What is the scope of legal self-defense in International Law?

Jus ad bellum with a special view to new frontiers for self-defense

by SOPHIE CHARLOTTE PANK

This dissertation discusses to what extent existing international law is adequate to regulate the issues of cyber-attacks in relations to self-defense. More specifically, the thesis will encompass an examination of what legal authority states have to respond with forcible measures to cyber-attacks or cyber-threats by states or non-state actors. Initially, the legal framework surrounding self-defense and use of force in international law will be presented.

It will be explained that the fundamental principles of Article 2 (4) and Article 51 of the Charter of the United Nations are sufficient to meet the new challenges which cyber-attacks pose. The threshold for legal self-defense will be examined, and it will be explained that whether a cyber-attack can be categorized as an armed attack will depend on the damage and effect the attack causes more than the type of weapon which has been launched.

It is concluded that cyber-attacks which cause human fatalities or large-scale destruction on property can constitute an armed attack, which will allow states to take forcible measures in compliance with the rules and regulations set out in Article 51 and customary international law. It will also be concluded that states are allowed to respond to cyber-threats which are imminent or real. It will furthermore be determined that states can respond with forcible measures against cyber-terrorism even when the terrorists operate from the territory of another state.

Table of Contents

1. Introduction

Country A is the target of a cyber-attack on a dam in an inhabited area. The cyber-attack gives the hackers control of the dam and the hackers thereby unleash enormous amounts of water, which inevitable causes large-scale damage and destruction of property, but also causes the death and injury of thousands of people. A while after the attack it is discovered that the attack was executed by Country B.

Does Country A have the right to invoke self-defense? Does the cyber-attack amount to an armed attack as written in article 51 of the Charter? What if the attack had been executed by a non-state actor such as a terrorist group? Would it amount to an armed attack as written in article 51 in the charter if Country B had placed a worm in Country A´s network to spy?

When the Charter of the United Nations was drafted in 1945 the term “armed attack” meant one nation attacking another nation with a regular army. In today´s world you can completely paralyze a country from behind a computer screen. Just to give an example of the large damage a cyber-attack can cause, a hacker can hack into control-systems, take over a nuclear-power plant and melt its reactors causing a nuclear explosion.

These hypothetical situations present some of the more recent issues the world is facing when dealing with armed attacks and based on these hypothetical situations this thesis will examine to what extent cyber-attacks can constitute an armed attack, such as placing a virus and thereby destroying a state´s infrastructure, taking control over government facilities or causing severe damage and casualties. Secondly, it will examine if CNE or espionage can constitute an armed attack in accordance with Article 51. Finally this thesis will examine to what extent a state can exercise cyber-defense, both when responding to a cyber-attack, but also whether a state can take cyber-measures as a response to an armed attack. Specifically, this thesis will examine the following: Do cyber-attacks constitute an armed attack and thereby justify the resort to the use of armed force in response in compliance with jus ad bellum?

So the issue today is not whether or not an attack will invoke the UN Charters article 51´s inherent right to self- defense, when one country marches across another country´s borders with an army, but instead the issues we are facing are those of cyber-attacks, cyber-terrorism and cyber-warfare.

So how can we use old laws on modern world´s issues?

1.1. Abbreviations and terminology

CNA: Computer Network Attack. This is also referred to as cyber-attacks. Cyber-attacks are to be understood as an attack launched against a state by using cyber-measures

CND: Computer Network Defense. This is also referred to as cyber-defense. Cyber-defense is to be understood as the defensible measures a state resorts to as a response to a cyber-attack. Cyber-defense includes both military use of force and electronic use of force.

CNE: Computer Network Exploitations. This is also referred to as cyber-espionage. Cyber-espionage is to be understood as using cyber-measures to spy on a state.

CNO: Computer Network Operations covers the entire area of cyber-means, such as CAN´s, CNE´s and CND´s.

Congo Case: A case Concerning Armed Activities on the Territory of the Congo (2005) (Democratic Republic of the Congo *v.* Uganda), International Court of Justice.

Corfu Channel Case: Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania), April 9th, 1949, International Court of Justice.

Declaration on Friendly Relations: Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations, General Assembly Resolution 2625 (XXV), 1970.

Declaration on the Non-Use of Force: Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations, General Assembly Resolution 42/22, 1987.

Definition of Aggression: United Nations General Assembly Resolution 3314 (XXIX). Definition of Aggression, April 12 1974.

DOS-Attacks: Denial-of-Service Attack. Flooding an Internet site, server, or router with data requests to overwhelm its capacity to function—can be used to take down major information networks[1].

ICC: International Criminal Court.

ICJ: International Court of Justice.

Kellogg-Briand Pact/Pact of Paris: The General Treaty for the Renunciation of War of 27th August, 1928 Nations.

NATO: The North Atlantic Treaty Organization.

Nicaragua Case: Case Concerning Military and Paramilitary Activities in and against Nicaragua ICJ Reports (1986) (Nicaragua vs. the United States of America), International Court of Justice.

Nuclear Weapons Advisory Opinion: Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, 1996, International Court of Justice.

Nuremberg-Charter: Charter of the International Military Tribunal (Nuremberg Charter), 1945.

Nuremberg Judgment: Judgment of the International Military Tribunal for the Trial of German Major War Criminals (Nuremberg Judgment), Sept. 30, 1946.

Tallinn Manual: Tallinn Manual on the International Law Applicable to Cyber Warfare, 2013.

The Oil Platforms Case: Case concerning Oil Platforms (Islamic Republic of Iran v. United States of America), 2003 I.C.J. 161 (November 6, 2003), International Court of Justice

The Tribunal: International Military Tribunal for the Trial of German Major War Criminals.

UN: United Nations.

UN Charter: Charter of the United Nations.

Virus: A computer virus is malware that infects its target by attaching itself to programs or documents[2].

The Wall Case: Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, 2004, International Court of Justice Advisory Opinion, ICJ 136 (July 9, 2004).

Worm: A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers[3].

[1] (Waxman, 2011), page 423
[2] (Sanger, 2010), Direct link: http://www.nytimes.com/2010/09/26/world/middleeast/26iran.html?_r=0.
[3] Ibid

1.2. Problem statement

The main objective of this thesis is to examine to what extent existing international law is adequate to regulate the issues of cyber-attacks in relations to self-defense.

Specifically, this thesis will encompass an examination of what international legal authority states have to respond with forcible measures to cyber-attacks or cyber-threats by states or non-state actors.

1.3. Delimitation of the research object

Cyber-attacks can be used both as means of jus in bello as weapons in war, or as jus ad bellum where a cyber-attack is a first mover attack. In relation to this thesis it will only be the jus ad bellum perspectives on cyber-attacks that will be examined and the rules and regulations of means of warfare will therefore not be examined.

This thesis is delimited to self-defense under Article 51 of the Charter of the United Nations in international law. It does not include any further exposition of the United Nations. This thesis will therefore not include any description or exposition of the United Nations history, structure and competences.

This thesis is limited to self-defense under the Charter of the United Nations Article 51, customary international law and will not include an examination of the other exceptions to the prohibition on the use of force, such as the Chapter VII powers and the non-charter based exceptions to use of force such as humanitarian intervention and the responsibility to protect.

1.4. Methodology

In this thesis legal method[4] will be applied as the rules in force will be described, systematized and analyzed[5].

As the area of law is relatively new, this thesis will primarily be based on a comprehensive examination and systemization of previous adjudications and will consist of an independent analysis of customary international law, state practice and practice by the United Nations.

The provisions regarding the use of force and self-defense in international law in the Charter of the United Nations will provide the legal framework for analyzing the abovementioned issues. The research will be based on analogies within existing law, specifically the classic use of self-defense as a response to an armed attack, since no precedents or any specific sources of International law exists regarding cyber-attacks as an armed attack. Furthermore, the examination will be based on an examination of legal literature, reports, UN Security Council resolutions and General Assembly resolution.

1.5. Composition

The first part of this thesis will examine the legal framework surrounding cyber-attacks in relations to self-defense, which will include a short examination of the prohibition on the threat or use of force in international law and a thorough examination of the requirements for using forcible measures as legal self-defense in Article 51 and customary international law.

[4] (Evald, 2007), page 3
[5] (Sten Schaumburg-Müller & Jens Evald, 2004), page 226

The second part of this thesis will treat the new frontiers for self-defense based on the examinations and analyses in part one. It will focus primarily on the legal issues regarding cyber-defense and cyber-terrorism as a respond to a cyber-attack in relations to self-defense under article 51 of the UN Charter.

Chapter 2 includes an introduction and examination of cyber-attacks and the legal issues surrounding the technological development in the modern world. Chapter 2 will also include an introduction to the seriousness of cyber-attacks and present examples of important cyber-attacks that have already taken place.

Chapter 3 will create an overview of preceding and current legislation within the field of cyber-attacks. This chapter will especially consist of an exposition and analysis of the requirement of armed attack, which is the condition for exercising self-defense in Article 51. Chapter 3 will also shortly account for the main rule on the use of force in Article 2 (4). This is done to create an overview over the scope of self-defense and the limitations of self-defense in international law. The analysis and conclusions in this chapter will create the theoretical background for the next chapter.

Chapter 4 will consist of an examination of cyber-terrorism in relations to cyber-defense and the issues surrounding non-state actors in international law.

Chapter 5 will process the concept of cyber-defense. It will encompass the requirements which need to be met when responding to an armed attack with the use of force in self-defense. It will also include a short introduction to collective self-defense and collective security in international law. Chapter 5 will also consist of an examination of the new and controversial frontiers of self-defense, such as preemptive self-defense and anticipatory self-defense.

Chapter 6 is a summarizing analysis of the legal issues processed in the previous chapters.

It is assumed that the reader of this thesis has basic knowledge of the Law of the United Nations, International Law and customary international law.

2. Cyber-Attacks and the Inherent Right to Self-Defense in International Law.

The classic example of an armed attack which triggers the inherent right to self-defense is obviously an attack which is a sufficiently grave attack carried out by the armed forces of one state against another. But that the technological revolution has changed the face of warfare is undisputable, and in today´s world computers impose a great threat on national security since they can be used as a weapon against another computer network, and by these means attack, for example, a state´s infrastructure, banking systems and nuclear facilities. But computers can also be used as part of military operations where they serve as an instrument of command, control, intelligence and surveillance[6]. The more dependent states become on computer networks, the more vulnerable they will be to an attack on these networks.

The seriousness of cyber-attacks has already been established several times. In 2000 cyber-attacks were used in the Israeli-Palestinian conflict when Israeli hackers launched a DOS-attack on computers

[6] (Dinstein, Computer Network Attacks and Self-Defence, 2002), page 102

owned by the Palestinian terrorist organization Hamas and the Lebanese resistance movement Hezbollah. As a response to the Israeli attacks, anti-Israel hackers launched similar attacks on Israeli websites[7].

In 2007 a DOS-attack was launched against Estonia, which was considered to be one of the most "wired" countries in the world. The DOS-attack was used to take down major information networks and the attack disrupted government and commercial functions for weeks. Among the targets of the cyber-attacks were two of Estonia´s biggest banks, whose systems were paralyzed for several hours. Similarly to the Ghostnet operation mentioned below, it was never fully determined who had been responsible for the attack, although it was presumed that Russia was behind the attack[8].

In March 2009 a large-scale cyber-espionage operation known as the Ghostnet was discovered. This massive cyber-operation included espionage on around 1.295 computers worldwide of which a third of these were located within ministries of foreign affairs, embassies, news media and international medias which, of course, are presumed to have contained classified information. It has never been determined who was responsible for the attack, but it was alleged that China was behind the attack[9].

The most recent incident of cyber-attacks is the attack on the Iranian nuclear facility which was infected and significantly impaired with a sophisticated computer worm in 2010 named Stuxnet. The worm infected Iran´s uranium enrichment program by disrupting its control systems[10]. The worm was allegedly deployed by either Israel or the United States, but it was never proven who was responsible for the attack, because it is extraordinarily difficult to trace the source of any sophisticated computer worm and nearly impossible to determine its target for certain [11]. This makes it very difficult to show attribution in relations to self-defense.

The seriousness of cyber-attacks and the vulnerability of states risking being a victim of cyber-attacks have also been recognized by the international community[1213]. The UN panel of governmental experts acknowledges that cyber-attacks pose an enormous threat against "*public safety, the security of nations and the stability of the globally linked international community as a whole*"[14].

Cyber-attacks (also referred to as computer network attacks or CNA´s) are understood as "*operations to disrupt, deny, degrade, or destroy information resident in computers, computer networks, or the computers and networks themselves*"[15]. This definition is based on the US military doctrine[16], Matthew C. Waxmans definition[17] and the definition made by Yoram Dinstein[1819].

The definition of cyber-attacks made by the US military doctrine was part of a larger definition of computer network operations. According to the US military doctrine computer network operations can be divided into three categories:

[7] (World Affairs), Direct link: http://affairs1490.rssing.com/chan-26037939/all_p1.html.
[8] Ibid
[9] (Morozov, 2009), direct link: http://www.newsweek.com/nato-hammers-out-strategy-cyberattack-77499.
[10] (Waxman, 2011), page 423
[11] (Sanger, 2010), Direct link: http://www.nytimes.com/2010/09/26/world/middleeast/26iran.html?_r=0.
[12] (National Research Council, 2010)
[13] (The White House), direct link: http://www.whitehouse.gov/issues/foreign-policy/cybersecurity.
[14] (National Research Council, 2010)
[15] (Remus, 2013), page 179
[16] (United States Military Doctrine, 2012), Direct Link: http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf
[17] (Waxman, 2011), page 422
[18] http://www.iihl.org/iihl/Documents/DINSTEIN.pdf.
[19] (Dinstein, Computer Network Attacks and Self-Defence, 2002), page 105

- Computer Network Attacks (CNA)
- Computer Network Defenses (CND)
- Computer Network Exploitations (CNE)

CNDs are understood as "*defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation or destruction*"[20]. CNDs will also be referred to as cyber-defense. They "use security measures that seek to keep the enemy from learning about own military capabilities and intentions".

