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

Lisa Nevala

# What can be qualified as an armed attack in cyber operations under the Article 51 of the UN Charter under the energy sector in Finland?

Master thesis

HAJM08/18 – Law, specialization European union and international law

Supervisor: Kajander, Aleksi

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 18,616 words from the introduction to the end of conclusion.

Lisa Nevala, 04.01.2022
Student code: 194386HAJM
Student e-mail address: lineva@ttu.ee

Supervisor: Aleksi Kajander
The paper conforms to requirements in force

……
(signature, date)

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

# TABLE OF CONTENTS

# ABSTRACT

Armed attack definition is unclear in circumstances of cyber operations. The law applicable to this matter is the Article 51 of the United Nations Charter. The Article 51 is more reflective in the conflicts where kinetic weapons have been used instead of cyber weapons.

The topic of the thesis is what can be qualified as an armed attack in cyber operations under the Article 51 of the UN Charter under the energy sector in Finland. The Article 51 requires an armed attack, but it does not define what the "armed attack" is considered to be in cyber operations. This paper is going to answer the title question of the thesis.

The world is digitalizing even more. Digitalisation requires the energy sector for its functions. The energy sector has vulnerabilities for cyber operations. This thesis is focusing on the energy sector because the energy sector is an important issue due to the constantly evolving technology which uses electricity for its functions.

The thesis is divided into five different chapters. In the first chapter of the thesis, the thesis is going to give an overview of the importance of the energy sector. In the second chapter this thesis will answer to the research question by looking into the Article 51 of the UN Charter. In the third chapter, the thesis examines the research question through the Tallinn Manual 2.0. In the fourth chapter the thesis will examine the research question through the Finnish manual of cyber attacks. In the fifth chapter this thesis will give an answer to the research question through other non-NATO European Union countries that have qualified the armed attack definition in cyber operations.



**Keywords:** *article 51 of the united nations charter, armed attack, cyber actions, energy sector*

# INTRODUCTION

As internet and technology becomes an indispensable factor for the modern society, it sets threats for the states. Cyber attacks have been increasing globally[1]. Conflicts before have led to kinetic conflicts, as has been seen from the history in world wars, for example. Nowadays conflicts can lead to cyber attacks. As technology develops it is inescapable that states will attach computers to their weapon arsenal.[2] There have been numerous case examples about cyber attacks between states, for example, Russia against Georgia and the cyber attack against Ukraine's power grid. These attacks have shown the vulnerability of the technology which uses electricity. It has also shown the importance of cyber security.

Electricity is used in the energy sector to use and maintain technology as it is also used to heat houses. This study covers only the area where the energy sector is used in cyber operations. Electricity is important in Finland. In Finland, electricity consumption may triple over the next twenty years as a result of the technological developments.[3] It sets threats for the energy sector as pressure too from the perspective of a cyber operation.

Finland is an interesting subject because of its military relations. Finland is not a part of the NATO but Finland and NATO have cooperation in peace-support operations.[4] Finland and Sweden are the only non-NATO countries of the Nordic countries. Finland's neighbour is Russia which poses its own challenges for the NATO membership. Russian's President Vladimir Putin recently stated that he wants concrete agreements from NATO that they will not expand to east.[5] Even though

[1] Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. *Procedia Economics and Finance*, 28, 24-31.
[2] Lam, C. (2018). A Slap on the Wrist: Combatting Russia's Cyber Attack on the 2016 U.S. Presidential Election. *Boston College Law Review*, 59(6), 2167-2201.
[3] Helsingin Sanomat. (2021). *Kestääkö sähköverkko?* Retrieved from https://www.hs.fi/teknologia/art-2000007852046.html, 02.12.2021.
[4] NATO. (2021). *Relations with Finland.* Retrieved from https://www.nato.int/cps/en/natohq/topics_49594.htm, 02.12.2021.
[5] YLE. (2021). *Putin vaati Natolta, ettei sotilasliitto laajene itään – näin Niinistö kommentoi: uudet jäsenyydet ovat hakijamaan ja Nato-jäsenten välinen asia.* Retrieved from https://yle.fi/uutiset/3-12213883, 02.12.2021.

Finland and Russia have had their struggles, nowadays they have a good relationship between them. However, Russia has always tried to affect Finland's military relations.[6]

Russia also sets threats to Finland as a neighbour because Russia has been suspected of several cyber attacks, such as the attack against the Ukrainian power grid. Finland's geographical location could lead to a situation where Finland would be used as a battleground if a state would attack against Russia.

Finland has published a manual about its position in cyber operations. The manual was published in October of 2020. This thesis will also use the manual as assistance for solving the research question.

As the Article 51 does not define the word "armed attack" and as the energy sector becomes more relevant in the future as it is even today the research question of this thesis is what can be qualified as an armed attack in cyber operations under the Article 51 of the UN Charter under the energy sector in Finland. The thesis's aim is to research the definition of an armed attack from the UN Charter as well as from the Tallinn Manual 2.0 and the Finnish manual. Tallinn Manual 2.0 is a scientific research made by an international group of experts. Tallinn Manual 2.0 is done in cooperation with NATO. Tallinn Manual 2.0 has also defined the definition of an armed attack. This thesis will use the Tallinn Manual as assistance in solving the research question. The thesis will look into the Tallinn Manual 2.0 from the point of view of cyber operation, but the thesis will not examine the right for self-defence when a cyber operation occurs. As the thesis will research the research question through the presented sources, therefore the research will use qualitative methods.

This thesis will also search the answer to the research question through other manuals such as other cyber security strategies from other European Union countries which are not members of the NATO, because they have the same position as Finland. These countries are Sweden, Cyprus, Ireland, Malta and Austria.

To accomplish the aim of the thesis and answer to the research questions, the structure of the thesis is divided into five different chapters. The first chapter takes an overview of the importance of the

[6] Lukacs, J. (1992). Finland Vindicated. *Foreign Affairs*, 71(4), 50-63.

energy sector. The first chapter will present the vulnerabilities of the energy sector and present the importance why the energy sector is important to discuss in this thesis.

The second chapter of the thesis will examine the definition of an armed attack from the Article 51 of the UN Charter. The second part will analyse the definition from the peer-reviewed articles according to the article 51.

In the third chapter, the thesis will examine the definition of an armed attack from the Tallinn Manual 2.0. Tallinn Manual 2.0 is a novel scientific research concerning cyber operations. Tallinn Manual 2.0 has also noticed that the Article 51 of the UN Charter is unclear, and the international group of experts have also analysed the definition of an armed attack.

In the fourth chapter, the thesis will examine the research question from the Finnish manual of cyber actions. The thesis topic is concerning Finland and as Finland has made its own outcome for this matter it will be appropriate to use their own manual for this research.

In the fifth chapter the thesis will research the answer to the topic from other non-NATO European countries cyber strategies or cyber manuals that have taken their position in defining armed attack in cyber operations. The benefit of this approach is that because Finland is not part of the NATO these other non-NATO European countries give more value for the research.

The structure of the thesis is done so, that first the thesis will discuss about the energy sector which is important because the topic is focused on the energy sector. Then the thesis will discuss the Article 51 of the UN Charter in general. After that, the thesis goes deeper into the topic from Tallinn Manual 2.0 where the international group of experts have made a research about Article 51 of the UN Charter. In the end of the thesis, the thesis will concentrate to the Finnish aspect through the Finnish Manual. In the end of the thesis, the thesis will research other non-NATO European Union countries own outcomes to fulfil the whole topic of the thesis.

To achieve the aim of the thesis, which is answering the title question, this thesis will search the answer through peer-reviewed articles. In order to answer to the research question, this thesis will use as assistance case examples because they give a new perspective in analysing the research question through the examples.

# 1. CYBER ATTACKS AGAINST ENERGY SECTOR

This first section will be focusing on the threats that the energy sector has concerning cyber attacks. This section will give an outline for the topic and answer the questions of why the energy sector is important, topical and why this thesis will be focusing on the energy sector.

In this section the thesis will present new reports which show the vulnerability of the energy sector and also why the energy providers need to invest in their cyber security.

## 1.1. Definition of a cyber operation

Cyber operation is an operation which crosses sovereign boundaries contrary to any other kinetic weapon.[7] A cyber operation, which consists a cyber weapon, is usually called a cyber attack.[8] Later on the thesis it can be seen that qualifying armed attack's definition in cyber operations is usually used only when discussing about cyber attacks not cyber operations.

What is a cyber attack? There are different versions about the definition. One definition is that a cyber attack is a "deliberate exploitation of computer systems, technology-dependent enterprises and networks. Cyber attacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft."[9]

Other definition which is short and simple is the following: "cyber attack involves information technology employed as a weapon".[10] This definition is very different than the first one because

[7] Plazas, C. (2021). Information Crossroads: Intersection of Military and Civilian Interpretations of Cyber Attack and Defense. *University of Cincinnati Intellectual Property and Computer Law Journal*, 5.
[8] *Ibid.*
[9] Dynkin, B. (2018). Derivative Liability in the Wake of a Cyber Attack. *Albany Law Journal of Science & Technology*, 28(3), 23-44.
[10] Payne, C. (2017). Addressing Obstacles to Cyber-Attribution: A Model Based on State Response to Cyber-Attack. *George Washington International Law Review*, 49(3), 535-568.

this editorialises immediately the aspect of the weapon. Even though the definitions are different, they summarize together well the definition what a cyber attack can be. Cyber attacks can also be called cyber conflicts.[11] A conflict usually means different than an actual attack, the term cyber conflict doesn't determine the cyber attack very well because usually an attack's purpose is to cause something massive. Therefore, conflict as a term sounds less insignificant, because there can be conflicts between the states but they do not lead to an attack.

## 1.2. Attractiveness of the energy sector

The cyber security of the energy sector has noticed the possibilities that the energy sector can offer to the hackers. Hackers can cause a lot of damage to the power grid by leading a cyber attack against the power grid so the attack will have affects to the entire energy sector, for example the cyber attack against Ukrainian power grid, which will be presented later in the thesis. The energy sector is an attractive target because so many matters are depending on the energy sector, especially technology which uses electricity to operate. The energy sector has many dimensions because of the various range of technology and other matters which are using electricity. To name a few, people need energy for their houses, the equipment inside the house such as coffee makers, computers, TVs, this list could go on indefinitely. As technology develops and people are using even more technology, the need of electricity takes more position in people's everyday life. The energy sector and technology are increasingly connected and interdependent on each other.[12] These two matters go hand in hand. As technology develops in the future, the technology is more depended on the energy sector because it increases the use of electricity which increases the threats of a cyber attack against the energy sector.

Because of the increase of technology which uses electricity, the energy sector becomes more attractive for hackers because it increases possibilities for cyber attacks. Targeting cyber attacks against the energy sector can cause major damages not just for the citizens but also to the states and companies. A cyber attack against citizens could be for example one where the household electricity would be shut off as happened in the cyber attack against the Ukrainian power grid.[13]

---

[11] Plaza (2021), *supra nota* 7.
[12] Fleury, T., *et al*. (2008). Towards a Taxonomy of Attacks Against Energy Control Systems. *The International Federation for Information Processing*, 290, 71-85.
[13] Zetter, K. (2016). *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*. Retrieved from https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/, 06.09.2021.

The cyber attack against the Ukrainian energy sector caused major damages for the power grid.[14] If this trend of cyber attacks targeted against the energy sector keeps continuing, it will cause major problems in the future because the development of items working with energy is attractive for the perspective of the states. As mentioned about the attractiveness in the perspective of states, it means for example that in Finland the Finnish government has removed the tax entirely from electric cars because they are more ecological than cars which use internal combustion engines.[15] As the Finnish government supports the purchase of an electric car it will raise the position of electric cars.[16] As the use of electricity keeps increasing by electric cars or anything which is using energy for its functions, there are a lot of different scenarios what hackers can do for the energy sector, for example targeting a cyber attack against electric cars.

