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

Eva Lotta Penjam

A RIGHT FOR COLLECTIVE COUNTERMEASURES ON A CYBER-ATTACK: THE CONTEXT OF THE EU'S MEMBER STATES

Bachelor's thesis
Programme: Law; Specialisation: International relations

Supervisor: Vlad Alex Vernygora, LL.M., MA

Tallinn 2022

I hereby declare that I have compiled the thesis independently
and all works, important standpoints, and data by other authors
have been properly referenced and the same paper
has not been previously presented for grading.
The document length is 10,349 words from the introduction to the end of conclusion.

Eva Lotta Penjam

……

(signature, date)

Student code: 192605HAJB

Student e-mail address: evpenj@ttu.ee

Supervisor: Vlad Alex Vernygora:

The paper conforms to requirements in force

……

(signature, date)

Chairman of the Defense Committee:

Permitted to the defense

……

(name, signature, date)

TABLE OF CONTENTS

ABSTRACT

The European Union (EU) can be regarded as one of the most interconnected entities globally, and this factor is often assumed by academia without further elaborations. On this particular occasion, this research paper asked whether those interconnections that the EU Member States have as sufficient for them to frame up the right to take collective countermeasure against cyber-attack and aimed to develop a better argumented viewpoint on the issue. The discussion relied on the existence of cyber-related interconnections between the Member States of the EU and the existence of the right to collective countermeasures in cyber space. Both were established to pose no contradictions to the right of the Member States of the EU to use collective countermeasures on cyber-attacks. The main arguments which support the claim are, that cyber-attacks conducted on critical infrastructure of one of the Member States will result in injuries to other states and that there are no legal conflicts to the right.

Keywords: the EU, cyber-attacks, collective countermeasures, international law

INTRODUCTION

The international legislation in force has developed over a considerable period, and been influenced by the international system, wars, and other forces and events that were taking place globally. It is an agreement between nations, which has, in many cases, found initiation from negative experiences and shocks of some kind, like did the development of international humanitarian law after the horrors of WW2[1]. It is important that international legislation is created, however it would be far more effective if the initiation did not stand in sufferings, but the hope of creating a system that would prevent such happenings. Although the result of both ways is initially the same, method of prevention and preparation is far more effective than dealing with consequences. In assumption of a prospective exponential rise in cyber-attacks against states, it is necessary in such a case to act preventively fast rather than reflexively slow, figuring out the form of measures post-factum.

It could be argued that the European Union (EU) is thriving to be a pioneer in the field of cybersecurity, it is the promoter of cyber diplomacy. Although it does well, and is moving towards further developments, it is yet not quite in the possession of cyber power it would wish for. Objectively, the EU has the capacities to become the leading power in the field of cybersecurity, however, it is not yet there, where it shall be, and has several developments that are necessary to be conducted before they will reach the desired position of cyber power[2]. In the practical scope, the security perception of the EU has taken a rather definite turn since the start of Russian aggression on Ukraine, many of the cornerstones of foreign policy of the EU have been altered and thus suitable conditions for long awaited changes is being created.

The security perception of the EU has taken a turn within the period and the time when decisions need to be made has arrived. Besides border protection and the financing of defense of the entity, new methods of warfare, including cyber warfare must be recognized as a potential threat. The EU has spent the past decades believing in the modern world order and good intentions of its

[1] Sterio, M. (2008). T*he Evolution of International Law. Boston: Boston College International and Comparative Law Review*. 31(2). 235-239 (2008), https://lawdigitalcommons.bc.edu/iclr/vol31/iss2/3

[2] Kasper, A. & Vernygora, V. A. (2021). The EU's cybersecurity: a strategic narrative of a cyber power or a confusing policy for a local common market. Cuadernos Europeos de Deusto. 29-71. 10.18543/ced-65-2021. 29-71.

neighbors, nonetheless those illusions need to be demolished now. Even without having witnessed a large-scale cyber-attack against critical infrastructure, it needs to be considered as a real and existing security issue, against which a framework of response is necessary to be developed.

Besides creating a *per se* preventive framework of regulations, that contribute into development of effective protection against cyber-attacks, framework of response to cyber-attacks must be set. Collective countermeasures, which could allow the Member States of the EU to help each other in case one is incapable of taking them itself. The research focuses on the interconnection of the EU as a ground for the justification of the use of collective countermeasures. Thus, collective countermeasures can seem like an effective collective solution, but are they in the case of the EU and the interconnection that its Member States share, operationally and legally feasible or even politically justified? The paper claims, that the Member States of the EU have the right to use collective countermeasures on cyber-attack, because they are highly interconnected in cyber space

The paper will first, analyze and explore the possibility of using collective countermeasures on cyber-attacks conducted on the EU's Member States and then, secondly, to provide a legally argumented overview for the operational use for the entity's common framework on cyber security. It will analyze the two fields, the interconnection of the EU and collective countermeasures separately to gain extensive understanding in both, and then continue to tie the two topics together.

In the center of the discussion is the question of whether the EU's interconnection in cyber space provides its Member States with the right to collective countermeasures. The interconnectivity levels in the EU are high, and thus, an attack on systems of special importance spreads or its effects spread across the Union. The discussion will be conducted based on two separate variables, the first one being the interconnection of the EU and the second collective countermeasures in cyber space. The first theoretical part will provide an overview of the EU and its predominant fields of interconnection. It will in addition discuss the effects of interconnections in cyber space in the context of the EU with the focus on the fields identified beforehand. An overview of the relevant strategies adopted by the EU will be provided in the last sub-paragraph of the chapter. Second of the theoretical parts will focus on cyber security. It will start off by defining and describing cybersecurity, cyber-attacks, and related concepts with the focus on developing a comprehensive understanding of the field for legal analysis. An overview will be given about applicable law, with the focus on agreements over the extent of applicability of international law in cyber space. It will be followed by a sub-paragraph focusing on collective countermeasures, its definition and scope

in cyber space. The existing position of the Member States and relevant documents issued by the EU and the practical scope of collective countermeasures will be described in the end of the second chapter.

The main methodological approach of this research work is predominantly qualitative[3]. The author will be collecting and analyzing various academic sources, appropriate legislation together with existing statements of key decision-shapers and decision-makers within and outside of the EU. Legal discourse analysis[4] will prevail over the other qualitative methods. The method is chosen as suitable because the topic explores the need for changes in legal discourse and normative, rather than qualitative framework. The research could well benefit decision-makers and legislators in understanding the topic and potential necessity of collective countermeasures and the possible scope of using those in the context of the EU Member States.

[3] Chui, W. H. and McConville, M. (2017). *Research Methods for Law*. UK: Edinburgh University Press Second Edition. ISBN 978 1 4744 0425 9. 18

[4] White, N. (2018). *Legal Analysis: There's a Template for That!* ALSB Journal of Business Law & Ethics Pedagogy, 2(1) Retrieved from: https://ssrn.com/abstract=3248471

1. INTERCONNECTION OF THE EU

1.1. The EU and its policymaking

The well-known story behind the creation of the EU starts with the Coal and Steel Community, which was created in 1952 to make another war between France and Germany impossible[5]. The model followed liberal theory of international relations, *pax mercatoria*, peace from trade, which assumes that high interconnections between states make the war happening impossible. The Community developed further and in 1992 the EU as we know it today was formed.[6]

The Union bases on 4 freedoms – free movement of goods, people, capital, and services. The aim of those freedoms is to abolish all barriers to the movement of those. It has been proposed that 5th freedom is included in the list – free movement of data. It has been described as a fundamental element to information society. Sharing of data and access to critical information provide the functioning of information society and innovation, where complex problems could be solved by simple data distribution between competent and necessary authorities.[7] The Single Market Strategy would benefit the Union in respect to ICT, copyright, data protection, radio services and practical scope of competition law [8].