Computer Network Exploitations (CNE) cover the collecting and monitoring of enemy information. Usually they involve espionage performed with tools that penetrate systems and return information or copies of files enabling the military to gain an advantage over the enemy[21].

3. The Legal Framework

When examining whether or not cyber-attacks can constitute an armed attack that leads to a state´s right to exercise its right to self-defense, the first step is to separate use of force from armed attacks. In the Nicaragua Case[22] the ICJ divided the use of force into two categories: The most grave forms of use of force, which constitute an armed attack, and the use of force of lesser gravity[2324].

This creates a gap between Article 2 (4) and Article 51 and it is therefore necessary to distinguish between the two stipulations. It can be difficult to fully separate the use of armed force in relations to Article 2 (4) from an armed attack which is the precondition for using force in Article 51[25]. An examination of use of force is therefore highly relevant in relation to this thesis since all armed attacks are use of force, but not all uses of force amount to an armed attack[26]. The absolute prohibition on the threat or use of force in Article 2 (4) of the UN Charter is the main rule in international law regarding use of

[20] (Remus, 2013), page 179

[2121] (United States Military Doctrine, 2012), Direct Link; http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf, and (Remus, 2013), page 179-180

[22] On April 9th the ambassador of the Republic of Nicaragua filed in an application, which instituted the proceedings against the United States of America concerning the use of military and paramilitary activities in and against Nicaragua. Nicaragua charged the United States with using military force against Nicaragua, intervening in Nicaragua's internal affairs and violating the sovereignty, territorial integrity and political independence of Nicaragua. These violations were committed by training, financing and supplying around 10.000 contras in Honduras along the border of Nicaragua with medication, weapons, ammunition and food. Nicaragua submitted that this was in violation of Article 2 (4) of the UN Charter, customary international law and general treaty law. The contras which had been supported by the United States had caused considerable material damage and widespread loss of life, and had furthermore tortured, killed and raped both prisoners of war and civilians. They also kidnapped civilians with the purpose of overthrowing the government of Nicaragua . Nicaragua also claimed that some of the military and paramilitary activities were carried out directly by persons paid by the United States and thereby acted under the command of the United States where they were responsible for attacks on ports, oil installations and naval bases. Finally Nicaragua claimed that the United States had breached its territorial integrity by overflight of its lands and creating economic difficulties for Nicaragua by imposing trade embargoes, withdrawing its own aid to Nicaragua and by using its influence on different banks .
The first question of the ICJ is the question of the law applicable to the dispute. The ICJ decided that it was required to apply the multilateral treaty reservation made by United States but that the content of customary international remained applicable . This meant that the ICJ had to make its judgment based on customary international law.

[23] (Case Concerning Military and Paramilitary Activities in and Against Nicaragua, 1986)para 191

[24] (Committee on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, 2010), page 162

[25] (Dinstein, Computer Network Attacks and Self-Defence, 2002), page 100

[26] Ibid, page 163

force, and is considered to be a cornerstone of the UN Charter[27]. Article 51 is therefore to be read and interpreted in conjunction with Article 2 (4), which makes Article 2(4) and Article 51 somewhat intertwined.

Article 51 of the Charter of the United Nations was the first example of the right to self-defense being inserted into a treaty. War was not prohibited until the Kellogg-Briand Pact in 1928 and therefore the right to self-defense had been a concept of very little importance. The need to reserve a right to self-defense thereby suddenly became very explicit after the prohibition on war and the United States only ratified the Pact on the condition that the participation did not limit its inherent right to self-defense[28]. This could be viewed as the beginning of the importance of self-defense and the interpretation of the scope and limitations of self-defense in both customary international law and treaty law have afterwards been the subject of much debate.

The UN Charter does not explicitly define what is contained in Article 51 and especially the meaning of "armed attack" and "inherent right" has been the subject of much debate. Article 51 of the Charter is an exception to the prohibition of the threat or use of force in Article 2 (4), and reads;

> "Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, 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-defense 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"[29].

3.1. Use of Force in International Law

War was not outlawed until 1928 when the Kellogg-Briand Pact[30] was signed. The main purpose was to outlaw war and to limit international conflicts. Initially, the pact was supposed to have been a bilateral agreement between France and the United States, which is why the pact is named after the U.S Secretary of State, Frank B. Kellogg, and the French foreign minister, Aristide Briand[31]. The United States however feared that the agreement could be misinterpreted as an alliance with France which would require the United States to intervene if France was attacked and so the United States suggested that they should invite all nations to join the agreement. The trea-

[27] (Case Concerning Military and Paramilitary Activities in and Against Nicaragua, 1986), merits, para 193
[28] (U.S Department of State), Direct link: http://history.state.gov/milestones/1921-1936/kellogg.
[29] Charter of the United Nations Article 51
[30] The Kellogg-Briand Pact, also known as the Pact of Paris or the General Treaty for the Renunciation of War, was an international agreement signed on August 27th 1928 by 15 states including the United States, Japan, Great Britain, France and Germany. Later on the pact was signed by additional 47 states, and was thereby signed by almost all of the established states in the world at the time.
[31] (Princeton), Direct Link: http://www.princeton.edu/~achaney/tmve/wiki100k/docs/Kellogg-Briand_Pact.html.

ty came into effect on July 24th 1929 and was registered in the League of Nations[32] Treaty Series on the 4th of September 1929 according to Article 18 of the Covenant of the League of Nations[3334]. The contracting states agreed to two things. First of all they outlawed war by "condemning the recourse to war as a solution of international controversies", and they "renounce it as an instrument of national policy"[35]. Secondly they agreed to solve any disputes by peaceful means[36]. The United States ratified the pact on the condition that the participation did not limit its inherent right to self-defense[37].

The power of the Kellogg-Briand Pact was put to the test in 1931 when Japan openly violated it by invading Manchuria. However, neither the League of Nations nor the United States wanted to take action and the lack of enforcement ultimately meant that the Kellogg-Briand Pact did little to prevent World War II, even though the actions taken by Japan were illegal beyond any doubt.

3.1.1. Crimes against Peace

In 1945 the International Military Tribunal was established with the purpose of punishing the major war criminals of the European Axis[3839]. The Tribunal was given the power to try and punish the major war criminals who had been acting in the interest of the European Axis, both as individuals or as members of organizations[40].

The Charter of the Tribunal stated three crimes which were within the jurisdiction of the Tribunal and for which there should be individual responsibility: crimes against peace[41], war crimes[42] and crimes against humanity[43].

Crimes against peace included "planning, preparation, initiation or waging of a war of aggression or a war in violation of international treaties, agreements or assurances, or participation in a common plan or conspiracy for the accomplishment of any of the foregoing". According to the Charter of the Tribunal the Tribunal had the power to punish anyone participating in any of these acts, such as leaders, organizers, instigators and accomplices. This is elaborated in Article 7 and 8 of the Charter of the Tribunal where it is stated, that it did not free them from responsibility, that the defendants had an official position, as for example Heads of States or responsible officials in Government Departments[44] and that the de-

[32] The League of Nations was the first attempt to create a universal, international, political organization with a mandate to maintain international peace and security. It was founded as a result of the Paris Peace Conference, and was built into the Treaty of Versailles which ended World War I. The participation was voluntary, and anyone meeting the conditions could join. The concept of the League of Nations was similar to the one at Westphalia in the sense that it also was based on the idea that peace should be maintained by the big powers.
[33] The Covenant of the League of Nations, Article 18
[34] (Princeton) Direct link: http://www.princeton.edu/~achaney/tmve/wiki100k/docs/Kellogg-Briand_Pact.html.
[35] The General Treaty for the Renunciation of War of 27th August, 1928, Article 1
[36] Ibid, Article 2
[37] (U.S Department of State) Direct Link: http://history.state.gov/milestones/1921-1936/kellogg.
[38] Germany, Japan and Italy
[39] The Charter of the International Military Tribunal, Article 1
[40] Ibid, Article 6
[41] Ibid, Article 6 (a)
[42] Ibid, Article 6 (b)
[43] Ibid, Article 6 (c)
[44] Ibid, Article 7

fendants had followed orders from the government or superiors did not free them for responsibility[4546].

According to the Charter of the International Military Tribunal it was a crime to wage a war of aggression, or a war in violations of international treaties[47]. The Tribunal found several defendants guilty in planning and waging aggressive wars against twelve nations, which according to the Tribunal makes it unnecessary to discuss the subject in further detail and to consider the full extent to which these aggressive wars also were a violation of international treaties[48]. The treaties which are of principal importance are The Hague Conventions, the Versailles Treaty and the Kellogg-Briand Pact,[49] and the full extent of the treaties which were violated are set out in Appendix C of the Indictment[50].

3.1.2. The Prohibition on the Threat or Use of Force

Use of force in international law is prohibited by both customary international law[51] and treaty law[52], and has the status of Jus Cogens[5354] .

In customary international law obligations arise from practice contrary to obligations arising from treaty based law. Customary international law is a general practice accepted as law, and is acknowledged by the ICJ. In article 38 (1) it states that the Court shall apply international custom, as evidence of a general practice accepted as law and the general principles of law recognized by civilized nations. The ICJ has established that the applicability of customary international law is determined by two factors. The first factor is that the practice must be generally accepted by states and, secondly, customary international law is determined by Opinio Juris[55]. The extent of customary international law has not been exactly established since it is a vague and controversial topic that is based on values considered to be fundamental by the international society[56].

Jus Cogens is a peremptory norm of general or customary international law accepted and recognized by the international community as a norm from which no derogation is permitted and which can be modified only by a subsequent norm of general international law having the same character. A rule which has the status Jus Cogens also means that it is applicable for all states, independently of their membership of the UN. If any existing treaty is in conflict with a new peremptory norm of customary international law that treaty becomes void and terminates.

[45] Ibid, Article 8
[46] (Judgment of the International Military Tribunal for the Trial of German Major War Criminals (Nuremberg Judgment), 1946), Section dealing with "The Law of the Charter"
[47] The Charter of the International Military Tribunal, Article 6 (a)
[48] (Judgment of the International Military Tribunal for the Trial of German Major War Criminals (Nuremberg Judgment), 1946), Section dealing with "The Law of the Charter"
[49] Ibid, Section dealing with "Violations of International Treaties"
[50] Ibid, Vol. 1, Appendix C
[51] (Case Concerning Military and Paramilitary Activities in and Against Nicaragua, 1986)
[52] Charter of the United Nations, Article 2 (4)
[53] (Dinstein, Computer Network Attacks and Self-Defence, 2002), page 99
[54] (Case Concerning Military and Paramilitary Activities in and Against Nicaragua, 1986)
[55] (Case Concerning Military and Paramilitary Activities in and Against Nicaragua, 1986)
[56] (Lepard, 2010), page 3

The Charter provisions on the threat or use of force stated in article 2 (4) of the UN Charter are the main rules and are important to always have in mind. It reads:

> "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations[57]".

The drafters of the Charter of the United Nations deliberately chose to use the phrase "use of force" instead of the more narrow term "war"[58]. This definition originates from the League of Nations were the phrase "war" was used and turned out to be inadequate. The phrase "war" limits the prohibition to the actual situations where countries declare war or decide to lead a war of aggression. Use of force on the other hand covers both actual wars of aggression, but also attacks on one's territorial integrity or political independence which are not actual wars, but mere frontier incidents[59].

The prohibition on the threat or use of force is a cornerstone in international law[60] and this principle is embodied throughout the entire UN Charter. The preamble of the UN Charter reads:

> "We the people of the United Nations determined… to save succeeding generations from the scourge of war, which twice in our lifetime has brought untold sorrow to mankind, and… to unite our strength to maintain international peace and security, and.. to ensure, by the acceptance of principles and the institution of methods, that armed force shall not be used, save in the common interest".

As the preamble to the UN Charter states the purpose of the UN Charter is to prevent the succeeding generations of war by maintaining international peace of security. Peace is the most important value of this Charter and the purpose of maintaining international peace recur in UN Charters Article 1 (1+2) which reads (excerpt):

> "The Purposes of the United Nations are:
>
> - To maintain international peace and security, and to that end: to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace;
> - To develop friendly relations among nations based on respect for the principle of equal rights and self-determination of peoples, and to take other appropriate measures to strengthen universal peace".

Article 1 (1+2) elaborates what has already been stated in the preamble and the entire UN Charter is imbued with the purpose of maintaining universal peace and taking measures that can prevent and remove any threat to, or breach of, international peace and security.

[57] Charter of the United Nations Article 2 (4)
[58] (Gray, 2008), Page 7
[59] See Chapter 3.2.1.1; Frontier Incidents
[60] (Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), 2005)

Article 2 is the most important substantive article. Article 2 (1) states that there exists equal sovereignty between states (however, practically speaking, this is not true, since for example the United States is not equal to Micronesia). The maintenance of peace and security and the condemnation of use of force, acts of aggression or breach of peace are also mentioned in Articles 11 (1+2), 43 (1), 47 (1), 48 (1), 51, 52 (1), 73 (c), 84, 99 and 106.