## 1.3. The vulnerability of the energy sector

The cyber attackers, also called hackers, have many different motives for conducting a cyber attack against the energy sector. To present a few motives why the hackers want to conduct a cyber attack it is easier to understand the attractiveness of the energy sector. Hackers' motives for cyber attacks against the energy sector can be for example to gain glory and attention, criminal hackers may want financial gain from the cyber attack, inside hackers' motives can be retribution, industrial and government hackers motives can be gathering intelligence, and hackers as botnet operators may want to have inclusion of their bot armies.[17] The energy sector can nowadays also be an easy target for the hackers because the vulnerability of the energy sector has been noticed in many different dimensions by people who are responsible of the cyber security in companies.[18]

"November 2014, Michael Rogers, director of the NSA and head of US Cyber Command, said that China and "one or two" other countries had the ability to take down the entire US power grid and other critical systems".[19] The vulnerability of the energy sector is having more serious threats all the time because the target can be as major as an entire state. The more electricity is used in

[14] *Ibid.*
[15] Heima, T-P., Pantzar, M. (2021). *Näin autoveron historiallinen poisto näkyy uuden sähköauton hinnassa – Riittääkö alennus nopeuttamaan liikenteen sähköistymistä?* Retrieved from https://yle.fi/uutiset/3-12094199, 04.10.2021
[16] *Ibid.*
[17] Fleury *et al*. (2008). *supra nota* 12, 72.
[18] Nhede, N. (2021). *Mitigating grid vulnerabilities to boost cyber resilience*. Retrieved from https://www.smart-energy.com/features-analysis/mitigating-grid-vulnerabilities-to-boost-cyber-resilience/, 05.10.2021.
[19] Kshetri, N., Voas, J. (2017). Hacking Power Grids: A Current Problem. *The IEEE Computer Society*, 50(12), 91-95.

different functions, the more suitable of a target it is for cyber attacks. Michael Rogers has stated that China would have had the ability to take down the whole US power grid.[20] He has also stated that there are other states who have this ability.[21] Michael Rogers' statement presents that a cyber attack can also have political motives, if states can threaten each other with a cyber attack.[22]

Researchers have stated earlier that cyber weapons are not developed enough that they could replace the nuclear weapons except the United States, the researchers has stated that the United States is already in at an advanced stage of cyber weapon development, so the states are not in a competitive position against each other.[23] Maybe in the future it could be possible that states threaten their enemies with cyber attacks instead of a nuclear weapons, because the word "yet" does not exclude the future. If the cyber weapons' development will increase it could be possible that cyber weapons could be replacing the nuclear weapons and kinetic weapons. Like Michael Rogers has earlier stated, China and one or two other states have the ability for conducting a cyber attack against a state's power grid, meaning that there are only a few states that have this ability.[24] Rogers has not specified which states have the ability other than China. Regarding to other research, it is stated that Russia is also in an advanced stage of "cyber warfare".[25] The research states that Russian hackers have many attributions for committing a cyber attack.[26] Based on these statements it can be concluded that Russia, China and the United States have the most advanced technology for acting in cyberspace against other states. Because great powers such as Russia, China and the United States have this ability for committing a cyber attack, it can be assumed that in the future the cyber weapons can be the weapons on what states compete against each other. One also cannot ever know the whole truth because these kind of matters are highly secured by the states. According to these researches, it can be assumed that all the great powers presented above have the ability to threaten with cyber weapons. Director of the NSA and head of US Cyber Command M. Roger's research is an example which presents that it cannot be known which states actually have the ability to work with cyber weapons because there are so many researches as there

[20] *Ibid*.
[21] *Ibid*.
[22] Kshetri, Voas (2017), supra nota 19.
[23] Libicki, M. (2011). Cyberwar as a Confidence Game. *Air University Press*, Vol. 5(1), 132-147.
[24] Kshetri, Voas (2017), supra nota 19.
[25] Softness, N. (2017). How Should the U.S. Respond to a Russian Cyber Attack. *Yale Journal of International Affairs*, 12, 99-114.
[26] *Ibid.*

are states in the world.[27] This also presents that the cyber weapon development is serious and it is known for sure that in the future the cyber operations against energy sector will be increasing.

Energy sector is concerning different types of matters. Infrastructure engineering and construction consultancy Black & Veatch ranked cyber security as the second most pressing issue for electric utilities in 2016, the research is about the vulnerability and importance of the energy sector. This report stated that only 32 percent of electricity utilities had the proper segmentation, monitoring and redundancies in their cyber security systems.[28] The same report also stated that there were 48 percent electricity utilities who had not considered these capabilities at all in their cyber security.[29] The report stated that the concern of the missing cyber security in electric utilities had been the same concern in the two previous years too and the report indicates the matter that cyber threats are a novel issue for the energy sector because the electric utilities have not taken into account the cyber threats in their cyber security.[30] Even though the electric utilities have noted the problems in their cyber security, they have not solved it. Electric utilities may not consider that cyber attacks can be a possible threat for them. This could be the reason why they do not invest more in their cyber security and fix the problems that the report has shown. Cyber attacks against the energy sector are a topical issue in the light of current research but the attacks usually are not major which also explains why the media does not report about them. Because the media does not report about these cyber attacks, it can be possible that electric utilities do not perceive the threat of a cyber attack to be topical for them because they do not have enough information about the cyber attacks against energy sector. As seen in the case of the attack against the Ukrainian power grid, the problems that the cyber attack caused were fixed in a few hours. But the main concern was that there were also problems that the Ukrainian power grid needed to solve for months. The media may not think it was important because the power was on and the media did not make any news about the later problems which was major. A cyber attack can cause long term effects but if companies do not have enough information, they may consider that the threat is not important. As the cyber security is not taken care of, it increases the attractiveness for hackers and for states to attack against the energy sector.

[27] Kshetri, Voas (2017), supra nota 19.
[28] *Ibid*., 1.
[29] *Ibid*.
[30] *Ibid*.

## 1.4. Statistics of cyber attacks in energy sector

As stated above, cyber attacks against the energy sector is a topical issue. There have been reported several cyber attack cases against the energy sector. These case examples presented below also presents that the energy sector has multiple different matters than just the product itself – electricity. Energy sector covers the suppliers of electricity, power plants and producers.

The research presented above made by Kshetri N. and Voas J. is a research about cyber attacks against the energy sector in the USA, and this thesis will present the results of the research.[31]
The research states that in February 2011 a Brazilian electric utility was hacked by a worm, and the attack caused the electric utility's management not to work which caused that the systems did not work and did not display the data.[32]

The research also states that in June 2011 there was a cyber attack against a Brazilian energy company Petrobras made by a hacker group. Petrobas is the Latin America's largest energy provider. The attack itself was not targeted directly to the energy infrastructure but it was targeted against the company's website, the website crashed for a part of a day, even though this attack was not directly targeted to concern the electricity itself, it was made against the energy providers website which is also a part of the energy sector.[33]

The research also states that in 2013 and 2014, a hacker group which was linked to the Russian government, committed a cyber attack. The cyber attack injured more than 1000 energy companies in 84 different countries, including the US, Germany, France, Italy, Spain, Turkey and Poland.[34] The cyber attacks' motive has been assumed to be industrial sabotage.[35] As stated about the motives above, the motives can be different. However, it is difficult to know about the motives if the attacker has not published the motives. In some cases, even the attacker's identity cannot be proved. Reasoning about attackers' motives are usually speculation.

The research also states that in 2015 a hacker group used a malware which cut off the electricity in Ukraine, Ukraine has suspected that Russia was behind this attack.[36] This case has been very

[31] *Ibid.*
[32] *Ibid*.
[33] *Ibid*.
[34] *Ibid*.
[35] *Ibid*.
[36] *Ibid*.

major because it affected numerous citizens in Ukraine. This case example is reviewed more closely later in this thesis.

The research also states that in 2016 there was another cyber attack against the Ukraine's power grid.[37] This cyber attack was made outside of Kiev and the electricity was off in some parts of the city area for an hour.[38]

The research also states that in 2017 a cyber attack was made against India's electricity distribution company. The attack was targeted to concern four billing offices, the attack did not cause any electricity shut offs in India but the customers could not use the bill-payment operations on that day.[39] This case example is also one against electricity providers.

The research also states that in 2017 a hacker group based in Russia hacked into approximately 20 different western energy companies, the breaks were made against the energy companies' networks.[40] It has also been assumed that the hacker group got access to some US and Turkish companies' operational accesses.[41]

The US Department of Homeland Security (DHS) has made a report about the critical infrastructure.[42] In the report there are the Chemical sector, Communications Sector, Dams Sector, Emergency Services Sector, Financial Services Sector, Government Facilities Sector, Information Technology Sector, Transportation System Sector, Commercial Facilities Sector, Critical Manufacturing Sector, Defence Industrial Base Sector, Energy Sector, Food and Agriculture Sector, Healthcare and Public Health Sector, Nuclear Reactors, Materials and Waste Sector, Water and Wastewater Systems Sector.[43] The author has stated that these infrastructures are critical for the energy sector because they all require electricity. Cyber attack against these sectors could cause major economic loss and also the cyber attack could cause affects for citizens. It has also other consequences, such as consequences of shortage of food and agriculture sector.

---

[37] *Ibid*.
[38] *Ibid*.
[39] *Ibid*.
[40] *Ibid*.
[41] *Ibid*.
[42] Cybersecurity & Infrastructure Security Agency. (2020). *Critical infrastructure sectors*. Retrieved from https://www.cisa.gov/critical-infrastructure-sectors, 11.04.2021.
[43] *Ibid*.

These examples where Russia has been suspected to be behind the cyber attacks shows the statement in the thesis introduction that Russia is a threat to Finland because there are many different cyber attacks where Russia has been suspected to be behind. Finland's position is difficult because of the geographical location as a neighbour of Russia because it can be threat to Finland.

## 1.5. Cyber threats in the energy sector in the European Union

The European Union has also noticed the connection between technology, energy sector and cyber threats. The Directive on Security of Network and Information Systems (NIS directive) is a first general security statute covering the entire European Union, and it has been in force since 2016. [44] According to the NIS directive, Finland has an obligation to report security breaches and threats concerning critical infrastructure.[45] Energy is one of the critical infrastructure sectors mentioned in the NIS directive.[46]

The European commission started also a framework in 2017 considering cybersecurity in the energy sector. The reports topic is "Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector" and the report has concerns about the energy sectors cybersecurity in relation to cyber threats.[47]

The report states the same issue discussed above; technology. Technology has developed fast and development continues. As digitalization keeps continuing it requires more of the energy sector. Today, the digitalization is covering not just the people but states too. There are examples of e-governances which are built up to cover the states administrative matters. Estonia is a good example of the developed e-governance system. Estonian public services are serving online 24 hours a day which is a good example of an advanced state of e-governance.[48]

---

[44] Hartikainen, J. (2018). *NIS-direktiivi ja toimeenpano Suomessa*. Retrieved from https://vm.fi/documents/10623/10333141/7_Jarna_Hartikainen_NIS-direktiivi_toimeenpano_Suomessa__JHDTTK_0810_2018.pdf/66d3cf26-d418-4344-84df-af0dddb76b98, 01.12.2021.
[45] *Ibid*.
[46] *Ibid*.
[47] Energy Expert Cyber Security Platform, EECSP. (2017). *Cyber Security in the Energy Sector – Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector*. Retrieved from https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf, 21.12.2021.
[48] *e-Estonia*. Retrieved from https://e-estonia.com/solutions/e-governance/government-cloud/, 21.12.2021.

Energy Expert Cyber Security Platform (EECSP) is also concerned about the energy sector because it is not designed to withstand cyber attacks as the energy sector is mainly built so it can protect itself against physical attacks.[49] As the energy sector is built up to protect itself from physical attacks, it should be noted that energy sector should be aware of the cyber attacks also. The EECSP is concerned because there are many dimensions of the energy sector who have not designed their security systems to cover the cyber attacks.[50] As showed above, there has happened many cyber attacks against the energy sector and the report is concerned if the cyber attacks against energy sector is increasing. The attackers have noticed the vulnerability of the energy sector and as the energy sector's design has not been developed to withstand the cyber attacks, the cyber attacks against energy sector can cause major consequences to the energy sector.

The report itself shows the vulnerability of the energy sector against cyber attacks. The reports' existence presents the energy sectors importance and also the interest that the European Union has for the threats against energy sector. The European Union has gone further to the development of taking measures from the cyber security. The European Union's framework which began in 2017 has been divided to different parts and one part is designed to report about the threats in the energy sector. There are also other dimensions which are concerned that do not include the energy sector. As the energy sector has been divided to be one part itself, it shows that the concern about energy sector is real.

[49] Energy Expert Cyber Security Platform, EECSP. (2017). *supra nota* 47.
[50] *Ibid*.

# 2. ARMED ATTACK UNDER THE ARTICLE 51

As the thesis has introduced the energy sector aspect above, the thesis will now concentrate on the qualification of an armed attack under the Article 51 of the UN Charter. As the research question of the thesis is extended, this thesis is divided to different parts because it will be easier to follow and in the end the thesis will summarize the research in the conclusion part. The thesis will present cyber operations such as cyber attacks and cyber espionage but cyber attack is closest to qualifying some cyber operation consisting an armed attack and that is the reason why the cyber attack has been mentioned many times during the thesis.

The United Nations (UN) Charter is published in 1945. As the charter is written during a time when there were no cyber weapons, it may not answer to the questions on today or in the future such as cyber attacks. This paper's aim is to solve the problem on whether the Article 51 applies to the armed attack definition in cyber attacks concerning the energy sector. The charter has been published during a time when the conflicts were dealt by making kinetic actions such as "war actions" or kinetic attacks with kinetic weapons. This means that as the cyber attacks characteristics are usually immaterial but its consequences can be physical the indirection between these two actors may mean that the current legislation does not answer to current problems such as cyber attack cases, which are the new means of handling conflicts. In this chapter, the article 51 of the UN Charter is analysed and examined from different perspectives to solve whether its application is also suitable for cyber attacks and also if the Article 51 of the UN Charter concerns cyber attacks and whether cyber attacks can constitute an armed attack.

