail/?lng=en&id=156941", Ibid, 75.

However, concluding that cyberattacks that severely disrupt the functioning of CI can potentially be an "armed attack" does not automatically entitle the victim state to use force in self-defense in all cases, as such use must still be necessary and proportionate to the purpose of repelling the attack.

Thus, the author of the thesis agrees that the effects of cyberattacks are of a diverse nature. The presence of serious damage, destruction or death is not mandatory, it is enough to disrupt the functioning of the CI of the state for a sufficiently long period, which may entail further serious consequences. Also, the author found a difference in views on such approaches of NATO member states. A single approach within NATO is necessary, its form can be different.

2.5 Anticipatory self-defense against an imminent armed attack by cyber means

2.5.1 General overview

Article 51 of UN Charter states that an armed attack must 'occur' in order to trigger the right of self-defense by the victim.[143]

Clearly, this covers incidents in which the effects of the armed attack have already materialised, that is, when the cyber armed attack has caused, or is in the process of causing, damage or injury. It also encompasses situations in which a cyber operation is the first step in the launch of a kinetic armed attack.[144]

In the case concerning *Armed activities in the territory of the Congo* the Court expressed no view on this issue, as Uganda eventually claimed that its actions were in response to armed attacks that had already occurred.[145] The Court, however, was aware that the security needs that Uganda aimed to protect were "essentially preventative" and held that 'Article 51 of the Charter may justify a use of force in self-defense only within the strict confines there laid down.

[143] Article 51, United Nations Charter, 26 June 1945, http://www.un.org/en/sections/un-charter/chapter-vii/index.html

[144] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (UK: Cambridge University Press, 2017), 350.

[145] "Cite from: *Armed Activities on the Territory of the Congo (DRC v Uganda)*, Judgment, 19 December 2005, ICJ Reports 2005 ('*DRC v Uganda*'), para 143", Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 77.

In 2004, a High-Level Panel on Threats, Challenges and Change (appointed by the United Nations Secretary-General) stated unequivocally: "We do not favour the rewriting or reinterpretation of Article 51".[146]

On the other hand, Judge Schwebel – in his Dissenting Opinion in the Nicaragua case – did express his position on the subject in no uncertain terms. In conformity with a scholarly school of thought maintaining that Article 51 only highlights one form of self-defense (viz. response to an armed attack), without negating other patterns of permissible action in self-defense vouchsafed by customary international law,[147] Judge Schwebel rejected a reading of the text which would imply that the right of self-defense under Article 51 exists "if, and only if, an armed attack occurs".[148]

2.5.2 Philosophical approaches

There are three philosophies have formed since 1945 in the existing scholarly debate over the coexistence of anticipatory self-defense and the Charter in 1945. It is helpful to provide a basic description of the essence of each philosophy before analysing their respective legal bases.[149]

The positivist philosophy believes that a literal interpretation application of the words "if an armed attack occurs" in Article 51 of the Charter impliedly extinguished anticipatory self-defense in international law in 1945. This is based on the assumption that the temporal effect of the word "occurs" is that self-defense must only be occasioned with or after the physical commencement of an armed attack. *The realist philosophy* says that the positivist philosophy cannot be accepted because it condemns a state to suffer the consequences of the physical commencement of an armed attack before being lawfully entitled to defend itself. Realists conclude that such an outcome is unprecedented, illogical and is suicidal given the powerful

[146] "Cited from: Report of High-Level Panel on Threats, Challenges and Change Addressed to the Secretary General (2004, UN doc. A/59/565), para. 192.", Yoram Dinstein, *War, Aggression and Self-Defence*, 5th edn (Cambridge: Cambridge University Press, 2011), 203.

[147] "Cited from: D.W. Bowett, *Self-Defence in International Law* 187–92 (1958); M. S. McDougal and F. P. Feliciano, *Law and Minimum World Public Order* 232–41 (1961); Stone, *supra* note 501, at 44", Ibid.

[148] "Cited from: Nicaragua case (Merits), supra note 14, at 347", Ibid., 196.

[149] Murray Colin Alder, *the Inherent Right of Self-Defence in International Law* (Springer Dordrecht Heidelberg New York London, 2013), 96.

nature of contemporary weapons of war. *The neutralist philosophy* acknowledges the respective legal bases of the positivist and realist philosophies, but does not unconditionally adopt either.[150]

None of the three philosophies provides a generally-accepted basis for reconciling their division.

The analysis of the pre-Charter legal history has shown two strands—a narrow and a wider understanding of self-defense. *The broader understanding* of self-defense allowed for preventive action against possible and probable dangers, in the sense put forward by Gentili and Vattel. This understanding was indeed considerably restricted by the beginning of the twentieth century and was generally viewed as unlawful at the time of the adoption of the Charter. Conversely, *the narrow understanding* of self-defense continued to be accepted as customary law at the time of the Charter. On its basis, self-defense could be exercised against imminent threats or ongoing attacks as well as after an attack had already occurred if a new attack had to be warded off.[151]

Kinga argued that at worst, "anticipatory action in self-defense is a legal basis for the use of force that can easily be abused as a result of a general lack of regulation of its content in UN practice. At best, anticipatory action in self-defense is a legal basis for the use of force that is acquiring increased relevance in twenty-first century conflicts and, for that reason, needs to be better defined".[152] Because, it is also that modern warfare technology and modern threats make resort to anticipatory action in self-defense necessary.

2.5.3 Interceptive self-defense

Dinstein employs the notion of "*interceptive self-defense"* to indicate "a reaction to an event that has already begun to happen even if it has not yet fully developed in its consequences" and maintains that, in such case, self-defense can be invoked under Article 51 because an armed attack "is already in progress, even if it is still incipient".[153]

He argued that the adjective 'interceptive' in the context of self-defense is set in opposition to 'preemptive', 'anticipatory' or 'preventive' self-defense. The contrast is due to a conceptual distinction between action (which is 'preemptive', 'anticipatory' or 'preventive') in the face of a

[150] Ibid.

[151] Kinga Tibori Szabó, *Anticipatory Action in Self-Defence, Essence and Limits under International Law* (*T*.M.C. ASSER PRESS, The Hague, The Netherlands, 2011), 286.

[152] Ibid. p. 287.

[153] Yoram Dinstein, *War, Aggression and Self-Defence*, 5th edn (Cambridge: Cambridge University Press, 2011), 203.

mere threat, on the one hand, and reaction to an event that has already begun to happen (even if it has not yet fully developed in its consequences), on the other. The crux of the issue, therefore, is not who fired the first shot but who embarked upon an apparently irreversible course of action, thereby crossing the legal Rubicon.[154]

As Waldock said it: "*Where there is convincing evidence not merely of threats and potential danger but of an attack being actually mounted, then an armed attack may be said to have begun to occur, though it has not passed the frontier".*[155]

Thus, author of thesis could agree with this a point that interceptive self-defense is lawful, even under Article 51 of the Charter, for it takes place after the other side has committed itself to an armed attack in an ostensibly irrevocable way. Whereas a preemptive (or preventive or anticipatory) strike is directed at an armed attack that is merely "foreseeable" (or even just 'conceivable'), an interceptive strike counters an armed attack which is already in progress, even if it is still incipient.

Marco Roscini pointed out that: "under a literal reading of this provision, the armed attack must 'occur', but, according to Article 32 of the 1969 Vienna Convention on the Law of Treaties[156], the application of the Article 31 interpretive criteria should not lead to an interpretation which is "manifestly absurd or unreasonable".[157]

In any case, it is doubtful that a reaction in self-defense would be necessary when the vulnerability, once discovered, can be neutralized through the use of passive cyber defenses or active defenses below the level of the use of force.[158]

In the 1967 Six Days War, Israel had reacted to the massing of troops at its border by its Arab neighbours and to the blockade of the Strait of Tiran not by bombing the Egyptian air force on the ground before the aircraft could take off and deliver the attack on the Jewish state, but by incapacitating Egypt's air force radars and command and control systems with a massive

---

[154] Ibid.

[155] "Cited from: Waldock, supra note 483, at 498", Ibid.

[156] Article 31, 32, Viena Convention on the Law of Treaties , 23 May 1969, United Nations, Treaty Series, vol. 1155, entry into force: 27 January 1980, https://treaties.un.org/doc/publication/unts/volume%201155/volume-1155-i-18232-english.pdf

[157] Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 78.

[158] Ibid.

cyberattack, the legality of such attack would have probably not been doubted. In the absence of an associated kinetic attack, however, anticipatory self-defense by cyber or kinetic means against an imminent standalone cyber armed attack will be extremely difficult to invoke in practice.[159]

Indeed, as will be seen, states claiming a right of anticipatory self-defense will have to provide, as a minimum, "clear and convincing" evidence of the imminent attack.

2.5.4 Imminent armed attack

Group of Experts took the position that even though Article 51 does not expressly provide for defensive action in anticipation of an armed attack, a State need not wait idly as the enemy prepares to attack. Instead, a State may defend itself once an armed attack is *"imminent"*. Such action is labelled 'anticipatory self-defense' in international law.[160]

This position is based on the standard of imminence articulated in the nineteenth century by US Secretary of State Webster following the *Caroline* incident. In correspondence with his British counterpart, Lord Ashburton, regarding a British incursion into American territory to attack Canadian rebels during the Mackenzie Rebellion, Webster opined that the right of self-defense applies only when "the necessity of self-defense is instant, overwhelming, leaving no choice of means, and no moment for deliberation".[161] Indeed, the Nuremberg Tribunal cited the Caroline correspondence with approval.[162]

In 1997 Gabčíkovo-Nagymaros Project Judgment, ICJ addressed the issue of imminence in the disparate setting of a dispute concerning the construction of a system of locks in the Danube River. It has been suggested by several scholars that the Court's dictum can be applied to anticipatory self-defense. What the Court here said was: *"Imminent" is synonymous with 'immediacy' or 'proximity' and goes far beyond the concept of 'possibility"*.[163]

---

[159] Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 79.

[160] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (UK: Cambridge University Press, 2017), 350.

[161] "Cited from: Letter from Daniel Webster to Lord Ashburton (6 August 1842), reprinted in 2 Int'l L. Dig. 412 (John Bassett Moore ed., 1906).", Ibid.

[162] International Military Tribunal (Nuremberg) Judgment of 1 October 1946, https://crimeofaggression.info/documents/6/1946_Nuremberg_Judgement.pdf

[163] "Cited from: *Gabčíkovo-Nagymaros Project* case, supra note 1173, at 42", Yoram Dinstein, *War, Aggression and Self-Defence*, 5th edn (Cambridge: Cambridge University Press, 2011), 203.

In its Santiago Resolution of 2007, the *Institut de Droit International* – while declaring that "there is no basis in international law for the doctrines of "preventive" self-defense' – pronounced that "the right of self-defense arises for the target State in case of an actual or manifestly imminent armed attack". In actuality, interceptive self-defense may be exercised even when the armed attack is still in an embryonic stage and, therefore, falling short of being "manifest".[164]

2.5.5 "Last feasible window of opportunity" standard

Group of Experts noted of the 'last feasible window of opportunity' standard. By this standard, a State may act in anticipatory self-defense against an armed attack, whether cyber or kinetic, when the attacker is clearly committed to launching an armed attack and the victim State will lose its opportunity to effectively defend itself unless it acts. In other words, it may act anticipatorily only during the last window of opportunity to defend itself against an armed attack that is forthcoming. This window may present itself immediately before the attack in question, or, in some cases, long before it occurs.[165]

Consider a situation in which the intelligence service of a State receives incontrovertible information that another State is preparing to launch a cyber operation that will destroy the former's primary oil pipeline within the next two weeks. The operation involves causing microcontrollers along the pipeline to increase the pressure in it, resulting in a series of explosions. Since its intelligence service has no information on the specific vulnerability to be exploited, the first State cannot mount an effective cyber defense of the microcontrollers. However, the service does have information that those involved in conducting the operation will gather at a particular location and time. The target State would be justified in concluding that an armed attack is imminent, using force to defend itself is necessary, and strikes against those individuals would be lawful as proportionate anticipatory self-defense.[166]

In this chapter, the author of the thesis researched the nature of the scale and effects required for an act to be characterized as an armed attack as cyberattack necessarily exceed those qualifying the act as a use of force. It should be emphasized that scales and effects are an appraisal concept in international law, the sources of which are the decision of ICJ. It must be

[164] "Cited from*: Institut de Droit International*, Resolution, 'Self-Defence', 72 AIDI 233, id. (Santiago, 2007), (Articles 3, 6)", Ibid, p 206.

[165] "Cited from: US Justice Dept. White Paper, Lawfulness of a Lethal Operation Directe against a U.S. Citizen Who Is a Senior Operational Leader of Al–Qa'da or an Associate Force (n.d), at 7.", Michael N. Schmitt, Tallinn Manual 2.0 on *the International Law Applicable to Cyber Operations* (UK: Cambridge University Press, 2017), 351.

[166] Ibid. p. 352.

acknowledged, however, that the Nicaragua Judgment has complex application in the case of cyberattacks.

Moreover, it was focused on the nature of an action's consequences of "Armed Attack" as cyberattack for understanding scale and effects within meaning Nicaragua Judgment. After the analysis it becomes clear that the consequences can be different, both with damage or destruction, injures, death, and with the outage of CI of states.

Also, it was researched anticipatory self-defense against an imminent armed attack by cyber means. Despite the generally accepted definition "occur armed attack" of Article 51 of the Charter and Article 5 of the Treaty, the application of interceptive self-defense or in the case imminent armed attack in the light of new threats, such as cyberattacks with severe consequences, is necessary. This is in accordance with modern international law.

3. THE MAIN REQUIREMENTS OF COLLECTIVE SELF-DEFENSE AGAINST CYBERATTACKS

Self-defense against cyberattacks must meet three criteria – necessity, proportionality, immediacy. The ICJ acknowledged this criteria in the Nicaragua judgment[167] and later confirmed them in its Oil Platforms judgment[168]. The Nuremberg Tribunal[169] also recognised the criteria. As illustrated by these decisions, they undoubtedly reflect customary international law. Moreover, author of thesis would research such criteria as request of the victim state and reporting the self-defense measures to the UN Security Council. The main purpose of this chapter is to research the specifics of these criteria in the light of conducting cyberattacks on the alliance.

3.1 Necessity

Even though Article 51 does not refer to this criteria, in the *Nuclear Weapons Advisory Opinion* the ICJ reiterated that "the submission of the exercise of the right of self-defense to the conditions of necessity is a rule of customary international law" and "this condition applies equally to Article 51 of the Charter, whatever the means of force employed".[170]

The requirements of necessity are often traced back to the 1837 *Caroline* incident. States invoke the famous formula that there must be a "necessity of self-defense, instant, overwhelming, leaving no choice of means and no moment of deliberation".[171] Necessity is commonly interpreted as the requirement that no alternative response be possible. Questions of necessity also help states to distinguish unlawful reprisals from lawful self-defense.[172]

---

[167] Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America), 27 June 1986, para. 176, 194, http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf,

[168] Case concerning oil platforms (Islamic republic of Iran v. United States of America), 12 December 1996, para. 43, 73-74, 76, http://www.icj-cij.org/files/case-related/90/090-19961212-JUD-01-00-EN.pdf

[169] International Military Tribunal (Nuremberg) Judgment of 1 October 1946, para. 435, (referring to the Caroline formula), https://crimeofaggression.info/documents/6/1946_Nuremberg_Judgement.pdf

[170] Nuclear Weapons advisory opinion: Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 ICJ 226 (8 July), para. 41, http://www.icj-cij.org/files/case-related/95/095-19960708-ADV-01-00-EN.pdf

[171] Christine Gray, *International Law and the Use of Force, Third Edition* (UK: Oxford University Press, 2008), 149-145.

[172] Ibid.