Today it is a general agreement that use of force only covers armed force and thereby does not cover for example psychological or economic pressure[61]. In the Nicaragua Case the ICJ established that the United States had violated its obligation under international law not to use force "by training, arming, equipping, financing and supplying the contra forces or otherwise encouraging, supporting and aiding military and paramilitary activities"[62], and that the "assistance to rebels in the form of the provision of weapons or logistical or other support" also can constitute the use of force or may amount to intervention in states internal or external affairs[63]. The ICJ also determined that the mere supply of funds does not constitute illegal use of force[64][65]. The ICJ further established that the "laying of mines in the internal or territorial waters of the Republic of Nicaragua"[66], also constituted the use of force.

3.1.3. Definition of Aggression

The Definition of Aggression contains a further clarification of what constitutes the threat or use of force and is described as[67]:

> *"(a)* The invasion or attack by the armed forces of a State of the territory of another State, or any military occupation, however temporary, resulting from such invasion or attack, or any annexation by the use of force of the territory of another State or part thereof,
> *(b)* Bombardment by the armed forces of a State against the territory of another State or the use of any weapons by a State against the territory of another State;
> *(c)* The blockade of the ports or coasts of a State by the armed forces of another State;
> *(d)* An attack by the armed forces of a State on the land, sea or air forces, or marine and air fleets of another State;
> *(e)* The use of armed forces of one State which are within the territory of another State with the agreement of the receiving State, in contravention of the conditions provided for in the agreement or any extension of their presence in such territory beyond the termination of the agreement;
> *(f)* The action of a State in allowing its temtory, which it has placed at the disposal of another State, to be used by that other State for perpetrating an act of aggression against a third State;
> *(g)* The sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to the acts listed above, or its substantial involvement therein.[68]"

[61] (Remus, 2013), page 182
[62] Ibid, subnote (3)
[63] Ibid, para 195
[64] Ibid, para 227-228
[65] (Gray, 2008), page 30
[66] (Case Concerning Military and Paramilitary Activities in and Against Nicaragua, 1986), subnote (6)
[67] Ibid, Article 3 (a-g)
[68] (General Assembly, 1974), Definition of Aggression, Article 3 (a-g)

The Definition of Aggression is to be read in conjunction with the Declaration on Friendly Relations and contains a closer examination of the scope and meaning of Article 2 (4)´s prohibition on the threat or use of force. The Declaration on Friendly Relations determines that war of aggression is a crime against peace[69] and it defines aggression in accordance with Article 2 (4) as the use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations. It defines certain actions which are to be considered illegal in accordance with the prohibition on the threat or use of force and it establishes that states have a duty to refrain from such actions as military occupation, organizing, instigating, assisting or participation in acts of civil strife or terrorist acts in and against another state if these actions can be considered to be a threat or use of force[70]. In other words it prohibits both direct and indirect use of force. A supplement to the abovementioned declarations is the Declaration of the Non-Use of Force which was adopted by the General Assembly in 1987[71], which basically resembles the Declaration of Friendly Relations.

It is important to note that the abovementioned definitions of the threat or use of force are to be meant only as examples and that the list is not exhaustive[72].

3.1.4. The Exceptions to the Prohibition to the Use of Force

The main rule in Article 2 (4) states an absolute prohibition on the threat or use of force, and currently only two exceptions to this main rule are stated in the UN Charter[73]; the Security Council using its Chapter VII powers[7475] and the inherent right to self-defense[76]. If it does not fall within any of these legal exceptions, threat or use force cannot be legally applied[7778].

In this context it is relevant to mention that it has been widely debated whether some other fundamental rights to use force exist beyond Security Council authorization, such as humanitarian intervention and the responsibility to protect[79]. It has been established that each individual state has a responsibility to protect its people from for example genocide, war crimes and crimes against humanity[80]. If a state fails to live up to its responsibility the international community will take action using diplomatic, humanitarian and other peaceful means to protect the people, and if necessary also Chapter VII powers[81], as it for example has been done in Libya[82]. It is important to note that responsibility to protect so far on-

[69] Rome Statute of the International Criminal Court, Article 5, 1 (d)
[70] (General Assembly, 1970), Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, General Assembly Resolution 2625 (XXV), 1970
[71] (General Assembly, 1987), Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations, General Assembly Resolution 42/22, 1987
[72] (General Assembly, 1974), Definition of Aggression, Article 4
[73] (Dinstein, Computer Network Attacks and Self-Defence, 2002), page 1
[74] Charter of the United Nations, Chapter VII
[75] Ibid, Article 42
[76] Ibid, Article 51
[77] (Dinstein, Computer Network Attacks and Self-Defence, 2002), page 1
[78] (Kelsen, 1950), page 782
[79] (Council on Foreign Relations, 2013): The Dilemma of Humanitarian Intervention
[80] (United Nations General Assembly, 2005), World Summit Outcome Document, paragraphs 138-139
[81] Ibid
[82] UN Security Council Resolution 1970 and 1973

ly is legitimate when conducted in accordance with Chapter VI and VII of the Charter[83], so the question of whether such fundamental rights exist beyond Security Council authorization in customary international law remains unanswered. At the time being Security Council authorization and self-defense are therefore still the only certain legitimate exceptions to use of force[84], and the topics of humanitarian intervention and responsibility to protect will therefore not be the subject of any further examination in this thesis.

3.2. Armed Attack

According to Article 51 of the UN Charter the first requirement to exercise legal self-defense is that "… an armed attack occurs against a Member of the United Nations…" The rule requires that a state must have been the victim of the illegal use of force which in scale and effect amounts to an armed attack and it has been determined that this rule is in force in both treaty law and customary international law[8586].

This part of the thesis will examine to what extent cyber-attacks can constitute an armed attack which allows a state recourse to use force based on the previous examination of Article 51. As it has already been determined that only use of force, which has sufficiently grave consequences, amount to an armed attack this part will examine to what extent cyber-attacks can cross the threshold to armed attacks.

In the Nicaragua case the ICJ established several key-principles regarding the scope and limitation of self-defense and the case is therefore in many ways one of the most important cases when interpreting the scope of self-defense in international law. It is especially important because the ICJ chose to express its view on self-defense. The ICJ stated that the United States had violated its obligation under international law not to use force "by training, arming, equipping, financing and supplying the contra forces or otherwise encouraging, supporting and aiding military and paramilitary activities"[87], and that the "assistance to rebels in the form of the provision of weapons or logistical or other support" also can constitute the use of force or may amount to intervention in states' internal or external affairs[88], but in the last case it does not contain the scale required to amount to an armed attack[89]. The ICJ further established that the "laying of mines in the internal or territorial waters of the Republic of Nicaragua"[90], also constituted the use of force.

In the Nicaragua Case the ICJ, when processing the question of what might constitute an armed attack, stated that the definition of an armed attack must be interpreted with guidance from the Definition of Aggression[91] and the ICJ therefore applied the Definition of Aggression[92] as a basis for determining what may constitute the threat or use of force and armed attacks[93].

[83] (United Nations General Assembly, 2005) World Summit Outcome Document, paragraph 139
[84] Ibid, Article 2 (4)
[85] Charter of the United Nations, Article 51, (Case Concerning Military and Paramilitary Activities in and Against Nicaragua, 1986), para 211
[86] (The Oil Platforms Case (Iran v. US), 2003), para 51 and 57
[87] Ibid, subnote (3)
[88] Ibid, para 195
[89] (Case Concerning Military and Paramilitary Activities in and Against Nicaragua, 1986), para 195
[90] (Case Concerning Military and Paramilitary Activities in and Against Nicaragua, 1986), subnote (6)
[91] (General Assembly, 1974), Definition of Aggression, Article 3 (a-g)
[92] Ibid
[93] (Case Concerning Military and Paramilitary Activities in and Against Nicaragua, 1986), para 195

Similarly to the Nicaragua Case the ICJ in the Oil Platform Case[94] is narrowing the scope of self-defense making it more difficult for states to resort to use of force by claiming self-defense. In the Oil Platform Case the ICJ also examined the question of what triggers the right to self-defense, and first of all the United States had to prove that they have been the victim of an armed attack within the meaning of self-defense in Article 51 and customary international law[95].

The Oil Platforms Case concerns the United States´ destruction of three offshore Iranian oil platforms as a response to a missile attack on the vessel Sea Isle City, which had been reflagged to the United States, and the destruction of the warship USS Samuel B Roberts which struck a mine. In the first incident the ship was damaged and 6 crewmembers were injured[96]. These two incidents led to the abovementioned attacks on the Iranian oil-platforms and in both incidents the United States claimed to be acting in self-defense.

In the first incident regarding the attack on the Sea Isle City the ICJ concluded that the United States had failed to prove that Iran was responsible for the attack and thereby failed to show attribution. The use of force by the United States was therefore not legal self-defense[97]. The United States had however not relied solely on the attack on the Sea Isle City, but stated that the attack was part of a series of attacks which together amounted to an armed attack. The ICJ therefore also processed the hypothetical question of whether the attack on Sea Isle City either in itself or in combination with the other incidents would amount to an armed attack. The ICJ concluded that the evidence produced by the United States did not amount to an armed attack, not even if all the incidents were taken cumulatively. The ICJ states that the definition of an armed attack is reserved to the most grave forms of use of force, and thereby upholds the definition of an armed attack established by the ICJ in the Nicaragua Case[98].

The ICJ further concluded that the "attack" on the USS Samuel B Roberts in this case does not constitute an armed attack, however, the ICJ does note that they will not reject that the mining of a single warship can constitute an armed attack and thereby bringing the right to self-defense into play[99]. It has furthermore been determined by the ICJ in the Oil Platform Case that the burden of proof is on the state claiming to be the victim of an armed attack[100]. This burden of proof is very strict and the state must prove not only that it has been the victim of the use of force, but also

[94] The Government of the Republic of Iran filed in an application on the November 6th 1992 which initiated the proceedings against the United States of America. The case concerned the attack on and destruction of three off-shore oil-platforms in the Persian Gulf by several of warships belonging to the United States Navy. The attacks occurred on October 19th 1987 and on April 18th 1988. The three oil-platforms were owned and operated by the Iranian Government. The background of the dispute is based on actions which have occurred in the Persian Gulf between 1980 and 1988 when Iran and Iraq were in an armed conflict which spread to the Persian Gulf, and in 1984 Iraq began attacking Iranian ships in the Persian Gulf, notably Iranian Oil ships. Between 1984 and 1988 commercial vessels and warships of different nationalities where attacked by aircrafts and warships. Because of the disturbances in the Gulf Kuwait requested the United States, United Kingdom and the Soviet Union among others to reflag ships to ensure their protection. The Kuwait Oil Tanker Company then reflagged 11 ships so they would sail under United States flags. In addition to this, the United States agreed to provide the United States flagged vessels with a naval escort and called the operation "Operation Earnest Will". The basis for the naval deployment was the anticipated protection of non-US shipping as well as the protection of United States warships. Despite this several of Kuwait's tankers suffered attacks or struck mines, including those who had been reflagged.. Iran claimed not to be responsible for the attacks.

[95] (The Oil Platforms Case (Iran v. US), 2003), para 51 and 57

[96] Ibid, para 52

[97] (The Oil Platforms Case (Iran v. US), 2003), para 61

[98] Ibid, para 64

[99] Ibid, para 72

[100] Ibid, para 51

that the scale and effect of the alleged attack amounts to an actual armed attack and is not only a frontier incident[101]. In the Oil Platform Case the ICJ stated that because it was the United States who had violated the prohibition on the use of force, so the burden is on them to present their case[102].

It is important to note that the abovementioned definitions of the threat or use of force and armed attacks are only meant as examples and that the list is not exhaustive[103].

3.2.1. Scale and effect

As it was determined when establishing the legal framework of cyber-attacks, the qualification of cyber-attacks depends on an evaluation of the scale and effect the attack causes. An attack can easily constitute illegal use of force without amounting to an armed attack[104][105].

The right to self-defense in international law is therefore limited to the incidents where the use of force ,which the state has been victim of reaches the threshold in scale and effect to be characterized as an armed attack[106].

The term “scale and effect” originates from the Nicaragua Case and the ICJ applies the concept of scale and effect when separating use of force of lesser gravity from use of force which is grave enough to pass the threshold of an armed attack. However, the ICJ did not provide any further guidance regarding the interpretation of scale and effect. An exact definition of the term therefore remains uncertain.

The criteria of scale and effect are similar to the criteria defined in the Definition of Aggression. It is stated in Article 2 that the determination of whether an act of aggression has been committed will include whether the concerned acts or consequences of these acts are sufficient in gravity[107]. This seems to cover the scale of the attack in relations to time and place, but also the scale of the impact of the attack[108].

In the Tallinn Manual the International Group of Experts did however agree upon some indications which can be used when separating lesser grave forms of use of force from the gravest forms. However, the incidents where use of force lead to the death of human beings or destruction or damage to property would in scale and effect constitute an armed attack[109].

Yoram Dinstein uses the same criteria when separating lesser forms of use of force from armed attacks. He concludes that illegal use of force will amount to an armed attack,

[101] (Case Concerning Military and Paramilitary Activities in and Against Nicaragua, 1986), (The Oil Platforms Case (Iran v. US), 2003)
[102] (The Oil Platforms Case (Iran v. US), 2003), para 58
[103] (General Assembly, 1974), Definition of Aggression, Article 4
[104] (Case Concerning Military and Paramilitary Activities in and Against Nicaragua, 1986)para 191
[105] (Committee on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, 2010), page 162
[106] (Schmitt, 2013), page 55
[107] (General Assembly, 1974), Definition of Aggression, Article 2
[108] (Gray, 2008), page 178
[109] (Schmitt, 2013), page 54-55

whenever it causes the death of human beings or when it results in serious destruction of property[110].