Article 51 of the UN Charter states that: "*Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and*

*responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.*"[51]

As the Article 51 of the UN Charter does not define what the term "armed attack" signifies in the presented article it may be assumed that the UN Charter has not defined the term "armed attack" on purpose.[52] UN Charter may not be willing to define the term, "armed attack", because the UN Charter's mission may have been, that the term would apply in the future to the upcoming conflicts, that cannot be predicted. The term "armed attack" is not precisely defined because it leaves the applier more leeway for consideration. Also, the UN Charter has no binding definition for the word, therefore it leaves consideration in the future for new situations that the UN Charter could not define at the time the Charter was written. It is typical for law to be written extensively so that the law is applicable to many different situations. It cannot be directly stated that the Article 51 of the UN Charter does not apply today. Because the Article is written extensively, it leaves room for interpretation for todays and futures problems. The legislation leaving room for interpretation is a better situation, because the legislator could not have known when writing the legislation that there will be technologies using energy sector and that the technology using energy sector will only increase in the future and technology entails new challenges such as cyber attacks against the technology. But the legislator may have known that if discretion is leaved, the law could be applicable to new situations. Article 51 of the UN Charter would need more topical case law of its applicableness in the new situations such as cyber attacks.

## 2.1. What is armed?

Defining the term "armed attack", armed as a term, usually means that the attacker is armed by weapons and using the weapons makes it an attack. Weapons can be different than just kinetic weapons, like guns. Weapons can be anything from knives or sticks from a tree to even martial art, if the person has trained martial arts, it may be considered to be as a weapon because it gives the person more condition to cause injuries to others. Hence, the kinetic weapons can be anything. Could it be thought that cyber weapons could also fall under "anything"? The main problem is that cyber weapons are not physical objects like kinetic weapons. Cyber weapons can be codes which

[51] United Nations. *Chapter VII: Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression (Articles 39-51)*. Retrieved from https://www.un.org/en/about-us/un-charter/chapter-7, 11.04.2021.
[52] Todd, G. (2009). Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition. *Air Force Law Review*, 64(1), 65-102.

can be observable in cyber space but usually the code is hidden so well that the attacked state observes the attack when the attack has already been done. According to this, cyber weapons can be observable. As the UN Charter has used the term "armed", there is no commentary on what the term "armed" consists of; is it consisting of just the kinetic weapons or all weapons which can cause an attack. It can be assumed that "armed" consists of all weapons which qualifies the term "armed" because there is not an exhaustive manifest of the weapons which fall under the term armed. The term is not limited to consider only kinetic weapons. On the other hand, "armed" as a term can be a descriptive term, which can imply that the armed as an adjective should be observable on the outside. Hence, the one who is being attacked, should notice from the outside that the attacker is armed. For example, in a cyber attack against energy sector, the cyber weapon can be immaterial so the attacked state cannot observe it from the outside, for example if the code that attackers use is hidden so well that it cannot be observable. The state only observes the cyber attack when the power outage has happened but the state cannot prepare to it. Or the attacker's code can be observed so it makes the weapon observable and the attacked state can observe the attackers weapon and thus it is an armed attack.

However, does it make a difference if the weapon is observable because it has been stated that as the cyber weapons and cyber attacks are immaterial, the immaterial aspect should be insignificant.[53] This means that cyber weapons should be considered to be weapons in the same way that kinetic weapons are weapons. The immaterial aspect should not be valuable.

Cyber attacks as cyber war should be contrast to other non-kinetic actions such as chemical weapons.[54] Cyber weapons can be considered to be a new matter in the field of weapons and that is why there is no legislation for the matter. But chemical weapons are not a new matter, chemical weapons have been used in military forces since the world war one and they are still considerate to be weapons in the same way as guns.[55] Chemical weapons have the same characteristic that cyber weapons have, observing the weapon. A chemical weapon can be for example gas, which can be so clear that people cannot observe it from the air. If an attacker uses toxic gas which cannot be observed, the attacked state can observe the attack only after the gas has affected people.

[53] Palojärvi, P. (2009). Battle in bits and bytes - computer network attacks and the law of armed conflict. *Helsingin yliopisto*.
[54] *Ibid*.
[55] Palmen, J. (2013). *Kemiallisten aseiden lyhyt historia*. Retrieved from https://yle.fi/uutiset/3-6789736, 15.11.2021.

Chemical weapons have been defined to be weapons in the Geneva convention, written in 1925, where the parties engaged that they will abstain from using chemical weapons.[56]

What about the attackers aim or if the attack does not succeed defining the term armed? For example, if the hacker (attacker) is attacking against a state. The hackers main aim is to destroy state's cyber space or some part of it. The cyber space is considered to be the states territory. The Finnish manual states that the whole cyber infrastructure is considered to be a state's territory.[57] Later in the thesis, more will be found out about the Finnish manual and their position to this matter. If the attacker is attacking using a cyber weapon which cannot be observed from the outside and the attacked state does not notice that they have been attacked, is it then an armed attack? What if the attacker gets access to the state's cyber space, which is considered to be the state's territory, and the attacker's purpose is to destroy some part of the cyber infrastructure of the state, but the attack did not succeed? In this presented scenario the attacker has only succeeded by accessing the states cyber space but the aim about destroying the state's cyber space or some part of it has failed. If there are not any consequences, the attack cannot be defined as an armed attack. Or can it? The attacker's aim has been to destroy the states cyber space entirely or partly. Hence, the attackers aim has been to commit a cyber attack in order to destroy the state's cyber space, it is obvious that it is an attack and it is also an armed attack if the cyber weapons are considered to fall inside of the term armed. Cyber attacks are complicated from this perspective because the attacker can hide their trace. If the state notices that someone has been inside of their systems, it is hard to find out who it was. Usually, the state does not even find out who to blame. It has been stated that even though a cyber attack itself could be proved, it is hard to prove the cyber attacks origin and possibility of other states participation.[58] For example, China has many times denied their involvement in cyber attacks against the United States. It is hard to prove that some state has been involved.[59] Russia is a good example also to the matter that some state has been a suspect in a cyber attack. Later on the thesis, case examples where Russia has been suspected to be the attacker in cyber attacks will be presented.

---

[56] *Ibid.*
[57] Valtioneuvosto. (2020). *Kansainvälinen oikeus kyberympäristössä Suomen kansallisia kantoja*. Retrieved from https://um.fi/documents/35732/0/KyberkannatPDF-FI.pdf/c69fce1e-5753-3731-0b46-356b8216df51?t=1603097434415, 03.09.2021.
[58] Dinstein, Y. (2001). War, Aggression and Self-Defence. *Cambridge University Press,* Third edition.
[59] Hodgson, G. (2016). Cyber Attack Treaty Verification. *A Journal of Law and Policy for the Information Society*, 12(2), 231-260.

Attacked state has responsibilities to prove the attacker's identity, for it to have right for self-defence against the attacker. It has been assumed that this requirement will find its position in the future because it can be hard to find evidence of a cyber attack.[60]

It has to be noted that a cyber attack which is done for the purpose of gathering information, is called cyber espionage. Espionage is legitimate under the Hague conventions and it applies to information society and also to cyber space.[61] Even though, cyber espionage is a complicated matter because the Tallinn Manual 2.0 experts states that there are different forms for legitimate and illegitimate cyber espionage.[62] It cannot be directly said that cyber espionage is always legitimate or illegitimate, this is just a note because cyber espionage is related to cyber operations, the thesis is not going to go further into this matter.

## 2.2. Consequence of a cyber attack

An important question is whether the term "armed" is defined from the consequences of what the attack can cause. Cyber espionage for example does not need any considered cyber weapons for its action but if the consequence is unlawful or the attacker obtains information which it should not have, but the attacker has benefit from the information what it has been gathered, is it then considered to be an armed attack? If the hacker uses some cyber objectives in the cyber espionage, is the objective then considered to be a cyber weapon even though it was not meant to be used as a weapon? Is the objective that the hacker uses in the cyber espionage always considered as a weapon even though it was not meant to be a weapon? For example, code can be used as a cyber weapon and also in many other dimensions such as making websites. Kinetic weapons such as guns usually cannot do anything different than shoot and the consequences are usually known in advance. This interpretation's purpose is to examine if the term "armed" is even necessary, or if "attack" as a term is sufficient enough to define the whole term "armed attack". If the consequences of the attack are sufficiently powerful, does it matter what objective has been used to achieve the consequences? The objectives cannot be defined as lawful objectives in general because the objectives also have other dimensions which are used in other purposes. If the attacker attacks

[60] Brunner, I., Dobric, M., Pirker, V. (2015). Proving a State's Involvement in a Cyber-Attack: Evidentiary Standards before the ICJ. *Finnish Yearbook of International Law*, 25, 75-108.
[61] Dinstein, Y. (2004). The Conduct of Hostiles under the Law of International Armed Conflict. *Cambridge University Press*.
[62] Schmitt, M. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. *Cambridge University Press*, Second edition.

against hospitals electricity and patients who are using breathing apparatus dies, the consequence is the same as it would be in a kinetic attack, death. In Finland a patient died after a power outage. The patient was using a breathing apparatus and after the power outage the breathing apparatus cut off the patient was without oxygen 17 minutes. The Finnish police started an investigation about the matter but the results were not revealed to the media.[63] If it would have been an cyber attack against hospitals energy sector, would it be armed attack because the consequence was death. Does it make a difference if death has been caused with a gun or with a code?

The issue has been discussed in the United Nations and the general consensus has been that for a cyber attack to be considered to be an armed attack it needs to have the same consequences and effects as a kinetic armed attack would have .[64] The consequences and harm of a cyber attack should be comparable to a corresponding kinetic armed attack. The qualification about the consequences is challenging because usually in kinetic armed attacks the use of violence is more extensive than in cyber attacks. Usually, in a kinetic armed attack there is no question if the attack is an armed attack because the use of violence and the consequences are observable. If a cyber attack causes the same kind of consequences as a kinetic armed attack, it is usually directed to the civilians. If a cyber attack causes injury and harm directly to the civilians and society, it should be considered that cyber attacks would be prohibited by law and the cyber attack like that would be an armed attack.

It has also been stated that it cannot be appropriate that the definition for a cyber attack would be considered to be significantly different to the rules which restrict the use of armed forces in general or the definition would be in contradiction to the interpretation of the UN Charters rules and aims.[65] This statement from the ministry for foreign affairs of Finland can be considered to include the armed attack definition in cyber operations because the definition of an armed attack cannot be significantly different as it would be in a kinetic attack.

---

[63] Ilta-Sanomat. (2004). *Sähkökatko pysäytti laitteen, potilas kuoli*. Retrieved from https://www.is.fi/kotimaa/art-2000000270708.html, 09.12.2021.

[64] Klimburg, A., Tirmaa-Klaar, H. (2011). Study, Cybersecurity and Cyberpower: concepts, conditions and capabilities for cooperation for action within the EU. *European Parliament*.

[65] Ulkoasiainministeriö. (2015). *Voimankäytön oikeussäännöt selvitys eduskunnan ulkoasiainvaliokunnalle*. Retrieved from https://um.fi/documents/35732/48132/voimank%C3%A4yt%C3%B6n_oikeuss%C3%A4%C3%A4nn%C3%B6t__selvitys_eduskunnan_ulkoasiainvaliokunnalle_/56324b9e-6ce1-e3cd-5782-248662df5580?t=1525861360553, 28.09.2021.

It has been stated that cyber attacks are generally seen as soft actions if one compares them to an action of kinetic armed attacks such as military actions or weapons of mass destruction.[66] The statement means that cyber attacks do not usually cause the same consequences as kinetic attacks. The statement also increases the value of the consequences defining the term armed. As perceived in this section, cyber attacks are usually considered to be softer actions than kinetic actions. The main reason for this is the consequences that these attacks cause.

Even though there have been suggestion that cyber attacks should be treated as acts of war, which is more prescriptive and also restrictive definition than armed attack.[67] It sounds more right that "cyberwar" includes a cyber attack but the attack itself is not defined to be an act of war.[68] This thesis is not going to qualify the terms of warfare or the law of war because the thesis is not going to research this topic further from the point of view of international humanitarian law.

The hospital example presented above caused one patient's death. Would the patient's death be enough or should there be more deaths that it would be qualified as an armed attack? The Article 51 of the UN Charter does not give any strict guidelines about the amounts of the consequences such as amounts of deaths and injuries.

To summarize and analyse what has been discussed above; armed as a term means weapons but is cyber weapons considered to be included in the term armed? There are opinions for and against. Cyber weapons should be considered to be included in the term armed, because what cyber weapons would then be if the person committing a cyber attack would not use any weapons by committing it. It is not significant, whether the weapon is observable or not because chemical weapons are not observable but they are still defined to be weapons, and attacking with a chemical weapon is an armed attack. Consequences on the other hand is an important matter, because a cyber attack can cause great damages such as deaths and injuries. Attackers aim or purpose is not significant, because it does not change the definition of an armed attack in cyber operations. Attacker's aim or purpose does not affect directly the consequences which is the significant matter when defining an armed attack. For example, covid-19 has caused consequences such as deaths and injuries what was not anyone's aim or purpose according to the information that one has now,

---

[66] Turvallisuuskomitean sihteeristö. (2013). *Suomen kyberturvallisuusstrategia*. Retrieved from https://www.defmin.fi/files/2368/Suomen_kyberturvallisuusstrategia_ja_taustamuistio.pdf, 20.10.2021.
[67] Hathaway, O., *et al.* (2012). The Law of Cyber-Attack. *California Law Review*, 100(4), 817-886.
[68] Davis, P. (2015). Deterrence, Influence, Cyber Attack, and Cyberwar. *New York University Journal of International Law and Politics*, 47(2), 327-356.

is covid-19 still considered to be an armed attack from a non-state actor because one cannot know who is behind the attack.