It is arguable that the only aspect of the *Caroline* "necessity" formulation that needs to be satisfied if an armed attack has occurred within the meaning of Article 51 is that of 'instancy': "that is, when the act is accomplished, damage suffered, and the danger passed, then the incidents of self-defense cease".[173]

Necessity requires that a use of force, including cyber operations that amount to a use of force, be needed to successfully repel an imminent armed attack or defeat one that is underway. This does not mean that force has to be the only available response to an armed attack. It merely requires that non-forceful measures be insufficient to address the situation. Of course, the forceful actions may be combined with non-forceful measures such as diplomacy, economic sanctions, or law enforcement.[174]

The key to the necessity analysis in the cyber context is, therefore, the existence, or lack, of alternative courses of action that do not rise to the level of a use of force. Necessity is judged from the perspective of the victim state. The determination of necessity must be reasonable in the attendant circumstances. For example, consider a case in which one State is conducting cyber armed attacks against another State's cyber infrastructure. The victim state responds with forceful cyber operations of its own to defend itself. Unbeknownst to that State, the attacking State had already decided to end its attacks. This fact would not render the victim state's defensive cyber operations unnecessary and, therefore, an unlawful use of cyber force in self-defense.[175]

Ago argued that necessity requires that the forcible reaction be a means of last resort and the only effective way to repel the armed attack.[176]

However, Schachter, for example, is of the view that a State subjected to an armed attack is "under a necessity of armed defense irrespective of probabilities as to effectiveness of peaceful settlement".[177]

---

[173] Judith Gardam, *Necessity, Proportionality and the Use of Force by States* (Cambridge: Cambridge University Press, 2004), 149-150.

[174] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, (UK: Cambridge University Press, 2017), 348.

[175] Ibid. p. 349.

[176] "Cited from: As Ago puts it, '[t] he reason for stressing that action taken in self-defence must be necessary is that the State attacked (or threatened with imminent attack, if one admits preventive self-defence) must not, in the particular circumstances, have had any means of halting the attack other than recourse to armed force. . . . Self-defence will be valid as a circumstance precluding wrongfulness of the conduct of the State only if that State was unable to achieve the desired result by different conduct involving either no use of armed force at all or merely its use on a lesser scale' (Ago, Addendum, p 69; emphasis in the original).", Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 89.

In turns, Roscini pointed out that as a minimum, it entails an obligation to *"identify the author*[178]*, verify that the cyberattack is not an accident, that it was really aimed at the state invoking self-defense, and that the matter cannot be settled by less intrusive means* (eg, by preventing the hackers from accessing the networks and computers under attack through the use of passive cyber defenses or by conducting a counter cyber operation not amounting to a use of force)".[179]

The US Presidential Policy Directive of 2012, for instance, requires to first try law enforcement or network defense techniques before resorting to active defenses against a cyberattack on the United States and provides that, if used, such defenses must employ "the least intrusive methods feasible to mitigate a threat".[180]

The 2011 AIV/CAVV Report on Cyber Warfare states that: "in the context of self-defense, *necessity* usually refers to the existence of an armed attack or the imminent threat of attack. It also refers to the absence of feasible alternatives, such as law enforcement in the case of an organised group operating in the territory of another state without the direct involvement of that state. In most cases, mutual assistance in a law enforcement context would be a feasible and available alternative, removing the grounds for self-defense. The option of a military response in self-defense is relevant only where a cyberattack is comparable to an armed attack and is conducted by a group of people operating with some measure of coordination but cannot be stopped by a law enforcement agency because the state in which the attack originated is either not willing or not able to take the necessary law enforcement measures".[181]

Even then, it is only relevant if there are no alternatives, *"there is sufficient certainty regarding the identity of the author of the attack and the self-defense measures can be taken in a targeted and proportional manner".*[182]

---

[177] "Cited from: Schachter, Theory and Practice, p. 152",Judith Gardam, *Necessity, Proportionality and the Use of Force by States*, (Cambridge: Cambridge University Press, 2004), 153.

[178] "When a CNA (Computer Network Attack) qualifies as an armed attack identifying the actual aggressor may create a major problem.", Yoram Dinstein, *War, Aggression and Self-Defence*, 5th edn (Cambridge: Cambridge University Press, 2011), 231.

[179] Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 89.

[180] "Cited from: US Presidential Policy Directive 20, p 8. See also the 2011 US International Strategy for Cyberspace", Ibid.

[181] Cyber Warfare, No 77, AIV / No 22, CAVV December (2011): 22, https://aiv-advies.nl/download/da5c7827-87f5-451a-a7fe-0aacb8d302c3.pdf

[182] Ibid.

Dinstein noted that, victim state must also verify that the armed attack mounted by attacker was intentional. In other words, the use of force by attacker must not be due to a mere accident or mistake, for which subject of armed attack may incur State responsibility without bearing the blame for an armed attack. Much depends on whether an interval of time is realistically available between the attacker use of force and the victim state recourse to counter-force.[183]

The relevance of the temporal aspect of necessity is also confirmed in the judgment of the ICJ in the *Nicaragua Case*. The Court was considering the plea of collective self-defense by the United States in response to an alleged armed attack by Nicaragua against El Salvador. The armed attack, it was argued, consisted of the provision of aid by Nicaragua to insurgents in El Salvador. The Court concluded that no armed attack had occurred. Not even strict compliance by the United States with the elements of necessity and proportionality in their actions. In relation to necessity, it was the lapse of time between the events on which the necessity was based and the change in circumstances that the Court regarded as inconsistent with a plea of necessity.[184]

Roscini noted that certain commentators have suggested that responses in self-defense to a cyberattack against CI should be allowed even without first attributing and characterizing the attack. However, he pointed that this position it cannot accepted.[185]

State practice is generally consistent with the desirability of pursuing peaceful means of resolving a dispute once an armed attack is over. There is reluctance, however, to accept that the continued existence of the right to self-defense is dependent as a matter of law on so doing.[186]

3.2 Proportionality

To what, exactly, must the measures taken in self-defense be proportional? On this there are two broad schools of thought. *The first* is that proportionality should relate to the armed

---

[183] Yoram Dinstein, *War, Aggression and Self-Defence*, 5th edn (Cambridge: Cambridge University Press, 2011), 232.

[184] *"*Cited from Nicaragua Case*: these measures were only taken, and began to produce their effects, several months after the major offensive of the armed opposition against the Government of El Salvador had been completely repulsed and the actions of the opposition considerably reduced in consequence. Thus it was possible to eliminate the main danger to the Salvadorian government without the United States embarking on activities in and against Nicaragua*", Judith Gardam, *Necessity, Proportionality and the Use of Force by States*, (Cambridge: Cambridge University Press, 2004), 152.

[185] M. Roscini, "World Wide Warfare – Jus ad Bellum and the Law of Cyber Force", 14, MPYUNL, (2010):85, 119.

[186] Judith Gardam, *Necessity, Proportionality and the Use of Force by States* (Cambridge: Cambridge University Press, 2004), 153.

attack, as suggested by a literal interpretation of the ICJ formula– 'proportional to the armed attack'. This is a quantitative or 'tit-for-tat' approach, where the forcible response is equivalent to the armed attack in terms of scale or means of attack, or the harm or damage caused. *The other school* of thought is that the response should be proportionate to the aim of halting or repelling the attack, and the response might therefore be of a greater or lesser scale than the original attack.[187]

Proportionality is strictly linked to necessity and is the other side of the same coin.[188] The quantum of armed force used in the defensive reaction could be balanced either against the scale and effects of the armed attack or against the purpose of repelling the armed attack.

The first step in applying the proportionality equation is to determine the legitimate aim of self-defense under the UN Charter.[189]

The majority of decisions required to ensure the proportionality of a forceful response will be taken at the planning stage and at a senior level of command. Nevertheless, any ensuing forceful action will need to be monitored continuously to ensure that the strategic objectives and the methods chosen to achieve them remain proportionate to the aim of the response.[190]

Proportionality addresses the issue of how much force, including use of cyber force, is permissible once force is deemed necessary. The criterion limits the scale, scope, duration, and intensity of the defensive response to that required to end the situation that has given rise to the right to act in self-defense. It does not restrict the amount of force used to that employed in the armed attack since the level of force needed to successfully mount a defense is context-dependent; more force may be necessary, or less force may be sufficient, to defeat the armed attack or repel one that is imminent.

---

[187] Alison Pert, P*roportionality in Self-Defence – Proportionate to What?* (Sydney Law School, Legal Studies Research Paper No. 17/92 November 2017), 2.

[188] "Cited from: Ago, Addendum, p 69. The ICJ expressed the view that proportionality does not per se exclude the use of a weapon in self-defence 'in all circumstances' (*Nuclear Weapons*, para 42)", Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 90.

[189] Judith Gardam, *Necessity, Proportionality and the Use of Force by States* (Cambridge: Cambridge University Press, 2004), 156.

[190] Ibid.

As correctly remarked by Ago, the principle of proportionality must be applied with some degree of flexibility.[191]

David Kretzmer argued that: "the main source of disagreement and confusion of the meaning of the principle of proportionality flows from the lack of consensus over the legitimate ends of force employed by a state that is exercising its inherent right to self-defense. Even when it is accepted that the appropriate test of proportionality is a 'means-end' test, in the absence of agreement on these ends it is obviously impossible to agree on the necessary means to achieve them".[192]

Proportionality relates to the size, duration and target of the response, but clearly these factors are also relevant to necessity. It is not clear how far the two concepts can operate separately. If a use of force is not necessary, it cannot be proportionate and, if it is not proportionate, it is difficult to see how it can be necessary.[193]

In addition, there is no requirement that the defensive force be of the same nature as that constituting the armed attack and does not mean that the defending state is restricted to the same numbers of armed forces as the attacking state; nor is it necessarily limited to action on its own territory.[194] Therefore, a cyber use of force may be resorted to in response to a kinetic armed attack, and *vice versa.*[195]

In fact, a response in-kind against a cyberattack may not always be possible or effective, either because the victim state does not have the technology to hack back or because the aggressor is a low-technology state, or a non-state actor, with no digital infrastructure to hit.[196]

---

[191] "Cited from: Ago, supra note 1099, at 69", Yoram Dinstein, *War, Aggression and Self-Defence*, 5th edn (Cambridge: Cambridge University Press, 2011), 232.

[192] David Kretzmer, The Inherent Right to Self-Defence and Proportionality in Jus Ad Bellum, *The European Journal of International Law* Vol. 24 no. 1 EJIL (2013), Vol. 24 No. 1, 2013. Published by Oxford University Press, (2013): 282.

[193] Christine Gray, *International Law and the Use of Force, Third Edition* (UK: Oxford University Press, 2008), 149-150.

[194] Ibid.

[195] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (UK: Cambridge University Press, 2017), 349.

[196] "Cited from: Greenberg, Goodman, and Soo Hoo, *Information Warfare*, p 32; Blank, 'International Law', p. 419.", Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 90.

The problem with calculating proportionality in the cyber context resides in the speed and covert nature of cyberattacks: it might be difficult to readily establish their magnitude and consequences.[197] In relation to the cyber reaction, proportionality could also be difficult to calculate in advance because of the interconnectivity of information systems: as with biological weapons, malware sent through cyberspace might spread uncontrollably. Financial institutions and companies might also be reluctant to provide information on the damage suffered because of business confidentiality.[198] It is also doubtful whether a series of small-scale attacks can be considered cumulatively when assessing the proportionality of the reaction.[199]

In any case, a disproportionate reaction would not per se turn a self-defense measure into an unlawful reprisal, but only renders the State responsible of an act of excess (or abuse) of self-defense.

The 2011 AIV/CAVV Report on Cyber Warfare states that: "proportionality in the context of self-defense has both a quantitative and a qualitative dimension. In effect, proportionality means the action must be directed at ending the attack and preventing further attacks in the near future. Moreover, it must be in proportion to the scale of the attack. A cyberattack that has comparable consequences to an armed attack (fatalities, damage and destruction) can justify a response with cyber weapons or conventional weapons provided the intention is to end the attack, the measures do not exceed that objective and there are no viable alternatives. The proportionality requirement rules out measures that harbour the risk of escalation and that are not strictly necessary to end the attack or prevent attacks in the near future".[200]

The ICJ considered the question of proportionality in the *Nicaragua Case*, in the context of collective self-defense. As the Court found that no armed attack had in fact occurred to justify the forceful response, the issue of proportionality was moot. The Court stated that: "whatever uncertainty may exist as to the exact scale of the aid received by the Salvadorian armed

[197] "Cited from: Matthew Hoisington, 'Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense', Boston College International and Comparative Law Review 32 (2009), p 452", Ibid.

[198] "Cited from: Eneken Tikk, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm, and Liis Vihul, Cyber Attacks Against Georgia: Legal Lessons Identified (CCDCOE, November 2008), p 17, <http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf>; Waxman, 'Cyber Attacks', p. 444", Ibid.

[199] M. Roscini, "World Wide Warfare – Jus ad Bellum and the Law of Cyber Force", 14, MPYUN, (2010): 85, 120.

[200] Cyber Warfare, No 77, AIV / No 22, CAVV December (2011): 23, https://aiv-advies.nl/download/da5c7827-87f5-451a-a7fe-0aacb8d302c3.pdf

opposition from Nicaragua, it is clear that these latter United States activities in question could not have been proportionate to that aid".[201]

However, Judge Schwebel also seemed to relate proportionality to the purpose of halting and repelling the attack, when he cited the 1980 Report of Roberto Ago, the International Law Commission's then Rapporteur on State Responsibility. Indeed, it is this report which is often cited in support of the second school of thought.[202]

David Hannay, the United Kingdom representative at the relevant time on the Security Council, illustrate the significance attached to factor in the assessment of what was a proportionate response:[203] "*some have suggested that military action being taken by the allies is in some way excessive or disproportionate and thus exceeds the 'all necessary means' authorized in resolution 678 (1990) to bring about the liberation of Kuwait. But the nature and scope of the military action is dictated not by some abstract set of criteria but by the military capacity of the aggressor, who has refused all attempts to remove him from Kuwait".*[204]

The ICJ did not elaborate on proportionality in its advisory opinion on the Legality of the Threat or Use of Nuclear Weapons, merely referring to proportionality as a requirement of self-defense. In another dissenting opinion, however, Judge Schwebel quoted the United Kingdom Attorney-General's oral submissions to the Court during the hearing: "*If one is to speak of 'disproportionate', the question arises: disproportionate to what? The answer must be 'to the threat posed to the victim state'. It is by reference to that threat that proportionality must be measured. So one has to look at all the circumstances, in particular the scale, kind and location of the threat. To assume that any defensive use of nuclear weapons must be disproportionate, no matter how serious the threat to the safety and the very survival of the State resorting to such use, is wholly unfounded […] any government faced with such a threat will have to decide, what reliance on deterrence or degree of action is necessary for self-defense".*[205]

---

[201] Judith Gardam, *Necessity, Proportionality and the Use of Force by States* (Cambridge: Cambridge University Press, 2004), 158.

[202] Alison Pert, P*roportionality in Self-Defence – Proportionate to What?* (Sydney Law School, Legal Studies Research Paper, 2017), No. 17/92 November 2017, 4.

[203] "Cited from: UN Doc. S/PV.2977, Part II, para. 72, 14 February 1991", Judith Gardam, *Necessity, Proportionality and the Use of Force by States*, (Cambridge: Cambridge University Press, 2004), 158.

[204] Ibid. p. 160.

[205] "Cited from: Nuclear Weapons advisory opinion: Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 ICJ 226 (8 July), para. 321, http://www.icj-cij.org/files/case-related/95/095-19960708-ADV-01-00-EN.pdf, Alison Pert, P*roportionality in Self-Defence – Proportionate to What?* (Sydney Law School, Legal Studies Research Paper No. 17/92 November 2017), 4.

Judge Schwebel spoke again of deterrence when referring to the 1991 First Gulf War, commenting that if Iraq had used weapons of mass destruction against coalition forces, then even if the use of nuclear weapons were treated as prohibited, "their proportionate use [against Iraq] by way of belligerent reprisal in order to deter further use of chemical or biological weapons would have been lawful".[206]

The likelihood of future attacks is assessed on the evidence: factors such as the occurrence of past attacks, the nature of the attacker, and the severity of the threat will be relevant. Viewed this way, proportionality in self-defense should permit a state to use the minimum degree of force that is reasonably necessary to protect itself from any present or likely future attacks.[207]

Author of thesis could agree with opinion of Judith Gardam, that although there is belated acknowledgment in some quarters of the potential of proportionality in *jus ad bellum* to contribute significantly to limiting the destructive impact of armed conflict for all victims, its detailed application in the practice of States awaits further development.