In relation to cyber-attacks this is definitely one of the most important parameters when determining if and when cyber-attacks can constitute armed attacks, and it will be applied regularly throughout the thesis.

3.2.1.1. Frontier Incidents

Another important conclusion made by the ICJ in the Nicaragua Case is that the ICJ distinguishes between an actual armed attack and frontiers incident. It has been debated that frontier incidents are not to be considered as armed attacks, because frontier incidents in scale and effect not will amount to an armed attack, but that they can constitute the threat or use of force[111].

Christine Gray[112] states that the ICJ in the Nicaragua Case divides the distinguishing of frontier incidents into two classifications, which helps determine if the incident is merely a frontier incident or if it amounts to an armed attack. The first distinguishing features the scale and effect of the attack[113][114][115].

The distinction made by the ICJ between frontier incidents of lesser gravity and armed attack in the Nicaragua Case has according to Christine Gray been the subject of much criticism afterwards, because it has been argued that the distinction is unnecessary since the protection against excessive use of force already exists within the other requirements of necessity and proportionality[116].

Yoram Dinstein finds the assumption that mere frontier incidents cannot have the scale and effect to constitute an armed attack bothersome[117][118]. He further argues that the trivial use of force, such as a few stray bullets across the border that hits a tree cannot in scale and effect amount to an armed attack, because the action is below the minimum threshold[119] and there will not be room for counter-measures in self-defense. The same incidents will however result in an armed attack whenever illegal use of force causes the death of human beings, or when it results in serious destruction to property[120]. Yoram Dinstein refers to Fitzmaurice[121] who states that "*there are frontier incidents and there are frontier incidents. Some are trivial, some*

[110] (Dinstein, Computer Network Attacks and Self-Defence, 2002), page 100
[111] (Dinstein, Computer Network Attacks and Self-Defence, 2002), page 100
[112] Professor of International Law, University of Cambridge, Faculty of Law
[113] (Case Concerning Military and Paramilitary Activities in and Against Nicaragua, 1986), para 195
[114] (Gray, 2008), page 178
[115] (Dinstein, War, Aggression and self-defence, 2011), page 210
[116] Ibid, page 179
[117] (Dinstein, War, Aggression and self-defence, 2011), page 210
[118] (Gray, 2008), page 179-180
[119] (Dinstein, War, Aggression and self-defence, 2011), page 210
[120] (Dinstein, Computer Network Attacks and Self-Defence, 2002), page 100
[121] 1901 – 1982) was a British barrister and judge. He was a member of the Permanent Court of Arbitration between 1964 and 1973 and a Senior Judge of the International Court of Justice between 1967 and 1973, before becoming a Judge of the European Court of Human Rights at Strasbourg in 1974.

may be extremely grave"[122]. This position is similarly argued by Hargrove[123] who states that Article 51 in no way limits itself to especially large, direct or important attacks[124][125].

The assumption that frontier incidents can have the scale and effect to amount to an armed attack seems to be supported by the ICJ in the Oil Platforms Case where the ICJ determines that it "does not exclude the possibility that the mining of a single military vessel might be sufficient to bring into play the inherent right to self-defense"[126]. The arguments made by Yoram Dinstein therefore seem to be the most correct. On this basis it must seem to be concluded that frontier incidents can amount to an armed attack in scale and effect[127].

The second distinguishing within the concept of frontier incidents features the motivation behind the attack[128]. The ICJ had noted in the Nicaragua Case that the circumstances and motivations for the incursion are part of its legal classification[129]. According to Christine Gray it would seem that the ICJ includes incidents where there is no intent to carry out an armed attack into the concept of frontier incidents, for example incidents where officials has disobeyed order, or accidental incursions. The difficulties behind a state´s intentions and motives are very controversial, and have been the subject of much debate. The ICJ leaves the question unanswered in the Nicaragua Case and the subject of accidental incursions will not be part of any further examination in this thesis, since it is not highly relevant to establish the legal framework of accidental attacks in relations to cyber-attacks. Frontier accidents caused by internal riots and disturbances are likewise not very relevant in relations to cyber-attacks and therefore not a subject which needs to be examined any further. The incidents where officials have disobeyed orders will however be processed shortly in Chapter 5.1, Non-State Actors operating with the Support from a State.

3.2.2. New Frontiers for Armed Attacks

The scale and effect of cyber-attacks varies and the damage a cyber-attack can cause range from large-scale destruction of military and civilian infrastructure to malicious hacking and defacements of websites[130][131]. In order to determine whether or not a cyber-attack can constitute an armed attack, it needs to be determined if "armed attack" in Article 51 is limited to the incidents where an actual armed attack occur using kinetic force, or if the concept "armed attack" is the subject of a wider interpretation.

The first approach regarding the interpretation of "armed attack" is to follow Article 51 literal, which means that anything, which is not armed force/kinetic force, is allowed according to jus ad bellum principles. This would mean that cyber-attacks and other electronic at-

[122] (Dinstein, War, Aggression and self-defence, 2011), page 210
[123] JOHN LAWRENCE HARGROVE, Director of Studies, The American Society of International Law, Washington, D, C.
[124] (Gray, 2008), page 180
[125] Ibid, page 211
[126] (The Oil Platforms Case (Iran v. US), 2003), para 72
[127] (Schmitt, 2013), page 55
[128] (Gray, 2008), page 179
[129] (Case Concerning Military and Paramilitary Activities in and Against Nicaragua, 1986), para 231
[130] (Waxman, 2011), page 422
[131] (National Research Council, 2010), page 3

tacks would be legal[132]. This approach does however not seem to have gained much support by neither academic writers nor many states.

Another approach is to evaluate cyber-attacks on the basis of the damage and effect they cause, instead of the weapon used to launch the attack. This approach seems to be supported by most states and academic writers. One idea of how to categorize cyber-attacks was set forth by Walter Gary Sharp, who proposed that "any computer network attack that intentionally causes any destructive effect within the sovereign territory of another state is an unlawful use of force within the meaning of Article 2 (4) which may produce the effects of an armed attack prompting the right to self-defense"[133].

In the National Research Council Committee Report from 2010 it is argued that when the UN Charter was drafted in 1945 the drafters hardly considered the devastating consequences of non-kinetic attacks, such as cyber-attacks, and that the drafters would have allowed for self-defense as a response against these measures, including measures such as cyber-attacks. The National Research Council Committee bases its argument on the purpose of Article 51, and states that the intent of the drafters of the UN Charter was to preclude premature forceful reactions by states, while still allowing states to react forcefully when the consequences had justified it. In continuance of this it can be argued that the fact that the drafters of the UN Charter failed to predict the change in scope and means of force would not, and should not, preclude the UN Charter and Article 51 to be applied on modern world issues.

This point of view is also indirectly supported by the Tribunal in the Nuremberg-Judgments where it was stated that law is not static, but always changing and adapting to the surrounding world, and treaties are therefore in many cases only an expression of laws which already exist[134]. This line of reasoning can also be applied analogically in relation to jus ad bellum and cyber-attacks, and can be used as an argument to support the right to self-defense when a state has been the victim of a cyber-attack.

The National Research Council further defines the phrase "armed" as the "causation, or risk thereof, or death of or injury to persons or damage or destruction to property and other tangible objects" , and states that the term "armed" clearly includes the use of kinetic military force[135]. When determining whether cyber-attacks can trigger the right to self-defense the Nationel Research Council Committee applies a consequence-based approach, which is to be understood as that the classification of armed attacks must be based on the effect of the attack, and not on the weapon employed[136][137].

This view also seems to be consistent with the Nuclear Weapons Advisory Opinion from 1996 by the ICJ, where it was established that Article 51 is not limited to specific weapons:

> *39.* "These provisions do not refer to specific weapons. They apply to any use of force, regardless of the weapons employed. The Charter neither expressly prohibits, nor per-

[132] (Remus, 2013), page 181
[133] Ibid, page 182 and (Sharp, 1999)
[134] (Judgement of the International Military Tribunal for the Trial of Major German War Criminals, 1946)
[135] (Committee on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, 2010), page 163
[136] (Waxman, 2011), Page 423
[137] (Committee on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, 2010), page 163

mits, the use of any specific weapon, including nuclear weapons. A weapon that is already unlawful per se, whether by treaty or custom, does not become lawful by reason of its being used for a legitimate purpose under the Charter."

40. "The entitlement to resort to self-defense under Article 51 is subject to certain constraints. Some of these constraints are inherent in the very concept of self-defense. Other requirements are specified in Article 51."[138]

The definition of armed attack is not limited to choice of weapons, but instead the effect of the attack, which is also supported by Yoram Dinstein[139]. According to him the statement of the ICJ in the Nuclear Weapons Advisory Opinion is to be understood so as the right to self-defense in Article 51 does not depend on the choice of weapons by the attacking party, but instead it depends on the end product of its delivery to a selected objective. Yoram Dinstein argues that the classification of an armed attack must rely on the damage the attack causes, and not the medium at hand, for example the use of cyber-attack vs. the use of an artillery battery. He concludes that the classification of an armed attack by cyber-measures must rely on whether there is a cause and effect chain between the cyber-attack and the violent consequences. Yoram Dinstein bases his conclusion on the amount of damage cyber-attacks can cause today, and compares it to the poisoning of wells which may give rise to severely grave results. He further states that a premeditated CNA can qualify as an armed attack just the same as a kinetic attack[140] so far as they resemble kinetic attacks and conventional military attacks[141].

In the Tallinn Manual the International Group of Experts unanimously concluded in accordance with the Nuclear Weapons Advisory Opinion that the choice of means of an attack is immaterial when qualifying if an attack can amount to an armed attack. The International Group of Experts further concluded that some cyber-operations may be sufficiently grave to amount to an armed attack and that this approach is in accordance with state practice. The International Group of Experts compares cyber-attacks to chemical, biological and radiological attacks which are universally accepted as weapons that in scale and effect can constitute an armed attack. Just as Yoram Dinstein makes clear the importance is not the type of weapon applied for the attack, but the scale and effect the attack causes[142][143].

Based on the abovementioned arguments, Yoram Dinstein concludes that espionage is an unfriendly act which cannot constitute an armed attack, since it in scale and effect does not cause the damage or the destruction which is needed to amount to an armed attack. He further determines that neither cyber-attacks, which does not cause human fatalities or large-scale damage or destruction to property, can be categorized as an armed attack. Cyber-attacks which does cause human fatalities or/and the destruction or large-scale damage to property will however constitute an armed attack which will give rise to self-defense. As examples of cyber-attacks which will constitute an armed attack, Yoram Dinstein mentions shutting down computers which control waterworks or dams, and

[138] (Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, 1996, International Court of Justice , 1996), para 39-40
[139] (Dinstein, War, Aggression and self-defence, 2011), page 212
[140] A kinetic attack is to be understood as the act of attacking a planetary surface with an inert projectile, where the destructive force comes from the kinetic energy of the projectile impacting at very high velocities.
[141] (Dinstein, Computer Network Attacks and Self-Defence, 2002), page 103
[142] See Chapter 3.2.1; Scale and effect
[143] (Schmitt, 2013), page 54-55

thereby generating floods in inhabited areas, or for example deadly crashes caused by deliberately engineering misinformation on aircraft computers. The clearest example of cyber-attacks which can constitute an armed attack is of course attacks on nuclear facilities instigating a core-meltdown of its nuclear reactor causing a nuclear explosion[144].

Once again, the Tallinn Manual agrees consistently with Yoram Dinstein. The International Group of Experts also reaches the conclusion that "acts of cyber intelligence gathering and cyber theft, as well as cyber operations that involve brief or periodic interruption of non-essential cyber services, do not qualify as armed attacks"[145]. The incidents where use of force leads to the death of human beings or destroys property would however in scale and effect constitute an armed attack, according to the International Group of Experts[146].

So far no cyber-attack has met the threshold of armed attack. The 2007-attack on Estonia was referred to as a cyber-war, but was not publicly referred to as an armed attack on Estonia. This assessment is supported by the International Group of Experts in the Tallinn Manual on the International Law Applicable to Cyber Warfare, where the Group argues that the attack on Estonia not in scale and effect can constitute an armed attack. The Stuxnet attack on the Iranian nuclear reactor in 2010 has however been viewed by some members of the International Expert Group as an armed attack, but since it has never been established who launched the attack self-defense is not an option[147]

3.3. Sub-Conclusion

There is no exhaustive list of what constitutes an armed attack and how grave the use of force must be in order to constitute an armed attack. Furthermore there will probably never be an exact definition of this. The interpretation of an armed attack versus the lesser grave forms of use of force will depend on an evaluation of the specific case, the circumstances of the case and probably also the motivation behind the use of force[148]. Especially the scope of the cyber-attacks is one the important reason for why a precise legal interpretation of the concept is so hard to make since the range of damage cyber-attacks can cause varies from small incidents to large-scale destruction.

The threshold of what constitutes an armed attack is set pretty high by the ICJ in previous case law. It would seem that the ICJ is trying to narrow the scope of what constitutes an armed attack, and that they furthermore are restricting the option for states to resort to self-defense, making sure that resorting to self-defense is not easy[149].

Whether a cyber-attack can be categorized as an armed attack will depend on the damage and effect they cause more than the type of weapon which has been launched. From a legal point of view there does not seem to be any reason for differentiating between damage caused by conventional military force and damage caused by cyber-means. Whether or not cyber-means against a state can be categorized as an armed attack must be assessed on the same grounds as a regular armed force acting on the behalf of a state and the key principle in separating armed attacks from mere use of force is the scale and effect of the attack.