## 2.2. Armed attack = Aggression

It has been stated that "armed attack" is a synonym to the word "aggression".[69] Aggression is defined in Article 8 of the Rome Statute of the International Criminal Court, the article states that aggression means "using armed forces against other state, blocking the states ports or coasts, preventing of shipping and using states territory in hostile actions".[70] Cyber attacks could be in the category of blocking the states ports or coasts, if an attacker attacks against states energy sector and shuts off the entire state's electricity, then nothing will work, would it then be considered to be blocking the states ports or coasts or both.

Considering these two words, aggression and armed attack mean the same matter. Usually aggression is the starting point which leads to an armed attack, but are they considered to mean the same matter? The answer would be no rather than yes. Because there are different dimensions in the word aggression, which are not concerning about armed attacks definition at all. Usually the conflicts between states arises from emotions which leads to aggressive behaviour which leads to conflicts which can be armed attacks. Aggression itself as an emotion does not always lead to an armed attack. Aggression as a term is more descriptive like an adjective not a subjective which armed attack is.

It should also be noted that the term "aggression" has two dimensions in international law. First is the prohibition of the use of force against states and second is criminal liability in use of force by individuals.[71] Use of force by non-state actors is always criminalized by international law.[72] This means that someone or some group who commits a cyber attack on behalf of a state or a subordinate to it, has criminal liability for these actions. The criminal liability considers only the individual who has committed the cyber attack. What comes to the states, the situation is different

[69] Cassese, A. (2008). International Criminal Law. *Oxford University Press*, Second edition, 154.
[70]United Nations. *The United Nations Treaty Collection*. Retrieved from https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-10-b&chapter=18&clang=_en, 26.05.2021.
[71] Cassese (2008), *supra nota* 69.
[72] Henderson, C. (2014). Non-state Actors and the Use of Force. *Hart Publishing*.

and more complicated because the states have a prohibition of the use of force but only a threat of the use of force does not have any clear policy whether it has criminal liability or not.[73]

Cyber attacks should be considered to be armed attacks in the consideration of the whole entity. Cyber attacks can be considered to be an act of aggression which leads to an armed attack which makes the whole entity to be a cyber attack. Cyber attack should be considered to be a new means of the military forces.

The UN charter does not define what are the weapons that makes the armed attack to be considered as armed. If a kinetic attack occurs where kinetic weapons are used, it is obvious that the rules of UN Charter will apply. Even though, it should be that if an armed attack occurs, no matter whether kinetic or cyber weapons have been used, the rules should be the same even though the matter is different if the consequences are the same. The Charter of the United Nations have not defined armed attack. Would the Charter of the United nations apply to a cyber attack if the attack would have the same elements that a kinetic attack usually has? Meaning that the attack could be observed from the outside or the consequences would be the same as they would be in the kinetic attack.

It has been stated that if an cyber attack causes major number of deaths, it should be considered to be a kinetic attack instead of a cyber attack.[74] If a cyber attack causes major number of deaths, it should still be considered to be an cyber attack because the attack is made by using cyber weapons and cyber means. It should be also considered to be an armed attack because of the consequences. If cyber attack causes major number of deaths the consequence aspect should be the determining factor. As the Charter of the United Nations does not define the armed attack, as seen above, the main qualifying matter has been in various different sources the consequences. If a cyber attack causes the same consequences as a kinetic attack they cannot be considered to be the same matter. If they would be the same matter, then there would be no problem in this research.

The existing law to this matter has been written long time ago. As the law is written widely and it can apply to many different matters, it would still need a clarification. Or it could be considered that there would be a whole new legislation for this matter. The existing one could be converted to answer better the questions of today and of the future. If the existing law would have been applied

[73] Upeniece, V. (2018). Conditions for the lawful exercise of the right of self-defence in international law. *Rīga Stradiņš University*.
[74] Dinstein (2001), *supra nota* 58.

more in courts, it would have more topical case law, which could answer to the questions of this thesis. Many states or confederations have taken their own position for this matter. In the next chapters, this thesis will examine this matter from the Tallinn Manual 2.0 and also from the Finnish manual. Both manuals have taken their own positions for this matter through the Charter of the United Nations. As the article 51 of the United Nations Charter is a widely written article, it can be developed to different perspectives.

# 3. ARMED ATTACK UNDER THE TALLINN MANUAL 2.0

This chapter will be discussing the definition of an armed attack in cyber operations under the Tallinn Manual 2.0. In the previous chapter the definition of an armed attack was analysed through the Article 51 of the UN Charter.

Tallinn Manual 2.0 has been published in 2017 and it is written by international law experts in cooperation with NATO.[75] Tallinn Manual 2.0 gives their own position for the problems in the cyber incidents. Tallinn Manual 2.0 takes its position on matters which have not yet been regulated by law. Tallinn Manual's experts gives their perspective on how the problems should be solved. As the Tallinn Manual 2.0 is a novel research it gives valid points to this research. Tallinn Manual 2.0 is a very broad research about problems that cyber space is giving to us today and in the future.

## 3.1. Armed attack definition by Tallinn Manual 2.0

Rule 71 of the Tallinn Manual 2.0 is about self-defence against armed attack.[76] This research will only determine the cyber operations which consists an armed attack, it is not going to examine the right of self-defence. The research goes through the right of self-defence but it will not go into that topic more completely in this research.

### 3.1.1. Act of aggression

Rule 71 of the Tallinn Manual 2.0 states that: "Although an act of aggression can constitute an armed attack, it may not always do so."[77] The international group of experts agreed that act of aggression is not always an armed attack.[78] It can be concluded that cyber operation is not always an armed attack as a cyber attack is not always an armed attack either but it can constitute an armed attack. Armed attack versus aggression is often compared to mean the same matter, some

[75] Schmitt (2017), *supra nota* 62.
[76] *Ibid*.
[77] *Ibid*.
[78] *Ibid*.

researches thinks that these two words mean the same matter, as discussed earlier in this thesis, it came to the conclusion that it does not mean the same thing, but these two are very close to each other. Aggression usually leads to an armed attack. The International group of Experts in the Tallinn Manual 2.0 had the same opinion, that these two words do not mean the same. But the international group of experts agreed that aggression can constitute an armed attack.[79] The expert's opinion is a bit different than discussed above, because the experts thought that aggression can constitute an armed attack. Hence, the expert's opinion is that aggression can constitute an armed attack, it means that these two words can be in the same sentence but as they use the term "can" it gives consideration that they can be and also, they cannot be. And also, in the end of the Rule 71 of the Tallinn Manual 2.0 experts claim that "it may not always do so", which concludes that armed attack and aggression can be considered to be together or not. As seen from history, is that aggression leads to an armed attack, the conflict between the states can be inflamed and it leads to aggression or the aggression has been there all the time, and when the aggression comes to its limit, the only solution for handling the conflict is an armed attack. Or aggression can be present for a long time but it does not lead to anything, that is maybe the reason why the international group of experts states that "it may not always do so".

### 3.1.2. Non-state actors

As the thesis will focus on defining the term armed attack, it needs to examine also the non-state actors, although it has to go a bit beyond of the scope of the research topic. As non-state actors are not the topic, this will give new perspective for defining the armed attack. The thesis will not go deeply to this matter but it is significant for this topic to make a note about it. As the rule 71 of the Tallinn Manual 2.0 is comprehensive, this thesis will examine the whole rule from the perspective of an armed attack. The rule 71, article 3: "An armed attack must have a trans-border element. This criterion is always met when one State engages in a cyber operation otherwise qualifying as an armed attack against another State, or directs non-State actors, wherever they may be, to act on its behalf of it doing so."[80] The international group of experts noticed that there should always be a trans-border element when considering a cyber operation to constitute to be an armed attack. This criterion is usually met in the situation when another state attacks against another state by cyber means (cyber weapons). It is also met in the situation where a hacker group who is committing a cyber operation on behalf of a state and attacks against another state (= a non-state actor). As the

[79] *Ibid*.
[80] *Ibid*., 340.

experts state, a cyber attack made by a non-state actor cannot be defined as an armed attack because the armed attack definition must have trans-border element. Experts explain that the reason why there always has to be the trans-border element is because the Article 51 gives the states a right for self-defence.[81] The Article 51 does not apply to non-state actors because they are not considered to be states, and the article 51 gives the right to self-defence only to actual states. This is a complicated matter because Tallinn Manual 2.0 also states that international community was characterizing the 9/11 attack as being an armed attack, even though the attacker Al Qaeda was a non-state actor. The International court of Justice did not agree with the statement of the international community, even though there was a disagreement between the members of the court.[82] But the trans-border element what the experts has stated means more that another state attacks another state, than the non-state actor point of view.

Armed attack definition should be considered to be separated from other matters for example the right of self-defence. It should be defined as it is. The 9/11 attack was an armed attack because of the consequences. It caused a lot of injuries and deaths. It is another case to consider whether the United States had the right to self-defence or not because the attacker was a non-state actor.

Sometimes states try to avoid their responsibility by blaming a non-state actor. That is why there is legislation which makes it difficult to avoid responsibility. The article 4 of the UN Charter states that: "A non-state actor's wrongful behaviour is attributable to a state if the non-state actor is acting as an organ of the state or is acting under the instructions, directions, or control of the state"[83]. The meaning of the charter is obvious; that states cannot use non-state actors as an organ to avoid responsibility because if the original attacker reveals the state which has been the initiator, it will have the responsibility as an original attacker. The problem is that sometimes the original initiator stays unrevealed.

### 3.1.3. Grave

Rule 71 of the Tallinn Manual 2.0 continues, "The International Group of Experts unanimously concluded that some cyber operations may be sufficiently grave to warrant classifying them as an 'armed attack' within the meaning of the Charter."[84] As the international group of experts states

[81] *Ibid*., 345.
[82] *Ibid*.
[83] Tran, D. (2018). The Law of Attribution: Rules for Attribution the Source of a Cyber-Attack. *Yale Journal of Law and Technology*, 20, 376-441.
[84] Schmitt (2017), *supra nota* 62, 340.

that if a cyber operation is sufficiently grave it can be classified to being an armed attack. Is the word "grave" the one which determines the meaning of an armed attack? Is the term "grave" consisting of the previously discussed major consequences such as deaths, injuries and material damages? As the international group of experts' states, an armed attack should be grave in order to be classified as an armed attack, which makes the definition of an armed attack easier to understand or even to define. The international group of experts agreed unanimously about the definition of grave constituting an armed attack. Rule 69 of the Tallinn Manual 2.0 stated that the International Court of Justice stated in their Nicaragua judgment that "scale and effects" have to be considered when determining an armed attack in cyber operations.[85] This statement means that an armed attack in cyber operations should be comparable to the armed attack in kinetic operations. According to this principle, if a cyber attack is comparable on its scale and effects to a kinetic armed attack, a state can respond to the attack by using the same amount of kinetic force which would correspond to the attack. This principle is meant to be considered as the right of self-defence but if one only considers the effects that this principle offers for an armed attack, it can be assumed that if a cyber attack has the same effects that a kinetic attack has, it is considered to be an armed attack. If a cyber attack has the same effects, it is then considered to be an armed attack. If the cyber operation causes major consequences and effects such as deaths, injuries or material damage, then the cyber operation or cyber attack should be considered to constitute an armed attack.

It has to be noted that it is universally accepted that chemical, biological, and radiological attacks are affecting major and grave consequences they are usually defined to constitute as an armed attack even though they are not kinetic attacks.[86] As stated earlier, chemical weapons are considered to be weapons, and therefore it is natural that an attack committed by using chemical weapons constitutes as an armed attack.

### 3.1.4. Armed

As discussed in the previous chapter about the term "armed" in the rule 71 the international group of experts also takes its position in this matter. They discussed about whether the term "armed" involves weapons, and the international group of experts took the position that it did not require weapons. The international group of experts thought that the critical factor is about the effects that

[85] *Ibid*., 330.
[86] *Ibid*., 340.

the cyber operation has and not how it is done.[87] They also concluded that a cyber operation usually consists of cyber weapons and therefore cyber operations can be defined to be armed attacks.[88] This thesis came to the same conclusion above. The characteristic of the weapons should be insignificant because if the attack has the same consequences that a kinetic attack would cause, the attack should be considered to be an armed attack.

### 3.1.5. Scale and effects

Rule 71 of the Tallinn Manual 2.0 continues about qualifying the scale and effects. "The International Group of Experts agreed that a cyber operation that seriously injures or kills a number of persons or that causes significant damage to, or destruction of, property would satisfy the scale and effects requirement".[89] The international group of experts has come to the same conclusion that has been stated in the previous chapters about the consequences of an armed attack. The meaningful matter is the consequence that the attack causes. Even though cyber operations can be immaterial attacks because the action is made in cyber space, they still usually have physical scale and effects. The experts also took their position by stating that cyber operations should cause deaths or serious injuries to a number of persons. Above, the thesis presented a hospital case example where only one patient died during a power outage. According to this statement, the case example would not have been considered to be an armed attack because one patient doesn't qualify the definition of a death of number of persons.