European Common Foreign and Security Policy (CFSP) works for regional and international peace and security and strengthens rule of law and stability in those areas. It is a measure of external that is agreed between the Member States and allows for deeper cooperation in the field of foreign affairs. It conducts military and civilian missions, can pose sanctions, and takes part in conflict prevention, peace building and mediation. In addition, it has instruments of crisis response and

[5] Eichengreen, B. (2009) *European Integration*. Oxford: The Oxford Handbook of Political Economy. Doi: 10.1093/oxfordhb/9780199548477.003.0044

[6] Ramiro Troitino, David (2013*). European Identity the European People and the European Union. Sociology and Anthropology*. 1. 135−140. doi: 10.13189/sa.2013.010301.

[7] Kala, K. (2017*) Free movement of data as the 5th fundamental freedom of the European Union*. e-Estonia. Retrieved from: https://e-estonia.com/free-movement-of-data-as-the-5th-fundamental-freedom-of-the-european-union/

[8]European Commission (2015) COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. *A Digital Single Market Strategy for Europe*. SWD(2015) 100 final

management, and stability on sea and land. The CSFP is covered by the Treaty of the EU Title V. The execution of the Common Foreign and Security Policy is exercised by High Representative of the Union for Foreign Affairs and Security Policy in cooperation with the Member States in accordance with the Treaties of the EU. The policy shall be carried out by the Member States in good faith and in accordance with the interests of the Union with the goal of enhancing mutual political solidarity (between the Member States).[9]

The key role in defining the Unions interests is in the hands of the European Council (EC), who can adopt decisions necessary for the employment of the policy. In accordance to the Treaty "*The common security and defense policy shall include the progressive framing of a common Union defense policy. This will lead to a common defense when the European Council, acting unanimously, decides. It shall in that case recommend to the Member States the adoption of such a decision in accordance with their respective constitutional requirements".* The Member States should as well as improve their defense capacities and implement measures necessary for the European capabilities. The Treaty also includes a clause of mutual aid and assistance in power in Article 42, if any of the Member States is a victim of armed aggression on its territory. In addition, Article 222 of the TEU acts a solidarity clause, which applies if a Member State becomes an object of a terrorist attack or a victim of a natural or man-made disaster. Those measures are complemental to the membership of NATO.[10]

1.2. Cyberspace as a domain

Cyber space was on wide international stage first recognised a domain of operation during the 2016 NATO Warsaw summit, held on 8-9 July[11]. The Summit included head of state and government from NATO countries, which were complimented by other nations outside of NATO, including Ukraine and Russia. It was a step forward from the 2014 Wales Summit where the applicability of international law in cyber space was recognised and cyber defense was identified as core task of NATO's collective defense.[12] The main outcome of the conference was the

[9] European Parliament (2021). *FOREIGN POLICY: AIMS, INSTRUMENTS AND ACHIEVEMENT*S. Fact Sheets on the European Union – 2021. Retrieved from: https://www.europarl.europa.eu/factsheets/en/home
[10] *Ibid*.
[11] NATO (2017). *Warsaw Summit Communiqué*. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016. Retrieved from: ://www.nato.int/cps/en/natohq/official_texts_133169.htm
[12] Alatalu, S. (2017). *One year after Warsaw: The growing need for a NATO cyber command*. 59-66. 10.1109/CYCONUS.2017.8167513.

recognition of cyber space as a domain of operations, meaning that cyber space defense is as important as is air, land, and sea defense. It was significant statement, which was back upped by several adoption of definitions to cyber operation. The statement mentioned amongst else "broader deterrence and defense […,] integrat[ion] into operational planning and Alliance operations and missions […,] more effective organisation of NATO's cyber defense and better management of resources, skills, and capabilities".[13]

1.3. EU's interconnection in cyber space

In 2015 the European Commission released communication from the Commission to the European Parliament (EP), the Council, the European Economic and Social Committee and the Committee of the Regions on A Digital Single Market Strategy for Europe. This communication lays down reasons why the Digital Single Market is necessary and proposes a 3-pillar system for building it. Those pillars are access, environment, and economy & society. Consumers and businesses should be granted with better access to online service and data, whereas the barriers to cross-border online activities should be reduced. The environment, where digital activities are carried out should be reliable, trustworthy, high-speed, affordable, and safe for both consumers and businesses. Therefore, several existing rules should be rewritten to better fit the purpose. Third, growth potential should be maximized by the smart use of digital economy to benefit economy and consequently societies.[14]

Companies tend to use services of multiple digital service providers, so that their needs could be fulfilled the best. In the EU it is usual that the service providers come from multiple different locations, which means that data moves from one Member State to another brining along concerns on the safety and compliance of such. Highest levels of interconnection are to be found in businesses of compliance and interconnection, however other private enterprises are found to be interconnected as well, e.g., providers of financial services, supply chains, telecommunications, and IT-cloud services.[15]

[13] CCDCOE (2016) *NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit.* The NATO Cooperative Cyber Defence Centre of Excellence. Retrieved from: https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/
[14] European Commission (2015). COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. *A Digital Single Market Strategy for Europe*. SWD(2015) 100 final
[15] *Ibid.*

1.3.1. Banking

The interconnection of the EU banks has two levels, one being the direct interconnection of banks and second indirect interconnection. The direct interconnection includes interbank loans, banks loans to other corporate and retail clients and security holdings, while the indirect interconnection covers exposures to common asset classes. The interconnection as such poses a risk to security of the banking systems, where first, the direct interconnections can be devaluated, or the indirect interconnection potential risks ignored.[16]

1.3.2. Energy

Most EU Member States rely largely on imported energy resources, gas, oil, and fuels, and are therefore dependent on each other on their supply chains, such as pipelines. The EU is gradually moving towards becoming the most environment considerate region in the world, whereas remaining its economic capacities.[17] A major plan, the European Green Deal was announced on December 11, 2019, with the main objective to make Europe the first climate neutral continent by 2050. The plan shall besides the achievement environmental objectives promote the economy and improve the quality of life and health of people.[18]

The Green Deal calls for a change in policies of clean energy supply, bringing it to all users of energy, from industries to transport to governmental agencies. The Green Deal should include all areas and invest in and transform necessary digital tools which can benefit the objectives. (2.1. Designing a set of deeply transformative policies).[19]

The largest contributor to greenhouse gas emission is production and use of energy in economic sectors, making over 75% of the total emissions in the EU. To change that number, energy production must be largely based on renewable resources together with the lesser use of coal and decarbonising gas. To achieve such objective, the energy market needs to be integrated, interconnected, and digitalized. The infrastructure of energy suppliance must be smart and cost

[16] Roncoroni, A., Battiston, S., D'Errico, M., Halaj, G. & Kok, C. (2019). *Interconnected banks and systemically important exposures*. Working Paper Series. 2331. European Central Bank. Retrieved from: https://EconPapers.repec.org/RePEc:ecb:ecbwps:20192331. 1-12 Siddi

[17] Siddi, Marco. (2020). The European Green Deal: Assessing its current state and future implementation. Finnish Institute of International Affairs. FIIA Working paper.

[18] European Commission. (2019). COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS *The European Green Deal*. COM/2019/640 final.