3.3 Immediacy

The requirement of immediacy of the reaction, which should not be confused with the imminence of the armed attack in relation to anticipatory self-defense, reflects the fact that the ultimate purpose of self-defense is not to punish the attacker, but rather to repel an armed attack.[208]

Immediacy can be used in two different contexts. Firstly, in relation to the concept of an imminent or immediate threat of an attack within the context of anticipatory self-defense. Secondly as a requirement for taking action in self-defense within a short span of time subsequent to an attack in order to distinguish self-defense from reprisal. Used in the latter sense, immediacy is often seen as one of the requirements for the exercise of self-defense alongside necessity and proportionality.[209]

---

[206] Ibid. p. 6.

[207] Alison Pert, P*roportionality in Self-Defence – Proportionate to What?* (Sydney Law School, Legal Studies Research Paper No. 17/92 November 2017), 14.

[208] Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 91.

[209] T.D. Gill, "The Temporal Dimension of Self-Defence: Anticipation, Pre-emption, Prevention and Immediacy", *Journal of Conflict and Security Law*, Volume 11, Issue 3, 1 December (2006): 361–369, https://academic.oup.com/jcsl/article-abstract/11/3/361/793706?redirectedFrom=PDF

Like proportionality, while immediacy serves as a core element of self-defense, it must be interpreted reasonably.[210]

The requirement of immediacy distinguishes an act of self-defense from mere retaliation. It refers to the period following the execution of an armed attack within which the victim state may reasonably respond in self-defense. Factors such as the temporal proximity between attack and response, the period necessary to identify the attacker, and the time required to prepare a response are relevant in this regard.[211]

A further issue is how to assess the period during which a self-defense situation continues following the completion of the particular incident providing the basis for the right of self-defense. For instance, a cyber armed attack may commence with a wave of cyber operations against the victim state. The self-defense situation does not necessarily conclude with the termination of those cyber operations. If it is reasonable to conclude that further cyber operations are likely to follow, the victim state may treat those operations as a 'cyber campaign' and continue to act in self-defense. However, if such a conclusion is not reasonable, any further use of force, whether kinetic or cyber, is liable to be characterised as mere retaliation. In the final analysis, the requirement of immediacy rests on a test of reasonableness in light of the circumstances prevailing at the time.[212]

In some cases, the fact that a cyber armed attack has occurred or is occurring may not be apparent for some time. This could be so because the cause of the damage or injury has not been identified. Similarly, the initiator of the attack may not be identified until well after the attack. The classic example of both situations is employment of a worm such as Stuxnet. In such cases, the criterion of immediacy is not met unless the conditions described above justify taking action.[213]

Immediacy does not mean 'instantaneous' and must be applied flexibly: what it entails is that 'there must not be an undue time-lag between the armed attack and the exercise of self-

[210] "Cited from: T. D. Gill, 'The Temporal Dimension of Self-Defense: Anticipation, Pre-emption, Prevention and Immediacy', International Law and Armed Conflict: Exploring the Faultlines, supra note 1059, at 113, 154", Yoram Dinstein, *War, Aggression and Self-Defence*, 5th edn (Cambridge: Cambridge University Press, 2011), 233.

[211] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (UK: Cambridge University Press, 2017), 353.

[212] Ibid. p. 354.

[213] Ibid. p. 354.

defense in response'.[214] Lapse of time is almost unavoidable when – in a desire to fulfil, letter and spirit, the condition of necessity – a tedious process of information-gathering or diplomatic negotiations evolves.[215]

The first phase of the Gulf War is emblematic. The invasion of Kuwait by Iraq took place on 2 August 1990, yet the Security Council authorized the use of 'all necessary means' only as from 15 January 1991, namely, after almost half a year.

However, in *the Nicaragua Judgment*, ICJ rejected on other grounds a claim of collective self-defense by the United States, and –as a result – no decision in respect of necessity and proportionality, because United States had commenced its activities several months after the occurrence of the presumed armed attack and when the main danger could be eliminated in a different manner.[216]

As has been observed, "[a] state does not . . . forfeit its right of self-defense because it is incapable of instantly responding or is uncertain of who is responsible for the attack or from where the attack originated".[217] Some flexibility in assessing the immediacy of the reaction is especially required in the case of cyberattacks: if a state's military computer systems and networks have been incapacitated by the attack, for instance, it might take some time for it to be able to react in self-defense either by cyber or kinetic means. The gathering of sufficient evidence that allows to confidently point the finger against a certain state or non-state actor can also be a time-consuming task in the cyber context.[218]

Furthermore, if the aggressor uses logic or time bombs, the actual damage could occur well after the cyberattack, which might delay the reaction.[219]

---

[214] "Cited from: Dinstein, War, Aggression and Self-Defence, p 233", Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 91.

[215] Yoram Dinstein, *War, Aggression and Self-Defence*, 5th edn (Cambridge: Cambridge University Press, 2011), 233.

[216] Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America), 27 June 1986, para. 195, http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

[217] Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 91.

[218] Ibid.

[219] M. Roscini, "World Wide Warfare – Jus ad Bellum and the Law of Cyber Force", 14, MPYUNL 85, 120 (2010), 85.

Immediacy must not be justified by unduly and unnecessarily delay in the time of the fulfillment of the right to self-defense. A State must be allowed the necessary time to overcome practical and legal hurdles before it decides to react to an attack. [220]

Whether one sees immediacy used in this sense as an independent criterion alongside necessity and proportionality, or as forming part of the criterion of necessity is immaterial; the point is that a State exercising self-defense should do so within a reasonable period, on the basis of persuasive evidence and with a view towards thwarting, or where necessary, overcoming the attack and removing the threat of further attack.[221]

"Immediacy" should not be interpreted rigidly to restrict the defensive measures to simply reacting to or interception of an attack which has been initiated, but can include response of a truly anticipatory character to a clear and concrete threat of an attack within the foreseeable future.[222]

3.4 Request of the victim state

The right of self-defense may be exercised collectively. Collective self-defense against a cyber operation amounting to an armed attack may only be exercised at the request of the victim state and within the scope of the request.[223]

The right to collective self-defense authorizes a State or multiple States to either conduct a joint defense against an attack launched against all of them or to come to the assistance of another State (or States) that is the victim of a cyber armed attack.[224] This right, explicitly set forth in Article 51 of the United Nations Charter, is recognized in customary international law.

In 2003, in the *Oil Platforms* case, the Court reiterated this requirement of a request made to the third State by the direct victim of an armed attack. In the 2005 *Armed Activities* case, the Court noted that 'a State may invite another State to assist it in using force in self-defense'. The

[220] T.D. Gill, "The Temporal Dimension of Self-Defence: Anticipation, Pre-emption", Prevention and Immediacy, *Journal of Conflict and Security Law*, Volume 11, Issue 3, 1 December (2006): Pages 361–369, https://academic.oup.com/jcsl/article-abstract/11/3/361/793706?redirectedFrom=PDF

[221] Ibid.

[222] Ibid.

[223] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (UK: Cambridge University Press, 2017), 354.

[224] Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America), 27 June 1986, para. 199, http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

Institut de Droit International, in its Santiago Resolution of 2007, followed suit, stating that 'collective self-defense may be exercised only at the request of the target State'.[225]

Before a State may come to the assistance of another State in collective self-defense, it must have received a request for such assistance from the victim of the armed attack. There is no rule in customary international law permitting one State to engage in collective self-defense of another State solely on the basis of the former's own assessment of the situation. *(Nicaragua case*).[226]

Judge Jennings went on to say that the reasoning was also objectionable in that the Court was giving the impression that the third state need not itself have an interest for it to exercise collective self-defense.[227] Some have even argued that the right to collective self-defense is essentially the right of the party giving aid to the victim, and that the ICJ itself should not be taken to have rejected this position.[228]

The direct victim of an armed attack must first "form and declare the view" that it has been subjected to such an attack. Moreover, a request for help has to be made by the victim state: in the absence of such a request, collective self-defense by a third State is excluded.[229]

When a State exercises collective self-defense on behalf of another State, it must do so within the scope of the other's request and consent. In other words, the right to engage in collective self-defense is subject to the conditions and limitations set by the victim state. The latter State may, for instance, limit the assistance to non-kinetic measures or restrict the types of targets that may be made the object of cyber operations while operating in collective self-defense.[230]

---

[225] Yoram Dinstein, *War, Aggression and Self-Defence*, 5th edn (Cambridge: Cambridge University Press, 2011), 294.

[226] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (UK: Cambridge University Press, 2017), 355.

[227] "Cited from: Jennings, Dissenting Opinion 545", Christine Gray, *International Law and the Use of Force, Third Edition* (UK: Oxford University Press, 2008), 187.

[228] "Cited from: Macdonald 'The Nicaragua case: New Answers to Old Questions', 1986 Canadian Yearbook of International Law 127 argued that 'if there is an armed attack, what the victim believes to have occurred is otiose because the aid-giving state is also subject to the armed attack", Ibid. p. 188.

[229] Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America), 27 June 1986, para. 105, http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

[230] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (UK: Cambridge University Press, 2017), 355.

Collective self-defense may be exercised either on the basis of a previously concluded collective defense treaty or an ad hoc arrangement. As an example, NATO Allies have agreed about Article 5 of NATO Treaty. As argued Group of Experts, there would be no bar to engaging in cyber operations pursuant to Article 5 of the NATO Treaty.[231]

As argued Dinstein, the issue has important practical dimensions. In general, as already observed, self-defense is a right and not a duty. Victim state is not obligated, therefore, to attempt to repel an invasion or any other form of an armed attack by attacker (unless a pledge to exercise individual self-defense is incorporated in a treaty in force, such as a permanent neutrality arrangement). Third state cannot coerce victim state to accept help against its will (again, unless both Parties are bound by a specific treaty regulating collective self-defense, e.g., a military alliance).[232]

In the absence of a special treaty conferring on third state the right to despatch an expeditionary force to victim state, third state must await a call for help from the country that it purportedly seeks to assist (victim state).[233]

The legal position is completely different when the third state response to the aggressor armed attack takes place outside the territorial boundaries of victim state. When attacker commences an armed attack (the direct victim of which is victim state), and third state perceives that its own security is jeopardized, third state is entitled under Article 51 of the Charter to resort to counter-force. There is no allusion in the Article to prior approval by victim state as a condition to the exercise of the right of collective self-defense by third state.[234]

In many of the episodes the intervening state did in fact have a pre-existing treaty relationship with the 'victim' state, but in the other cases where there was no such treaty this was not mentioned as a ground of illegality even by those otherwise critical of the use of force.[235]

---

[231] Ibid.

[232] "Cited from: The requirement of a request by the victim of an armed attack, as a condition for external assistance, is apparently not reconcilable with many existing treaties. See F. L. Morrison, 'Legal Issues in the Nicaragua Opinion', 81 AJIL 160, 163 (1987). Cf. D. K. Linnan, 'Self-Defense, Necessity and U. N. Collective Security: United States and OtherViews', 1 DukeJCIL 57, 103 (1991)", Yoram Dinstein, *War, Aggression and Self-Defence*, 5th edn (Cambridge: Cambridge University Press, 2011), 295.

[233] Ibid. p. 296.

[234] Ibid.

[235] "Cited from: Thus the absence of a treaty in the cases of USA/Lebanon (1958), UK/Jordan (1958), Cuba/Angola (from 1975), USA and UK/Kuwait (1990), and Angola, Namibia and Zimbabwe/ DRC (1998) was not singled out as a ground for criticism", ", Christine Gray, *International Law and the Use of Force, Third Edition* (UK: Oxford University Press, 2008), 188.

3.5 Reporting the self-defense measures to the UN Security Council

Measures involving cyber operations undertaken by States in the exercise of the right of self-defense (individual and collective) pursuant to Article 51 of the United Nations Charter shall be immediately reported to the United Nations Security Council (UN Security Council).[236] The report consists, as a minimum, of a plain notification of the invocation of the right of self-defense in response to an armed attack.[237]

Moreover, it should be noted that Article 5 of NATO defines that any armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council.[238]

Perfect example of reporting the self-defense measures is the American communication to the Council on 7 October 2001, reporting that the United States (together with some allies) had initiated action that day against Taliban-led Afghanistan in response to the armed attack of 9/11.[239] However, there are still occasions when States exercise self-defense without immediately reporting their action to the Security Council.[240]

This rule is limited practical relevance for the next reasons.

The requirement to report exercises of self-defense to the UN Security Council is found in Article 51 of the UN Charter. The failure of a Member of the United Nations to report actions that it takes in self-defense against a cyber armed attack to the Security Council is a violation of its obligations under Article 51.[241]

---

[236] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (UK: Cambridge University Press, 2017), 355.

[237] Yoram Dinstein, *War, Aggression and Self-Defence*, 5th edn (Cambridge: Cambridge University Press, 2011), 237.

[238] Aricle 5, The North Atlantic Treaty, Washington D.C., 4 April 1949, https://www.nato.int/cps/en/natohq/official_texts_17120.htm

[239] "Cited from: Letter from the Permanent Representative of the United States of America to the President of the Security Council, 7 October 2001, 40 ILM 1281 (2001)", Yoram Dinstein, *War, Aggression and Self-Defence*, 5th edn (Cambridge: Cambridge University Press, 2011), 239.

[240] "The failure of the USA to report on its use of force to the Security Council under Article 51 was taken by the Court as an indication that the USA was not exercising the right of collective self-defense, Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America), 27 June 1986, para. 235, http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf", Christine Gray, *International Law and the Use of Force, Third Edition* (UK: Oxford University Press, 2008), 188.

[241] Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America), 27 June 1986, para. 235, http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

Roscini worthily noted that such an obligation might be difficult to comply with in the case of a cyberattack in self-defense: it has been seen that, because of their inherent features and the current architecture of cyberspace, cyber operations are the perfect tool for covert actions.[242]

As pointed Dinstein, the State under attack has no choice but to defend itself as best it can. It must also act without undue loss of time, and, most certainly, it cannot afford the luxury of waiting for any juridical (let alone judicial) scrutiny of the situation to run its course.[243]

In the *Nicaragua case*, Judge Schwebel in his Dissenting Opinion pointed out that it would be 'bizarre' if it would follow from the duty to report that aggressors are free to act covertly while those who defend themselves are not.[244] He arrived at the conclusion that the report to the Security Council is a procedural matter, and that, therefore, nonfeasance must not deprive a State of the substantive right of self-defense.[245]

Group of Experts were considering that the reporting requirement should not be interpreted as customary international law and the failure not divest the State in question of the right to act in self-defense. In Nicaragua case, it held that "it is clear that in customary international law it is not a condition of the lawfulness of the use of force in self-defense that a procedure so closely dependent on the content of a treaty commitment and of the institutions established by it should have been followed".[246]

According to Article 51, the right to act in self-defense continues until the Security Council 'has taken measures necessary to maintain international peace and security'. Group of Experts agreed that the Council must expressly divest the State of its right of self-defense under Article 51 in such cases.[247]

---

[242] Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 103.

[243] Yoram Dinstein, *War, Aggression and Self-Defence*, 5th edn (Cambridge: Cambridge University Press, 2011), 234.

[244] "Cited from: Nicaragua, Dissenting Opinion of Judge Schwebel, para 222. See similarly Ronzitti, 'The Expanding Law', p 356, who argues that non-compliance with the duty to report is an 'excusable violation'; Pierluigi Lamberti Zanardi, La legittima difesa nel diritto internazionale (Milano: Giuffrè, 1972), pp 275–6", Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 104.

[245] Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America), 27 June 1986, para. 200, http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

[246] Ibid.

[247] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (UK: Cambridge University Press, 2017), 356.

It can therefore be concluded that the covert character of defensive cyber operations does not per se render them unlawful under Article 51 of the UN Charter, providing that all other requirements for the exercise of self-defense are met.