Would the hospital case example presented above qualify the definition of an armed attack if the attack would have been grave? Even though, the international group of experts has concluded that cyber operations should cause deaths of number of persons but is the amount of deaths significant if the attack is grave?

### 3.1.6. Legislation

In the rule 71 the experts have also noted that the law is ambiguous on what comes to an armed attack in cyber operations.[90] Article 51 of the UN Charter is ambiguous but is it ambiguous because it leaves consideration for the upcoming conflicts. Has the legislator done it on a purpose that it has given leeway to the consideration for the future and therefore the law is ambiguous? Cyber

[87] *Ibid*., 340-341.
[88] *Ibid*.
[89] *Ibid*., 341.
[90] *Ibid*.

attacks are also complicated because the attacked state should prove who has been behind the attack. Knowing the attacker is important because that is the only way to use the applicable legislation for the current circumstance. As the Tallinn Manual 2.0 has stated, the Article 51 of the UN Charter is only applicable if the attacker is a cross-border attacker, so the UN Charter applies to attacks where the attackers are states or groups working on behalf of a state.

### 3.1.7. Smaller attacks constitute an armed attack

The international group of experts also presented a case example which applies to armed attacks.[91] The international group of experts discussed about an example where the attacker has carried out many smaller cases of cyber operations, the international group of experts considered that if there is convincing evidence then the incidents together constitutes an armed attack.[92] This example was a new perspective for this matter, as presented in the first chapter, sometimes cyber attacks can be smaller attacks and they do not qualify to the classification of the "scale and effects". But if the attacker has been the same and the attacked state has been the same, then the attacks can be considered together so they create a larger cyber attack when the classification of "scale and effects" apply and it will constitute an armed attack.

### 3.1.8. Economic loss

In the rule 71, there has been a gap between the experts' opinions about if a cyber operation does not cause injury, death, damage or destruction but otherwise it causes extensive negative effects, such as financial loss.[93] This question is still unsettled between the experts. This matter should be also considered from the perspective of the "scale and effects" as the International Court of Justice has stated. If a cyber attack causes financial loss, it can mean that it prevents the action of society which has straight effects to the civilians. As the cause is concerning civilians it should be always considered as an armed attack. The example what was used in the Tallinn Manual 2.0 was the attack against international stock exchange.[94] Crashing the markets will have a straight effect to the society. It should be considered that the attacker itself than is the consequences enough to determine the definition of an armed attack. If it can be proved that the attacker has cross-border elements, meaning that the attacker is a state or a group working on behalf of a state, and the attack causes major consequences, for example financial loss, then it should be considered to be an armed

[91] *Ibid*., 342.
[92] *Ibid*.
[93] *Ibid*., 342-343.
[94] *Ibid*., 343.

attack. In an aspect of financial loss, it could be also considered that the cyber attack is a political action, political actions should be considered to be armed attacks, because the state who is acting usually has political aspects such as their own interests. This matter is also raised up in the next chapter about the Finnish manual. The Finnish manual also considers that cyber attacks that causes economic consequences should be considered to be armed attacks. More on that in the next chapter.

### 3.1.9. Foreseeable consequences and imminent attack

Foreseeable consequences were one point in the rule 71 of the Tallinn Manual 2.0. The international group of experts agreed that if a cyber attack is targeted to a state's infrastructure, for example a water purification plant, which contaminates the water and causes deaths and injuries for the people, it should be considered to be an armed attack.[95] This example can be used as a consideration of the energy sector. If a cyber operation attacks against the energy sector by causing foreseeable consequences to the electricity, such as cutting electricity from households which affects the citizens, that should be considered to be an armed attack because the effects are straight targeted at the civilians. There are foreseeable consequences when targeting the energy sector.

One other same kind of matter is the imminence of the attack. "Caroline doctrine, which allows for anticipatory self-defence when an opponent's act of war is imminent".[96] Caroline doctrine is accepted by the international community. If a state cannot evaluate the foreseeable consequences, it may evaluate if the attack they are facing is imminent. Imminent also gives a right for self-defence. So it can be concluded that "imminent" attack makes the attack defined as an armed attack.

Usually the attack itself can be foreseeable and the state can prevent the attack before it has happened.[97] Every day there are many cyber attacks made against companies and states. Companies and states can prevent these attacks because of their own cyber security.

### 3.1.10. Summary

Rule 71 of the Tallinn Manual 2.0 states that if a cyber operation is qualified to be an armed attack it should have different kind of elements presented next. The cyber operations qualified to be an

[95] *Ibid*.
[96] Hayward, R. (2017). Evaluating the Imminence of a Cyber Attack for Purposes of Anticipatory Self-Defense. *Columbia Law Review*, 117(2), 399-434.
[97] Finch, B., Spiegel, L. (2013-2014). Litigation following a Cyber Attack: Possible Outcomes and Mitigation Strategies Utilizing the Safety Act. *Santa Clara High Technology Law Journal*, 30(3), 349-374.

armed attack needs to have a trans-border element which means a state to state situation. The Charter of the UN does not apply to non-state actors such as groups acting behalf of a state. The attack needs to be grave. The "scale and effects" of the attack should be injuries and deaths of a number of people. Financial loss may be considered to be an armed attack but the experts had opinions for and against. Foreseeable consequences can also define the attack to be an armed attack. There are a lot of different dimensions to be taken into account when qualifying a cyber operation to be an armed attack. This is good research about the matter and gives opinions to all of the angles that there are when discussing the armed attacks definition in cyber operations.

There has also been criticism against the Tallinn Manual 2.0. It has been stated that it is still unclear when a cyber attack meets the requirements of "scale and effects" so that it can be regarded, classified and handled as an armed attack.[98]

Tallinn Manual 2.0 gives the tools for on occasion consideration. Tallinn Manual's experts has also stated that UN Charter is unambiguous and it does not give a clear definition for an armed attack but the Tallinn Manual 2.0 has made the consideration of the topic and considered the matter from different perspectives. Tallinn Manual 2.0 has also compared the article 51 to the judgements of the International Court of Justice on how the court would have defined the armed attack definition. Other problem is of course the applicability of the International humanitarian law to the issue of cyber attacks but as mentioned before this thesis is not going to research the topic from the perspective of International humanitarian law.[99]

[98] Apostolopoulos, T., *et al*. (2018). A new strategy for improving cyber-attacks evaluation in the context of Tallinn Manual. *Computers & Security,* 74, 371-383.
[99] Schmitt, M. (2014). Rewired warfare: rethinking the law of cyber attack. *International Review of the Red Cross*, 96(893), 189-206.

# 4. FINNISH MANUAL

In this chapter the thesis will examine the research question through the Finnish manual of cyber actions. As the thesis is focused on Finland, the thesis will now look the answer for the research question through the Finnish manual which is Finland's own position to this matter.

Finland is on its own because it does not have military cooperation with NATO. Finland and NATO has a partnership for peace.[100] There are other European Union countries which have the same position that Finland has, meaning that they are members of the European Union but not members of the NATO. They will be discussed later on this thesis. But the difference about Finland to these other non-NATO European Union countries is that Finland's geographical location is challenging because of its neighbour Russia. Russia is not part of the NATO and NATO is maybe a threat to Russia. Russia wants that NATO stays as far as possible from them. Russia does not want any NATO allies near to it. In recent news Russia wanted to have guarantees from NATO that it would not accept Ukraine's NATO-membership and the NATO will not expand to the eastern Europe or Caucasus.[101] Russia has always tried to affect to Finland's position about NATO cooperation. As the Tallinn Manual 2.0 is a far gone research about today's problems in cyber space made by NATO, Finland cannot enjoy it because of the missing membership to NATO. Nevertheless, Finland has made its own position for this matter.

In the beginning of the Finnish manual, it states that: "In the same vein, the UN Group of Governmental Experts (GGE) has reaffirmed that "international law, and in particular the Charter of the United Nations, is applicable [cyber environment] and is essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment".[102] This

[100] NATO (2021), *supra nota*, 4.
[101] Vainio, S. (2021). Venäjä vaatii, ettei Nato ota uusia jäseniä ja pysyy poissa Itä-Euroopasta – ehdottaa neuvotteluja Yhdysvaltojen kanssa "vaikka huomenna". Retrieved from https://www.hs.fi/ulkomaat/art-2000008484463.html, 15.11.2021.
[102]Finnish Government. (2020). *International law and cyberspace Finland's national positions*. Retrieved from https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727, 03.09.2021.

sentence sounds simple because it states that Charter of the United Nations is applicable also in the cyber environment. The deeper one goes through the Finnish manual it can be seen that it is not that simple. The Finnish manual states that: "While the existing rules and principles of international law are applicable in cyberspace, the application of certain provisions may give rise to practical problems due to the specific characteristics of cyberspace".[103] Cyber environment has many different dimensions as well as cyber attacks. Cyber attacks cannot be directly comparable to an armed attack because cyber attacks' scope and effectiveness can be very different than an armed attack itself. Armed attacks usually have the same effects and consequences, for example if a state attacks against another state with military forces and uses kinetic weapons, it is then defined to be an armed attack, and it can be assumed that the armed attack causes deaths and injuries to the people. Cyber attacks instead do not usually have the same effects and consequences that armed attacks have; usually cyber attacks effects cannot be known in advance. Cyber attacks can cause harm to the cyber environment and through that they have effectiveness to the civilians but usually they do not cause deaths and injuries. They of course can cause those too, but usually the consequences are more indirect than in armed attacks. As seen in the cyber attack against Ukrainian power grid, the consequences what the attack affected were noticed much later. And the consequences what the attack caused were repaired for a long time. Cyber attacks are problematic because they can cause different effects. Cyber attacks cannot be assumed to cause something because the effectiveness can usually be calculated from the aftermath of the cyber attack. That is one of the reasons why it is so problematic to compare cyber attacks and kinetic attacks. Because of the difference between cyber attacks and kinetic attacks, it makes the definition hard for the state to determine what kind of attack they are facing off. The difference between cyber space and the kinetic space is very wide. The kinetic space, where we are living, is very different from the cyber space because in the kinetic space one can see and sense everything. In a kinetic space it is impossible to commit an armed attack in silence so that nobody would not know. Kinetic space, if considered to be land without space, cannot expand in the same way as cyber space can.

How long does it take to notice that one has been a victim to a cyber attack? International Business Machines Corporation (IBM) has made research about the cost of a data breach. According to the report of the research it states that in the organizations of the Nordic countries it takes more than

[103] *Ibid.*

200 days to notice hacking and it takes over 70 days to prevent it from spreading.[104] The report shows that cyber attacks can be done in total silence. Hence, there is a big gap between the cyber space and the kinetic space. The Finnish manual's purpose is to give their own position for what qualifies an armed attack situation in the cyber space. Cyber attacks can be very different, there are so many different motivations behind the cyber attacks, and cyber attacks can cause various different problems to a state.[105] As mentioned before about the motivations, cyber attacks can be directed to concern some part of the state's cyber infrastructure, for example means of a cyber terrorism or to achieve some economic benefit.[106]

Finnish manual honours the Charter of the United Nations and gives a new perspective for the situations made in the cyber space. The Finnish manual does not speak out of the legislation and whether the existing one is even the right one for this matter. Finnish manual's purpose is to give their own position for this conversation using the valid legislation.[107]

## 4.1. Sovereignty

The Finnish manual considers that a state's principle of sovereignty includes undoubtedly the state's cyber infrastructure.[108] Cyber infrastructure, which is considered to be under the state's sovereignty, is the cyber infrastructure located in the state's territory and also the people who are involved in the cyber operations in the state's territory.[109] Sovereignty at this point means that the states have exclusive right for exercising their competence in their own territory, even though, the Finnish manual states that cyber infrastructure is something which cannot be conquered because of its wideness.[110] Sovereignty as a right has been agreed in the treaty of Rome in 1957.[111] Hence, the sovereignty has been agreed upon in the treaty of Rome, the sovereignty in general covers to borders of the state, according to the interpretation of the Finnish manual, the state border also

[104] Valkama, V. (2019). *Mustan rekan valtasi paniikki ja sekasorto: Niin pitikin käydä, sillä se joutui kyberhyökkäyksen kohteeksi – näin "valkohattujen" avulla opetellaan, miten haavoittuvuudet tilkitään*. Retrieved from https://www.aamulehti.fi/uutiset/art-2000007440651.html, 20.10.2021.
[105] Shea, J. (2017). NATO: Stepping up its game in cyber defence. Cyber Security: *A Peer-Reviewed Journal*, 1, 165-174.
[106] *Ibid.*
[107] Finnish Government (2020), *supra nota* 102.
[108] *Ibid.*
[109] *Ibid.*
[110] *Ibid.*
[111] Europian Parliament. Treaty of Rome. 25.11.1957. Retrieved from https://www.europarl.europa.eu/about-parliament/en/in-the-past/the-parliament-and-the-treaties/treaty-of-rome, 22.09.2021.

extends to cyber space, although it is not specifically mentioned in the treaty of Rome. Tallinn Manual 2.0 agrees on the matter about sovereignty in cyber space that the Finnish manual undoubtedly considers.[112]

Sovereignty is usually thought as a primary right of a state. As the research question is narrowed to consider the Article 51 of the UN Charter this discussion will be considering the Article 51. Sovereignty is one factor in the Article 51 of the UN Charter, because it gives the state the right to self-defence if an armed attack occurs. If the Finnish Manual and also the Tallinn Manual 2.0 considers that sovereignty also applies to the cyber space, then it would be considered that if a cyber attack considered to be an armed attack occurs, the state has the right to self-defence. States could, for example, "hack back" in the circumstance of a cyber attack. It sounds simple but it is not. If a state has the right for self-defence when an armed attack occurs, what is self-defence? The right of self-defence can be found in the customary international law. It states that there has to be: "a necessity of self-defence, instant overwhelming, leaving no choice of means, and no moment for deliberation".[113] Even though a state would have the right to self-defence, the right is usually calculated from the aftermath of the case. However, the legislation concerning self-defence gives a presumption that a state needs to act for self-defence fast and there is no time for consideration. The legislation leaves the responsibility for the state. Because of this, it is necessary that there would be a clear rule for cyber attacks, and also the definition as to what can be qualified as an armed attack in cyber operations.