[19] *Ibid.*

effective, thus innovative new technologies must be taken into the use on the side of the existing.[20] Another aspect of the Deal is creation of circular economy, where resource is reused, where possible, or recycled. The same goes with digital services and ICT technologies, where circulation and sustainability shall be the key factors.[21]

1.4. A Europe fit for the digital age

As a part of its climate-neutrality objectives for 2050 the European Commission has also included plans over creation of sustainable and prosperous digital future. The Commission has in its Communication to the European Parliament, European Council and European Economic and Social Committee and the Committee of the Regions on 2030 Digital Compass: the European way for the Digital Decade stressed the necessity of digital transformation in the Union by the means of joining forces. A notion "digital sovereignty" was used by the President of the European Commission, Ursula von der Leyen, who emphasized on the need for a European Cloud and the leadership of the EU in digital sphere. The 4 key components for the benefit of the goal listed in the Communication were a digitally skilled population and highly skilled digital professionals (1), secure and performant sustainable digital infrastructure (2), digital transformation of businesses (3) and digitalization of public services (4). In addition, it underlined the need for digital citizenship, that could allocate the same benefits as the citizens of the EU currently enjoy to the digital space. Principles of data protection and fundamental rights shall apply there and new principles suitable for digital space, e.g., Universal Access to internet services should be enlisted for the benefit of the citizens.[22]

The 4 key components and the strategy overall require the cooperation between the Member States and the EU, as there is need for critical mass of funding and cross-sector alignment of all actors. The Multi-Country Projects are already in discussion between the Member States, and thrive to

[20] Ramiro Troitino, D. (2013). *Energy Policy in the EU and its Influence on East and Central Europe.* Journal on Legal and Economic Issues of Central Europe. 4. 106−113.
[21] *Supra nota* 18.
[22] European Commission (2021) COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS *2030 Digital Compass: the European way for the Digital Decade*. COM/2021/118 final

connect, scale up, modernize, reskill and upskill. Together with the support by the Commission and the smart allocation of funding such projects could easily meet their targets.[23]

Therefore, besides the existing interconnection in cyber-space, the EU is moving towards increasing the cyber-related cooperation between Member States and higher alignment of several services. At the same time, to provide the security for the cyber related systems that have vital importance to the well-being of the Union. Hence, together with the growth in interconnectivity and the creation of Europe Fit for Digital Age, it shall be followed by development in the area of cyber-security and defense capabilities, which should, logically, start from the development of international law interpretations in cyber space and adoption of principles, which shall be discussed in the following chapter.

[23] *Supra nota* 13.

2. COLLECTIVE COUNTERMEASURES IN CYBER SPACE

2.1. Cyber-attacks and legislation

2.1.1. Cybersecurity

Cybersecurity lies on 3 main pillars, CIA, namely confidentiality (1), integrity (2) and availability (3). Each of the pillars is a core element to information security. Confidentiality serves the purpose of keeping the information secure over an unauthorized accession, unavailable for irrelevant third parties. A more confidential type of data should be accessible to lesser number of parties and organized correspondingly. Integrity refers to the protection of accuracy and completion of the information. Once submitted, data should be free from unauthorized modifications. Data, especially critical data should be accessible in times necessary. Systems critical to the well-being and functioning of societies are deemed especially important in availability, thus strict requirements shall apply on their security controls and software. Those pillars if operating as intended, secure cyber space for its users and provide a mean of analysing and direction of management of systems to organizations involved.[24]

The 3-pillar approach is relevant to both, private enterprises, and public sector. Ensuring security in cyber space, to the best possible extent can help to prevent and manage possible cyber-attacks. Although the preventive measures are useful and contribute into lessening the number of cyber-attacks conducted, it unfortunately is, that a smart hacker can hide itself on the Internet and thus can be anonymous even in the case of wide-scale attacks.[25] A paradox that exists in cyber space is that those more developed are under a greater risk of being harmed by a cyber-attack, as they have more to lose if attacked. In contrast to logical perception, a better and more advanced equipment in cyber space does not provide a state with greater protection, but greater probability of being harmed, as an misfunctioning of some system is more influential.[26]

[24] Haber, M. & Rolls, D. (2020). *The Three Pillars of Cybersecurity*. 10.1007/978-1-4842-5165-2_1.
[25] Geers, K. (2011). Strategic Cyber Security. Tallinn: CCD COE Publications. 11. ISBN 978-9949-9040-5-1.
[26] *Supra nota* 21. 10

One of the great problems with the current regulation of cyber space is the lack of rules on attribution. The general result of this shortage is that the probability of non-warned attacks against critical national infrastructures. Anonymity of actors in cyber space provides the attackers with advantage over the attacked, as detection and counteracting of the villain is made difficult.[27] There are 3 main principles of international law, which application could help to track and target cyber-attackers and render responsibility to states for cyber operations conducted on their territories. Those principles are sovereignty, *due diligence*, and collective countermeasures.[28] Sovereignty means simply that a state shall respect the sovereignty of another state, more specifically in cyber context it means that if a cyber operation has effect on the another, it is a violation of its sovereignty and if a cyber operation interferes the government functions (e.g., election process) of another. Such recognition of the sovereignty principle could help to identify if a state has been harmed in a cyber operation, that for now remains a grey area.[29]

Due diligence, as mentioned above, gives a state responsibility over actors under its sovereignty. This means if an actor A conducts a cyber-attack for state B against infrastructure of state C the attack could be effectively attributed to state B. Without *due diligence* applying it is difficult to attribute the responsibility of initiation to state, as it is easy for them to claim to have no connection to the attack.[30] Collective countermeasures in cyber space first provide states with a kind of insurance of protection, if infrastructures get damaged to the extent where it becomes incapable of responding, the attackers can be tracked and targeted by other states. Collective countermeasures are especially effective in cases of highly interconnected cyber spaces, where the level of small threats is constantly high.[31]

The flexible nature cyber space gives an advantage to an attacker as well as to the defender, who both can use that off for their benefit. An attacker can easily re-evaluate and target its focus, while the defender can relocate the strategic data and critical infrastructure.[32] The threat to cyber-attacks is real and perceptible, it is no more a futuristic concept, but a tangible form of interference, that provides the interferer with a wide range of possibilities for an attack. Cyber threats are named to

[27] *Supra nota* 21. 11
[28] Kelsen, H. (1952). *Principles of International Law* (New York: Rinehart & Co., 1952)
[29] Schmitt, M. (2021). *Three International Law Rules for Responding Effectively to Hostile Cyber Operations*. Just Security. Retrieved from: https://www.justsecurity.org/77402/three-international-law-rules-for-responding-effectively-to-hostile-cyber-operations/
[30] *Supra nota* 20.
[31] Kosseff, Jeff (2020). *Collective Countermeasures in Cyberspace,* Notre Dame Journal of International & Comparative Law: Vol. 10 : Iss. 1 , Article 4. Retrieved from: https://scholarship.law.nd.edu/ndjicl/vol10/iss1/4
[32] *Supra nota* 21. 13-15

be the most extensive and powerful, as they provide the attacker with unprecedent speed and and scale. The impact of such attacks is difficult to predict, and cyber arms control is hard, or better said impossible, to exercise for the vast size of cyber space.[33] However, exercise of the three of general principles mentioned above, sovereignty, *due diligence*, and countermeasures, have high potential of making the attribution and management of possible cyber events easier and thus contribute into the prevention of advantage taking of the lack of rules existing.[34]

Development of IT systems and Internet has brought governments worldwide in front of a decision of finding balance in the appropriate number of restrictions and freedoms in cyber space. Too little freedom may violate the evolving rights of citizens and make the government tempted to use off their restrictive and surveillance powers, while an extensively liberal approach can result in flourishing of Internet related crimes and disorder.[35]