[144] (Dinstein, Computer Network Attacks and Self-Defence, 2002), page 105
[145] (Schmitt, 2013), page 55
[146] (Schmitt, 2013), page 54-55
[147] (Schmitt, 2013), page 57
[148] (Case Concerning Military and Paramilitary Activities in and Against Nicaragua, 1986), para 231
[149] See Chapter 4.1; Response to a Cyber-Attack

Based on this examination it must be concluded that cyber-attacks can constitute an armed attack, which will allow a state to take forcible measures against its attackers in compliance with the rules and conditions contained in Article 51 and customary international law in the incidents where the cyber-attack either causes human fatalities, large-scale damage or destruction to property. The approach set forth by some academic writers who argues that Article 51 is to be interpreted literal therefore seems to be insufficient, in conflict with both the meaning of Article 51, and self-defense in customary international law.

Even though some cyber-attacks can constitute armed attacks if they in scale and effect amount to an armed attack, most of the cyber-attacks will not, simply because they will be viewed as insignificant.

As a result of the gap between Article 51 and Article 2 (4) a state, which has been the victim of use of force that does not constitute an armed attack is limited to non-forcible countermeasures or non-forceful actions unless the Security Council has given authorization to do so[150].

4. Cyber-Defense

A state, which has been the victim of an armed attack as established in the previous chapter, has the right to take forcible measures against the attacker[151][152]. The scope of the legality of the measures taken by a state acting in self-defense needs to be examined further in order to answer the research question regarding what legal right states has in response to a cyber-attack with military force and what the scope and limitations exists to this legal respond[153].

4.1. Response to a Cyber-Attack

In order for the use of force in self-defense to be considered legal, several conditions need to be met. Some of these conditions originate directly from the wording of Article 51:

1. The state acting in self-defense must have been the victim of an armed attack[154][155];
2. The victim state must have declared itself to have been so attacked, and[156][157];
3. It must have requested the assistance of the states which comes to its aid[158][159]

The first condition involves the delimitation and definition of what constitutes an armed attack, and has been the subject of a thorough examination in the previous chapter.

[150] (Committee on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, 2010), page 163
[151] Chapter **Fejl! Henvisningskilde ikke fundet.**. Armed Attack
[152] (Dinstein, War, Aggression and self-defence, 2011), page 188
[153] Chapter 1.2, problem statement
[154] Charter of the United Nations, Article 51
[155] (Case Concerning Military and Paramilitary Activities in and Against Nicaragua, 1986), para 195
[156] Charter of the United Nations, Article 51
[157] (Case Concerning Military and Paramilitary Activities in and Against Nicaragua, 1986), para 196
[158] Charter of the United Nations, Article 51
[159] (Case Concerning Military and Paramilitary Activities in and Against Nicaragua, 1986), para 195-199 and 232-233, and (Greig, 1991), page 369

The second condition involves the requirement to report to the Security Council and this condition will be examined further in the second chapter.

The third condition involves the right to collective self-defense and a victim state's right to ask for assistance and thereby also third party states' right to intervene when another state has been the victim of an armed attack.

Relevant case-law has also established that some non-treaty bases conditions exists when resorting to the use of force in response to an armed attack[160][161][162][163];

1. Necessity[164][165]
2. Proportionality of response[166][167]
3. Attribution[168][169]

The victim state must also prove that its counter-attack is a necessity to protect essential security interests and that the use of force is a proportionate response to the attack[170]. Finally the victim state must prove attribution to the state which they launch their counter-attacks against. An interpretation of these three conditions will also be part of a more thorough examination in the following chapter.

4.1.1. The Security Council and Self-Defense

Self-defense in accordance with Article 51 of the UN Charter contains a requirement to report to the Security Council. This condition is a two-phased rule which regulates a state's obligations to report its use of force when claiming to be acting in self-defense, whether individual or collective[171][172]. The first requirement is that measures taken in self-defense are only legal "until the Security Council has taken the measures necessary to maintain international peace and security"[173]. Secondly these measures taken in self-defense "shall be immediately reported to the Security Council"[174].

The first requirement regulates the duration of self-defense, and determines that self-defense is a temporary right. It is argued by Yoram Dinstein that the right to self-defense only exists until the Security Council has taken effective measures to prevent the state from further attacks and that the right to self-defense exists until the Security Council has "suc-

[160] (Case Concerning Military and Paramilitary Activities in and Against Nicaragua, 1986)
[161] (The Oil Platforms Case (Iran v. US), 2003)
[162] (Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), 2005)
[163] (Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, 2004)
[164] (The Oil Platforms Case (Iran v. US), 2003), para 76
[165] (Dinstein, Computer Network Attacks and Self-Defence, 2002), page 109
[166] (The Oil Platforms Case (Iran v. US), 2003), para 77
[167] (Dinstein, Computer Network Attacks and Self-Defence, 2002), page 109
[168] (The Oil Platforms Case (Iran v. US), 2003), para 61
[169] Ibid, para 72
[170] (Case Concerning Military and Paramilitary Activities in and Against Nicaragua, 1986) and (The Oil Platforms Case (Iran v. US), 2003)
[171] (Dinstein, War, Aggression and self-defence, 2011), page 234
[172] See Chapter 4.1.5; Collective Self-Defense
[173] Charter of the United Nations, Article 51
[174] Ibid

ceeded in restoring international peace and security[175]". This position seems to be in accordance with other academic writers[176] and it seems by far to be the most reasonable. The argument for this position is that Security Council measures should not paralyze a victim-state in the case that the Security Council measures prove to be inadequate to "maintain international peace and Security". It would seem that the purpose of the phrase must be to allow a state to protect itself until the Security Council has taken effective measures.

The second part of the rule leaves the question of whether or not a state loses the validity to take measures in self-defense if these measures are not reported to the Security Council. So is the rule mandatory or directory?

The question was processed in the Nicaragua Case where the majority of the ICJ determined that not reporting that a state has taken measures in self-defense by using force against its alleged attackers, may preclude the state's right to exercise self-defense if it fails to report to the Security Council[177][178]. Academic writers seem to understand this message, as non-reporting will be an indication of whether the state itself believes it in fact is acting in self-defense, but not as something which in itself can illegalize a victim-state's right to self-defense. It would seem that the requirement rule is a limitation of self-defense which is not necessarily to be taken lightly, but should not be understood as non-reporting being fatal for a states right to self-defense[179]. The ICJ´s message in the Nicaragua Case that not reporting may be a factor when determining whether the state itself actually believes it is acting in self-defense is one which also seems to be taken serious by states[180][181].

In the Congo Case the ICJ also noted that Uganda never claimed to have been the subject of an armed attack committed by the government of Congo and that Uganda had failed to report to the Security Council that it was acting in self-defense in accordance with Article 51[182]. The ICJ did not process the question any further, but the fact that they note Uganda's failure to report their actions should be understood as an indicator that Uganda did not act in legal self-defense and that this probably was a factor when determining the unlawfulness of Uganda's actions[183].

The Congo Case concerned the armed activities which took place on the territory of the Democratic Republic of the Congo between August 1998 and 2003 by Uganda. Uganda was found guilty in violating the prohibition on the use of force in international law as well as violating international human rights law and international humanitarian law.

The ICJ also stated in the Nicaragua Case that it is not a requirement to report to an international body in customary international law and thereby only a requirement in treaty law[184].

[175] (Dinstein, Computer Network Attacks and Self-Defence, 2002), page 114
[176] (M. Halberstam, 1996-1997)

[177] (Dinstein, Computer Network Attacks and Self-Defence, 2002), page 113
[178] (Case Concerning Military and Paramilitary Activities in and Against Nicaragua, 1986), para 200
[179] (Dinstein, War, Aggression and self-defence, 2011), page 239-241, (Gray, 2008), page 121-124 and (Greig, 1991)
[180] (Case Concerning Military and Paramilitary Activities in and Against Nicaragua, 1986), para 200
[181] (Gray, 2008), page 121
[182] (Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), 2005), para 145
[183] (Gray, 2008), page 122
[184] (Greig, 1991), page 369

The answer to the question of whether the condition that use of force in self-defense must be reported to the Security Council is mandatory seems to be no. But whether a state has reported to be acting in self-defense or not, has in several cases been a component in the evaluation of the legality of the actions and therefore not reporting will be part of the evaluation of the legality of the measures exercised in self-defense. It has also been concluded that the right to self-defense exists until the Security Council has taken effective measures to protect the state and thereby to secure international peace and security.

4.1.2. Necessity

The ICJ determined in the Nicaragua Case that the lawfulness of self-defense also depends on the necessity of the measures taken in self-defense[185]. The right to self-defense is a temporary right which means the state acting in self-defense only is allowed to use force as long as it is necessary to protect its security interests[186]. In the Nicaragua Case the ICJ determined that the United States waited too long to take actions and therefore their actions would still have been illegal, even if they had met the other criteria[187][188].

Necessity is usually interpreted as the requirement that no alternative response is possible[189]. There exists an obligation in the Charter of the United Nations to resolve disputes peacefully[190] and unlike the League of Nations solving disputes peacefully is not just a first resort, but also a last resort, since it does not ever become justified to use force to solve disputes. States must try and try again to resolve their disputes peacefully[191] and only when there are no other options can the state use force in self-defense[192][193]. This does however not mean that use of force is the only available response to an armed attack, but it merely requires that non-forcible means are insufficient to resolve the dispute[194].

It can be difficult to treat the concepts of necessity and proportionality completely separate from each other, since the two issues walks hand in hand. If the use of force in a specific case is not necessary it cannot be proportionate, and the other way around, the use of force can hardly be necessary if it is not proportionate.

Thus, however much the concepts of necessity and proportionality have been debated, it seems that academic writers do agree on the principle that self-defense must not be retaliatory or punitive, because the aim of self-defense always shall be to halt and repel an armed attack[195]. Both necessity and proportionality are not expressed directly in the UN Charter, but are part of customary international law. In order to create an overview of the

[185] (Case Concerning Military and Paramilitary Activities in and Against Nicaragua, 1986), para 195
[186] (The Oil Platforms Case (Iran v. US), 2003), para 23
[187] Ibid, para 237
[188] (Gray, 2008), page 151
[189] (Gray, 2008), page 150
[190] Charter of the United Nations, Article 2 (3)
[191] (General Assembly, 1970), Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, General Assembly Resolution 2625 (XXV), 1970
[192] (The Oil Platforms Case (Iran v. US), 2003), para 76
[193] (Dinstein, Computer Network Attacks and Self-Defence, 2002)
[194] (Schmitt, 2013), page 62
[195] (Gray, 2008), page 150

concepts and delimitation will be treated separately, and proportionality will therefore not be treated further in this chapter, but instead it will be examined further in the next chapter[196].

With reference to the Nicaragua Case the ICJ establishes in the Oil Platform Case that it is a condition for the legality of measures taken in self-defense that these measures are both proportionate and necessary. Importantly the ICJ also concluded in the Oil Platform Case that even if the United States had shown attribution to Iran and the attacks by Iran had been of a scale and effect which would amount to an armed attack, the use of force committed by the United States would still not have been legal self-defense. First of all because the United States had failed to show that the attacks on the oil platforms were necessary to protect essential security interests[197].

In the Congo Case the same approach was followed and the ICJ stated that there was no need for them to inquire into necessity, since the ICJ had already rejected Uganda´s claims of self-defense on other grounds. The ICJ did however note that "The Court cannot fail to observe the taking of airport and towns many hundreds of kilometers from Uganda´s border would not seem … necessary to that end"[198].

In the Wall Case the ICJ also determined, based on the evidence produced by Israel, that the construction of the security barrier did not seem necessary to attain its security objectives[199].

The Wall Case concerns the construction of a wall in the occupied Palestinian Territory built by Israel in and around East Jerusalem. The construction of the wall was initiated in 2002 by the Israeli Prime Minister at the time, Ariel Sharon, as a response to Palestinian suicide bombers and other terrorist attacks launched from Palestine against Israel. On December 8th 2003 the General Assembly requested the International Court of Justice for an advisory opinion on the following question:

> "What are the legal consequences arising from the construction of the wall being built by Israel, the occupying Power, in the Occupied Palestinian Territory, including in and around East Jerusalem, as described in the report of the Secretary-General, considering the rules and principles of international law, including the Fourth Geneva Convention of 1949, and relevant Security Council and General Assembly resolutions?"[200]

The ICJ answered the question and the key point of the case was that the wall was in contradiction with international law, among other reasons, because the construction of the wall did not seem necessary to attain its security objectives[201]. The ICJ´s opinion in this case is just an advisory opinion and therefore it is not binding.

[196] See Chapter 4.1.3; Proportionality
[197] Ibid, para 76
[198] (Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), 2005), para 147
[199] (Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, 2004), para 137
[200] (General Assembly, 2003), Resolution ES-10/14
[201] (Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, 2004), para 137

4.1.3. Proportionality

Proportionality is to be understood in the sense that the counterattack or the amount of force used is proportionate in relation to what is desired to accomplish, or proportionate in relation to the wrong-doing against a victim state (self-defense), when the use of counter-force has been deemed necessary[202]. Proportionality refers to the size, duration and target of the response[203].

In relation to targets it was stated in the Oil Platforms Case by the ICJ that the United States, who claimed to be acting in self-defense, had to prove that the attacked oil platforms were legitimate military targets relevant to an attack in self-defense[204]. Proportionality is, equally to necessity, a basic core of self-defense[205][206] and resembles necessity somewhat. The principles of necessity mentioned above are therefore also relevant factors to proportionality[207].

It will be quite hard to make a full assessment of the exact scope of proportionality, because the evaluation of whether or not a response is proportionate always will depend on the specific case[208][209]. The ICJ has however in different cases treated the question of proportionality.