This case presented next gives an understanding on how fast states need to act and also an understanding for the responsibility aspect. A state needs to be sure that they have the right to self-defence. This thesis will use the same case presented in the Tallinn Manual 2.0 because it shows well the right for self-defence. On 11th of September in 2001 a terrorist group Al Qaeda attacked against the United States. A terrorist group attacked against the twin towers in New York and Pentagon.[114] The United States attacked against Al Qaeda's headquarters as an act of self-defence.[115] This was not the first time when the United States attacked against a terrorist group.[116]

---

[112] Finnish Government (2020), *supra nota* 102.
[113] Shiryaev, Y. (2007-2008). The Right of Armed Self-Defense in International Law and Self-Defense Arguments Used in the Second Lebanon War. *Acta Societatis Martensis*, 80-97.
[114] Haybes, J. (2005). Al Qaeda: Ideology and action. Critical Review of International Social and Political Philosophy. Vol. 8, No. 2, 177–191.
[115] Ibid.
[116] Beard, J. (2001). America's New War on Terror: The Case for Selfdefense Under in Defense Under International Law. *Harvard Journal of Law & Public Policy*, 25, 559-590.

But this was the first time when the United Nations security council accepted the United States act to be an act of self-defence which is recognized in the Article 51 of the UN Charter.[117] As the UN Security council has agreed that United States had the inherent right to self-defence, it can be said that Al Qaeda's attack was an armed attack which occurred. The attack against the United States killed and injured a number of people, which is, as stated previously, the definition for an armed attack including the consequences and the amount of the people affected. According to the Finnish manual and Finland's position in this matter, Finland thinks that if a case like this terrorist attack against the United States would happen in the cyber environment it would violate the states sovereignty and the state would have the right to defend itself.[118] The discussion about violating sovereignty is always a case by case assessment according to the Finnish manual.[119] This case is also difficult because Al Qaeda is a terrorist organisation, not a state, but this terrorist organization is located in another state's territory. This thesis is not going to explain the situation about non-state actors. This case example only presents the issue of an armed attack and the issue on the right to self-defence. The case also presents that the consequences, or should one say scale and effects, that the attack causes has a significant purpose about qualifying the definition of an armed attack.

## 4.2. Armed attack under the Finnish manual

The Finnish manual states that even though there is not an established definition, when a cyber attack responds to an armed attack designated in the Article 51 it is still widely accepted that equivalence depends on the cyber attack's consequences. It states that a cyber attack must be sufficiently serious and have similar affects that an armed attack would have.[120] The Finnish manual took its position on defining what consequences a cyber attack should cause if it would be comparable to an armed attack. The Finnish manual has stated from the very beginning that a cyber attack's consequences should be the main source on deciding whether the attack is comparable to the armed attack in the Article 51 of the UN Charter.

[117] *Ibid.*
[118] Finnish Government (2020), *supra nota* 102.
[119] *Ibid.*
[120] *Ibid.*

### 4.2.1. Threatening with a cyber attack

Finland has introduced a few examples when they consider that a cyber attack would fulfil the definition of an armed attack. Firstly, the Finnish manual states that even threatening with a cyber attack could violate the prohibition of use of force.[121] However, it would also violate the states sovereignty. The threat also needs to be sufficiently exact and targeted towards another state.[122] The threat of a cyber attack should be exact and also real, so it would give the state a right to self-defence. The threat should also be considered to be qualified as an armed attack, so the states would have the right for self-defence. There should also be some evidence which increases the threats reliability. Threatening with a cyber attack would also require that the threatener and threatened state have had a long-standing conflict or other unbalanced relationship, so that the threat would be perceived as a real threat. For example, Russia, China and the United States have always had difficult relationship between each other.[123] If Russia would threaten the United States with a cyber attack, the threat would be assumed to be real. Even though, if a state has been threatened by a cyber attack, is it even possible to define the matter considered to be the same as the state would have been threatened with an armed attack? It is a difficult question because the definition of an armed attack in a cyber operation has not been defined yet. So, it is complicated to define whether just a threat would give the right to self-defence.

### 4.2.2. Consequences

Another example about defining armed attack in cyber attacks in the Finnish manual is the consequences that they cause. Consequences presented in the Finnish manual is that a cyber attack should have the same consequences as an armed attack.[124] A cyber attack should cause deaths, injuries and significant material damages.[125] The Finnish manual states that even though many commentators have agreed that the consequences is the definition of an armed attack, there is not any exact limit of the amount.[126] Even though the experts have agreed in their comments about the consequences of a cyber attack, it would also need case law or legislation. The Finnish manual also states that other circumstance factors should also be taken into account in the overall assessment.[127] Other circumstance factors can be anything, there should be a clear outcome from

---

[121] *Ibid.*
[122] *Ibid.*
[123] Graham, A. (2018). China and Russia: A Strategic Alliance in the Making. Retrieved from https://nationalinterest.org/feature/china-and-russia-strategic-alliance-making-38727, 08.10.2021.
[124] Finnish Government (2020), *supra nota* 102.
[125] *Ibid.*
[126] *Ibid.*
[127] *Ibid.*

the consequence and what they should be. Cyber attacks' consequences are challenging to measure because their effects can also be noted later.

An armed attack is easier to identify as an armed attack because its consequences are usually those mentioned above. The threat of an armed attack is also more serious because the consequences of armed attacks are always known. Cyber attacks intrinsically can be diverse and have unpredictable consequences that the attacked state cannot know in advance, and there is not any historical data on which a state could rely on when measuring the effects of cyber attacks. That is one of the reasons why threatening with a cyber attack is very challenging because the states cannot know the consequences what the threatened cyber attack could cause. Cyber attack's consequences can be unknown in advance. States have to be very careful by measuring the consequences of the cyber attack that they are facing because the right to self-defence is not always certain. The worst dilemma would be that a state would use their right to self-defence and in the aftermath the UN security council would measure that the threat was not serious enough and the state did not have the right for self-defence. If the state would not have the right for self-defence then the act could be considered to be just a counter attack.

The Finnish manual also articulates about the indirect and long-term consequences in cyber attacks which is equivalent to an armed attack.[128] Cyber attacks consequences can be indirect, so they can be harming something that the state could not have known in advance. There are a lot of different kinds of methods conducting a cyber attack, presenting a few examples to show the indirect and long-term consequences.

For example, this long lasting Covid-19 pandemic has arisen a question about the healthcare information system. If a cyber attacker would attack against a hospitals healthcare information system, it would have fatal and indirect consequences if the number of infected people increases.[129] This example illustrates the diversity of a cyber attack and the fact that cyber attacks can affect many unpredictable matters. Cyber attacks can also have long-term consequences. For example, when the Ukraine power grid was attacked, the attacks consequences lasted for a few hours before the state got the electricity back on but it took months for the state to repair all the damages that

[128] *Ibid.*
[129] Viljamaa, J. (2021). Valtiolliset kybervaikuttamisen keinot ja vaikutukset - case Kiina. *Jyväskylän yliopisto*.

the cyber attack caused.[130] The Finnish manual also conducts that if these indirect and long-term consequences would be taken into consideration the evaluation should be sufficiently precise.[131] As the Finnish manual demands the evaluation to be sufficiently precise it makes the evaluation very difficult because the indirect and long-term consequences can be seen much later after the cyber attack has been completed. As has been discussed about the right to self-defence, it has been noticed that states need to act fast if they want to defend their own territory. The sentence from the Finnish manual about the sufficient precise evaluation makes state's fast decisions impossible.

The Finnish manual gives an aspect about the economic consequences that an cyber attack could cause.[132] The Finnish manual articulates that should a cyber attack be defined as an armed attack if the attack would have economic consequences, for example if the state's financial system would collapse or some part of the state's economy would collapse, because of an cyber attack.[133] This issue is remarkable because there are a numerous of studies which show that cybercrimes are increasing and it is very detrimental to states because it is unprofitable.[134] Introducing an example about the research made on this matter, European Parliament made a report which shows that cybercrimes cost to the world economy around 5500 billion in the year 2020, the amount has doubled from the year 2015.[135] The amount of the cost is high and this information is significant and the Finnish manual is right about the fact that economic consequences should be taken into consideration.

The same research also introduces its own example of the hospital scenario that the Finnish manual introduced above. It states that if a cyber attack is made against a hospital it can postpone urgent surgeries and treatments, the research also states that if a cyber attack is made against an energy grid it can leave people without essential services .[136] These examples show that cyber attacks can also cause injuries and deaths which is what the Finnish manual states to be the main consequence when defining a cyber attack to be an armed attack. Examples also show the economic harm that

---

[130] Whitehead, D., *et al*. (2017). Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. *70th Annual Conference for Protective Relay Engineers (CPRE)*, 1-8.
[131] Finnish Government (2020), *supra nota* 102.
[132] *Ibid*.
[133] *Ibid*.
[134] Johnson, A. (2016). Cybersecurity for Financial Institutions: The Integral Role of Information Sharing in Cyber Attack Mitigation. *North Carolina Banking Institute*, 20, 277-310.
[135] European Parliament. (2021). *Miksi kyberturvallisuus on tärkeää EU:lle?* Retrieved from https://www.europarl.europa.eu/news/fi/headlines/society/20211008STO14521/miksi-kyberturvallisuus-on-tarkeaa-eu-lle, 19.10.2021.
[136] *Ibid*.

cyber attacks can cause. Cyber attacks can be more harmful in the economic perspective for the world's economy than armed attacks and, as the research presents, the cost is increasing.

The Finnish manual concludes the paragraph by stating that cyber use of force should honour the Charter of the United Nations; its articles, purpose and aim which is preventing the escalation of an armed attack.[137] Even though the mission is to avoid the situation of an armed attack, it needs to be underlined that there is a difference between an armed attack and lesser use of force.[138] And the aim is not trying to put these two together. The Finnish manual gives a new point of view on what should be taken into consideration when defining an armed attack in cyber attacks.

[137] Finnish Government (2020), *supra nota* 102.
[138] *Ibid.*

# 5. NON-NATO EUROPEAN COUNTRIES POSITION'S

This research will use novel contributions from other European Union countries about the matter of qualifying the definition of an armed attack in cyber operations under the energy sector. Finland is an EU country but not a member of NATO. To answer to the research question it is more justified to use statements about the topic from countries which have a similar position as Finland.

Sweden, Cyprus, Ireland, Malta and Austria are EU countries but they are not members of the NATO. They all do not have exact manuals as the Tallinn Manual 2.0 but they have taken their positions about this matter, some have stated their position in their cyber security strategy, some have done extensive and detailed research about it, some of them not but the main focus is still that they have taken their position about the matter. In this chapter the thesis will present the positions of the non-NATO European Union countries about the matter of the thesis topic.

## 5.1. Sweden

Sweden has announced in year 2021 that it will establish its own cyber security centre as one of the latest one of the Nordic countries.[139] As use of technology increases it will constitute problems to the state's cyber security, which is why it is important that states such as Sweden will take care of their cyber security. Nowadays it is a default value that states have their own cyber security centres as the cyber threats become more common. Cyber threats are not just a problem for companies but they affect an entire state and especially the state's cyber infrastructure. As thought about the state's cyber infrastructure it is very important for the energy sector that states have prepared for the cyber attacks, because a cyber attack against the energy sector can cause major damages which can have straight consequences for the citizens. European Union has noticed the threat of a cyber attack and wanted to secure the critical infrastructures such as the energy sector by NIS directive.

[139] O'Dwyer, G. (2021). *Sweden to establish national cyber security centre*. Retrieved from https://www.computerweekly.com/news/252495978/Sweden-to-establish-national-cyber-security-centre, 03.12.2021.

Sweden has announced in 2016 about their own national cyber security strategy where they have taken concern the problems in the cyber infrastructure. It states that: "Covert intrusions and attacks can be used in order to prepare for sabotage against critical infrastructure in peacetime. These can also be used openly as a tool primarily in the initial stages of military operations. Cyberattacks can have major consequences for vital societal functions and critical IT systems similar to a conventional armed attack and can therefore, in some cases, be considered an armed attack".[140] The Swedish strategy states that if the attacks were to be targeted against vital societal functions and critical IT systems it can cause similar consequences as an kinetic armed attack would cause, and therefore it could be considered to be as an armed attack in cyber operations. The statement is correct because cyber attacks targeted to the critical infrastructure such as states energy sector can lead to various different impacts which can affect major consequences. If a cyber attack causes a power grid such what Ukraine experienced it can cause deaths of civilians if the attack is targeted for example to the hospitals electricity. Hospitals need electricity all the time for situations that are life-threatening to the patients.