2.1.2. Categories of cyber operations

To understand the potential scope of cyber-attacks, the common categories of cyber operations need to be identified. There are 3 main means that cyber-attacks can be conducted by. Those are unauthorized access to computers or computer systems (1), malicious software (2) and DoS attacks (3). The first, access to computers or computer systems means in the first place the access to information, which can include for example classified information or personal data. Such data can be used off for the creation of fake identities or accounts, demand of ransom or other similar purposes, while it is also possible that the data accessed is modified or reprogrammed. The computers and computer systems can also be misused if access is gained.[36]

Malicious software, also known as malware, has 4 principal categories: viruses and vorms (1), Trojans (2), bots (3) and spyware (4). Viruses, vorms and Trojans serve the same purpose of disabling and accessing information and functions of the device. Bots allow computers to be controlled remotely. Spyware monitors the use of system and communicates with third-party, who can use the information received for the conduct of surveillance.[37] DoS, denial of service attacks makes the computer or computer systems unfunctional and can thus be used to target some service

[33] Brown, G. (2019). *Commentary on the Law of Cyber Operations and the DoD Law of War Manual*. In M. Newton (Ed.), *The United States Department of Defense Law of War Manual: Commentary and Critique*. Cambridge: Cambridge University Press. 337-359. doi:10.1017/9781108659727.015
[34] *Supra nota* 21. 155-157
[35] *Supra nota* 21. 70-71
[36] Clough, J. (2015). *Principles of Cybercrime.* (2nd ed.). Cambridge: Cambridge University Press. doi:10.1017/CBO9781139540803. 33-37
[37] *Ibid*. 37-43

or function. DDoS, distributed denial of service attacks allows for more rapid attacks with a wider scale of target.[38]

2.2. What is a cyber-attack?

Cyber-attack has been defined by the EU legislation as actions that involved access to information systems, information system interference, data interference and/or data interpretation which is unauthorized and non-legal under the legislation of the Union or Member States.[39]

In the EU legislation cyber-attacks having a (potential) significant effect are those, which[40]:

1) originate, or are carried out, from outside the Union;
2) use infrastructure outside the Union;
3) are carried out by any natural or legal person, entity or body established or operating outside the Union; or
4) are carried out with the support, at the direction or under the control of any natural or legal person, entity or body operating outside the Union.

The significant effect of an attack constitutes influence amongst other on information systems, that constitute[41]:

1) critical infrastructure, including submarine cables and objects launched into outer space, which is essential for the maintenance of vital functions of society, or the health, safety, security, and economic or social well-being of people;
2) services necessary for the maintenance of essential social and/or economic activities, in particular in the sectors of energy (electricity, oil and gas); transport (air, rail, water and road); banking; financial market infrastructures; health (healthcare providers, hospitals and private clinics); drinking water supply and distribution; digital infrastructure; and any other sector which is essential to the Member State concerned;
3) critical State functions, in particular in the areas of defense, governance and the functioning of institutions, including for public elections or the voting process, the functioning of

[38] *Supra nota* 36. 43-45
[39] Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.
[40] *Ibid.*
[41] *Ibid.*

economic and civil infrastructure, internal security, and external relations, including through diplomatic missions;

4) the storage or processing of classified information; or
5) government emergency response teams.

2.3. Applicable law

"Absence of legal prohibition constitutes the presence of a legal permission" is a dated view on international law, that was once used to justify certain state activities. Thus, even in the absence of field specific regulations, customary law and treaties shall be applied to cyber-attacks, as they are on regular cases of use of force. The following chapter will use relevant arguments to determine the rightfulness of the assumption.[42]

International Court of Justice (ICJ) has concluded in its ruling of Dispute Regarding Navigational and Related Rights (Costa Rica v Nicaragua)[43]:

Where parties have used generic terms in a treaty, the parties necessarily having been aware that the meaning of the terms was likely to evolve over time over time, and the treaty has been entered into for a very long period or is "of continuing duration", the parties must be presumed, as a rule, to have intended those terms to have an evolving meaning.

Such a ruling is in accordance with the implementation of the Vienna Convention on the Law of the Treaties Article 31(3)(b) and the interpretive reorientation.[44] Furthermore, the applicability of the norms of international law is affirmed to influence cyber operations according to several state's positions. The applicability of *jus in bello* norms is especially important for the protection of civilian population, who can easily become the unwanted targets of cyber-attacks.[45]

Overall, the applicability of international law in cyber space has been recognized and stated already a few times, by different states and international organizations. It has become a common position

[42] Roscini, M. (2014). Cyber Operations and the Use of Force in International Law. Oxford: Oxford University Press. doi:10.1093/acprof:oso/9780199655014.001.0001
[43] International Court of Justice (2019). *Dispute Regarding Navigational and Related Rights*, (Costa Rica v. Nicar.). I.C.J. (July 13)
[44] Gardiner, R. (2015). *Part II Interpretation Applying the Vienna Convention on the Law of Treaties, A The General Rule, 5 The General Rule: (1) The Treaty, its Terms, and their Ordinary Meaning.* Treaty Interpretation (2nd Edition). Oxford: Oxford Scholarly Authorities on International Law. ISBN: 9780199669233.
[45] Lin, H. (2012). *Cyber conflict and international humanitarian law*. International Review of the Red Cross, 94(886), 515-531. doi:10.1017/S1816383112000811.

in general, however the scope of applicability is that what is argued over. The discussion evolves over the necessity for a new treaty of international law and the context of such a treaty, which is largely a political, not legal discussion.[46]

2.4. Collective countermeasures in cyber space

2.4.1. Countermeasures and collective countermeasures

The Oxford Dictionary of Law defines countermeasures as:

"Actions, military or economic, taken in response to the conduct of another state that are not necessary or justifiable as self-defense. As with other forms of force, the unilateral use of such countermeasures may be illegal under the UN Charter unless it be approved by a UN Security Council resolution (..)"

Countermeasure is a proceeding taken against an act of another. Countermeasure is not per se justified, it needs to be approved by the UN Security Council resolution, that deems the countermeasure necessary. A countermeasure does not always imply military actions, but can also be economic, while the extent of both types of measures is subject to be decided by the UN Security Council. A countermeasure can be taken only as response to an act from another state, which makes it different from sanctions, that can be used to target possible threats.[47]

The right to take countermeasures offers a state possibility to act on the conduct of another state, foremost in cases where peaceful resolution of the matter would be ineffective or slow. It is a well-functioning measure of self-help, that gives a state possibility to protect its own territory and citizens.[48] The Articles on Responsibility of States for Internationally Wrongful Acts allocates the right to take countermeasures over a state responsible for an internationally wrongful act to an injured state. The purpose of the countermeasure shall be to remake the breaching state comply with its obligations and make amends for the act of incompliance.[49] Countermeasure shall not be

[46] Delerue, F. (2020). *Does International Law Matter in Cyberspace?* In *Cyber Operations and International Law* Cambridge Studies in International and Comparative Law. Cambridge: Cambridge University Press. 10-28. doi:10.1017/9781108780605.001.
[47] Orakhelashvili, A. (2011). *Collective Security.* Oxford: Oxford University Press.
[48] Aust, A. (2005). *Handbook of International Law*. Cambridge: Cambridge University Press. 424-426. ISBN-13 978-0-521-82349-4.
[49] *Supra nota* 46. 425-426

seen as a mean of punishment, but necessary acts of achieving desired effect, termination of breach of obligations. Thus, once the objective is achieved, the countermeasures shall be extinguished.[50]

In its essence, a countermeasure shall be proportional to the injury borne: 'the gravity of the wrongful act' and 'the rights in question'.[51] Although there is no system of equivalate, the common understanding is that the countermeasure taken shall be as closely related to the breach as possible.[52] Hence, any countermeasure taken, needs to be proportional to the breach of international obligations of the other state and the rights of the measure-taking state. To take a countermeasure, a state needs to follow a procedure specified in the Article 52 on conditions relating to resort to countermeasures.