In the Nicaragua Case it was concluded by the ICJ that the lawfulness of self-defense, among other considerations, depend on the proportionality of the measures taken in self-defense[210]. The ICJ states that the activities by the United States relating to the mining of the ports and the attacks on oil installations in Nicaragua could not be considered proportionate responses to the aid received by the Salvadoran opposition[211]. These considerations were however not necessary for the judgment by the ICJ, since it had already found the use of force by the United Nations to be illegal on other grounds, but the criteria of proportionality added to the wrongfulness done by the United States[212].

The ICJ also took the concept of proportionality into consideration in the Oil Platforms Case with reference to the Nicaragua Case, where it eternined that it is a condition for the legality of measures taken in self-defense that these measures are proportionate[213]. The ICJ discussed whether the action taken by the United States in response to the attacks on the Sea Isle City and the USS Samuel B. Roberts respectively, would have been legitimate if the United States had shown attribution and the attacks by Iran had been of the scale and effect, which would constitute an armed attack.

In the first incident regarding the Sea Isle City the ICJ found that the response might have been proportionate if it had been necessary. In the second incident regarding the case of

[202] (Schmitt, 2013), page 62-63
[203] (Gray, 2008), page 150
[204] (The Oil Platforms Case (Iran v. US), 2003), para 51
[205] (Gray, 2008), page 148
[206] (Dinstein, War, Aggression and self-defence, 2011), page 232-233
[207] Ibid, page 150
[208] (Dinstein, War, Aggression and self-defence, 2011), page 232-233
[209] (Gray, 2008), page 151
[210] (Case Concerning Military and Paramilitary Activities in and Against Nicaragua, 1986), para 195
[211] (Case Concerning Military and Paramilitary Activities in and Against Nicaragua, 1986), para 237
[212] (Gray, 2008), page 151
[213] (Gray, 2008), page 151

USS Samuel B. Roberts, which was part of a much more extensive operation, the scale of the response was not a proportionate response to the use of force[214]. The ICJ therefore concluded that the use of force committed by the United States still would not have been legal self-defense even if it had been necessary, because some of the attacks would not meet the criteria of proportionality[215].

In the Congo Case the same approach was followed and the ICJ stated that there was no need for them to inquire into necessity and proportionality, since the ICJ had already rejected Uganda´s claims of self-defense on other grounds. The ICJ did however note that "The Court cannot fail to observe the taking of airport and towns many hundreds of kilometers from Uganda´s border would not seem proportionate to the series of transborder attacks it claimed had given the rise to the right of self-defense…"[216]

4.1.4. Attribution

The ICJ established in the Oil Platforms Case that the burden of proof is on the state claiming to be victim of an armed attack[217]. This burden of proof also include proving attribution to the state which the victim-state has taken counter-measures against[218]. In the Oil Platforms Case the ICJ stated that because it was the United States who had violated the prohibition on use of force the burden of proof is on them to show their case[219]. In other words; the United States need to show, that it was Iran and not somebody else that attacked them.

In the first incident regarding the attack on the Sea Isle City the ICJ concluded that the United States had failed to prove that Iran was responsible for the attack and thereby failed to show attribution. The use of force by the United States was therefore not legal self-defense[220]. In the second case regarding the warship USS Samuel B. Roberts the ICJ also concluded that the United States had failed to show attribution to Iran and that the measures taken in self-defense therefore were illegal[221].

The ICJ noted in the Congo Case[222] that Uganda never claimed to have been the subject of an armed attack committed by the government of Congo and the ICJ did not find sufficient proof that the government of Congo was involved in these actions directly or indirectly. On

[214] (The Oil Platforms Case (Iran v. US), 2003), para 77-78
[215] Ibid, para 77
[216] (Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), 2005), para 147
[217] (The Oil Platforms Case (Iran v. US), 2003), para 51
[218] (Case Concerning Military and Paramilitary Activities in and Against Nicaragua, 1986), (The Oil Platforms Case (Iran v. US), 2003)
[219] (The Oil Platforms Case (Iran v. US), 2003), para 58
[220] Ibid, para 61
[221] Ibid, para 71
[222] The case concerned the armed activities which took place on the territory of Congo when Uganda according to Congo invaded Congo on August 2nd 1998, and occupied a third of Congo until April 2003 . Uganda claimed to be acting in self-defence to protect essential security interests, on the grounds that the territory of Congo was being used as a base and launching pad for attacks against Uganda, and that the government of Congo was not in effective control of the territory in question. Uganda further claimed that it had no intentions of overthrowing the government of Congo, and that its forces were to jointly operate with the Congolese army against the rebel forces .

these grounds the ICJ concluded that the circumstances to exercise the right to self-defense by Uganda against Congo were not present[223].

4.1.5. Collective Self-Defense

According to Article 51 "Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations…". Collective self-defense can be defined as a states right to defend itself from an armed attack with the assistance of two or more states[224]

Collective self-defense requires, just as individual self-defense, that a state has been the victim of an armed attack and the definition of armed attack is the same as in individual self-defense[225][226]. The same conditions that exist when claiming individual self-defense such as necessity, proportionality, reporting to the Security Council and attribution are also required when claiming collective self-defense. The ICJ further imposed two more conditions upon the right of collective self-defense in the Nicaragua Case, both of which are regarded as of great significance. First of all the victim state of the armed attack must have declared itself to have been so attacked. Secondly the victim must have requested the assistance of the State which comes to its aid. The ICJ argues that there are no rules in customary international law which make it legal for a third state to exercise the right of collective self-defense on behalf of the attacked state by its own assessment.[227]. In the present case the ICJ therefore decided that collective self-defense by the United States was not justified[228].

The natural-law doctrine takes the same position as the ICJ in the Nicaragua Case and is of the opinion that the right to self-defense belongs to the person or state which is the victim of the attack, which also means it is not possible for another state to defend the attacked on its behalf without the request of assistance by the attacked state[229].

It can on this basis be concluded that the right to self-defense can only be exercised when the victim-state specifically has requested the assistance of a third state. This approach is undoubtedly desirable, because it protects smaller states from unwanted outside intervention by requiring that the state in question itself asks for help. This approach makes it hard for states to intervene without consent, but does so without limiting states right to ask for assistance – all they need to do is ask.

4.1.5.1. Collective Security

The phrase "collective self-defense" in Article 51 of the UN Charter has given rise to the debate as to how military alliances, mutual assistance treaties and treaties of guarantee affect the right to collective self-defense in relations to the UN Charter[230]. However, it would seem clear that any such treaty, which would be in violation with Article 51 and the remaining part of the UN Charter, would therefore become void.

[223] (Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), 2005), para 146-147
[224] (Kelsen, 1950), page 792
[225] (Case Concerning Military and Paramilitary Activities in and Against Nicaragua, 1986), para 195
[226] (Dinstein, Computer Network Attacks and Self-Defence, 2002), page 109
[227] (Case Concerning Military and Paramilitary Activities in and Against Nicaragua, 1986), para 195-199 and 232-233
[228] (Judgment in the Case Concerning Military and Paramilitary in and Against Nicaragua (Nicaragua vs. the United States of America), 1986), para 2
[229] (Kelsen, 1950), page 792
[230] (Dinstein, War, Aggression and self-defence, 2011), page 282-293

According to Article 103 of the UN Charter the UN Charter has primacy over any conflicting charters and treaties. Article 103 of the UN Charter states:

> "In the event of a conflict between the obligations of the Members of the United Nations under the present Charter and their obligations under any other international agreement, their obligations under the present Charter shall prevail."[231]

This does not mean that treaties of assistance or military alliances necessarily are incompatible with the UN Charter and some of the treaties explicitly state that they are subordinate to the UN Charter, such as the North Atlantic Treaty Organization. Therefore, the UN Charter must govern the exercise of collective self-defense by the contracting parties of NATO[232]. Conclusively, this means that collective self-defense is a right and not a duty unless a state has entered into a mutual assistance treaty[233]. NATO´s defense agreement is probably the most prominent agreement on collective security and is a great example of a mutual assistance treaty that co-exists with the UN Charter. According to NATO an attack of one of the countries of the NATO is an attack on all the countries, and it has only been invoked once, which was after the terror attacks on 9/11[234]. Article 5 of the NATO treaty provides:

> "The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defense recognized by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area".

Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security"[235].

4.2. The Threat of Cyber-Attacks: Preemptive Self-Defense and Anticipatory Self-Defense

In today´s world you can kill thousands, or completely paralyze a country, by the press of a button. So do we need to prevent this before the action takes place, because it will be too late to react otherwise? Does this give us more power to prevent use of force in self-defense than it has done previously? In relation to cyber-attacks it is important to discuss if the scope of self-defense has changed, because the amount of damage you can do is so much more devastating than it was in 1945. This chapter will examine the question: how distant or close must the threat be before you can act?

[231] Charter of the United Nations, Article 103
[232] (Dinstein, War, Aggression and self-defence, 2011), page 292-293
[233] (Dinstein, Computer Network Attacks and Self-Defence, 2002), page 112-113
[234] (Greig, 1991), page 370
[235] The North Atlantic Treaty Organization, Article 5

The phrase "Nothing in the present Charter shall impair the inherent right of… self-defense.. if an armed attack occurs.." has created much debate in the academic world because it is a vague and unclear definition, which does not shed much light on what the phrase "inherent right" encompasses.

That the right to self-defense in international law is regulated by both treaty law and customary international law has already been determined by the ICJ in the Nicaragua Case with the ICJ stating that the UN Charter "by no means covers the whole area regulating the use of force in international law"[236][237]. This has created disagreement as to whether or not the interpretation of "inherent right" can pave the way for a wider interpretation of self-defense which includes preemptive self-defense and anticipatory self-defense[238]. It specifically leaves out the question if the phrasing "armed" limits self-defense in Article 51 to explicit cases where an armed attack has occurred, or if a state can take forcible measures before the attack occurs.

The discussion of preemptive self-defense and anticipatory self-defense is important in relations to cyber-attacks, because the question of the legality of these topics is crucial when establishing the scope of self-defense and a states right to take legal measures against its attackers.

The academic debaters have divided into two groups. The first group argues that a right to self-defense exists beyond Article 51 and that it thereby has a status as a "natural law"[239] that goes beyond the limitation in Article 51. The opposing group argues that self-defense is limited to Article 51 and needs to be interpreted narrowly meaning that self-defense only is legal when you have been the victim of an armed attack[240][241].

One of the prominent advocates for a wider interpretation of Article 51 is Hans Kelsen[242]. According to Hans Kelsen, self-defense in international law is regulated by both treaty law and customary international law[243][244] and is defined by the natural-law doctrine as the right of an individual or a state to defend itself, its property and its people against a real or imminent threat[245]. According to Hans Kelsen the right to self-defense is considered to have the status of jus cogens and is therefore viewed by him as a right so fundamental and essential that it cannot be changed or altered by treaty law. So the insertion of Article 51 was seen by Hans Kelsen as writing down a rule already in force and that self-defense is not limited to positive international law[246], but instead there exists a wider right to self-defense which goes beyond the right to respond to an armed attack in Article 51[247]. Hans Kelsen also argues that the reason for why the right to self-defense has not been mentioned or inserted into earlier treaties before the UN Charter, such as the League of Nations, was because it was considered to be a matter of course and therefore it had not seemed necessary to insert it[248].

---

[236] (Case Concerning Military and Paramilitary Activities in and Against Nicaragua, 1986), merits, para 176
[237] Ibid, para 193
[238] (Gray, 2008), page 115-116
[239] (Dinstein, War, Aggression and self-defence, 2011), page 191
[240] Ibid, page 187
[241] (Reisman, 2006), page 525
[242] http://www.denstoredanske.dk/Samfund,_jura_og_politik/Jura/Juridiske_biografier/Hans_Kelsen.
[243] (Case Concerning Military and Paramilitary Activities in and Against Nicaragua, 1986)
[244] (Kelsen, 1950), page 792
[245] Ibid, page 792
[246] (Kelsen, 1950), page 191
[247] (Gray, 2008), page 117
[248] (Kelsen, 1950), page 792

On the opposite side of the debate is Yoram Dinstein. He strongly disagrees that self-defense should be interpreted to a wider extent than what is contained in Article 51. Contrary to Hans Kelsen, he views the theory of self-defense as a natural law to be wrong and states that the legal right to self-defense should be limited to the framework of positive international law[249]. He believes that the legal basis for the right to self-defense should be found in the principle of states' sovereignty[250]. Dinstein describes sovereignty as being an ever-changing concept which needs to be interpreted in light of the modern world. Dinstein explains that sovereignty has already changed a lot if we look at what sovereignty meant in the 19th and 20th century compared to today. Those supporting a narrow interpretation of the right to self-defense argue that the right to self-defense is an exception to Article 2 (4) and that the meaning of Article 51 is that the right to self-defense only arises when you are a the victim of an armed attack in accordance with Article 51[251].

The issues regarding anticipatory self-defense and preemptive self-defense have also been debated by war theorists and they are much divided in the matter. Where Michael Walzer believes that the best defense is an offense and that a state has a duty to protect its people, others, like Fransisco de Vitoria, believe that "you cannot punish someone for an offence they have yet to commit" [252].

4.2.1. Anticipatory Self-Defense and Cyber-Attacks

Anticipatory self-defense is to be understood as the right to take forcible measures against a threat before the attack is actually launched[253] and while some legal theorists seem to believe that anticipatory self-defense was not in the contemplation of the drafters of the UN Charter, and thereby only legal when an attack has been launched[254], many (as stated above) seem to believe it is legitimate through customary international law[255][256].