As the Article 51 of the UN Charter gives states the inherent right for self-defence, this statement is also problematic because in the beginning it states that "covert intrusions and attacks", which may mean that the state cannot identify the attacker. Article 51 of the UN Charter gives the inherent right for self-defence against another state but it leaves consideration if the attacker is a non-state actor. Covert intrusions can also be States but the problem is that the attacker must be identified, as the Article 51 of the UN Charter considers armed attack definition only consisting states.

Sweden's statement continues the same line as the previous interpretations of this matter about the qualification of an armed attack in cyber operations about the consequences. Sweden has its own outcome for defining the consequences such as vital societal functions and critical IT systems. Sweden's position is different as the consequences have been classified to consist only of vital societal functions and IT Systems.

[140] Government Offices of Sweden Ministry of Justice. (2016). *A national cyber security strategy*. Retrieved from https://www.government.se/4ada5d/contentassets/d87287e088834d9e8c08f28d0b9dda5b/a-national-cyber-security-strategy-skr.-201617213, 03.12.2021.

## 5.2. Republic of Cyprus

Republic of Cyprus has taken its position about cyber security. Cyprus has noticed in the recent years that they have to build up cyber security for the state after a few cyber attack cases which were targeted against companies in Cyprus.[141] Even though Cyprus is in the beginning of their cyber security, they still have noticed the problems in their system and know what they need to improve. Cyprus has plans for the future about building up their own position but it's not there yet.

In the Review of the cybersecurity capacity it noted a point about the internet users in Cyprus. The review stated that in Cyprus there is the highest percentages of social media users. The people in Cyprus also use internet as one of the most active countries in the whole Europe. This proves the risk about technology, when the technology increases or people are using it even more, it also raises the risk of a cyber attack. This problem was also noted in the review, that as the users become more active, it gives more space for the cyber attacks and that was one of the problems in the review that Republic of the Cyprus needs to put effort for the cyber security. It is a good note because although the problem about cyber threats is the development of technology, it is also a problem when the number of the user's increases. The users are the ones buying technology such as computers and smartphones. The devices are the weapons in cyber operations.[142] It could also be seen that the users are the product and everything else around it including technology is the manufacture. And the product is the weapon, because without the users there would be no technology and cyber attack could not be targeted to anywhere because nobody would not use it.

In a situation of a cyber operation against the energy sector it is possible that the attack is made using a random user's device and the attack is committed by using some innocent person's device, as the number of the users is increasing there are a lot of different devices that cyber criminals can use for conducting a cyber attack. It is a very different situation as in kinetic armed attacks, because kinetic armed attack is usually made by the military. Cyber attacks gives a wide range for even amateur hackers to commit a cyber attack on behalf of a state. As stated that devices are the cyber weapons, in the world full of technology it can be counted that the number of those weapons is major.

---

[141] Bada, M., Agrafiotis, I. (2017). Cybersecurity Capacity Review: Republic of Cyprus. *Global Cyber Security Capacity Centre*.

[142] Kirchner, S. (2014). Protection of Privacy Rights of Internet Users against Cross-Border Government Interference. *International Journal of Legal Information*, 42(3), 493-503.

## 5.3. Ireland

Ireland has a legislation on cybercrime. The Criminal Damage Act 1991 states that: ”a person who damages or recklessly damages property belonging to another, without lawful excuse, shall be guilty of an offence”[143]. The act contains the data which person adds, corrupts, erases or moves and also within the state, outside the state and makes an omission causing damages.[144]

As the Act has consequences committing these criminal actions it may apply to the situation of an armed attack because the armed attack has not been limited from this Criminal Damage Act. The problem is that the Act is stating that “a person”, so it does not apply to states. However, Ireland’s legislation is a good start for the discussion about the cyber operations qualified as an armed attacks.[145]

Ireland is the only one of these non-NATO European Union countries which has its own national contribution to this matter. Even though, all these states presented in this chapter are members of the Budapest convention (except Ireland is an observer country) which has criminalized cybercrimes. The problem in the legislation of Ireland is the same as it is in the Article 51 of the UN Charter, the legislation is old so it does not answer to today’s problems. Ireland’s Criminal Damage Act has different difficulties what Article 51 has, it has written too strict so it does not leave any room for interpretation. Article 51 leaves room for consideration so it could be used in a circumstance of an armed attack if case law would answer to this problem.

## 5.4. Malta

Malta has taken its position by defining armed attack in cyber operations in their cyber security strategy from 2016. In the cyber security strategy Malta states that: “As an independent sovereign state and as a member or the United Nations (UN), Malta has the right to defend its own territory and its infrastructure from acts of aggression from other states. Cyber-space is no exception and Malta has the right and obligation to defend its cyber-space territory to ensure that the security of the nation is maintained. Such measure entails ensuring that the following are addressed: cyber-

[143] O’Malley, G. (2013). Hacktivism: Cyber Activism or Cyber Crime. *Trinity College Law Review*, 16, 137-160.
[144] Osborne, P. (1995). The Irish criminal legal response to computer misuse. *International yearbook of law computers and technology*, 9, 65-82.
[145] O’Malley (2013), *supra nota* 143.

space defences, structures to counter terrorist attacks, ability and capacity to detect threats in cyber-space, capability to disrupt attacks on the country from cyber-space, active consideration of direction being taken at EU level on areas such as cyber diplomacy and on ways to counter hybrid threats.[146]" The text has a reference to the Article 51 of the UN Charter. Malta states that the entire cyber space and cyber infrastructure is included to the states sovereignty and they have the inherent right for defending it. This is an actual statement which states that all the acts of aggression which offends Malta's cyber space gives Malta an inherent right for self-defence. Hence, as the topic of this research is what can be qualified as an armed attack in cyber operations under the Article 51 of the UN Charter under the energy sector? After this statement, it could be stated that all the acts of aggression in cyber operations is consisting definition of an armed attack. After this statement an act of aggression in cyber operation targeted to energy sector would be qualified as an armed attack. Malta also takes the same position as the Article 51 of the UN Charter that the armed attack definition is consisting only states.

## 5.5. Austria

Austria has not made its outcome for qualifying armed attack definition in cyber operations. Austria has a security strategy – Security in a new decade, which has mentionings about cyber attacks but not a position about qualifying armed attacks definition in cyber operations. Austria has stated in their security strategy that there are threats in the future for their IT-systems' security such as cyber attacks.[147]

Austria has been criticized for not taking a position about qualifying self-defence terms in cyber operations such as Article 51 of the UN Charter or "hack-back"-situations.[148] Austria faced an cyber attack against its governmental institutions in January 2020, and it has been assumed that the attacker has been another state.[149] If the attacker would be another state, it may fulfil the criteria

[146] Ministry for competitiveness and digital maritime and services economy. (2016) Malta cyber security strategy. Retrieved from https://mita.gov.mt/wp-content/uploads/2020/07/Mita-_Malta-Cyber-Security-Strategy-Book.pdf, 15.12.2021.
[147] Federal Chancellery of the Republic of Austria. (2013). Austrian Security Strategy - Security in a new decade—Shaping security. Retrieved from https://www.bundesheer.at/pdf_pool/publikationen/sicherheitsstrategie_engl.pdf, 15.12.2021.
[148] Schweighofer, E., *et al*. (2020). Malicious Cyber Operations, "Hackbacks" and International Law: An Austrian Example as a Basis for Discussion on Permissible Responses. *Masaryk University Journal of Law and Technology*, 14(2), 227-258.
[149] BBC. (2020). *'Serious cyber-attack' on Austria's foreign ministry*. Retrieved from https://www.bbc.com/news/world-europe-50997773, 03.01.2021.

of the Article 51 of the UN Charter of an inherent right for self-defence and qualification of an armed attack. As Austria has not taken any position about defining the attack or defined their rights, it has caused criticism. As Austria faced the cyber attack it would be assumed that they would have wanted to respond to the attack, for self-defence or "hack-back" in cyberspace.

In Austria's security strategy it can be noticed that Austria relies on their cooperation's with another states and communities, such as the European Union, stabilisation and association process of the countries in the Western Balkans, the United Nations ,cooperation with the countries of the Mediterranean, the EU Strategy for the Danube Region, the European Neighbourhood Policy, development cooperation, and OSCE [150]. Although, this is a special situation as the Austria is not a member state of NATO but still counts on different cooperation's instead of making something own.

As Austria is counting on European Unions' cooperation if a cyber attack occurs and the European Union is worried about the member states critical infrastructure such as the energy sector should they also considered that as a threat and do something about it. Although, Austria is a larger country than Finland by its population, and Finland has its own position for this matter.

## 5.6. Summary

Even though these countries above have the same situation about their main cooperation and non-cooperation. They still have very different position about qualifying armed attack definition in cyber operations under the energy sector. Sweden has started their cyber security strategy later than other Nordic countries but Sweden has gone very far in their research. Sweden, like Finland has taken a cautious position and only to some parts of the problem, not so extensively as Tallinn Manual 2.0. However, Malta has taken a strong position which does not leave room for the cautions as Finland and Sweden have. Malta does not consider opinions in the various range as Tallinn Manual 2.0. In the case of Cyprus and Austria, they should consider their future soon because Cyprus has the highest percentage of users in technology and internet in Europe and Austria has recently faced a cyber attack.[151] As cyber operations will be the problems of todays society, no state can avoid to be a victim of a cyber attack. Ireland is the only one who has a national

[150] Federal Chancellery of the Republic of Austria (2013), *supra nota* 147.
[151] BBC (2020), *supra nota* 149.

contribution for this matter. As the energy sector keeps growing because of the increase of technology which uses electricity, there is a threat of a cyber attack against energy sector which is critical infrastructure for the state.

# CONCLUSION

As technology increases and the users along with it, it gives pressure for the cyber security because of a threat of a cyber operation such as cyber attacks. Technology which is using electricity for its functions makes pressure for the energy sector. Energy sector is a critical infrastructure for states and as has been seen cyber attacks targeted against the energy sector can cause serious harm. In the future the cyber attacks targeted against the energy sector can cause major consequences for the energy sector such as power outage from critical points such as hospitals and governmental devices.

Armed attack definition has not been qualified in cyber operations. As the Article 51 of the UN Charter gives the states the inherent right for self-defence if an armed attack occurs, it is necessary to qualify the term armed attack in cyber operations also. If the term armed attack could be qualified it would give the state, the inherent right for self-defence in cyber operations such as situations called “hack-back’s”. Article 51 of the UN Charter is old and it may not answer to today’s problems but it has been written comprehensively, so it leaves space for interpretation.

Finland is a part of the European Union but Finland is not a member state of NATO. Finland has always had a difficult geographical position because Finland’s neighbour Russia has always tried to have an impact on Finland’s political and military cooperation. Russia has also had its own interests about Finland’s cooperation’s because Russia does not want any NATO allies too close to it. Russia is currently having a situation in Ukraine which can affect Finland. Finland is so close to Russia that it could be possible that Finland would be used as a battlefield in Russia’s conflicts. Russia is also being suspected in many different cyber operations as an attacker, which makes it an even bigger threat to Finland.

There is not any clear legislation about the matter of qualifying armed attack in cyber operations. Finland has taken its own position by publishing their manual of cyber operations. Wider manual about the matter is the Tallinn Manual 2.0 which is made in a cooperation with NATO. These both

manuals are non-binding researches but they both have good points on how these problems should be solved. There is not any current case law which would apply to this matter.

As Finland is not a member state of NATO the answer for the research question has been examined from states that have a similar position as Finland does. Sweden, Cyprus, Ireland, Malta and Austria are all European Union countries but they are not member states of NATO. Even though these countries have a same kind of position, they have their own comments to the same issue.

As this research has been explored from Article 51 of the UN Charter, Tallinn Manual 2.0, Finnish Manual, non-NATO European countries position's, peer-reviewed articles and examples the answer has always been the same. Based on these materials, qualifying armed attack in cyber operations under the Article 51 of the UN Charter under the energy sector is the consequences what the operation or the attack causes. If a cyber operation or attack would be considered to qualify the term of armed attack it should cause the same consequences what a kinetic armed attack would cause. Consequences that a kinetic armed attack would cause is usually deaths and injuries. A cyber operation or attack can also cause, additionally to deaths and injuries, material damages such as economical loss or destruction of important objects, they are also considered to be consequences which could qualify an attack to be an armed attack.

As the UN Charter is the main legislation to this matter, it could be possible that the member states of the United Nations would cooperate together and make a clear legal act on this matter. The legal act should be clear, with strict guidelines which does not leave any room for interpretation. Tallinn Manual 2.0 is a good research about this matter, it would be helpful legalizing this matter. As the technology increases it demands even more from the energy sector, and cyber operations and cyber attacks are todays problems and they are increasing. The missing clear legislation concern is justified because the legislation to this matter will be needed for future cyber attacks.