First, a call over ceases of the breach and offer to pay reparations shall be made by the injured state towards the state responsible for the breach. It should be followed by a notification of the implementation of countermeasures by the injured state and an invitation to negotiations.[53] While the two conditions are absolute in a broad range of breaches, an exception is made, if the preservation of one's rights expects an immediate employment of countermeasures.[54] Fourth, a countermeasure can only be exercised until the breach is ceased or the dispute is pending in a court relevant in jurisdiction or a constituted tribunal. Fifth, a countermeasure is only to be taken if the state responsible does not show good faith in reaching a solution by any other mean or demonstrates non-compliance measures.[55]

Together with the conditions above, a state intending to use countermeasures needs respect 4 obligations, that cannot be disregarded by countermeasures taken. They are[56]:

a) the obligation to refrain from the threat or use of force as embodied in the Charter of the United Nations;
b) obligations for the protection of fundamental human rights;
c) obligations of a humanitarian character prohibiting reprisals;
d) other obligations under peremptory norms of general international law.

[50] The Articles on Responsibility of States for Internationally Wrongful Acts
[51] *Supra nota* 50. Article 51
[52] *Supra nota* 46. 426-427
[53] *Supra nota* 50. Article 52(1)
[54] *Supra nota* 50. Article 52(2)
[55] *Supra nota* 50. Article 52(2)
[56] *Supra nota* 50. Article 50(1)

Countermeasures do not exempt a state from fulfilling obligations:

a) under any dispute settlement procedure applicable between it and the responsible State;
b) to respect the inviolability of diplomatic or consular agents, premises, archives, and documents.

It is important to differentiate between a countermeasure and retorsions, reprisals, sanctions, and suspensions of treaties. Retorsions are acts that are taken against another state, which do not interfere its rights under international law. [57] Reprisal is a retaliation taken in time of war, that can be taken in a response to breach of international humanitarian law. It can be considered illegal under normal circumstances, however, must not target civilians or be unproportionate.[58] Sanctions are peaceful measures of making a breaching state comply with international law. They are restrictive in the nature, preventing a state from conducting an otherwise lawful act. Sanctions can be related to trade, finance, travel etc, thus can be targeted against a relevant field.[59] Treaty suspension and termination can be used, as a response to the breach of the relevant treaty[60].

2.4.2. Countermeasures in cyber space

Applicability of right for countermeasures in cyber space is partly deemed an integral part by several states, but on the other hand challenged by others. There is no specific treaty targeted towards cyber operations, only some legal analysis on the issue, for example the Tallinn Manual I and II.[61]

2.5. EU and its Member States positions

Unlike to some areas, e.g., sovereignty, where EU member states have common understanding of implementation of principles of international law in cyber space, countermeasures and collective countermeasures have received little commodity. On the first level, states have not agreed on the need for notification of countermeasures, where Italy, France and Netherlands argue that notification of countermeasures is not always necessary. Estonia, Germany, and Netherlands agree

[57] *Supra nota* 46. 425
[58] *Supra nota* 46. 257
[59] *Supra nota* 46. 217-221
[60] *Supra nota* 46. 103
[61] Schmitt, M. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd ed.). Cambridge: Cambridge University Press. doi:10.1017/9781316822524

that attribution is a necessary step before taking any countermeasures, while Finland argues that attribution may be possible after taking the countermeasures. Collective countermeasures in cyber space are promoted by Estonia, while France position excludes such possibility.[62]

Estonia considers countermeasures as inherit right of self-protection of a state, which can be be realised by injured states, if cyber operation is unfriendly or violates international law obligations. The aim of such measures is to motivate the violating state to re ensure peace and responsibility in cyber space. A countermeasure can only serve the purpose of making the violating state to comply with its international obligations again and cannot thus take non-proportional countermeasure. A countermeasure can be either individual or collective and can, taking into consideration the latter, violate some principles of international customary law and treaties. Attribution must be exercised prior to taking of countermeasures.[63]

France on the other hand does not allow for collective countermeasures to be taken. They argue that countermeasure can be taken by a state to protect its interests and ensure these interests are respected or to induce the responsible state to comply with its obligations. The aim of the countermeasure shall be to make the responsible state comply with its obligations, thus attribution is necessary, as responsible state must be identified, however, notification to that state does not have to be delivered if the injured state interests are on the stake.[64]

There have been some recommendations by EU Commission to develop a common strategy towards the response on "cybersecurity incidents and crises". One of such is the COMMISSION RECOMMENDATION (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises. The principal idea of the Recommendation is that Member States and Eu institutions shall have a common response to large-scale cybersecurity incidents and crisis on national and European level. This response should also include the practice of the response and political response, together with private sector involvement if necessary. The response may be in several forms, from identification to investigation to operational decisions. The political level shall allow for use of Framework for a Joint response to malicious cyber activities or European protocol for countering hybrid threats.[65]

[62] CCDCOE (2021). European Union. Retrieved from: https://ccdcoe.org/organisations/eu/
[63] *Supra nota* 48. Article 2.
[64] CCDCOE (2019). National position of France. Countermeasures. Retrived from https://cyberlaw.ccdcoe.org/wiki/National_position_of_France_(2019)#Countermeasures
[65] COMMISSION RECOMMENDATION (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises.

The Commission has also proposed building a Join Cyber Unit in 2021. The purpose of such Cyber Unit would be the coordination of EU and Member States actions to large-scale cyber incident and crises. Such an Unit would allow mutual assistance and shared expertise, together with private sector actors.[66]

2.6. Tallinn Manual 2.0 interpretation

Tallinn Manual focuses on the interpretation of existing laws in cyber space, with the main argument being that those existing norms can be converted into cyber space, without the need to create new norms and treaties. The argument is (by EU, US, Canada, UK, Australia etc.) that there is enough of legal norms in existence and there is no need for new legislation on the topic, but the interpretation of the existing into the field of cyber security. While the argument is challenged by China and Russia, who argue for the need of specific convention for cyber security issues, some work is however has been started in the name of Tallinn Manual, which is created by international experts, who interpret the existing norms regarding cyber space and create so called guidelines for the topic. So far Tallinn Manual I and II have been published and the III is in the process of writing. The main question that is posed by the authors is "How international law applies in cyber space?".[67]

The main argument in the Manual is that international law, especially the UN Charter applies in cyber space. Tallinn Manual I addressed issues of risks and probabilities of events happening, together with humanitarian issues, while the second looks further into specific issues regarding cyber security and cyber warfare. Neither of the Manuals touches the topic of collective countermeasures, only state countermeasures.[68]

2.7. Practical scope of cyber-attacks

US oil pipeline system Colonial Pipeline became target of a cyber-attack on 7 May 2021. A day before approximately 100 GB of data was stolen from the company, so the attackers could hold it

[66] COMMISSION RECOMMENDATION (EU) 2021/1086 of 23 June 2021 on building a Joint Cyber Unit.
[67] CCDCOE. (2022). The Tallinn Manual. The NATO Cooperative Cyber Defense Centre of Excellence. Retrieved from: https://ccdcoe.org/research/tallinn-manual/
[68] *Ibid.* and Schmitt, M. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

against ransom[69]. The attack made systems of the Colonial Pipeline inaccessible to its operators and thus resulted in disruptions in fuel supply chains. As a result, 5,500 miles of pipeline, carrying 45% of US East Coasts fuel supply were disrupted. While Colonial Pipelines were able to get their systems back to functioning and prevent massive disruptions, it is believed by experts that another one may not go as easy. The aim of the attack in that case was not to cause damage to the systems, but to demand ransom, while another attack against such critical infrastructure may be aimed to target the infrastructure and thus result in far worse outcomes.[70]

[69] Kelly, S. and Resnick, J. (2021). One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators. Reuters. Retrieved from: https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/

[70] Morrison, S. (2021). How a major oil pipeline got held for ransom. Vox. Recode. Retrieved from: https://www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices

3. DISCUSSION

3.1. Potential scope of cyber-attacks against the Member State of the EU

3.1.1. Energy Market

As because EU Member States are very dependent on each on other on their energy supplies and infrastructures that allow for the supply, they are vulnerable to disruption caused to the infrastructure. Such disruption could be, as was shown by the example of Colonial Pipelines caused by cyber-attacks, targeted against the computer system of the supplier or distributor. Energy is one of the most fundamental needs of society, as almost everything else needs energy to function or to be produced or distributed.