The modes of action open to the Security Council are diverse. Inter alia, the Council may (i) give its retrospective seal of approval to the exercise of self-defense by one of the Parties; (ii) impose a general cease-fire; (iii) demand withdrawal of forces to the original lines; (iv) insist on the cessation of the unilateral action of the defending State, supplanting it with measures of collective security; or (v) decide that a State engaged in so-called self-defense is in reality the aggressor.[248] When convinced that forcible measures were taken by a State in self-defense, the Council ought to issue a ruling to that effect, despite the absence of a report. It would be a gross misinterpretation of Article 51 for the Council to repudiate self-defense, thus condoning an armed attack, only because no report has been put on record.[249] A failure by a State resorting to force to formally report its recourse to self-defense should not be fatal, provided that the substantive conditions for the exercise of this right are met.[250]

To sum up the main requirements of collective self-defense NATO against cyberattacks, it should be noted that observance of the above criteria of collective self-defense is necessary for the implementation of Article 5 of the NATO Treaty and 51 of the UN Charter. However, it must be emphasized that, in the light of cyberattacks, there are complications of the standard of evidence and their nature, as well as the identification of the attacker, especially when it comes to non-state actors or attacks from third states.

[248] Yoram Dinstein, *War, Aggression and Self-Defence*, 5th edn (Cambridge: Cambridge University Press, 2011), 237.

[249] Ibid. p 241.

[250] "Cited from: L. C. Green, 'Armed Conflict, War, and Self-Defense', 6 Ar.V. 387, 434 (1956–7)", Yoram Dinstein, *War, Aggression and Self-Defence*, 5th edn (Cambridge: Cambridge University Press, 2011), 241.

4. THE STANDARD OF EVIDENCE REQUIRED FOR THE EXERCISE OF COLLECTIVE SELF-DEFENSE AND THE MAIN PROBLEMS OF ATTRIBUTION AND IDENTIFICATION OF THE ATTACKER IN THE CASE OF CYBERATTACK

This chapter will analyze the standards of evidence in international law and how it relates to the application of Article 5 of the NATO Treaty and Article 51 of the UN Charter. In addition, this chapter will analyze the problems of identification and attribution of the attacker from point of view of international law. In conclusion, it will be an assessment of the cyberattacks against members of NATO has already encountered, although Article 5 of the NATO Treaty was not put into effect.

4.1 The standards of evidence in international law

The problem of the identification of the actor of cyberattack is of course primarily a question of fact, but there is a legal matter tied to it: the question of the standard of evidence. The standard of evidence is 'the quantum of evidence necessary to substantiate the factual claims made by the parties'.[251] Evidence is required to prove both the objective (be it an act or an omission) and subjective elements of an internationally wrongful act.

In the cyber context, the state invoking self-defense against cyberattacks will therefore have to demonstrate: (a) that the cyberattack actually occurred and that its scale and effects reached the threshold of an 'armed attack'; and (b) that it was attributable to a certain state or non-state actor.[252]

It is well-known that, while in civil law systems there are no specific standards of proof that judges have to apply as they can evaluate the evidence produced according to their personal convictions, in international law there is classification of standards *ad hoc*, including: (from the most stringent to the least) 1) beyond reasonable doubt, 2) clear and convincing (or compelling) evidence (ie more than probable but short of indisputable) and 3) preponderance of evidence or balance of probabilities (more likely than not, probable).[253] Green also adds a fourth standard, 4) *prima facie* evidence that merely requires indicative proof of the contention.[254] International law

[251] "Cited from: James A Green, 'Fluctuating Evidentiary Standards for Self-Defence in the International Court of Justice', *International and Comparative Law* Quarterly 58 (2009), p 165", Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 97.

[252] Ibid. p. 98.

[253] James A Green, "Fluctuating Evidentiary Standards for Self-Defence in the International Court of Justice", *International and Comparative Law* Quarterly 58 (2009): 167, http://www.jstor.org/stable/20488277?loggedin=true

[254] Ibid. p. 166.

does not prescribe a general standard of evidence for all internationally wrongful acts, and international courts and tribunals have determined their own standards in each case, not always in a consistent manner.[255] The evidentiary standards applicable to the law on the use of force, as with international law more generally, remain extremely unclear.[256] Moreover, in most cases there is no requirement that the standard employed remains the same within a tribunal across its decisions.[257]

4.1.1 *Prima facie* standard of evidence

This represents a test of very low degree with regard to the assessment of evidence: it simply requires that the evidence produced is indicative of the proposition claimed. *Prima facie* evidence supporting the existence of "interventions" conducted by Nicaragua into Honduras and Costa Rica was rejected on the basis that such evidence was insufficient to establish that these constituted armed attacks.[258]

In the Democratic Republic of Congo (*DRC) v Uganda* judgment, the court rejected a "sketch map" provided by the DRC as being inadequate to establish such attacks. The map indicated the presence of Ugandan troops at various positions within the eastern part of the DRC. The map, in conjunction with other available evidence, would meet a low level prima facie test.[259] It should be noted that in this case, the court indicated that media reports and other secondary accounts, including witness statements[260] - was not seen as satisfying the standard of evidence applied by the court. However, it is necessary emphasized that the court in this case adopted a lower standard with regard to whether the actions of the Mouvement de Liberation du Congo and aerial attack at Kitona were similarly armed attacks.[261]

---

[255] James A Green, "Fluctuating Evidentiary Standards for Self-Defence in the International Court of Justice", *International and Comparative Law* Quarterly 58 (2009): 165, http://www.jstor.org/stable/20488277?loggedin=true

[256] Ibid. p. 163.

[257] "Cited from: 9 J Evensen, 'Evidence Before International Courts' (1955) 25 Nordisk Tidsskrift Int'l Ret 44.", Ibid.

[258] Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America), 27 June 1986, para. 109, http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

[259] Armed Activities on the Territory of the Congo (DRC v Uganda), Judgment, 19 December 2005, ICJ Reports 2005 ('*DRC v Uganda*'), para 75, 72, http://www.icj-cij.org/files/case-related/116/116-20051219-JUD-01-00-EN.pdf

[260] Ibid.

[261] James A Green, "Fluctuating Evidentiary Standards for Self-Defence in the International Court of Justice", *International and Comparative Law* Quarterly 58 (2009): 176, http://www.jstor.org/stable/20488277?loggedin=true

Interestingly, in the *Corfu Channel case*, the court said that in certain circumstances, State which has been the victim of a breach of international law but is often unable to furnish direct proof of facts giving rise to responsibility. Such a State should be allowed a more liberal recourse to inferences 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.[262]

4.1.2 Preponderance standard of evidence

This test is preponderance – or, alternatively, a "balance of probabilities" – standard. This refers to evidence that is more convincing than the evidence that is offered in opposition to it, or evidence that establishes that the factual proposition of the relevant party was more likely than not. It has been stated that this standard is predominantly applicable in international procedure. However, this is a difficult claim to make with degree of certainty.

In the *Oil Platform case*, the Court rejected a balance of probabilities approach, and indicative the need for a higher evidentiary standard. Also, the Court held that "the evidence indicative of Iranian responsibility for the attack on the Sea Isle City is not sufficient to support the contentions of the United States.[263]

It should be noted, that standard of prima facie evidence and preponderance would not be enough for justifying the use of force.

4.1.3 Beyond reasonable doubt standard of evidence

Beyond reasonable doubt standard is indisputable evidence, normally used in criminal proceedings. In the *Corfu Channel* Judgment, the ICJ inferences of fact that 'leave *no room* for reasonable doubt' in relation to the minelaying.[264] Roscini argued that a beyond reasonable doubt standard would be unrealistic in the cyber context: "the degree of burden of proof . . . adduced ought not to be so stringent as to render the proof unduly exacting".[265]

---

[262] The Corfu Channel Case, Judgment of 9 April 1949, International Court of Justice, p. 18, http://www.icj-cij.org/files/case-related/1/001-19490409-JUD-01-00-EN.pdf

[263] Case concerning oil platforms (Islamic republic of Iran v. United States of America), 12 December 1996, para. 61, http://www.icj-cij.org/files/case-related/90/090-19961212-JUD-01-00-EN.pdf

[264] The Corfu Channel Case, Judgment of 9 April 1949, International Court of Justice, p. 17, 18, http://www.icj-cij.org/files/case-related/1/001-19490409-JUD-01-00-EN.pdf

[265] "Cited from: Certain Norwegian Loans (France v Norway), Merits, Judgment, 6 July 1957, ICJ Reports 1957,

This standard is a strict standard of proof, requiring that the proposition being presented is supported with evidence of a nature that there can be no "reasonable doubt" as to the factual validity of the proposition. Under this standard, then a proposition must be virtually indisputable, given the evidence. [266]

As argued Green, "expecting a State faced with such a necessity to ensure that it can meet a "beyond a reasonable doubt" standard of proof before responding is wholly unrealistic".[267]

To illustrate, high standard of proof appears to have been used in the Corfu Channel Case, as against the allegation by Britain that the minefield that had damaged British ships was laid with the knowledge and assistance of Albania. The Court concluded that an allegation of such seriousness would warrant a very high degree of certainty which could not be proved by Britain.[268]

4.1.4 Clear and convincing standard of evidence

Falling in between the *prima facie*, preponderance as low level standards and "beyond a reasonable doubt" is often termed the "clear and convincing" evidentiary standard.[269] To prove something by a "clear and convincing" standard, the party with the burden of proof must convince the arbiter in question that it is *substantially* more likely than not that the factual claims that have been made are true. This is obviously a more onerous test than a mere *prima facie* or preponderance standard, but does not require the virtual certainty of the "beyond a reasonable doubt" test.

The ICJ has repeatedly demonstrated that, with regards to evidentiary standards, the context of each dispute will be an important factor. Green worthy noted that the evidentiary standard for establishing the factual basis for one claim of self-defense should be the same as for any other self-defense claim, and, if possible, that standard should be explicit.

Separate Opinion of Judge Sir Hersch Lauterpacht, p 39", Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 102.

[266] James A Green, "Fluctuating Evidentiary Standards for Self-Defence in the International Court of Justice", *International and Comparative Law* Quarterly 58 (2009): 167, http://www.jstor.org/stable/20488277?loggedin=true

[267] Ibid. p. 173.

[268] Rules of evidence before the international court of justice' (Lawteacher.net, April 2018), https://www.lawteacher.net/free-law-essays/international-law/rules-of-evidence-before-the-international-court-of-justice-international-law-essay.php?vref=1

[269] "Cited from: Brown (n 17) 99-100", James A Green, 'Fluctuating Evidentiary Standards for Self-Defence in the International Court of Justice', *International and Comparative Law* Quarterly 58 (2009): 167, http://www.jstor.org/stable/20488277?loggedin=true

"Clear and convincing evidence" standard was employed in the both the *Nicaragua* and the *Oil Platform* decisions. For example, in the *Nicaragua* decision the Court stated that "it must attain some degree of certainty regarding the claim of United States that El Salvador had suffered an armed attack and ensure that the facts on which it is based are *supported by convincing evidence*".[270] Also, the Court asserted that there was "no clear evidence of the United States having such a degree of control".[271]

In the *Oil Platforms* decision, the Court took the view that available evidence regarding the Iranian responsibility for the mine that struck the *US Samuel B Roberts* – being that it was surrounded by other moored mines bearing serial numbers attributable to Iran – was "highly suggestive, but not conclusive".[272]

The Court's approach to evidence is certainly indicative of reliance, in both *Nicaragua* and *Oil Platforms*, upon a "clear and convincing" standard, rather a prima facie or preponderance standard, or the converse "beyond a reasonable doubt" approach.[273] Green argued that, a "clear and convincing" standard appears particularly appropriate in the context of self-defense.[274] Also, O'Connell pointed out that there are indications that claims related to *jus ad bellum* violations, in particular in relation to the invocation of self-defense against an armed attack, require "clear and convincing evidence".[275] Marie Jacobsson pointed that the right of self-defense does not require evidence. The existence of the incident that gives rise to self-defense does. The kind of evidence that is needed depends on the situation. If a state claims that it is taking measures of self-defense in response to an overwhelming and immediate threat, evidence-at least of political character-is crucial. If the response has caused a dispute, such as in the Case concerning *Oil Platforms*, the

[270] Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America), 27 June 1986, para. 29, http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

[271] Ibid. para. 109.

[272] Case concerning oil platforms (Islamic republic of Iran v. United States of America), 12 December 1996, para. 71, http://www.icj-cij.org/files/case-related/90/090-19961212-JUD-01-00-EN.pdf

[273] James A Green, "Fluctuating Evidentiary Standards for Self-Defence in the International Court of Justice", *International and Comparative Law* Quarterly 58 (2009): 173, http://www.jstor.org/stable/20488277?loggedin=true

[274] Ibid.

[275] "Cited from: Mary Ellen O'Connell, 'Evidence of Terror', Journal of Conflict and Security Law 7 (2002), pp 22 ff", Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 98.

evidence required is of a formal, procedural character since it will be subject to evaluation in a court procedure.[276]

In the *DRC v Uganda* judgment, the court referenced different standards at points of the judgment with regard to the same question (that of the existence of an armed attack, be it an armed attack against Uganda, or, in the context of counter-claim, against DRC).[277] The ICJ held that: "Ugandan action in the eastern part of the DRC needed to have been "*convincingly* established by the evidence".[278]

When justifying its 2001 armed operation against Afghanistan, the US Permanent Representative to the United Nations referred to the fact that the US government had 'clear and compelling information that the Al-Qaeda organization, which is supported by the Taliban regime in Afghanistan, had a central role in the [11 September 2001] attacks'.[279] The same NATO's Secretary-General was stated.[280] NATO members heard the U.S. evidence regarding Afghanistan and found it "compelling".[281]

In the context of the proposed intervention to react against the alleged use of chemical weapons by the Syrian government, the US President stated that attacking another country without a UN mandate and without 'clear evidence that can be presented' would raise questions of international law.[282]

---

[276] Marie Jacobson, Evidence as an Issue in International Legal Practice, Notre Dame Law School NDLScholarship, (2006): 42.

[277] James A Green, "Fluctuating Evidentiary Standards for Self-Defence in the International Court of Justice", *International and Comparative Law* Quarterly 58 (2009): 174, http://www.jstor.org/stable/20488277?loggedin=true

[278] Armed Activities on the Territory of the Congo (DRC v Uganda), Judgment, 19 December 2005, ICJ Reports 2005 ('*DRC v Uganda*'), para 72, http://www.icj-cij.org/files/case-related/116/116-20051219-JUD-01-00-EN.pdf

[279] Letter dated 7 October 2001 from the Permanent Representative of the United States of America to the United Nations Addressed to the President of the Security Council, UN Doc S/2001/946, 7 October 2001, accessed 2018 2018 May 3, http://dag.un.org/handle/11176/31401

[280] Statement at NATO Headquarters, 2 October 2001, https://www.nato.int/docu/pr/2001/p01-124e.htm

[281] "Cited from: William Drozdiak & Rajiv Chandrasekaran, NATO: U.S. Evidence on Bin Laden "Compelling"; Allies Give Unconditional Support for Retaliatory Strikes; Taliban Official Asks to see Proof, WASH. POST, Oct. 3, 2001", Mary Ellen O'Connell, 'Rules of Evidence for the Use of Force in International Law's New Era', *America Society of International Law Proceedings* 100 (2006): 47.

[282] Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 99.

In the *Genocide* case, the ICJ confirmed that: "claims against a State involving charges of exceptional gravity must be proved by evidence that is fully conclusive. . . . The same standard applies to the proof of attribution for such acts".[283]

In *Ethiopia-Eritrea Jus Ad Bellum Claim*, decided on December 19, 2005, the Eriteria-Ethiopia Claims Commission referenced a standard of "clear" evidence: "it is clear from the evidence that these incidents involved geographically limited clashes between small Eritrean and Ethiopian patrols along a remote, unmarked, and disputed border".[284]

In the NATO CCDCOE Report on Georgia concludes that: "there is no conclusive proof of who is behind the DDoS attacks, even though finger pointing at Russia is prevalent by the media".[285]

In a Senate questionnaire in preparation for a hearing on his nomination to head of the new US Cyber Command, General Alexander argued that: 'some level of mitigating action' can be taken against cyberattacks 'even when we are not certain who is responsible'.[286]

Such evidence standard needs establishment not to penalize the claimant, but to protect the defendant against false attribution, which, thanks to tricks like IP spoofing, onion routing and the use of botnets, is a particularly serious risk in the cyber context.