# LIST OF REFERENCES

## Scientific Books

1. Schmitt, M. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. *Cambridge University Press*, Second edition.

## Scientific Articles

2. Apostolopoulos, T., Gritzalis, D., Mitrou, L., Thraskias, C., Pipyros, K. (2018). A new strategy for improving cyber-attacks evaluation in the context of Tallinn Manual. *Computers & Security,* 74, 371-383.

3. Beard, J. (2001). America's New War on Terror: The Case for Selfdefense Under in Defense Under International Law. *Harvard Journal of Law & Public Policy*, 25, 559-590.

4. Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. *Procedia Economics and Finance*, 28, 24-31.

5. Brunner, I., Dobric, M., Pirker, V. (2015). Proving a State's Involvement in a Cyber-Attack: Evidentiary Standards before the ICJ. *Finnish Yearbook of International Law*, 25, 75-108.

6. Cassese, A. (2008). International Criminal Law. *Oxford University Press*, Second edition, 154.

7. Davis, P. (2015). Deterrence, Influence, Cyber Attack, and Cyberwar. *New York University Journal of International Law and Politics*, 47(2), 327-356.

8. Dinstein, Y. (2004). The Conduct of Hostiles under the Law of International Armed Conflict. *Cambridge University Press*.

9. Dinstein, Y. (2001). War, Aggression and Self-Defence. *Cambridge University Press,* Third edition.

10. Dynkin, B. (2018). Derivative Liability in the Wake of a Cyber Attack. *Albany Law Journal of Science & Technology*, 28(3), 23-44.

11. Energy Expert Cyber Security Platform, EECSP. (2017). *Cyber Security in the Energy Sector – Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector*. Retrieved from https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf, 21.12.2021.

12. Finch, B., Spiegel, L. (2013-2014). Litigation following a Cyber Attack: Possible Outcomes and Mitigation Strategies Utilizing the Safety Act. *Santa Clara High Technology Law Journal*, 30(3), 349-374.

13. Fleury, T., Khurana, H., Welch, V. (2008). Towards a Taxonomy of Attacks Against Energy Control Systems. *The International Federation for Information Processing*, 290, 71-85.

14. Hathaway, O., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., Spiegel J. (2012). The Law of Cyber-Attack. *California Law Review*, 100(4), 817-886.

15. Haybes, J. (2005). Al Qaeda: Ideology and action. Critical Review of International Social and Political Philosophy. Vol. 8, No. 2, 177–191.

16. Hayward, R. (2017). Evaluating the Imminence of a Cyber Attack for Purposes of Anticipatory Self-Defense. *Columbia Law Review*, 117(2), 399-434.

17. Henderson, C. (2014). Non-state Actors and the Use of Force. *Hart Publishing.*

18. Hodgson, G. (2016). Cyber Attack Treaty Verification. *A Journal of Law and Policy for the Information Society*, 12(2), 231-260.

19. Johnson, A. (2016). Cybersecurity for Financial Institutions: The Integral Role of Information Sharing in Cyber Attack Mitigation. *North Carolina Banking Institute*, 20, 277-310.

20. Kirchner, S. (2014). Protection of Privacy Rights of Internet Users against Cross-Border Government Interference. *International Journal of Legal Information*, 42(3), 493-503.

21. Lam, C. (2018). A Slap on the Wrist: Combatting Russia's Cyber Attack on the 2016 U.S. Presidential Election. *Boston College Law Review*, 59(6), 2167-2201.

22. Libicki, M. (2011). Cyberwar as a Confidence Game. *Air University Press*, Vol. 5(1), 132-147.

23. Lukacs, J. (1992). Finland Vindicated. *Foreign Affairs*, 71(4), 50-63.

24. O'Malley, G. (2013). Hacktivism: Cyber Activism or Cyber Crime. *Trinity College Law Review*, 16, 137-160.

25. Osborne, P. (1995). The Irish criminal legal response to computer misuse. *International yearbook of law computers and technology*, 9, 65-82.

26. Payne, C. (2017). Addressing Obstacles to Cyber-Attribution: A Model Based on State Response to Cyber-Attack. *George Washington International Law Review*, 49(3), 535-568.

27. Plazas, C. (2021). Information Crossroads: Intersection of Military and Civilian Interpretations of Cyber Attack and Defense. *University of Cincinnati Intellectual Property and Computer Law Journal*, 5.

28. Schweighofer, E., Brunner, I., Zanol, J. (2020). Malicious Cyber Operations, "Hackbacks" and International Law: An Austrian Example as a Basis for Discussion on Permissible Responses. *Masaryk University Journal of Law and Technology*, 14(2), 227-258.

29. Schmitt, M. (2014). Rewired warfare: rethinking the law of cyber attack. *International Review of the Red Cross*, 96(893), 189-206.

30. Shea, J. (2017). NATO: Stepping up its game in cyber defence. Cyber Security: *A Peer-Reviewed Journal*, 1, 165-174.

31. Shiryaev, Y. (2007-2008). The Right of Armed Self-Defense in International Law and Self-Defense Arguments Used in the Second Lebanon War. *Acta Societatis Martensis*, 80-97.

32. Softness, N. (2017). How Should the U.S. Respond to a Russian Cyber Attack. *Yale Journal of International Affairs*, 12, 99-114.

33. Todd, G. (2009). Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition. *Air Force Law Review*, 64(1), 65-102.

34. Tran, D. (2018). The Law of Attribution: Rules for Attribution the Source of a Cyber-Attack. *Yale Journal of Law and Technology*, 20, 376-441.

35. Upeniece, V. (2018). Conditions for the lawful exercise of the right of self-defence in international law. *Rīga Stradiņš University.*

36. Whitehead, D., Owens, K., Gammel D., Smith, J. (2017). Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. *70th Annual Conference for Protective Relay Engineers (CPRE)*, 1-8.

## EU legislation

37. Europian Parliament. Treaty of Rome. 25.11.1957. Retrieved from https://www.europarl.europa.eu/about-parliament/en/in-the-past/the-parliament-and-the-treaties/treaty-of-rome, 22.09.2021.

38. United Nations. *Chapter VII: Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression (Articles 39-51)*. Retrieved from https://www.un.org/en/about-us/un-charter/chapter-7, 11.04.2021.

39. United Nations. *The United Nations Treaty Collection*. Retrieved from https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-10-b&chapter=18&clang=_en, 26.05.2021.

## Other sources

40. Bada, M., Agrafiotis, I. (2017). Cybersecurity Capacity Review: Republic of Cyprus. *Global Cyber Security Capacity Centre*.

41. Cybersecurity & Infrastructure Security Agency. (2020). *Critical infrastructure sectors*. Retrieved from https://www.cisa.gov/critical-infrastructure-sectors, 11.04.2021.

42. *e-Estonia*. Retrieved from https://e-estonia.com/solutions/e-governance/government-cloud/, 21.12.2021.

43. European Parliament. (2021). *Miksi kyberturvallisuus on tärkeää EU:lle?* Retrieved from https://www.europarl.europa.eu/news/fi/headlines/society/20211008STO14521/miksi-kyberturvallisuus-on-tarkeaa-eu-lle, 19.10.2021.

44. Federal Chancellery of the Republic of Austria. (2013). Austrian Security Strategy - Security in a new decade—
Shaping security. Retrieved from https://www.bundesheer.at/pdf_pool/publikationen/sicherheitsstrategie_engl.pdf, 15.12.2021.

45. Finnish Government. (2020). *International law and cyberspace Finland's national positions*. Retrieved from https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727, 03.09.2021.

46. Government Offices of Sweden Ministry of Justice. (2016). *A national cyber security strategy*. Retrieved from https://www.government.se/4ada5d/contentassets/d87287e088834d9e8c08f28d0b9dda5b/a-national-cyber-security-strategy-skr.-201617213, 03.12.2021.

47. Graham, A. (2018). China and Russia: A Strategic Alliance in the Making. Retrieved from https://nationalinterest.org/feature/china-and-russia-strategic-alliance-making-38727, 08.10.2021.

48. Hartikainen, J. (2018). *NIS-direktiivi ja toimeenpano Suomessa*. Retrieved from https://vm.fi/documents/10623/10333141/7_Jarna_Hartikainen_NIS-direktiivi_toimeenpano_Suomessa__JHDTTK_0810_2018.pdf/66d3cf26-d418-4344-84df-af0dddb76b98, 01.12.2021.

49. Heima, T-P., Pantzar, M. (2021). *Näin autoveron historiallinen poisto näkyy uuden sähköauton hinnassa – Riittääkö alennus nopeuttamaan liikenteen sähköistymistä?* Retrieved from https://yle.fi/uutiset/3-12094199, 04.10.2021

50. Helsingin Sanomat. (2021). *Kestääkö sähköverkko?* Retrieved from https://www.hs.fi/teknologia/art-2000007852046.html, 02.12.2021.

51. Ilta-Sanomat. (2004). *Sähkökatko pysäytti laitteen, potilas kuoli*. Retrieved from https://www.is.fi/kotimaa/art-2000000270708.html, 09.12.2021.

52. Klimburg, A., Tirmaa-Klaar, H. (2011). Study, Cybersecurity and Cyberpower: concepts, conditions and capabilities for cooperation for action within the EU. *European Parliament*.

53. Kshetri, N., Voas, J. (2017). Hacking Power Grids: A Current Problem. *The IEEE Computer Society*, 50(12), 91-95.

54. Ministry for competitiveness and digital maritime and services economy. (2016) Malta cyber security strategy. Retrieved from https://mita.gov.mt/wp-content/uploads/2020/07/Mita-_Malta-Cyber-Security-Strategy-Book.pdf, 15.12.2021.

55. NATO. (2021). *Relations with Finland.* Retrieved from https://www.nato.int/cps/en/natohq/topics_49594.htm, 02.12.2021.

56. Nhede, N. (2021). *Mitigating grid vulnerabilities to boost cyber resilience*. Retrieved from https://www.smart-energy.com/features-analysis/mitigating-grid-vulnerabilities-to-boost-cyber-resilience/, 05.10.2021.

57. O'Dwyer, G. (2021). *Sweden to establish national cyber security centre*. Retrieved from https://www.computerweekly.com/news/252495978/Sweden-to-establish-national-cyber-security-centre, 03.12.2021.

58. Palmen, J. (2013). *Kemiallisten aseiden lyhyt historia*. Retrieved from https://yle.fi/uutiset/3-6789736, 15.11.2021.

59. Palojärvi, P. (2009). Battle in bits and bytes - computer network attacks and the law of armed conflict. *Helsingin yliopisto*.

60. Valkama, V. (2019). *Mustan rekan valtasi paniikki ja sekasorto: Niin pitikin käydä, sillä se joutui kyberhyökkäyksen kohteeksi – näin ”valkohattujen” avulla opetellaan, miten haavoittuvuudet tilkitään*. Retrieved from https://www.aamulehti.fi/uutiset/art-2000007440651.html, 20.10.2021.

61. Turvallisuuskomitean sihteeristö. (2013). *Suomen kyberturvallisuusstrategia*. Retrieved from https://www.defmin.fi/files/2368/Suomen_kyberturvallisuusstrategia_ja_taustamuistio.pdf, 20.10.2021.

62. Ulkoasiainministeriö. (2015). *Voimankäytön oikeussäännöt selvitys eduskunnan ulkoasiainvaliokunnalle*. Retrieved from https://um.fi/documents/35732/48132/voimank%C3%A4yt%C3%B6n_oikeuss%C3%A4%C3%A4nn%C3%B6t__selvitys_eduskunnan_ulkoasiainvaliokunnalle_/56324b9e-6ce1-e3cd-5782-248662df5580?t=1525861360553, 28.09.2021.

63. Vainio, S. (2021). Venäjä vaatii, ettei Nato ota uusia jäseniä ja pysyy poissa Itä-Euroopasta – ehdottaa neuvotteluja Yhdysvaltojen kanssa ”vaikka huomenna”. Retrieved from https://www.hs.fi/ulkomaat/art-2000008484463.html, 15.11.2021.

64. Valtioneuvosto. (2020). *Kansainvälinen oikeus kyberympäristössä Suomen kansallisia kantoja*. Retrieved from https://um.fi/documents/35732/0/KyberkannatPDF-FI.pdf/c69fce1e-5753-3731-0b46-356b8216df51?t=1603097434415, 03.09.2021.

65. Viljamaa, J. (2021). Valtiolliset kybervaikuttamisen keinot ja vaikutukset - case Kiina. *Jyväskylän yliopisto*.

66. YLE. (2021). *Putin vaati Natolta, ettei sotilasliitto laajene itään – näin Niinistö kommentoi: uudet jäsenyydet ovat hakijamaan ja Nato-jäsenten välinen asia.* Retrieved from https://yle.fi/uutiset/3-12213883, 02.12.2021.

67. Zetter, K. (2016). *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*. Retrieved from https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/, 06.09.2021.

# APPENDICES

## Appendix 1. Non-exclusive licence

**A non-exclusive licence for reproduction and publication of a graduation thesis[152]**

I Lisa Nevala

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

What can be qualified as an armed attack in cyber operations under the Article 51 of the UN Charter under the energy sector in Finland,

supervised by Aleksi Kajander,

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.

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.

---

04.01.2022

[152] *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.*