The current vision of the EU is to enlarge the percentage of renewable energy resources to maximum by the year of 2050, in other words EU wants to become climate neutral by 2050, which means the use of non-renewable resources needs diminish. However, as green energy production does not provide yearly supply of sufficient energy resources in each state, such plans for climate neutrality do require further interconnections of infrastructures and supply chains that are capable of transporting energy from one side of the Union to the other.

The EU created Green Deal shall combine and connect the energy market of the Union and make the best use of the possible renewable energy resources of each region. The plan bases on interconnecting and digitalising energy market to make it more effective and climate neutral. The plans thus include a considerable rise in interconnections which the energy supply bases on. Consequently, the threat of EU wide disruption in supplies would become higher than ever and the exposure to potential cyber-attack threat affecting several Member States at once, would be higher than it is now.

While theoretically the discussion is only on the future aspect, as today's interconnection is lower, and the threat in that sense arguably smaller, it is still highly important that preventive measures instead of post factum ones would be set.

The Green Deal is a plan with a great potential, which can however have significant effects on the security of the Member States, when the levels of interconnection and digitalisation are used off. An attack against an energy supplier can constitute energy crisis on a large scale within the EU if the supplies do not reach their consumers. As energy is vital in the functioning of most developed states, as is the precondition of most other systems to work, the harm done can be considerably severe. As the energy market, in the case of the EU is not state-centric, but deeply interconnected (with developments towards further interconnections) it can be reasonably expected, that attack against one member state, can cause harm to many others. Therefore, as the injury will be borne by not only the state targeted, but many others, it means that the right over taking countermeasures is extended.

3.1.2. Banking sector

Finance is one of the bases for modern economies, as nothing functions without money flows. The importance of the banking sector is well portrayed by the monetary crisis of 2008, where the crisis in baking sector in only a few member states resulted in crisis in most others. It is the fact the big private banks of the EU as well as Central Banks are highly interconnected. The free movement of capital and single currency in the use in majority of the member states, together with remarkable connections due to public debt make the banks first highly reliable on each other, and second, gives the whole system control over the state of economy in the whole Union. A great deal of banking bases on the internet, and many of the transactions is made on online based mechanisms, thus banks are vulnerable towards cyber-attacks. Although it is not such to target the whole sector at once, it nonetheless brings it down to a fact where the levels of interconnections and on the stake of economic wellbeing,

3.2. Benefits of the ability to take collective countermeasures

Cyber-attacks can take down systems necessary for the normal functioning of states infrastructure and wellbeing of its citizens. Where a system is taken down and where the state, which is harmed is under severe attacks and cannot replace or relocate the systems, and unable to conduct counterattacks, it would provide a great help if other Member States could give the state suffering a hand.

Furthermore, such right to use collective countermeasure allows to effectively respond to serious breaches of international law in cyber space, as type of enforcement mechanism, which is essential if the international systems wants to continue to function as it is. While the legislation sets the boundaries for states to act in, then law enforcement mechanisms give the practical scope for laws and possible breaches.

While many used to believe in balance of powers and the principle not giving other reason to attack, it is fair to say that such beliefs should exist no longer, after the aggression of Russia on Ukraine. It is not that friendly relations should not prevail, but that having some guarantee of security. The possibility to use collective countermeasures would, for the Member States of the EU allow the states to have the guarantee, both for themselves and for the other, that is some important unit of infrastructure is attacked, the power that can take countermeasures is considerably higher, than only ones.

The use of collective countermeasures is a tool that can help to prevent attacks thought posing a higher risk in attack targeted against a state of the EU. It is clear, that no aggressor wants to go alone against a bigger coalition, therefore if the the use of countermeasures would be extended, it would consequently result in a smaller possibility of an actual attack taking place.

Another possible positive effect that the possibility of taking collective countermeasure would be that the cooperation for security in cyber space, as the stakes are higher, than they are if each individual state is responsible for its own cyber security. To able to help each other, the states shall have rather similar cyber resilience capabilities and strategies, which means that we field could develop from the cooperation. If the level of cyber defense capacities does not match, and there are some states who are far behind the average level, it means that the potential of an attack happening there is considerably higher, and thus the ones strongest shall contribute more. While this is not a negative denominator, it is still however that equal levels of capabilities would be more beneficial to all. Therefore, a positive effect to the larger field of cyber security and cyber defense capacities is detected.

3.3. Negative effects of collective countermeasures

Collective countermeasures and even simple countermeasures on cyber-attacks would unarguably require comprehensive considerations over the methods and extent of such. It is relatively easy to

take a countermeasure on a cyber-attack, without paying much regard to the consequences. However, as cyber-attacks are like non other, in the sense that the source of the attack can be extremely difficult to determine, and the extent and participation of actors is unclear.

It is fairly argued that the more actors there are involved in the conflict, the more difficult is gets and the further it can escalate. E.g., to take a hypothetical situation, where there are two states, that are involved in a military conflict, and third and fourth, each in a military union with one of the parties, get involved as well. The conflict escalates to further, as new powers and resources are brought into the conflict. Escalation is most certainly not something that should be reached for, but something that shall be avoided if possible.

The same applies to cyber-attacks, where escalation shall mean, that more and more systems are constantly under attack, and where the possibility of something severe happening rises because of that. If states are starting to take collective countermeasures against cyber-attacks, they may escalate the conflict.

3.4. Legal ground for countermeasures

The lack of cybersecurity regulation and the mere fact of recognition of international law being applicable in cyber space have resulted in rather narrow definition on cyber security related issues. As much of the framework, that states have agreed on bases on multilateral communications, but has not been *per se* agreed on, there is not much what could be interpreted as legislative. The EU has held its internal communications, and states published statements for a while now, however no consensus has been reached in a few of the utmost basics, such as is countermeasures and collective countermeasures.

It is a rather dated approach, that absence of legal prohibition constitutes a legal permission. In the view of more modern and updated view, which considers the changing nature of law, absence of legal prohibition must not be regarded as permission, as that only represents a dated view on states that wish to use the grey areas of international law for their benefit. It is clear, that no area of law can be fully developed and up to date every moment, as technologies, societies and views change that much faster. Similar applies to treaties, which should bear in mind the open interpretation and development that are to come, not the exact situation, which existed upon the ratification. It is

necessary to see the laws as interpretative, rather than exhaustive, because it is impossible to fully regulate and keep up to date all aspects that may be relevant at some point or another.

That is why, it is, in the consideration of future and nature of laws to take the best out of what already exists, for example the recognition of international law applying in cyber space has a great potential in saving a lot of resources, as that the only thing that could be necessary is the interpretations. As the international law allows for collective countermeasures to be taken and recognizes them as one of the core principles of international law, it is that international law as it is, poses no contradictions to collective countermeasures in cyber space whatsoever. Until there is no general agreement between the states on the interpretation of the international law in cyber space international cyber security can be considered as soft law, which is bound to generally regulate the area, and give some instructions and politically binding agreements, whereas there are developing in time. Soft laws are not legally binding, and thus they set a general framework, but leave room for flexibility and interpretation. They are very political in their nature, as they are based on agreements between states and represent some consensus between those states but have no real legal power.