A report prepared by Italy's Parliamentary Committee on the Security of the Republic goes further and requires to demonstrate 'unequivocally' that an armed attack by cyber means originated from a state and was instructed by governmental structures. The document also suggests that state attribution needs 'irrefutable digital "evidence", which—the Report concedes—is a condition very difficult to meet.[287]

Roscini pointed out that "clear and convincing evidence seems the appropriate standard not only for claims of self-defense against traditional armed attacks, but also for those against cyber operations: a *prima facie* or preponderant standard of evidence might lead to specious claims and

---

[283] Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro) Judgment of 26 February 2007, http://www.icj-cij.org/files/case-related/91/091-20070226-JUD-01-00-EN.pdf

[284] Mary Ellen O'Connell, 'Rules of Evidence for the Use of Force in International Law's New Era', *America Society of International Law Proceedings* 100 (2006): 45.

[285] "Cited from: Tikk, Kaska, Rünnimeri, Kert, Talihärm, and Vihul, Cyber Attacks, p 12", Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014):100.

[286] Ibid.

[287] "Cited from: *Relazione sulle possibili implicazioni*, p 26". Ibid. p.101.

false attribution, while a beyond reasonable doubt standard would be unrealistic. However, reasonable states neither respond precipitously on the basis of sketchy indications of who has attacked them nor sit back passively until they have gathered unassailable evidence".[288]

The clear and convincing evidence standard for cyber operations was criticized and relied on the fact that, due to the speed at which such operations may occur and produce their consequences, the requirement of a high level of evidence may, in fact, render impossible for the victim state to safely exercise its right of self-defense. However, it should be noted that if the cyberattack is continuing or is formed by a series of smaller-scale cyberattacks, the significance of clear and convincing evidence would considerably increase.

4.1.5 Burden of proof

The standard of evidence should be distinguished from the burden of proof, which (when narrowly intended) only identifies the litigant that has the onus of meeting that standard.[289] It is normally the party that relies upon a certain fact that is required to prove it (*onus probandi incumbit actori*).[290]

In the *Corfu Channel* case, the ICJ found that evidence is located exclusively on the territory of one party does not result in a reversal of the burden of proof.[291] Moreover, the fact that evidence is contained in classified documents, as is often the case in the cyber context, does not result in a reversal of the burden of proof: in both the *Genocide* and *Corfu Channel* cases, the ICJ did not demand the production of classified documents by the respondent states, attracting however the criticism of the minority judges.[292]

Mary Ellen O'Connell worthy pointed that we generally know which party carries the burden, but we do not know with certainty what the burden is.[293]

---

[288] Ibid. p. 102.

[289] James A Green, "Fluctuating Evidentiary Standards for Self-Defence in the International Court of Justice", *International and Comparative Law* Quarterly 58 (2009): 165, http://www.jstor.org/stable/20488277?loggedin=true

[290] Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America), 27 June 1986, para. 101, http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

[291] The Corfu Channel Case, Judgment of 9 April 1949, International Court of Justice, p. 18, http://www.icj-cij.org/files/case-related/1/001-19490409-JUD-01-00-EN.pdf

[292] "Cited form: Tsagourias, 'Cyber Attacks', p 235. See the Dissenting Opinion of Vice-President Al-Khasawneh appended to the Genocide Judgment, para 35", Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 103.

[293] Mary Ellen O'Connell, "Rules of Evidence for the Use of Force in International Law's New Era", *America Society of International Law Proceedings* 100 (2006): 44.

4.2 Attribution and identification of the attacker

Modern international law regulates the right to collective self-defense, includes the necessary requirements for its implementation, and establishes the necessary standards of evidence to justify the use of force. However, modern international law does not have the tools to carry out the identification of the attacker, especially in the case of cyberattacks, because it is not a purpose for international law. Basically, this is the competence of technical experts, methodologies and special programs. However, for effective identification and attribution, there must be a relationship between the international legal instrument and technical features in cyberspace. The author of the master thesis will research on legal features of identification and attribution of the attacker as one of the important elements of the fulfillment of the right to self-defense.

4.2.1 Identification of the attacker

No form of self-defense may be exercised without adequate proof of the origin or source of the attack and without convincing proof that a particular state or states or organized group is responsible for conducting or controlling the attack. International law does not have hard rules on the level of proof required, but practice and case law require sufficient certainty on the origin of the attack and the identity of the author of the attack before action can be taken. This requirement can therefore also be an obstacle to self-defense in response to a cyberattack.[294]

Identification of the originator of an attack has often been a difficult problem, especially when the intruder has used a number of intermediate relay points, when he has used an "anonymous bulletin board" whose function is to strip away all information about the origin of messages it relays, or when he has used a device that generates false origin information. Progress has been made, however, in solving the technical problem of identifying the originator of computer messages, and reliable identification of the computer that originated a message may soon be routinely available.[295]

Locating the computer used by the intruder does not entirely solve the attribution problem, however, since it may have been used by an unauthorized person, or by an authorized user for an unauthorized purpose. A parent may not know that the family computer is being used for

[294] Cyber Warfare, No 77, AIV / No 22, CAVV December (2011): 22, https://aiv-advies.nl/download/da5c7827-87f5-451a-a7fe-0aacb8d302c3.pdf

[295] An Assessment of International Legal Issues in Information Operations, Department of Defense Office of General Counsel of United States, (1999): 21, accessed 2018 May 3, http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf

unlawful attacks on government computer systems. Universities, businesses, and other government agencies may be similarly unaware that their computer systems are being misused. The owner of a computer system may have some responsibility to make sure it is not being used for malicious purposes.[296]

Similarly, characterization of an intruder's intentions may be difficult. Nevertheless, such factors as persistence, sophistication of methods used, targeting of especially sensitive systems, and actual damage done may persuasively indicate both the intruder's intentions and the dangers to the system in a manner that would justify use of right of collective self-defense. As with attribution, there may be useful intelligence on this issue from other sources, or it may be possible to reliably infer the intent of the intruder from the relationship of the attack to other events.[297]

A determination that an intrusion comes from a foreign country is only a partial solution to the identification problem, since the attack may or may not be state-sponsored. State-sponsored attacks may well generate the right of self-defense. State sponsorship might be persuasively established by such factors as "*signals or human intelligence, the location of the offending computer within a state-controlled facility, or public statements by officials*. In other circumstances, state sponsorship may be convincingly inferred from such factors as the *state of relationships between the two countries, the prior involvement of the suspect state in computer network attacks, the nature of the systems attacked, the nature and sophistication of the methods and equipment used, the effects of past attacks, and the damage which seems likely from future attacks"*.[298]

The above views seem to suggest an evidentiary standard lower than clear and convincing evidence on the basis that identification and attribution are more problematic in a digital environment than in the analogue world.[299]

Also, AIV/CAVV Report on Cyber Warfare worthy noted that: "in cyber warfare, unlike conventional forms of warfare, it will be often difficult to identify the origin and the author of the attack with sufficient certainty to justify a military response. In view of the high risk of error

[296] Ibid.

[297] Ibid.

[298] Ibid.

[299] "Cited from: David E Graham, 'Cyber Threats and the Law of War', Journal of National Security Law and Policy 4 (2010), p 93", Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 101.

and the political, legal and humanitarian consequences, *reliable intelligence* is required before a military response can be made to a cyberattack. However, the author of an armed attack can also be identified using non-technological means, especially in the case of a large-scale cyberattack that has a similar impact to a conventional armed attack".[300]

In the case when interests of state A are damaged by the private conduct of an individual who acts within the territory of another state B, state A will notify the government of state B and request its cooperation in putting a stop to such conduct.[301]

Only if the requested nation is unwilling or unable to prevent recurrence the doctrine of self-defense permit the injured nation to act in self-defense inside the territory of another nation. The U.S. cruise missile strikes against terrorists camps in Afghanistan on 20 August 1998 provides a close analogy in which the United States attacked camps belonging to a terrorist group located in the territory of a state which had clearly stated its intention to continue to provide a refuge for the terrorists.[302]

It should be noted that in some circumstances the National Command Authority (NCA) of US might decide to defend U.S. information systems by attacking a computer system overseas, and take the risk of having to make an apology or pay compensation to the offended government. Among the factors the NCA would probably consider would be the danger presented to U.S. national security from continuing attacks, whether immediate action is necessary, how much the sanctuary nation would be likely to object, and how the rest of the world community would be likely to respond.[303]

4.2.2 The role of the third states in the territory where a cyberattack occurred in the identification of attacker

Cyberattack by attacker can be attributed to the state from where they originate if this state is unable or unwilling to prevent or terminate the attacks. Only when the territorial state is

[300] Cyber Warfare, No 77, AIV / No 22, CAVV December 2011, 22, https://aiv-advies.nl/download/da5c7827-87f5-451a-a7fe-0aacb8d302c3.pdf

[301] An Assessment of International Legal Issues in Information Operations, Department of Defense Office of General Counsel of United States, (1999): 22, accessed 2018 May 3, http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf

[302] Ibid.

[303] Ibid. p. 23.

unaware of the terrorist actions conducted from its territory does it avoid attribution.[304] In the cyber context, this approach seems to have been adopted by the Head of the US Cyber Command, General Keith Alexander, where he states that: "every government is responsible for actions originating in its own country".[305]

The 2015 Report of the Group of Governmental Experts created by the UN General Assembly also concluded that states "should seek to ensure that their territories are not used by non-State actors for unlawful use of ICTs" (Information and Communications Technologies).[306]

The inability or unwillingness of the territorial state to prevent the attacks originating from its territory is what makes the reaction in self-defense in the territory of that state necessary.[307]

The intervening state should first try to secure the cooperation of the territorial state and request that it put an end to the attack originating from its territory or, alternatively, that it allow the victim state to do so, unless such request appears futile or immediate action is required.[308]

The unable/unwilling standard is one of due diligence.[309] This is particularly evident in the cyber context, where strict liability would be an unacceptable high burden on states, considering the difficulty of preventing cyber intrusions and the ease with which computers can be remotely controlled and identities spoofed.[310]

The UN General Assembly has recommended that:

"(a) States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies;

---

[304] "Cited from: Tams, 'The Use of Force', pp 385–6", Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 81.

[305] "Cited from: Responses to advance questions, Nomination of Lt Gen Keith Alexander, p 25", ibid.

[306] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Assembly, A/70/174, 2015, https://ccdcoe.org/sites/default/files/documents/UN-150722-GGEReport2015.pdf

[307] Claus Kress, 'Some Reflections on the International Legal Framework Governing Transnational Armed Conflicts', *Journal of Conflict and Security Law* 15 (2010): 250.

[308] "Cited from: Deeks, ' "Unwilling or Unable" ', pp 521–5", Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 86.

[309] Ibid. p. 87.

[310] Eric Talbot Jensen, "Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense", *Stanford Journal of International Law* 38 (2002): 236–7.

(b) Law enforcement cooperation in the investigation and prosecution of international cases of criminal misuse of information technologies should be coordinated among all concerned States;

(c) Information should be exchanged between States regarding the problems that they face in combating the criminal misuse of information technologies;

(d) Law enforcement personnel should be trained and equipped to address the criminal misuse of information technologies;

(e) Legal systems should protect the confidentiality, integrity and availability of data and computer systems from unauthorized impairment and ensure that criminal abuse is penalized;

(f) Legal systems should permit the preservation of and quick access to electronic data pertaining to particular criminal investigations;

(g) Mutual assistance regimes should ensure the timely investigation of the criminal misuse of information technologies and the timely gathering and exchange of evidence in such cases;

(h) The general public should be made aware of the need to prevent and combat the criminal misuse of information technologies;

(i) To the extent practicable, information technologies should be designed to help to prevent and detect criminal misuse, trace criminals and collect evidence.

(j) The fight against the criminal misuse of information technologies requires the development of solutions taking into account both the protection of individual freedoms and privacy and the preservation of the capacity of Governments to fight such criminal misuse".[311]

4.2.3 Attribution to the attacker

In 1987, the Iran-United States Claims Tribunal asserted that 'in order to attribute an act to the State, it is necessary to identify with reasonable certainty the actors and their association with the State'.[312] The second part of this construction – the association of a natural person with a State – is legally governed by Part One, Chapter II of the International Law Commission (ILC)

[311] UN General Assembly, Resolution, A/Res/55/63, 2001, Combating the criminal misuse of information Technologies, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf

[312] "Cited from*: Yeager v Islamic Republic of Iran*, (1987) U.S.C.T.R 17, 92, 101-2", Katharina Ziolkowski, *Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy* (Tallinn, Estonia: NATO CCD COE Publications, 2013), 623.

Draft Articles on Responsibility of States for Internationally Wrongful Acts (ILC Articles on State Responsibility), Articles 4 to 11.[313]

The crucial problem is rather hinted at in the first part of the the Iran-United States Claims Tribunal's assertion: the identification of the actor. As the technical peculiarities of cyberspace make it entirely possible to hide one's own identity and to obliterate the traces of one's actions. If it cannot be determined which individual has acted, then the provisions on the attribution of such conduct found in the Articles on State Responsibility are not of much use.[314]

Thus, the ensuing question must be what are the requirement to produce 'clear and convincing' evidence means in the cyber context. The problem of sufficiently proved authorship remains the most critical and to date unresolved obstacle in the application of the traditional regime of self-defense in the context of cyberspace. The reason for this has not changed: cyber infrastructure was never designed for tracking and tracing user behaviour.[315] Furthermore, software, either 'benign' or 'malicious', consists of nothing but code which, as a representation of data, is entirely capable of being manipulated in just about any measure.[316]

Scott J. Shackelfold noted that this is not the only problem – system vulnerabilities, but also include the facts that: the Internet was never designed to track or trace users, or resist untrustworthy users; a packet's source address itself is untrustworthy and is easily masked; and there are myriad strategies that hackers employ making tracking difficult, such as tunneling and the destruction of data logs.[317]

The current architecture of the internet and connected networks provides countless loopholes and methods to mask a user's identity or location; online identities and servers can be hidden, data packet flows and connections can be masked and redirected through multiple

[313] Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, 2001, http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf

[314] Katharina Ziolkowski, *Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy* (Tallinn, Estonia: NATO CCD COE Publications, 2013), 623.

[315] "Cited from: Lipson, 2002, Tracking and Tracing Cyber Attacks: Technical Challenges and Global Policy Issues, Carnegie Mellon Software Engineering Institute, available at: http://www.sei.cmu.edu/library/abstracts/reports/02sr009.cfm, 13-15", Ibid. p. 625.

[316] "Cited from: Gaycken, Krieg der Rechner, Internationale Politik, März/April 2011, 88, 92", Ibid.

[317] Scott J. Shackelford, "State Responsibility for cyberattacks: competing standards for a growing problem", University of Cambridge, UK, CCD COE Publications, Talinn, Estonia, (2010): 200, https://ccdcoe.org/sites/default/files/multimedia/pdf/Shackelford%20-%20State%20Responsibility%20for%20Cyber%20Attacks%20Competing%20Standards%20for%20a%20Growing%20Problem.pdf

servers, and an attacker can hijack a machine belonging to an unaware, innocent individual or organization in order to use it as a basis for launching cyberattacks.[318]

Because of those characteristics, reasonably sophisticated attackers will most often be able to effectively hide their traces. Even if an attacking computer can be located with sufficient certainty, what remains is the factor which commentators have called the 'human machine gap' or 'entry-point anonymity': the location of a computer rarely allows for definite conclusions regarding the identity of the individual operating the machine, and it is the latter's status that ultimately determines attribution pursuant to Articles 4 to 11 of the ILC Articles on State Responsibility.[319]

However, it should be noted that the failure of a State to take feasible measures to terminate harmful cyber operations originating in its territory constitutes an internationally wrongful omission by that State (due diligence). The feasible measures to terminate harmful cyber operations by State in own territory will give possibility make all necessary acts for attribution of the attacker. Such instruments of identification and attribution of the attacker are limited to the victim State which authority located outside the territory where was originated cyberattack.