The threshold for anticipatory self-defense is, according to the supporters of a wider interpretation of self-defense, that the threat of an attack is imminent[257]. Hans Kelsen argues that self-defense is legal if the threat is imminent or real[258]

The International Group of Experts in the Tallinn Manual has taken a similar view on anticipatory self-defense and argues that even though Article 51 does not explicitly allow for it, a state should not have to wait in the situations where an attack, which will amount to an armed attack, is imminent. The Group bases its position on the Caroline Doctrine[259] from the nineteenth century, and the Nuremberg Trials[260].

[249] (Dinstein, War, Aggression and self-defence, 2011), page 191
[250] Ibid, page 192
[251] (Gray, 2008), page 117
[252] (Stanford University, 2000)
[253] Notes from class: Use of force in International Law
[254] (Schmitt, 2013), page 64
[255] See Chapter 4.2; The Threat of Cyber-Attacks: Preemptive Self-Defense and Anticipatory Self-Defense
[256] (Reisman, 2006), page 526
[257] (Reisman, 2006), page 526
[258] (Kelsen, 1950), page 792
[259] (The Caroline Case, 1837)
[260] (Schmitt, 2013), page 63-66

This point of view is consistent with the United Nations High-Level Panel on Threats, Challenges and Change report from 2004, which states that a state can take forcible actions against a threat as long as the threat is imminent:

> "The language of this article is restrictive: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a member of the United Nations, until the Security Council has taken measures to maintain international peace and security". However, a threatened State, according to long established international law, can take military action as long as the threatened attack is imminent, no other means would deflect it and the action is proportionate. The problem arises where the threat in question is not imminent but still claimed to be real: for example the acquisition, with allegedly hostile intent, of nuclear weapons-making capability"[261].

The United Nations High-Level Panel on Threats, Challenges and Change from 2004 does not refer explicitly to Article 51, but to the report from the Secretary General from 2005; In Larger Freedom: Towards Development, Security and Human Rights for All does, and the report states that:

> "Imminent threats are fully covered by Article 51, which safeguards the inherent right of sovereign States to defend them against armed attack. Lawyers have long recognized that this covers an imminent attack as well as one that has already happened"[262].

4.2.2. Preemptive Self-Defense and Cyber-Attacks

Preemptive self-defense is different than anticipatory self-defense in the way that few can point to an imminent threat. Preemptive self-defense is the right to take forcible measures against incipient developments, which are not yet threatening or have fully materialized, but which could constitute an actual threat if they were permitted to mature[263].

Just as 9/11 has changed the face of war on terror and the right to act in self-defense against terrorist, it has also changed the view on preemptive self-defense[264]. Before the Bush-Doctrine very few states claimed wide rights of self-defense, but the United States has consistently argued over the past few years that it has the right to take preemptive measures in the name of self-defense[265]. The Bush Doctrine is a collection of strategy principles and practical policies, and used as guidelines for the United States foreign policy. The main elements of the Bush Doctrine are the right to preemptive self-defense and the promotion of democracy, and these have been drafted into the National Security Strategy document from 2002 and 2006[266]. According to the Bush Doctrine, the United States can act even before the threat fully materializes, thereby preserving the right to act even though it is not yet clear when or even if the event will occur, making preemptive self-defense somewhat more extreme than anticipatory self-defense.

---

[261] (United Nations Secretary General, 2004), United Nations High-Level Panel on Threats, Challenges and Change
[262] (United Nations Secretary General, 2005), In larger freedom: towards development, security and human rights for all, para 124
[263] (Reisman, 2006), page 526
[264] (Gray, 2008), page 165-166 and 208-222
[265] (Reisman, 2006), page 525 and 527-530
[266] (The Bush Doctrine Preemptive Strikes Against Threats To America's Security), direct link: http://www.thebushdoctrine.com/.

The Israeli raid on the Osirak reactor in Iraq in 1981 remains the clearest example of a preemptive use of force in the period following World War 2. The Israeli attack was condemned by the Security Council[267]. Israel bombed and destroyed a nuclear reactor in Baghdad, because they believed it was designed to make nuclear weapons to destroy Israel[268].

While the United Nations High-Level Panel on Threats, Challenges and Change seems to interpret Article 51 to include anticipatory self-defense, preemptive self-defense is not included[269]. According to the United Nations High-Level Panel on Threats, Challenges and Change extending the interpretation of Article 51 to also include self-defense against non-imminent or non-proximate threats would be to allow all acts in self-defense and explains[270]:

> "For those impatient with such a response, the answer must be that, in a world full of perceived potential threats, the risk to the global order and the norm of non-intervention on which it continues to be based is simply too great for the legality of unilateral preventive action, as distinct from collectively endorsed action, to be accepted. Allowing one to so act is to allow all".

The right to preemptive self-defense is highly debated and so far the ICJ has been reluctant to give its opinion on the subject. The ICJ has however in several cases, such as the Nicaragua Case, the Oil Platforms Case, the Wall Case and the Congo Case established that it is a condition for resorting to self-defense that a state has been the victim of illegal use of force, which in scale and effect reaches the threshold of an armed attack.

4.3. Sub-Conclusion

Based on the previous case-law it would seem that the ICJ is trying to narrow the scope of self-defense, by restricting the option for states to resort to self-defense by making sure that resorting to self-defense is not easy. This is done by laying down further principles which need to be met before a state can resort to forcible measures, besides the requirements of reporting to the Security Council which is already contained within Article 51, such as necessity, attribution and proportionality.

While some of these requirements for responding to an armed attack with forcible measures are relatively easy to apply on cyber-attacks, such as reporting to the Security Council, necessity and proportionality, the requirements of attribution will be specifically difficult to overcome. It can be very difficult to prove where the attack originated, let alone to prove that the state was the target of the attack. It can safely be concluded that the burden of proof is very strict[271] when establishing attribution and the state, which claims to be acting in self-defense ,must be prepared to satisfy the burden of proof. In relation to cyber-attacks this creates quite an issue, since it can be very difficult to lift this burden of proof when having been the victim of a cyber-attack. As it has already been shown in the examples of cyber-attacks in Chapter 2; Cyber-Attacks and the Inherent Right to Self-Defense that it can be very difficult to prove where the cyber-attack exactly came from. As previously stated highly sophisticated worms for example are almost impossible to trace and it is very difficult to prove what its target was. However, it would seem that this condition is

[267] (Reisman, 2006), page 537
[268] (BBC), direct link: http://news.bbc.co.uk/onthisday/hi/dates/stories/june/7/newsid_3014000/3014623.stm.
[269] (Reisman, 2006), page 532-533
[270] (United Nations Secretary General, 2004), The Secretary-General's High-level Panel Report on Threats, Challenges and Change, A more secure world: our shared responsibility
[271] (The Oil Platforms Case (Iran v. US), 2003)

consistent with the intentions of the ICJ to not let states resort to self-defense easily and to secure that a state is certain of the origin of the attack before using counter-force. This will prevent hasty counter-attacks, which later prove to have targeted an innocent state and, however challenging this condition proves to be in relation to cyber-attacks, it will still provide a high degree of protection from retaliatory and hasty counter-attacks, while at the same time it emphasizes the importance of the prohibition on use of force in international law.

In relation to cyber-attacks the legal authority states have to respond with forcible measures to cyber-threats also poses some interesting challenges. In relations to anticipatory self-defense it poses specific challenges, because it can be hard to determine when a threat is imminent or real, and it can be difficult to distinguish between preparatory actions and actions which constitute the initial phase of an armed attack. To clarify this, the Tallinn Manual uses the distinction between the insertion of a logic bomb[272] or the emplacement of remotely activated malware[273]. In the first incident the insertion will qualify as an imminent armed attack provided that the specified conditions for activating the bomb are likely to occur and the International Group of Experts states that the situation is analogue to the laying of naval mines. In the second incident on the other hand the threat becomes imminent when the initiator has decided to conduct an armed attack. This distinction between when the initiator is merely acquiring the capability to initiate an armed attack and when the initiator has actually decided to conduct an armed attack using the malware will, needless to say, be very difficult to make in practice[274]. While some legal theorists argue that anticipatory self-defense is legal after an attack has been launched but before it reaches its target (interceptive self-defense[275]). Others argue that it is already legal from the moment the threat becomes real and imminent[276]. The ICJ has never ruled on anticipatory self-defense and formalistically the ICJ has never given its opinion on the subject. The legality of anticipatory self-defense therefore remains uncertain, but however divided legal theorists seem to be regarding the subject, the majority of them seem to support this controversial right at least to some extent.

States are divided as to the legality of preemptive self-defense and even though preemptive self-defense can have some positive sides to it, such as preventing terrorist attack and thereby civilian casualties, it also has its downsides. North Korea and Iran has quickly adopted the concept of self-defense, which could ultimately cause them to attack the western world with the claim to be acting in self-defense. This development is of course highly unwanted. It has further been argued by Michael Reisman that preserving the right to preemptive self-defense undermines the entire international security system, because states simply will fit the language of preemption to their own national security strategies and thereby become free riders in the international legal system, e.g. as North-Korea has done[277]. On this basis it can be determined that preemptive self-defense according to international law is not recognized by the ICJ and such claims are clearly incompatible with recent verdicts[278], but the United States maintains the right to strike first against terrorism.[279].

---

[272] A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met, direct link: http://en.wikipedia.org/wiki/Logic_bomb.
[273] Malware, short for malicious software, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Opposite to a logic bomb the detonation of malware requires external command to launch the attack. Direct link: http://en.wikipedia.org/wiki/Malware.
[274] (Schmitt, 2013), page 65
[275] (Dinstein, War, Aggression and self-defence, 2011), page 203-205
[276] (Kelsen, 1950), page 792, and (Schmitt, 2013), page 63-66
[277] (Reisman, 2006), page 549
[278] (Reisman, 2006), page 548
[279] (Stanford University, 2000)

Regarding the possibility for a state to resort to cyber-measures as a response to an armed attack the answer will undoubtedly be that just as the categorization of armed attacks does not depend on the weapon employed, but the damage and effect it causes, similarly states will have the possibility to resort to cyber-means as a respond to a cyber-attack.

5. Cyber-Terrorism: The Conflict of Non-State Actors in International Law

In today´s world a terrorist group can launch an attack on states thousands of miles away and cyber-attacks can and will often be committed by either terrorist organizations or private persons operating from behind their computer screens. It is important to establish the legal framework for both the victim-state and the state from which the terrorist attack has been launched. For example to what extent the victim-state can use force within the territory of another state in the name of self-defense.

In the Wall Case it was established by the ICJ that Israel could not exercise the right to self-defense in Article 51, because the "attack" Israel was defending itself from came from within the territory of which Israel was in control[280]. This thesis focuses on cyber-attacks on international level, specifically the right to self-defense and cyber-attacks on national level will therefore not be part of this examination, since the right to self-defense in Article 51 focuses on trans-border actions[281]. When a cyber-attack originates from within the territory of the attacked state, and no foreign state is involved in the actions, this is a matter which should be regulated by national law[282], which can be found in the Convention on Cybercrime[283].

Before 9/11 the right to self-defense as a response to terror-attacks was controversial and many commentators argued that the right to self-defense in Article 51 was limited to armed attacks carried out by other states[284]. States then generally relied on the view taken by the ICJ in the Nicaragua Case[285], where the decision of whether the use of force by individuals could constitute an armed attack was based on the Definition of Aggressions, Article 3 (g)[286]:

> "Sending by or on the behalf of a state of armed bands, groups, irregulars of mercenaries, which carry out acts of armed force against another state of such gravity as to amount to an act of aggression"[287]

The ICJ determined in the Nicaragua Case that an armed attack includes the sending of regular forces across the borders of another state and also the sending of irregular forces if the scale and effect of the attack amount to that of an armed attack conducted by regular forces[288].

After the terror-attacks on World Trade Center on September 11th 2001 the legality of self-defense as a response to terror-attacks changed, with the United Nations Security Council passing Resolution 1368[289] and 1373[290], which explicitly allowed for self-defense as a response to the terror attacks. This

[280] (Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, 2004), para 139
[281] (Schmitt, 2013), page 54
[282] (Dinstein, Computer Network Attacks and Self-Defence, 2002), page 105
[283] (Council of Europe Treaty Office, 2001), Convention on Cybercrime
[284] (Dinstein, War, Aggression and self-defence, 2011), page 224-230
[285] (Case Concerning Military and Paramilitary Activities in and Against Nicaragua, 1986), para 195
[286] (Gray, 2008), page 193-202
[287] (General Assembly, 1974), Definition of Aggression, Article 3 (g)
[288] (Case Concerning Military and Paramilitary Activities in and Against Nicaragua, 1986), para 195
[289] (United Nations Security Council, 2001), Resolution 1368
[290] (United Nations Security Council, 2001), Resolution 1373

was the first time self-defense as a response to an armed attack was allowed and also the first and only time NATO invoked Article 5[291] of its treaty regarding collective security[292].

Yoram Dinstein divides the CNAs into four different categories of cyber-attacks originating from State A and directed against State B, which depend on whether they are unleashed by:

1) "individual computer hackers who are residents of State A, acting on their own initiative for whatever personal motive (benign or otherwise) without any linkage to the government of State A;
2) terrorists based in State A, acting on behalf of any chosen "cause" inimical to State B, unsupported by the government of State A;
3) terrorists overtly or covertly sponsored by the government State A; and
4) official organs-either military or civilian-of the government of State A"[293].

The first two issues concern the situation where hackers operate from one state, but where the actions taken by the states is on its own initiative and without any support or connection to the state from which the hackers operate. These hackers are non-state actors who operate within the territory from another state. The two last situations regard the incidents where the hackers act on the behalf of the state, or are official state organs. In relation to the examination of cyber-attacks launched by terrorists it will make sense to divide these four incidents into two groups: Non-state actors operating from within the territory of a another state without support by the state in question and non-state actors operating from within the territory of a another state that were directly or indirectly supported or/and sponsored by the state in question.