Thus, in the absence of hard law and soft law one the topic of collective countermeasures, it can be said, that there is an absence of legal regulation of the topic. Hereby, the analysis can be conducted based on general international norms and their interpretations on the applicability in cyber space, with a principle in mind, that the absence of legal prohibition does not constitute a permission.

There is no legal contradiction to the possibility of the EU Member States to take collective countermeasures in cyber space, as to the agreement between states on the applicability of international law in cyber space and principle of no legal prohibition not constituting a legal permission.

3.5. Can collective countermeasures be justified in the context of the EU Member States

In its nature, a countermeasure requires harm done towards an actor before it can be taken. Therefore, one of the first conditions for the EU Member States to have the ability to take collective countermeasures, would be that the influence of potential cyber-attack reaches outside one

Member State. A precondition, that allows for countermeasure to be taken is injury that is a result of a breach of international law of another state. Therefore, to be able to take collective countermeasures it is necessary that the states, who can take these countermeasures are are suffering from injury that is caused the breach of international law of the other state.

The definition of injury under the right to take collective countermeasures includes injuries that are indirect, as if the breach of international law, especially in cyber space is highly likely to spread outside the state borders and cause injuries, whether planned or unplanned, to those third states. Hence, the injury caused does not have to be direct, but real and perceivable, as well as measurable, as the countermeasures taken need to be proportional to the injury suffered. Second important factor that must be considered is legality of such countermeasures. Basing on the assumption that international law applies in cyber space, the answer should be rather finite, however, in the near non-existence of further interpretations, it is not as straightforward as.

Countermeasure goes beyond self-defense, it does not have to be justified or necessary measure of self-defense, but a response to conduct of another state. It does not include the notion of individual measure but needs to be proportional to the injury suffered by a state. That in the essence opens the possibility to take collective countermeasures, as mutual injuries give the states the possibility to act against the breaches and force them to stop using force, normally not allowed under international law.

It can be concluded, as there are no contradictions to international law, and the potential existence of mutual injuries caused by cyber-attacks to the states, which are caused by the interconnections the states share, that there is the Member States of the EU shall have the right to take collective countermeasures against cyber-attacks. The ability to take collective countermeasures, and such an agreement between states of the EU to use the ability in cases necessary does not only provide them with a more extensive defense capabilities, but also more effective preventive framework, which bases on collective security, where there is no longer only one vulnerable state in cyber space, but a Union of states that are able to take countermeasures if such need arises for each other. The greater are the defense abilities, the lower is the risk for security, as no more or less sensible state would not like to use force in cyber space against another, if the counterthreat to that state, in the form of collective countermeasures is considerably high, and its is likely that the initiator state will be forced to cease the attack with no aims reached, the probability of attack diminishes.

CONCLUSIONS

There has been discussion on the rules governing cyber space and cyber-attacks over a period of few decades, however no other conclusion than the mere understanding that international law applies in cyber space has not been reached. There has been some development in the area, as some states have issued their positions on the matter, however no certain outcome has been reached. In the heart of international law are its core principles, one of which is countermeasures, that can be, in the case of ordinary international law application either individual or collective. Although collective countermeasures have only been promoted by Estonia at this point and on the contrary rejected by France, the discussion focused on two aspects of right to use collective countermeasures in the context of the EU, the practical and legal right. The discussion was formed in the context of the EU Member States and their right to use collective countermeasures on a cyber-attack.

As the definition of countermeasures stresses the importance of state borne injury as a precondition that it can be taken, and thus, as it also applies to collective countermeasures, it must be, that a cyber-attack against Member States of the EU will result in injuries to others. Such distribution of effects of an attack can take place, if the interconnections between systems in use in the Member States are high, and their likeliness of the effects distributing is therefore considerable as well. One the basis of such assumption of existence of interconnection in two relevant sectors, energy, and banking, were analysed. It was found that both, assuming the continuation of at least the current levels, have considerable interconnections between the Member States of the EU and hence destructive cyber-attack against a system in considerable size in either sector will result in injuries to other states of the EU besides the one targeted.

The paper sought answer to the question whether collective countermeasures against cyber-attacks could be, for the interconnections they share be justified in the context of the EU. It analyses and explores the possibility of using collective countermeasures on cyber-attacks conducted on the EU's Member States and then, secondly, to provide a legally argumented overview for the operational use for the entity's common framework on cyber security. It will analyse the two fields,

the interconnection of the EU and collective countermeasures separately to gain extensive understanding in both, and then continue to tie the two topics together.

The hypothesis for the research were stated as follows: The EU's interconnection in cyber space provides its Member States with the right to collective countermeasures. The interconnectivity levels in the EU are high, and thus, an attack on systems of special importance spreads or its effects spread across the Union. The analysis on the interconnection of the EU concluded that there are, at least two areas in the EU cyber space, where the interconnections between the systems of Member States are as significant as that they could, if targeted by a cyber-attack result in mutual injuries.

Collective countermeasures are a core principle of international law and as to the fact that international law applies in cyber space and that the absence of legal prohibition does not result in legal permission, the conclusion was reached, that there are no legal contractions to the ability to take collective countermeasures if all conditions, required to take countermeasures are fulfilled. Therefore, the conclusion reached by the paper was, that collective countermeasures against cyber-attacks are justified in the context of the EU Member States, based on their significant interconnections in cyber space. Although only two fields of interconnections were discussed, they were chosen to represent the vital importance to the Union as a whole, by their sectoral relevance to the functioning of the EU. Both chosen sectors, banking and energy, included relevant interconnections to the Member States, which, if targeted by a cyber-attack could lead to mutual injuries to the majority of the Member States. Those sectors were analysed, and it was found that they are first potentially very vulnerable towards cyber-attacks, as they nonfunctioning of such could either cause harm to economy or in the case of energy, have a direct and noticeable influence on the lives of people living in the EU, as without energy, many of the basic necessities for the society to function would the be

The justification of the use of collective countermeasures in the context of the EU Member States is necessary for development of common EU Cyber Security Strategy, together with interpretations on the applicability of international law in cyber space globally. This interpretation of the feasibility of such collective countermeasures shall be regarded as supportive framework, that would allow states to better understand the conception and legal ground for the collective countermeasures, together with their necessity for the Union.

The topic could be developed in further research by either widening of the research on other sectors, narrowing it down to a specific sector or by developing an extensive interpretation how exactly could the collective countermeasures apply to the EU. It could be discussed whether the collective countermeasures include some legal ground for only specific sectors, where the interconnections exist, or the applicability extensive and thus allows for the use of collective 9countermeasures in any area, apart from whether it includes interconnection within the Member States or not. Further research possibilities include discussions of other other vital elements of international law interpretation in cyber space and their connections to each other.