Attribution is appropriate in a number of circumstances. The clearest case is when State organs, such as the military or intelligence agencies, engage in the wrongful acts.[320] For instance, all cyber activities of US Cyber Command or the National Security Agency are fully attributable to the US and engage its responsibility under international law.

The fact that a harmful cyber operation has been mounted using private cyber infrastructure, or has simply been routed through governmental or non-governmental cyber infrastructure in a State's territory, does not suffice to indicate association.[321] As an illustration, in 2013 a North Korean cyber operation shut down thousands of South Korean media and banking computers and servers. The operation employed more than 1,000 Internet Protocol (IP)

---

[318] "Cited from: Information Warfare Monitor, op. cit., 12", Katharina Ziolkowski, *Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy* (Tallinn, Estonia: NATO CCD COE Publications, 2013), 625.

[319] Ibid.

[320] Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, 2001, 668, http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf

[321] Michael N. Schmitt, "Cyber Activities and the Law of Countermeasures", *Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy* (Tallinn, Estonia: NATO CCD COE Publications, 2013), 668.

addresses in 40 countries. Obviously, most, if not all, of the countries involved were completely unassociated with the operation.[322]

Acts committed by persons or entities that do not qualify as State organs, but which are empowered by domestic law to exercise elements of governmental authority, are equally attributable to the State, albeit only with respect to the exercise of said authority (for example Computer Emergency Response Team (CERT). [323] Article 8 of the Articles on State Responsibility provides: "the conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of that State in carrying out the conduct".[324]

Moreover, responsibility of States arise when: State aiding the commission of an internationally wrongful act by another will bear responsibility if it does so knowing the circumstances surrounding the unlawful act, if it finances the operation (with knowing that those capabilities).

However, situations involving State organs or those exercising governmental functions, attribution based on direction and control does not extend to acts exceeding the direction. In other words, acts that clearly exceed the State's instructions do not result in attribution.[325]

There is one more problem related to situation when cyberattack, reaching the threshold of an armed attack within the scope of Article 5 of NATO Treaty and Article 51 of the UN Charter only several years after the event, could the victim have responded with force invoking self-defense after such a period of time?

Robin Geib and Henning Lahmann were considering this position that: "it has been observed that such a reading of the immediacy criterion 'undermines the temporal dimension of

[322] "Cited from: Lance Whitney, North Korea Behind March Cyber Attack, says South Korea, C/NET , Apr. 10, 2013, http://news.cnet.com/8301-1009_3-57578829-83/north-korea-behind-march-cyberattack-says-south-korea", Ibid.

[323] "Cited from: Articles on State Responsibility, supra note 13, Article 5. Note that pursuant to Article 6, if the organ of a State is placed at the disposal of another State to exercise elements of governmental authority, the conduct of that organ is attributable to the latter. In such a case, only the State which the organ was placed at the disposal of bears responsibility for the actions. Articles on State Responsibility Commentary, supra note 28, at 145", Ibid. p. 669.

[324] Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, 2001, http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf

[325] Ibid.

self-defense and risks turning a temporal right into an open-ended licence to use force".[326] In particular within the cyber context, the issue of uncertain attribution together with a softening of the immediacy requirement could critically raise the danger of escalation of inter-State conflict. They suggested that: "the community of States should continue to demand a more stringent temporal proximity between an armed attack and its response invoking self-defense".[327]

However, the recently completed position of Group of Experts point to the requirement of immediacy for self-defense to be permitted, meaning the period of time following the execution of an armed attack within which the victim State may reasonably respond in self-defense, with one relevant factor *inter alia* being 'the period necessary to identify the attacker. In cases where the initiator of the attack is not identified until well after the attack' the criterion of immediacy will usually not be met. However, they suggests that this conclusion may change if there is reason for the victim State to believe that 'further cyber operations are likely to follow' – in that case, the State 'may treat those operations as a "cyber campaign" and continue to act in self-defense.[328]

The author of the thesis fully agrees with this position of Group of Experts regarding the time for fulfilling the right to self-defense.

To determine attribution, it is necessary to pay attention on cyberattacks committed by non-state actors, but when they are under state control or perform state's function. There are two primary legal regimes of State responsibility for cyberattacks that could mitigate such State sponsorship: the effective and overall control standards. In brief, the effective control doctrine in the ICJ *Nicaragua* case, recognizes a country's control over paramilitaries or other non-State actors only if the actors in question act in "complete dependence" on the State.[329] In contrast, the overall control doctrine, illustrated in the ICTY *Tadic* case, held that where a State has a role in

[326] Robin Geib and Henning Lahmann, "Freedom and Security in Cyberspace: Shifting the Focus away from Military Responses towards Non-Forcible Countermeasures and Collective Threat-Prevention", *Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy* (Tallinn, Estonia: NATO CCD COE Publications, 2013): 627.

[327] Ibid.

[328] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (UK: Cambridge University Press, 2017), 354.

[329] Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America), 27 June 1986, para. 176, http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

organizing and coordinating, in addition to providing support for a group, it has sufficient overall control doctrine such that the group's acts are attributable to the State.[330]

4.2.3.1 Effective control standard of responsibility of state

The first standard that the courts have created is the ICJ *Nicaragua* effective "operational control" standard. Nicaragua requires that a country's control over paramilitaries or other non-State actors can only established if the actors in questions act in "complete dependence" on the State.[331] The majority interpreted the decision of the ICJ as requiring the government of a State to exercise "effective" control over the operations of a military force and the appropriate standard to apply at least in the paramilitary context of that case.

As argued Scott J. Shackelford, *"State sponsors of cyberattacks would be held accountable for their involvement would be if their effective control could be proven any doubt".*[332] He pointed that: "in a sophisticated global cyberattack, missing or corrupted data commands may be sufficient to disprove State control and defeat accountability. Without either new techniques such as the probabilistic tracing, or unsophisticated hackers, effective control would in essence give a free pass to State sponsors of cyberattacks".[333]

There are other important in this case formulation with regards to proving State responsibility for cyberattacks: "most grave" and "less grave" categories.[334] However, as noted Scott J. Shackelford: "this doctrine could give low-level cyberattacks and could invoke law enforcement, and not the armed forces".[335]

---

[330] Tadic Case, International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia since 1991, http://www.icty.org/x/cases/tadic/acjug/en/tad-aj990715e.pdf

[331] Scott J. Shackelford, "State Responsibility for cyberattacks: competing standards for a growing problem", University of Cambridge, UK, CCD COE Publications, Talinn, Estonia, (2010): 201, https://ccdcoe.org/sites/default/files/multimedia/pdf/Shackelford%20-%20State%20Responsibility%20for%20Cyber%20Attacks%20Competing%20Standards%20for%20a%20Growing%20Problem.pdf

[332] Ibid.

[333] Ibid. p. 202.

[334] Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America), 27 June 1986, para. 101, http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

[335] Scott J. Shackelford, "State Responsibility for cyberattacks: competing standards for a growing problem", University of Cambridge, UK, CCD COE Publications, Talinn, Estonia, (2010): 202, https://ccdcoe.org/sites/default/files/multimedia/pdf/Shackelford%20-%20State%20Responsibility%20for%20Cyber%20Attacks%20Competing%20Standards%20for%20a%20Growing%20Problem.pdf

4.2.3.2 Overall control standard of responsibility of state

The second standard is the ICTY *Tadic* "overall control" standard. The ICTY held that where a State has a role in organizing and coordinating, in addition to providing support for a group, it has sufficient overall control, and the group's acts are attributable to the State.

The most recent case was the *Application of the Genocide Convention ("Bosnian Genocide"),* where the Court adopted the effective control rather than the overall control standard in deciding that Bosnia lacked the specific intent to commit genocide. The standard laid down by the Court was beyond *any* doubt, not beyond a *reasonable* doubt.[336]

In its judgment on genocide in Bosnia, ICJ after satisfying itself that the Bosnian Serb armed forces had perpetrated genocide in Srebrenica, and only there, discussed a crucial question – whether, as claimed by Bosnia, those armed forces had in reality acted on behalf of the Federal Republic of Yugoslavia (FRY), in which case responsibility for genocide would have to be attributed to that state.[337]

ICJ rejected the "overall control" test resorted in *Tadic Case*, because if it can possibly be applicable when determining whether an armed conflict is international, is 'unpersuasive' if used to establish whether a state is responsible for acts performed by armed forces and paramilitary units that are not among its official organs. For the Court, the reason why *Tadic* test is 'unpersuasive' is twofold: 1) 'logic does not require the same test to be adopted in resolving the two issues, which are very different in nature', 2) the 'overall control' test overly broadens the scope of state responsibility because it goes beyond the three standards set out by the ILC in Article 8 of the Articles on State Responsibility.[338]

In *Tadic Case*, the Chamber first noted that: "it seemed logical to think that, for armed units fighting within a state to 'belong ' to another state, it was necessary for this latter state to wield some "degree of authority or control' over those armed units (para. 97)". It added that the necessary criteria were consequently to be found in those general rules of international law that

[336]Ibid.

[337] Antonio Cassese, "The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia", *European Journal of International Law*, Volume 18, Issue 4, 1, (2007): 650, https://academic.oup.com/ejil/article/18/4/649/453762

[338] Ibid. p. 651.

establish when individuals may be regarded as acting as de facto state officials: these rules, the Appeals Chamber noted, belonged to *the body of law on state responsibility.*[339]

Antonio Cassese worthy noted that ICJ did not do justice to Tadić either. The ICTY had held the view that the 'overall control' test was also applicable to state responsibility. To prove the ICTY wrong, ICJ should not have simply dismissed that test as solely applicable to the question of classification of armed conflict.[340]

Judge Antonio Cassese, the first President of the Hague Tribunal rejected the *Bosnian Genocide* judgment as demanding an effective control standard is unrealistically high standard of proof.[341] This burden of proof is nearly impossible to satisfy in the context of cyberspace without major improvements in the tracing of cyberattacks.

Scott J. Shackelford worthy noted that it is far too easy for governments to hide their information about cyberattacks under the effective control standard. It should thus be sufficient as matter of international law to prove overall control by a government in a cyberattack, rather than effective control.[342]

For example, if the overall control standard were used instead of effective control, it would be possible that Russia or Chinese incitement behind the cyberattacks on Estonia, Georgia, or the United States.[343]

4.3 Opponent Use of Force as cyberattacks and potential threats against NATO

During the 2007 cyberattack on Estonia, several Estonian officials raised the issue of whether Article 5 of the NATO Treaty could be invoked, which maintains that an assault on one allied country obligates the alliance to attack the aggressor. This was the first time in NATO

[339] Ibid. p. 652.

[340] Ibid. p. 667-668.

[341] Scott J. Shackelford, "State Responsibility for cyberattacks: competing standards for a growing problem", University of Cambridge, UK, CCD COE Publications, Talinn, Estonia, (2010): 202, https://ccdcoe.org/sites/default/files/multimedia/pdf/Shackelford%20-%20State%20Responsibility%20for%20Cyber%20Attacks%20Competing%20Standards%20for%20a%20Growing%20Problem.pdf

[342] Ibid. p. 204.

[343] Ibid.

history that a member State had formally requested emergency assistance in the defense of its digital assets.[344]

Estonia did receive limited help that it requested from NATO. Further assistance was unavailable since NATO and the international community alike viewed the 2007 cyberattacks on Estonia as an instance of cybercrime, or cyber terrorism.[345]

Scott J. Shackelford was considering that it was two primary reasons. *First*, the attacks were not serious enough to constitute an armed attack thus activating NATO Article 5. *Second*, State responsibility for the attacks could not be conclusively proven. NATO has taken steps to address the gaps in cyber security strategy that the cyberattacks on Estonia underscored, such as by creating NATO CCD COE in Tallinn, Estonia, and the new Cyber Defense Management Authority (CDMA) in Brussels, which is a NATO effort to centralize cyber defense capabilities.[346]

It is critical for NATO's future efforts in cyber security for its member States to have a comprehensive and settled standard to gauge State responsibility for cyberattacks. Specialists at the CDMA, or at the various CERTs of the member States, will not be able to gather the necessary intelligence to prove which nation or group launched a given cyberattack if the standard of proof itself is left undefined.

Cyber collective defense has become a central component of NATO planning. US intelligence sources assess that any unclassified NATO network that is directly connected to the internet should be considered potentially compromised and that cyber espionage is the principle threat to NATO systems. They also assess that Russia, given its record of effective cyber collection, poses the greatest espionage threat to NATO computer networks.[347]

The doctrine of today's potential opponents includes plans to use cyberattacks to shape the initial phases of conflict and disrupt NATO's response. Strikes against civilian targets risk escalating any conflict, but an opponent may judge the risk of escalation to be acceptable if the

---

[344] Hughes, R. B. 2009, April, NATO and Cyber Defence: Mission Accomplished?. NATO-OTAN, https://www.atlcom.nl/ap_archive/pdf/AP%202009%20nr.%201/Hughes.pdf

[345] "Cited from: Koms, S. W. & Kastenberg, J. E., 2008, Georgia's Cyber Left Hook, Parameteres, U.S. Army War College, Quarterly, 38, 60-76",Scott J. Shackelford, "State Responsibility for cyberattacks: competing standards for a growing problem", University of Cambridge, UK, CCD COE Publications, Talinn, Estonia, (2010): 202.

[346] Ibid. p. 205.

[347] James A. Lewis, "The Role of Offensive Cyber Operations in NATO's Collective Defence", *The Tallinn Papers*, NATO CCD COE, Publication on Strategic Cyber Security, (2015): 8, 1, https://ccdcoe.org/sites/default/files/multimedia/pdf/TP_08_2015_0.pdf

context for cyberattack is an offensive against a smaller nation, such as a Baltic country, that it plans to rapidly overrun and occupy.[348]

Moreover, we need take in an account that NATO's potential opponents will use cyber techniques in new ways, in what some have called "hybrid warfare" (Georgia and Ukraine case).[349] These include countries traditionally of concern to NATO, but cyber threats could also come from new actors, such as Iran or North Korea, and proxy or non-state actors such as the Syrian Electronic Army. These nations and groups, using cyber techniques, now have new ways to strike NATO countries.[350]

Opponents seek to circumvent NATO military power and use a blend of political action and "influence operations", special forces, proxies and irregular units, unconventional tactics and cyber techniques to apply force to gain their ends. Cyber techniques for political action and "influence operations" are not intended to destroy or disrupt, but rather to put coercive political pressure on targets. This new style of warfare will challenge planning for mutual defense.[351]

Cyber operations used for coercive effect create uncertainty and concern within the target government. The knowledge that an attacker may have infiltrated their networks, is monitoring communications, and perhaps considering even more damaging actions, can have a paralysing effect. The vast majority of these cyber operations are likely to fall below the level of an armed attack, even under the new NATO guidelines, complicating any response.[352]

Understanding the potential threats from particular countries against NATO makes it possible to react quickly during identification and attribution of the attacker, thus applying the right to collective self-defense.

---

[348] Ibid. p. 4.

[349] Michael Miklaucic, 'NATO Countering the Hybrid Threat' (23 September 2011), available at http://www.act.nato.int/nato-countering-the-hybrid-threat

[350] James A. Lewis, "The Role of Offensive Cyber Operations in NATO's Collective Defence", *The Tallinn Papers*, NATO CCD COE, Publication on Strategic Cyber Security, (2015): 8, 3, https://ccdcoe.org/sites/default/files/multimedia/pdf/TP_08_2015_0.pdf

[351] Ibid.

[352] Ibid. p. 6.

CONCLUSIONS

1. **Cyberattacks as "Armed Attack"**. Modern international law does not have a definition as a cyberattack neither in the Article 5 of the NATO Treaty nor the Article 51 of the UN Charter. However, the Nicaragua Judgment of the ICJ makes it possible to conclude that cyberattacks, as non-kinetic weapons, can reach the level of an armed attack, if there are corresponding scale and effects.