LIST OF REFERENCES

1. Alatalu, S. (2017). *One year after Warsaw: The growing need for a NATO cyber command*. 59-66. 10.1109/CYCONUS.2017.8167513.
2. Aust, A. (2005). *Handbook of International Law*. Cambridge: Cambridge University Press. 424-426. ISBN-13 978-0-521-82349-4 .
3. Brown, G. (2019). *Commentary on the Law of Cyber Operations and the DoD Law of War Manual*. In M. Newton (Ed.), *The United States Department of Defense Law of War Manual: Commentary and Critique*. Cambridge: Cambridge University Press. 337-359. doi:10.1017/9781108659727.015.
4. Chui, W. H. and McConville, M. (2017). *Research Methods for Law*. UK: Edinburgh University Press Second Edition. ISBN 978 1 4744 0425 9. 18.
5. Clough, J. (2015). *Principles of Cybercrime* (2nd ed.). Cambridge: Cambridge University Press. doi:10.1017/CBO9781139540803.
6. Delerue, F. (2020). *Does International Law Matter in Cyberspace?* In *Cyber Operations and International Law* Cambridge Studies in International and Comparative Law. Cambridge: Cambridge University Press. 10-28. doi:10.1017/9781108780605.001.
7. Eichengreen, B. (2009) *European Integration*. Oxford: The Oxford Handbook of Political Economy. Doi: 10.1093/oxfordhb/9780199548477.003.0044.
8. Gardiner, R. (2015). *Part II Interpretation Applying the Vienna Convention on the Law of Treaties, A The General Rule, 5 The General Rule: (1) The Treaty, its Terms, and their Ordinary Meaning.* Treaty Interpretation (2nd Edition). Oxford: Oxford Scholarly Authorities on International Law. ISBN: 978019966923.
9. Geers, K. (2011). *Strategic Cyber Security*. Tallinn: CCD COE Publications. ISBN 978-9949-9040-5-1.
10. Haber, M. & Rolls, D. (2020). *The Three Pillars of Cybersecurity.* doi:10.1007/978-1-4842-5165-2_1.
11. Kasper, A. & Vernygora, V. A. (2021). *The EU's cybersecurity: a strategic narrative of a cyber power or a confusing policy for a local common market.* Cuadernos Europeos de Deusto. 29-71. 10.18543/ced-65-2021. 29-71.

12. Kosseff, J. (2020). *Collective Countermeasures in Cyberspace*. Notre Dame Journal of International & Comparative Law. 10-1. Retrieved from: https://scholarship.law.nd.edu/ndjicl/vol10/iss1/4.
13. Lin, H. (2012). *Cyber conflict and international humanitarian law*. International Review of the Red Cross, 94(886), 515-531. doi:10.1017/S1816383112000811
14. Roscini, M. (2014). *Cyber Operations and the Use of Force in International Law.* Oxford: Oxford University Press. doi:10.1093/acprof:oso/9780199655014.001.0001
15. Orakhelashvili, A. (2011). *Collective Security.* Oxford: Oxford University Press. doi: :10.1093/acprof:oso/9780199579846.001.0001
16. Ramiro Troitino, D. (2013). *Energy Policy in the EU and its Influence on East and Central Europe. Journal on Legal and Economic Issues of Central Europe*. 4. 106−113.
17. Ramiro Troitino, D. (2013). *European Identity the European People and the European Union. Sociology and Anthropology*. 1. 135−140. doi: 10.13189/sa.2013.010301.
18. Siddi, Marco. (2020). *The European Green Deal: Assessing its current state and future implementation.* Finnish Institute of International Affairs. FIIA Working paper.
19. Sterio, M. (2008). *The Evolution of International Law*. Boston: Boston College International and Comparative Law Review. 31(2). 235-239 (2008), https://lawdigitalcommons.bc.edu/iclr/vol31/iss2/3 .
20. Schmitt, M. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd ed.). Cambridge: Cambridge University Press. doi:10.1017/9781316822524
21. White, N. (2018). *Legal Analysis: There's a Template for That!* ALSB Journal of Business Law & Ethics Pedagogy, 2(1) Retrieved from: https://ssrn.com/abstract=3248471
22. Kala, K. (2017) *Free movement of data as the 5th fundamental freedom of the EU.* e-Estonia. Retrieved from: https://e-estonia.com/free-movement-of-data-as-the-5th-fundamental-freedom-of-the-european-union/
23. Schmitt, M. (2021) *Three International Law Rules for Responding Effectively to Hostile Cyber Operations*. Just Security. Retrieved from: https://www.justsecurity.org/77402/three-international-law-rules-for-responding-effectively-to-hostile-cyber-operations/
24. Roncoroni, A., Battiston, S., D'Errico, M., Halaj, G. & Kok, C. (2019). *Interconnected banks and systemically important exposures.* Working Paper Series. 2331. European Central Bank. Retrieved from: https://EconPapers.repec.org/RePEc:ecb:ecbwps:20192331. 1-12
25. Treaty of the EU
26. Treaty on the Functioning of the EU
27. The Articles on Responsibility of States for Internationally Wrongful Acts

28. COMMISSION RECOMMENDATION (EU) 2017/1584 of 13 September 2017 on *coordinated response to large-scale cybersecurity incidents and crises*.
29. COMMISSION RECOMMENDATION (EU) 2021/1086 of 23 June 2021 on *building a Joint Cyber Unit.*
30. Council Decision (CFSP) 2019/797 of 17 May 2019 concerning *restrictive measures against cyber-attacks threatening the Union or its Member States.*
31. Costa Rica v. Nicar, 2009 I.C.J. (July 13). Dispute Regarding Navigational and Related Rights.
32. European Commission (2015) COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. *A Digital Single Market Strategy for Europe.* SWD(2015) 100 final
33. European Commission. (2019). COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS *The European Green Deal.* COM/2019/640 final.
34. European Commission (2021) COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS 2030 Digital *Compass: the European way for the Digital Decade*. COM/2021/118 final
35. European Parliament (2021). *FOREIGN POLICY: AIMS, INSTRUMENTS AND ACHIEVEMENTS.* Fact Sheets on the EU – 2021. Retrieved from: https://www.europarl.europa.eu/factsheets/en/home
36. CCDCOE (2016). *NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit.* The NATO Cooperative Cyber Defense Centre of Excellence. Retrieved from: https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/
37. CCDCOE (2019). *National position of France. Countermeasures*. Retrived from https://cyberlaw.ccdcoe.org/wiki/National_position_of_France_(2019)#Countermeasures
38. CCDCOE (2021). *EU*. Retrieved from: https://ccdcoe.org/organisations/eu/
39. CCDCOE (2021) *National position of Estonia.* Countermeasures. Retrieved from: https://cyberlaw.ccdcoe.org/wiki/National_position_of_Estonia_(2021)#Countermeasures
40. CCDCOE. (2022). *The Tallinn Manual.* The NATO Cooperative Cyber Defense Centre of Excellence. Retrieved from: https://ccdcoe.org/research/tallinn-manual/

41. Kelly, S. and Resnick, J. (2021). *One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators.* Reuters. Retrieved from: https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/
42. Morrison, S. (2021). *How a major oil pipeline got held for ransom*. Vox. Recode. Retrieved from: https://www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices
43. NATO (2017). *Warsaw Summit Communiqué.* Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016. Retrieved from: ://www.nato.int/cps/en/natohq/official_texts_133169.htm
44. Riigi Infosüsteemide Amet (2022) *RIA ohuhinnang: Ukraina vastased küberründed ja võimalik mõju Eestis.* RIA analüüsi- ja ennetusosakond koostöös CERT-EE-ga. 13.02.2022 Retrieved from: https://www.ria.ee/et/uudised/ria-ohuhinnang-ukraina-vastased-kuberrunded-ja-voimalik-moju-eestis.html

APPENDICES

Appendix 1. Non-exclusive licence

A non-exclusive licence for reproduction and publication of a graduation thesis[171]

I, Eva Lotta Penjam (*author's name*)

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis

A RIGHT FOR COLLECTIVE COUNTERMEASURES ON A CYBER-ATTACK: THE CONTEXT OF THE EU'S MEMBER STATES,

(title of the graduation thesis)

supervised by Vlad Alex Vernygora,

(supervisor's name)

1.1 to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;

1.2 to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.

[71] The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.

3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

May 12, 2022 (date)