2. **Consequences of cyberattack.** Cyberattacks as "Armed Attack" can be with consequences as physical damage, destruction, injury or death and without of such consequences if it significantly affects the performance of State functions in various sectors of security, defense, economy, and society.

3. **Intentions of cyberattack**. The fundamental factor of intentions of an "Armed Attack" was determined by the practice of the ICJ. In each case, NATO needs to determine the degree of intent of the armed attack as a cyber attack on the Alliance. The main goal is to avoid violating the sovereign rights of other States that are not involved in cyberattacks.

4. **The objects of the cyberattack**. The objects of the cyberattack can be either military and civilian, government or private, even situated outside the State's territory. When it comes to cyberattacks, in most cases they are conducted on CII, which is directly connected to the automatic control of critical infrastructure.

5. **The subjects of cyberattack**. The subjects of cyberattacks can be both the State and non-State actors on behalf of a State or under overall control, and non-State actors without involvement by a State such as armed bands, groups, irregulars or mercenaries. There is a serious problem in determining the attribution and identification of the subject of the cyberattack. This procedure takes quite a long time and requires improvement.

6. **Interceptive self-defense**. Interceptive self-defense is lawful, even under Article 51 of the Charter. Whereas a preemptive (or preventive or anticipatory) strike is directed at an armed attack that is merely "foreseeable", an interceptive strike counters an armed attack which is already in progress, even if it is still incipient. The application of interceptive self-defense in the light of new threats, such as cyberattacks with severe consequences, is necessary because the speed of data transmission in cyberspace seems to fit very well with the instantaneous and no moment for deliberation.

7. **Necessity, proportionality, immediacy**. Necessity usually refers to the existence of an armed attack or the imminent threat of attack. It also refers to the absence of feasible

alternatives. Proportionality means the action must be directed at ending the attack and preventing further attacks in the near future. Immediacy could apply if it is reasonable to conclude that further cyber operations are likely to follow. In the case of cyberattacks, compliance with immediacy criteria is very important, because the identification process and attribution of the attacker can take quite a long time.

8. **Standard of evidence**. Clear and convincing evidence seems the appropriate standard not only for claims of self-defense against traditional armed attacks but also for those against cyber operations: a prima facie or preponderant standard of evidence might lead to specious claims and false attribution, while a beyond reasonable doubt standard would be unrealistic.

9. **Identification and attribution**. Identification of attacker might be persuasively established by such factors as signals or human intelligence, the location of the offending computer within a state-controlled facility or public statements by officials, relationships between the two countries. The victim state needs a long time for attribution and identification of the attacker, taking into account technical features, as well as reliable grounds that such cyberattacks may be repeated in the future.

RECOMMENDATIONS

- NATO should create of the new regional legal instrument in regarding self-defense in the case of cyberattacks. This treaty should include such definitions and categories regulating the concept of cyberattack, a list of the consequences of such an attack, the requirements that are put forward to exercise the right to self-defense, as well as the specifics of attribution of the attacker. In addition, this treaty may also include legal regimes when the cyberattack does not reach a level that gives the right to self-defense, but it has other ways of conducting NATO defense (such as peaceful means, countermeasures, necessity).
- In international law, International Courts and countries should adopt the overall control standard of attribution of the non-state actor and the responsibility for committing a cyberattack (*Tadic* Case).
- ICJ should adopt a common standard of evidence to exercise the right to self-defense in the case of cyberattacks. This will effectively justify the right to self-defense in the case of cyberattacks.
- Within NATO, a cyber defense and defense strategy should be developed that could include a list of NATO institutions that could respond to cyberattacks, as well as a list of relevant plans and procedures for effective realization right to collective self-defense.
- Regularly conduct training courses among legal advisers under the military command of NATO member states in conjunction with technical experts in defense from cyberattacks. Such course will provide a practice-oriented survey of the international law applicable to cyber operations involving States. As an example, it could be International Law of Cyber Operations Course in NATO CCD COE (Tallinn, Estonia).

LIST OF BIBLIOGRAPHY

TREATIES AND LEGISLATION

International law

1. Draft articles on Responsibility of States for Internationally Wrongful Acts, 2001, http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf
2. United Nations Charter, 26 June 1945, (entered into force 24 October 1945), http://www.un.org/en/sections/un-charter/chapter-vii/index.html
3. The North Atlantic Treaty, Washington D.C., 4 April 1949, (entered into force 4 April 1949), https://www.nato.int/cps/en/natohq/official_texts_17120.htm
4. Vienna Convention on the Law of Treaties , 23 May 1969, United Nations, Treaty Series, vol. 1155, entry into force: 27 January 1980, (entered into force 27 January 1980), https://treaties.un.org/doc/publication/unts/volume%201155/volume-1155-i-18232-english.pdf

Resolutions of United Nations

1. Resolution 1368 (2001), adopted by the Security Council at its 4370th meeting, on 12 September 2001, https://www.treasury.gov/resource-center/sanctions/Documents/1368.pdf
2. Resolution 1373 (2001), adopted by the Security Council at its 4385th meeting, on 28 September 2001, https://www.unodc.org/pdf/crime/terrorism/res_1373_english.pdf
3. UN General Assembly, Resolution, A/Res/55/63, 2001, Combating the criminal misuse of information Technologies, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf

National law of member states of NATO

1. National cyber security strategy Finland's Cyber Security Strategy (2013), https://ccdcoe.org/cyber-security-strategy-documents.html
2. National cyber security strategy of Lithuania, Programme for the Development of Electronic Information Security for 2011–2019 (2011)", https://ccdcoe.org/cyber-security-strategy-documents.html
3. US International Strategy for Cyberspace, Prosperity, and Openness in a Networked World, (2011),

https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

OFFICIAL PUBLICATIONS

United Nations

1. Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, 2001, http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf
2. Letter dated 2001/10/07 from the Permanent Representative of the United States of America to the United Nations addressed to the President of the Security Council, http://dag.un.org/handle/11176/31401
3. Report of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Assembly, A/70/174, 2015, https://ccdcoe.org/sites/default/files/documents/UN-150722-GGEReport2015.pdf
4. Report of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Assembly, A/RES/68/243, 2013, https://www.un.org/disarmament/topics/informationsecurity/
5. Report of High-Level Panel on Threats, Challenges and Change Addressed to the Secretary General (2004, UN doc. A/59/565), http://www.un.org/en/peacebuilding/pdf/historical/hlp_more_secure_world.pdf
6. Report of the International, Court of Justice, 1 August 2003-31 July 2004, General Assembly, Official Records, Fifty-ninth Session, Supplement No. 4 (A/59/4), http://www.icj-cij.org/files/annual-reports/2003-2004-en.pdf
7. UN Doc. S/PV.2977, Part II, para. 72, 14 February 1991, http://repository.un.org/bitstream/handle/11176/55308/S_PV.2977(PartII)(closed-resumption1)-EN.pdf?sequence=3&isAllowed=y

NATO

1. NATO Parliamentary Assembly, Annual Session 2009, Committee Report 173 DSCFC 09 E bis-E bis and Cyber Defense, http://www.natolibguides.info/cybersecurity/documents

2. Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, North Atlantic Council, 5 September 2014, https://www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=en
3. Warsaw Summit Communiqué issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, North Atlantic Council, 8-9 July 2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en
4. Statement by the North Atlantic Council on 12 September 2001, NATO Press Release, https://www.nato.int/docu/pr/2001/p01-124e.htm

DOCUMENTS AND REPORTS

Members of NATO

1. Cyber Warfare, No 77, Advisory Council of International Affairs / No 22, Advisory Committee on Issues of Public International law, The Netherlands, December 2011, https://aiv-advies.nl/download/da5c7827-87f5-451a-a7fe-0aacb8d302c3.pdf
2. German Federal Ministry of Defense, White Paper 2006 on German Security Policy and the Future of the Bundeswehr, 2006, https://www.bundeswehr.de/resource/resource/MzEzNTM4MmUzMzMyMmUzMTM1MzMyZTM2MzIzMDMwMzAzMDMwMzAzMDY5NzE3MzM1Njc2NDYyMzMyMDIwMjAyMDIw/2016%20White%20Paper.pdf
3. Institut de Droit International, Resolution, ion, on, lution, (Santiago, France, 2007), http://www.idi-iil.org/app/uploads/2017/06/Hafner.pdf
4. International Security and Estonia, Estonian Foreign Intelligence Serviceetop Exercise Coherent Resilience (COR), 2018, https://www.valisluureamet.ee/pdf/raport-2018-ENG-web.pdf
5. United States Department of Defense Office of General Counsel, An Assessment of International Legal Issues in Information Operations, Department of Defense Office of General Counsel of United States (May 1999), http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf
6. US Justice Dept. White Paper, Lawfulness of a Lethal Operation Directe against a U.S. Citizen Who Is a Senior Operational Leader of AlFrance, (2007), https://fas.org/irp/eprint/doj-lethal.pdf
7. US Presidential Policy Directive, PPD-20, 2012, https://fas.org/irp/offdocs/ppd/ppd-20.pdf

Partner countries

1. Final Evaluation Report, Advanced Training Course on Critical Energy Infrastructure Security with Tabletop Exercise Coherent Resilience (CORE) 2017, NPS EAG, Kyiv, Ukraine, 2017

CASE LAW

ICJ and other International tribunals

1. Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro) Judgment of 26 February 2007, http://www.icj-cij.org/files/case-related/91/091-20070226-JUD-01-00-EN.pdf
2. Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda) judgment of 19 December 2005, http://www.icj-cij.org/files/case-related/116/116-20051219-JUD-01-00-EN.pdf
3. Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America), 27 June 1986, http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf
4. Case concerning oil platforms (Islamic republic of Iran v. United States of America), 12 December 1996, http://www.icj-cij.org/files/case-related/90/090-19961212-JUD-01-00-EN.pdf
5. Case concerning the Gabcikovo-Nagymaros project (Hungary/Slovakia) Judgment of 25 September 1997, http://www.icj-cij.org/files/case-related/92/092-19970925-JUD-01-00-EN.pdf
6. Certain Norwegian Loans (France v Norway), Merits, Judgment, 6 July 1957, Separate Opinion of Judge Sir Hersch Lauterpacht, http://www.icj-cij.org/en/case/29
7. Dissenting Opinion of Judge Schwebel, Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America), 27 June 1986, http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-09-EN.pdf
8. Dissenting Opinion of Vice-President Al-Khasawneh appended to Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro) Judgment of 26 February 2007,

http://www.icj-cij.org/files/case-related/91/091-20070226-JUD-01-01-EN.pdf

9. International Military Tribunal (Nuremberg) Judgment of 1 October 1946, https://crimeofaggression.info/documents/6/1946_Nuremberg_Judgement.pdf
10. Jennings, Dissenting Opinion, Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America), 27 June 1986, http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-10-EN.pdf
11. Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory Advisory Opinion of 9 July 2004, http://www.icj-cij.org/files/case-related/131/131-20040709-ADV-01-00-EN.pdf
12. Nuclear Weapons advisory opinion: Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 ICJ 226 (8 July), http://www.icj-cij.org/files/case-related/95/095-19960708-ADV-01-00-EN.pdf
13. Tadic Case, International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia since 1991, http://www.icty.org/x/cases/tadic/acjug/en/tad-aj990715e.pdf
14. The Corfu Channel Case, Judgment of 9 April 1949, ICJ, http://www.icj-cij.org/files/case-related/1/001-19490409-JUD-01-00-EN.pdf
15. Yeager v Islamic Republic of Iran, (1987) U.S.C.T.R 17, 92, 101-2, 1982, https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=1555796&fileOId=1563775

SPECIAL LITERATURE

Books

1. Avra Constantinou, *the Right of Self-Defense under Customary International Law and Article 51 of the UN Charter*. Ant. N. Sakkoulas, 2000.
2. Christine Gray, *International Law and the Use of Force*, Third Edition. UK: Oxford University Press, 2008.
3. D.W. Bowett, *Self Defense in International Law*. New York: Frederick A. Praeger. 1958. Pp. xv, 294.
4. James A Green, *The ICJ and Self-Defense in International Law*. Oxford and Portland, Oregon, 2009.
5. Janne Valo, *Cyber Attacks and the Use Force in International law*. Master thesis, University of Helsinki, 2014.

https://helda.helsinki.fi/bitstream/handle/10138/42701/Cyber%20Attacks%20and%20the%20Use%20of%20Force%20in%20International%20Law.pdf?sequence=2

6. Judith Gardam, *Necessity, Proportionality and the Use of Force by States*. Cambridge: Cambridge University Press, 2004.
7. Katharina Ziolkowski, *Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy*. Tallinn, Estonia: NATO CCD COE Publications, 2013.
8. Kinga Tibori Szabó, *Anticipatory Action in Self-Defense, Essence and Limits under International Law*. T.M.C. ASSER PRESS, The Hague, The Netherlands, 2011.
9. Marco Roscini, *Cyber Operations and the Use of Force in International law*. UK: Oxford University Press, 2014.
10. Michael N. Schmitt, *Tallinn Manual 1.0 on the International Law Applicable to Cyber Warfare*. UK: Cambridge University Press, 2013.
11. Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. UK: Cambridge University Press, 2017.
12. Murray Colin Alder, *the Inherent Right of Self-Defense in International Law*. Springer Dordrecht Heidelberg New York London, 2013.
13. Myres S. McDougal and Florentino P. Feliciano, *Law and Minimum World Public Order*: The Legal Regulation of International Coercion. Introduction by Harold D. Lasswell. London and New Haven: Yale University Press, 1961. Pp. Xxvi.
14. Yoram Dinstein, *War, Aggression and Self-Defense*, 5th edn. Cambridge: Cambridge University Press, 2011.

Journals and News Articles

1. Alison Pert, "Proportionality in Self-Defense – Proportionate to What?", *Sydney Law School, Legal Studies Research Paper* No. 17/92 November (2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3067750
2. Antonio Cassese, "The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia", *European Journal of International Law*, Volume 18, Issue 4, 1, (2007), https://academic.oup.com/ejil/article/18/4/649/453762
3. Ashley Deeks, "Unwilling or Unable': Toward an Normative Framework for Extra-Territorial Self-Defense", *Virginia Journal of International Law*, Vol. 52, No. 3, (2012), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1971326

4. Benatar, "The Use of Cyber Force: Need for Legal Justification?" *Goettingen Journal of International Law*, (2009),
5. Christian J. Tams, "The Use of Force against Terrorists", *The European Journal of International Law* Vol. 20 no. 2 EJIL (2009), http://www.ejil.org/pdfs/20/2/1793.pdf
6. Claus Kress, "Some Reflections on the International Legal Framework Governing Transnational Armed Conflicts", *Journal of Conflict and Security Law* 15 (2010), http://www.uni-koeln.de/jur-fak/kress/Materialien/Chef/HP882010/Final19022011.pdf
7. D. K. Linnan, "Self-Defense, Necessity and U. N. Collective Security: United States and OtherViews", 1 *DukeJCIL* 57, 103 (1991), https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1299&context=djcil
8. David E Graham, "Cyber Threats and the Law of War", *Journal of National Security Law and Policy* 4 (2010), http://jnslp.com/wp-content/uploads/2010/08/07_Graham.pdf
9. David Kretzmer, "The Inherent Right to Self-Defense and Proportionality in *Jus Ad Bellum*," *European Journal of International Law* 24, 1, Published by Oxford University Press (2013), https://academic.oup.com/ejil/article/24/1/235/438278
10. Dinstein, "Computer Network Attacks and Self-Defense", U.S. Naval War College, *International Law Studies*, Volume 76, (2002) http://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1397&context=ils
11. Duncan Blake and Joseph S Imburgia, "Bloodless Weapons"? The Need to Conduct Legal Reviews of Certain Capabilities and the Implications of Defining Them as "Weapons" ', *Air Force Law*, Review 66 (2010), https://poseidon01.ssrn.com/delivery.php?ID=064009119124117119111084122069118126031031005037095033119000096125086127095006082077009121016122105097101111064000001000018112026076045089042090121003097124011114088001075028120091095099004073103113112119102127029117079126087017126125097126071070102116&EXT=pdf
12. Elizabeth Wilmshurst, "Chatham House Principles of International Law on Use of Force in Self-Defense", *International & Comparative Law Quartely*, Volume 55, Issue 4, (2006), https://www.cambridge.org/core/services/aop-cambridge-core/content/view/83DCF94C30AB4D11DBEEB354430D98B9/S0020589300069815a.p

df/chatham_house_principles_of_international_law_on_the_use_of_force_in_selfdefence1.pdf

13. Eneken Tikk, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm, Liis Vihul, Cyber Attacks Against Georgia: Legal Lessons Identified, *NATO CCDCOE, Version 1.0*, (2008), http://www.ismlab.usf.edu/isec/files/Georgia-Cyber-Attack-NATO-Aug-2008.pdf
14. Enrico Benedetto Cossidente, " Legal Aspects of Cyber and Cyber-Related Issues Affecting NATO ", *NATO Legal Gazette* 61, 35 (2014), http://www.act.nato.int/images/stories/media/doclibrary/legal_gazette_35.pdf
15. Eric Talbot Jensen, "Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense", *Stanford Journal of International Law 38* (2002), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=987046
16. F. L. Morrison, "Legal Issues in the Nicaragua Opinion", 81 AJIL 160, 163 (1987), *American Journal of International Law*, 81 AJIL 160, (1987), http://www.heinonline.org/HOL/Page?collection=journals&handle=hein.journals/ajil81&id=180
17. Florentine J.M. de Boer, " Examining the Threshold of "Armed Attack" in light of Collective Self-Defense against Cyber Attacks: NATO's Enhanced Cyber Defense Policy", *NATO Legal Gazette* 61, 35 (2014), http://www.act.nato.int/images/stories/media/doclibrary/legal_gazette_35.pdf
18. Greenberg, Goodman, and Soo Hoo, "Information Warfare and International Law", *National Defense University Press*, (1988), https://www.researchgate.net/publication/235066729_Information_Warfare_and_International_Law
19. James A Green, "Fluctuating Evidentiary Standards for Self-Defense in the ICJ", *International and Comparative Law* Quarterly 58 (2009), http://www.jstor.org/stable/20488277?loggedin=true
20. James A. Lewis, "The Role of Offensive Cyber Operations in NATO's Collective Defense", *The Tallinn Papers, NATO CCD COE, Publication on Strategic Cyber Security*, No. 8, (2015) https://ccdcoe.org/sites/default/files/multimedia/pdf/TP_08_2015_0.pdf
21. Karl Zemanek, "Armed Attack", *Oxford Public International Law*, (2013), http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e241

22. Koms, S. W. & Kastenberg, J. E., 2008, Georgia's Cyber Left Hook, Parameteres, *U.S. Army War College, Quarterly*, (2008), http://www.dtic.mil/dtic/tr/fulltext/u2/a636632.pdf
23. L. C. Green, "Armed Conflict, War, and Self-Defense", 6 Ar.V. 387, 434 (1956–7)"
24. Laurie R. Blank, International Law and Cyber Threats from Non-State Actors, International Law Studies, U.S. Naval War College, Volume 89, 2013, accessed 2018 May 3, http://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1036&context=ils
25. Limba T.; Plėta T.; Agafonov K.; Damkus M., "Cyber security management model for critical infrastructure", *Entrepreneurship and Sustainability Issues* 4(4), (2017), http://dx.doi.org/10.9770/jesi.2017.4.4(12)
26. M. Roscini, "World Wide Warfare – Jus ad Bellum and the Law of Cyber Force", 14, MPYUNL 85, (2010), accessed 2018 May 3, http://www.mpil.de/files/pdf3/mpunyb_03_roscini_141.pdf
27. M. Shmitt, "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts", *Duhram University Law School, UK*, (2010), https://www.nap.edu/read/12997/chapter/12
28. Macdonald, "The Nicaragua case: New Answers to Old Questions, 1986" *Canadian Yearbook of International Law*, Cambridge University Press, Volume 24, (1987), https://www.cambridge.org/core/journals/canadian-yearbook-of-international-law-annuaire-canadien-de-droit-international/article/the-nicaragua-case-new-answers-to-old-questions/7F8049C0D32E5A29B01508B15466F28A
29. Marie Jacobson, "Evidence as an Issue in International Legal Practice", *Notre Dame Law School NDLScholarship*, (2006), https://www.questia.com/library/journal/1G1-158948780/evidence-as-an-issue-in-international-legal-practice
30. Mary Ellen O'Connell, "Evidence of Terror", *Journal of Conflict and Security Law* 7, Oxford University Press (2002), https://academic.oup.com/jcsl/article/7/1/19/1010628
31. Mary Ellen O'Connell, "Rules of Evidence for the Use of Force in International Law's New Era", *America Society of International Law Proceedings* 100 (2006), https://scholarship.law.nd.edu/law_faculty_scholarship/35/
32. Matthew C. Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)", Volume 36, Issue 2 *Yale Journal of International Law*, (2011),

http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1403&context=yjil

33. Matthew Hoisington, "Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense", *Boston College International and Comparative Law Review* 32 (2009), http://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=1115&context=iclr
34. Michael N. Schmitt, "Attack" as a Term of Art in International Law: The Cyber Operations Context", 2012 *4th International Conference on Cyber Conflict*, Tallinn, (2012), https://www.ccdcoe.org/publications/2012proceedings/5_2_Schmitt_AttackAsATermOfArt.pdf
35. Michael N. Schmitt, "Cyber Activities and the Law of Countermeasures", *Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy* (Tallinn, Estonia: NATO CCD COE Publications, 2013)
36. Natalino Ronzitti, "The Expanding Law of Self-Defense", *Journal of Conflict and Security Law,* Published by Oxford University Press, 17 November (2006), https://academic.oup.com/jcsl/article-pdf/11/3/343/2376434/krl021.pdf
37. Nicholas Tsagourias, "Cyberattacks, self-defense and the problem of attribution", *Journal of Conflict & Security Law*, Oxford University Press, (2012), https://poseidon01.ssrn.com/delivery.php?ID=660029082067072115113102068120087113007059056088020045126118021097091089104093114005013117053102018063007118116007016120070020112038078013065113003122094118114093068088040053112102119109127080127097127091000084020023003093023083072108070086007007114101&EXT=pdf
38. Priyanka R. Dev, "Use of Force" and "Armed Attack" Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response", *Texas International law Journal*, 50, 2, (2015)
39. Robin Geib and Henning Lahmann, "Freedom and Security in Cyberspace: Shifting the Focus away from Military Responses towards Non-Forcible Countermeasures and Collective Threat-Prevention", *Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy (Tallinn, Estonia: NATO CCD COE Publications, 2013)*
40. Schmitt, "'Computer Network Attack and the Use of Force in International law: Thoughts on a Normative Framework", *Research Publication 1, Information Series*, (1999), http://www.google.lt/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwiAkNvL0p7aAhWCAJoKHflOBZwQFggyMAE&url=http%3A%2F%2Fwww.dtic.mil%2

Fget-tr-doc%2Fpdf%3FAD%3DADA471993&usg=AOvVaw3jiDD9D911Kzu0ccUWii5t

41. Scott J. Shackelford, "State Responsibility for cyberattacks: competing standards for a growing problem", *University of Cambridge, UK, NATO CCD COE Publications*, Talinn, Estonia, (2010), https://ccdcoe.org/sites/default/files/multimedia/pdf/Shackelford%20-%20State%20Responsibility%20for%20Cyber%20Attacks%20Competing%20Standards%20for%20a%20Growing%20Problem.pdf
42. T.D. Gill, "The Temporal Dimension of Self-Defense: Anticipation, Pre-emption, Prevention and Immediacy", *Journal of Conflict and Security Law*, Volume 11, Issue 3, 1 December (2006), https://academic.oup.com/jcsl/article-abstract/11/3/361/793706?redirectedFrom=PDF
43. Taft, "Self-Defense and the Oil Platforms Decision", 29 *Yale Journal of International law* (2004), http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1232&context=yjil
44. Van Steenberghe, "Self-Defense in Response to Attacks by Non-state Actors in the Light of Recent State Practice: A Step Forward?", *Leiden Journal of International Law*, 23 (2010), https://www.cambridge.org/core/services/aop-cambridge-core/content/view/08CFA8E3AD85D5E2DB6EA745C0843A85/S0922156509990380a.pdf/selfdefence_in_response_to_attacks_by_nonstate_actors_in_the_light_of_recent_state_practice_a_step_forward.pdf
45. Woltag, "Cyber Warfare, in Wolfrum (ed.)", *Max Planck Encyclopaedia of Public International Law*, Oxford, (2010)

Electronic sources

1. Advance Questions for Lieutenant General Keith Alexander, USA, Nominee for Commander, United States Cyber Command, accessed 2018 May 3, https://epic.org/privacy/nsa/Alexander_04-15-10.pdf
2. For a comprehensive technical analysis of Stuxnet, see Symantec's Nicolas Falliere, Liam O Murchu, and Eric Chien, W32.Stuxnet Dossier, version 1.4, February 2011, accessed 2018 May 3, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

3. Hughes, R. B., “NATO and Cyber Defense: Mission Accomplished?”, NATO-OTAN, 2009, April, 2009, April, accessed 2018 May 3, https://www.atlcom.nl/ap_archive/pdf/AP%202009%20nr.%201/Hughes.pdf
4. International Cyber Incidents. Legal Considerations, *NATO CCDCOE*, 2010, accessed 2018 May 3, http://www.ccdcoe.org/publications/books/legalconsiderations.pdf
5. Lance Whitney, North Korea Behind March Cyber Attack, says South Korea, C/NET, Apr. 10, 2013, accessed 2018 May 3, http://news.cnet.com/8301-1009_3-57578829-83/north-korea-behind-march-cyberattack-says-south-korea
6. Letter from Daniel Webster to Lord Ashburton (6 August 1842), reprinted in 2 Int’l L. Dig. 412 (John Bassett Moore ed., 1906), accessed 2018 May 3, https://archive.org/stream/jstor-40734417/40734417_djvu.txt
7. Lipson, Tracking and Tracing Cyber Attacks: Technical Challenges and Global Policy Issues, Carnegie Mellon Software Engineering Institute, 2002, accessed 2018 May 3, https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=5831
8. Michael Miklaucic, ‘NATO Countering the Hybrid Threat’ (23 September 2011), accessed 2018 May 3, http://www.act.nato.int/nato-countering-the-hybrid-threat
9. NATO Cooperative Cyber Defense Centre of Excellence, Tallinn, Estonia, accessed 2018 May 3, https://ccdcoe.org/cyber-definitions.html
10. NATO: U.S. Evidence on Bin Laden "Compelling"; Allies Give Unconditional Support for Retaliatory Strikes; Taliban Official Asks to see Proof, WASH. POST, Oct. 3, 2001”, accessed 2018 May 3, http://qctimes.com/news/local/nato-evidence-points-to-bin-laden/article_a06b42f2-49a4-5340-bb59-a81788784a60.html
11. Nils Melzer, Cyberwarfare and International Law, UNIDIR Resources, 2011, accessed 2018 May 3, http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf
12. ÖykülIrmakkesen, The Notion of Armed Attack under the UN Charter and the Notion of International Armed Conflict – Interrelated or Distinct?, *Geneva Academy*, 2014, accessed 2018 May 3, http://www.prix-henry-dunant.org/wp-content/uploads/2014_IRMAKKESEN_Paper.pdf

13. Roberto Ago, Addendum - Eighth report on State responsibility, Special Rapporteur - the internationally wrongful act of the State, source of international responsibility, 1980, accessed 2018 May 3, http://legal.un.org/ilc/documentation/english/a_cn4_318_add5_7.pdf
14. Rules of evidence before the ICJ' (Lawteacher.net, April 2018), accessed 2018 May 3, https://www.lawteacher.net/free-law-essays/international-law/rules-of-evidence-before-the-international-court-of-justice-international-law-essay.php?vref=1
15. Statement by the North Atlantic Council on 12 September 2001, NATO Press Releases, accessed 2018 May 3, https://www.nato.int/docu/pr/2001/p01-124e.htm
16. The first case of a successful cyberattack on energy objects has been registered in Ukraine" Ukrainian National News, accessed 2018 May 3, http://www.unn.com.ua/uk/news/1552689-minenergovugillya-pershiy-u-sviti-vipadok-vdaloyi-kiberataki-na-obyekti-energetiki-zareyestrovano-v-ukrayini
17. When do cyber operations amount to use of force and armed attack, and what response will they justify?, accessed 2018 May 3, https://www.duo.uio.no/bitstream/handle/10852/50840/723.pdf?sequence=1

ABSTRACT

In the Wales Summit Declaration on 5 September 2014 and the Warsaw Summit Declaration on 9 July 2016, NATO recognized that international law, including international humanitarian law and the UN Charter, applies in cyberspace and recognized cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea. This master thesis work aims examine whether collective self-defense clauses of Article 5 of the NATO Treaty and the Article 51 of the UN Charter are applicable in the modern international law. Consequently, this work comes to conclusion that modern international law is not able to adequately regulate of legal relations in the field of collective self-defense in the case of cyberattacks. NATO should adopt a new treaty regarding self-defense in the case of cyberattacks.

Keywords: NATO, Collective Self-Defense, Armed Attack, Cyberattack, State actors, Non-state actors

SUMMARY

COLLECTIVE SELF-DEFENSE IN THE NATO FRAMEWORK AGAINST CYBERATTACKS AND MODERN INTERNATIONAL LAW

The purpose of Master thesis is in light of growing cyber security threats to examine whether collective self-defense clauses of Article 5 of the NATO Treaty and the Article 51 of the UN Charter are applicable in the modern international law.

The thesis consists of four parts which are divided into chapters. The first part of the thesis is devoted to analyze the main elements of "Armed Attack" as cyberattack in light Article 5 of the NATO Treaty and the Article 51 of the UN Charter (actions, consequences, intentions, motives, objects and subjects of cyberattacks). The analysis showed that special attention to the qualification of cyberattacks as an armed attack, it is necessary to pay attention to the consequences of such an attack. Such consequences can be both with the presence of heavy damage, and with the destruction of the state critical infrastructure. In addition, special attention was paid to the subjects of such attacks, namely to non-state actors, even without involving state structures.

The second part of the thesis analyses the nature of the scale and effects required for an act to be characterized as an armed attack as cyberattack necessarily exceed those qualifying the act as a use of force. It was necessary to focus on the nature of an action's consequences of "Armed Attack" as cyberattack for understanding scale and effects within meaning Nicaragua Judgment. Moreover, it was researched anticipatory self-defense against an imminent armed attack by cyber means.

The third part devoted the main requirements of collective self-defense NATO against cyberattacks such as necessity, proportionality, immediacy, request of the victim state for collective self-defense and the duty to report the self-defense measures to the UN Security Council. This part was focused on challenges which can arise on practice. Indeed, the analysis showed that, given the specifics and complexities in cyberspace, in practice there is a problem in determining the time through which the victim state can apply the right to self-defense.

The forth part analyses the standard of evidence required for the exercise of collective self-defense against cyberattacks and the main problems of attribution, identification of the attacker, and collective self-defense against cyberattacks by non-state actors. It must be stated that, despite NATO's generally accepted international law against cyberattacks, in practice there are problems with the collection and standard of evidence, which prevents attribution of the non-state actor as an attacker.

HONESTY DECLARATION

___/___/_____

Vilnius

I, _____, student of

(name, surname)

Mykolas Romeris University (hereinafter referred to University),

_____

(Faculty /Institute, Programme title)

confirm that the Bachelor / Master thesis titled

“_____

_____:

1. Is carried out independently and honestly;
2. Was not presented and defended in another educational institution in Lithuania or abroad;
3. Was written in respect of the academic integrity and after becoming acquainted with methodological guidelines for thesis preparation.

I am informed of the fact that student can be expelled from the University for the breach of the fair competition principle, plagiarism, corresponding to the breach of the academic ethics.

_____ _____

(signature) *(name, surname)*