5.1. Non-State Actors operating with the Support from a State

The Definition of Aggression has determined that the "sending by or on the behalf of a state of armed bands, groups, irregulars of mercenaries, which carry out acts of armed force against another state of such gravity as to amount to an act of aggression[294]". The Declaration on Friendly Relations also determines that actions committed by irregulars or armed mercenaries can constitute as the threat or use of force if a state has been responsible for encouraging or organizing these armed bands[295].

The ICJ determined in the Nicaragua Case, which is consistent with the Definition of Aggression, that an armed attack includes the sending of regular forces across the borders of another state and also the sending of irregular forces if the scale and effect of the attack amount to that of an armed attack conducted by regular forces[296].

In the Congo Case in 2005 the ICJ once again applied the Definition of Aggression when determining if the measures taken by Uganda could constitute self-defense. The ICJ concluded that there was no satisfactory evidence that the contended attacks committed by irregulars against Uganda

[291] North Atlantic Treaty Organization, Article 5
[292] For a further definition of Collective Security see Chapter 4.1.5 regarding Collective Self-Defence
[293] (Dinstein, Computer Network Attacks and Self-Defence, 2002), page 103
[294] (General Assembly, 1974), Definition of Aggression, Article 3 (g)
[295] (General Assembly, 1987), : Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations, General Assembly Resolution 42/22, 1987
[296] (Case Concerning Military and Paramilitary Activities in and Against Nicaragua, 1986), para 195

had been sent by the government of Congo or had been acting on behalf of Congo within the sense of Article 3 (g) of the Definition of Aggression[297][298].

It has also been established in the International Law Commission's Articles on State Responsibility that "the conduct of any State organ shall be considered an act of that State under international law, whether the organ exercises legislative, executive, judicial or any other functions, whatever position it holds in the organization of the State, and whatever its character as an organ of the central Government or of a territorial unit of the State"[299]. The International Law Commission further defines state organs as "any person or entity which has that status in accordance with the internal law of the State"[300].

Furthermore the International Law Commission defines that the state responsibility extends to conduct by persons or entities which are not organs of the state under article 4, but which are empowered by the law of that State to exercise elements of the governmental authority. Same as state organs in Article 4 this conduct shall be considered an act of the state under international law, provided the persons or entities are acting in that capacity in the particular instance[301]. This responsibility also extends to a person or group of persons acting on the instructions of the state, under the direction of the state or control of the state in question[302].

The International Law Commission places quite a large amount of responsibility on states and this means that a state is fully responsible for the actions committed by state organs, persons or entities empowered by the state even when the actions of these state organs, persons or entities exceed their authority or contravenes instructions[303]. That intention seems to be irrelevant as qualifying armed attacks is also supported by the International Group of Experts in the Tallinn Manual on the International Law Applicable to Cyber Warfare from 2013. This also includes attacks committed directly by the state in question, but where the damage the attack causes is not intended. What matters is not the intention and motivation behind the attack, but only the scale and effect of the attack[304].

5.2. Non-State Actors Operating from the Territory of a Another State without Support from the State in Question

This is a significant issue, because the victim state's right to defend itself will collide with the other state's right of sovereignty, territorial integrity and political independence, which also are fundamental principles of the United Nations[305]. The concept of sovereignty covers a state's right to self-determination and the definition of sovereignty is implied in Article 2 (4) which concerns the prohibition on the use of force. According to the Charter of the United Nations sovereignty is described as territorial integrity and political independence. Furthermore, intervention is strictly restricted in Article 2 (7) of the Charter. The concept of sovereignty dates back several centuries

[297] (Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), 2005), para 146-147
[298] (General Assembly, 1974), Definition of Aggression, Article 3 (g)
[299] (The International Law Commission, 2001), International Law Commission's Articles on State Responsibility on groups of State and non-State actors, whose conduct can be attributed to a State, Article 4 (1)
[300] Ibid, Article 4 (2)
[301] (The International Law Commission, 2001), International Law Commission's Articles on State Responsibility on groups of State and non-State actors, whose conduct can be attributed to a State, Article 4 (2)
[302] Ibid, Article 8
[303] Ibid, Article 7
[304] (Schmitt, 2013), page 57
[305] Charter of the United Nations Article 2 (1)

well before the first attempt to create nation-states in 1648 in Westphalia[306]. Sovereignty has been debated by philosophers ranging from Socrates to Luther, Hobbes and Machiavelli, and was originally meant as a reference to order within a state. Today it is defined in modernity as states supreme authority above all external laws[307]. Ernst Kantorowicz[308] describes the core meaning of sovereignty very well as "supreme authority within a territory" in *The King´s Two Bodies* from 1957[309].

Yoram Dinstein argues that the lack of effectiveness or permission by the state within which the terror group operates should not shield the group for reprisals. It was established in the Caroline Case[310] from 1837 that a state may use counter-force within the territory of another state when targeting armed bands if the state, in whose territory the actions arise from, remains ineffective. This sort of self-defense has been referred to as "extra-territorial law enforcement" or "state of necessity" [311].

The majority of the International Group of Experts in the Tallinn Manual on the International Law Applicable to Cyber Warfare seems to agree on this point view and just like Yoram Dinstein the Group reaches the conclusion that self-defense against a cyber-attack is permissible within the territory of the state when the territorial state is unable to repress the relevant elements of the cyber-attacks. "Unable" is understood by the International Group of Experts as the state lacking the expertise or technology to repress the hostilities, but also the unwillingness by the territorial state to take effective actions will allow the attacked state to take actions[312]. Contrary, the minority of the International Group of Experts argued that cross-border self-defense without the consent of the territory state, or Security Council authorization is impermissible, but that other responses to a cyber-attack, such as actions based on the plea of necessity, might be permissible[313].

The question of whether a state can violate the prohibition on the use of force and non-intervention by tolerating and accepting that rebel groups operate from their territory was examined in the Congo-Case. Uganda claimed a wider interpretation of the non-use of force and non-intervention to also extend to a duty of vigilance to ensure that such activities did not take place. However, Uganda failed to prove the absence of action by Congo on the grounds that Congo at first had not been capable to stop the rebels operating from its territory and afterwards actually had taken clear action[314]. This judgment is important for two reasons. First of all because the ICJ determined that a state´s inability or ineffectiveness for taking action against rebels operating from its territory do not make the state in question responsible for non-intervention[315] and secondly because it establishes that states have an obligation to secure that its territory is not knowingly being used for acts contrary to the rights of other states.

This claim is in accordance with the decision in the Corfu Channel Case where it was determined that states have an obligation to secure that its territory is not knowingly being used for acts con-

[306] The Peace of Westphalia, 1648 consists of two peace-treaties signed on October 24th 1648 by diplomats in Münster and Osnabrück, which ended the Thirty Years War that lasted from 1618-1648
[307] (Dhanapala, 2007)
[308] German historian of medieval political and intellectual history and art,
[309] (Stanford University, 2003)
[310] (The Caroline Case, 1837), Direct link: http://avalon.law.yale.edu/19th_century/br-1842d.asp.
[311] (Dinstein, Computer Network Attacks and Self-Defence, 2002), page 108
[312] (Schmitt, 2013), page 60-61
[313] (Schmitt, 2013), page 61
[314] (Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), 2005), para 302-303
[315] (Gray, 2008), page 80

trary to the rights of other states[316]. The ICJ concludes that the provisions in the Declaration on Friendly Relations are declaratory of customary international law, and thereby accepts a duty of vigilance[317].

The International Group of Experts who supports cross-border self-defense further determined that certain requirements must be met when resorting to cross-border self-defense. First of all the victim-state must have demanded that the territorial state put an end to the hostilities taking place from within its territory. Secondly the victim-state must afford the territorial state an opportunity to address the situation. These requirements are procedural safeguards against premature or mistaken conclusions as to the unwillingness or inability of the territorial state to take actions against the hostilities. Furthermore, these requirements derive from the international law obligations to respect states' sovereignty. The International Group of Experts also takes into account that some situations may occur where immediate action is necessary[318].

5.3. Sub-Conclusion

It can on this basis be concluded that actions committed by irregulars who act on behalf of a state, or has been sent by a state, can trigger the inherent right to self-defense in international law against the state who supports or orders the attack by the non-state actors.

In relation to self-defense as a response to cyber-terrorism this means that hackers sponsored by a state may be deemed de facto organs of that state and the state in question thereby becomes fully liable for these actions. This results in releasing the inherent right to self-defense in accordance with Article 51, provided that the actions in scale and effect amount to that of an armed attack[319]. A state, which has been the victim of an attack committed by non-state actors, where a state is liable for these actions as determined above, can therefore take forcible measures in self-defense against that state. It can direct its self-defense measures directly against the state which is responsible.

In the commentaries made by the International Law Commission it is stated that state responsibility requires attribution, which is in accordance with previous case law. It needs to be shown that a link, or relation, exists between the state and the group or person in question and according to previous case-law this threshold is set relatively high[320]. In order for a state's countermeasures to be legal self-defense, the victim-state will also need to meet the other requirements for responding in self-defense established in this thesis, such as necessity, proportionality and reporting that it is acting in self-defense to the Security Council.

It can furthermore be concluded that it usually calls for coercive actions by the state from where a terrorist group operates, when non-state actors operate from within the territory of the state in question and from there launches attacks on another state[321]. The goal of the state should be to terminate the hostile activities taking place within its territory and this point of view has been established by the ICJ in several cases.

When the state from which the terror cell is operating fails to take effective measures to terminate these hostile activities it creates the issue of if the attacked state can take actions. It has al-

[316] (Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), 2005), para 160-165
[317] Ibid, para 162
[318] (Schmitt, 2013), page 60-61
[319] (Dinstein, Computer Network Attacks and Self-Defence, 2002), page 104
[320] (Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), 2005)
[321] (Dinstein, Computer Network Attacks and Self-Defence, 2002), page 103

ready been determined by the ICJ in the Congo Case that failing to take effective measures against terror cells does not make a state responsible for the actions. However, in the previous examination, it must seem reasonable that the lack of effectiveness by the state, from which the terror group operates within, should not shield the group for reprisals.

So even though the territorial state is not responsible for the hostilities taking place, a victim-state will be allowed to take forcible measures against the terror group operating within the borders of the territorial state even though it will collide with that state's sovereignty. This view seems to be consistent with previous case law, legal literature and international law. This violation of the territorial state's sovereignty will require that certain conditions have been met. First of all the victim-state must have demanded that the territorial state put an end to the hostilities taking place from within its territory and, secondly, the victim-state must afford the territorial state an opportunity to address the situation.

6. Conclusion

The main objective of this thesis was to examine to what extent existing international law is adequate to regulate the issues of cyber-attacks. The outcome of this examination is that the fundamental principles of Article 51 are sufficient to meet the new challenges which cyber-attacks pose. This is to be understood as the fact that the current legislation regarding self-defense is fully equipped to handle the complex of problems in relation to cyber-attacks and that the answer to the above raised question can be found within Article 51 and customary international law.

Specifically, the thesis encompassed an examination of what kind of international legal authority states have to respond with in relation to forcible measures to cyber-attacks or cyber-threats by states or non-state actors.

Based on this examination it must be concluded that cyber-attacks can constitute an armed attack, which will allow a state to take forcible measures against its attackers in compliance with the rules and conditions contained in Article 51 and customary international law in the incidents where the cyber-attack either causes human fatalities or large-scale damage or destruction to property.

Cyber-espionage does on these grounds, not in scale and effect, constitute an armed attack, regardless of the illegality of espionage in international law. Cyber-attacks that cause damage without human casualties or severe property damage, similarly does not amount to an armed attack and do not trigger the right to self-defense. Cyber-attacks with human casualties and/or severe property damage can constitute an armed attack in accordance with Article 51 and thereby allow states that have been the victim of such an attack to use force in self-defense. However, it is important to note that it will be very difficult for the victim state to lift the burden of proof regarding attribution.

The legality of anticipatory self-defense remains uncertain, but the majority of legal theorists and reports seem to support this controversial right at least to some extent. Additionally, on the basis of this examination, it can be concluded that preemptive self-defense according to international law is not recognized and such claims are clearly incompatible with recent verdicts by the ICJ.

It can also be concluded that cyber-terrorism committed by non-state actors who act on behalf of a state, or has been sent by a state, can trigger the inherent right to self-defense in international law against the state who supports or orders the attack by the non-state actors. A victim-state will also be allowed to take forcible measures against the terror group operating within the borders of the territo-

rial state even though the territorial state is not responsible for the attacks, if the territorial state fails to take effective measures to end the hostilities taking place from its territory.

7. Bibliography

Treaties

Charter of the United Nations

The Covenant of the League of Nations (June 28,
1919) The Versailles Treaty, 1919
General Treaty for the Renunciation of War (Kellogg-Briand Pact), Aug. 27, 1928

Charter of the International Military Tribunal

North Atlantic Treaty Organization

Rome Statute of the International Criminal Court

Books

Aquinas, T. (u.d.). Summa Theologica. Summa Theologica. Thomas Aquinas.

Dinstein, Y. (2011). War, Aggression and self-defence. Cambridge University Press. Evald, J. (2007). At tænkte juridisk. nyt juridisk forlag.

Gray, C. (2008). International Law and the Use of Force. Oxford University Press.

Gross, L. (u.d.). The Peace of Westphalia, 1648-1948. American Journal of International Law. Henig, R. B. (1973). The League of Nations. Edinburgh: Oliver & Boyd.

Kelsen, H. (1950). The Law of the Unite Nations. London: Stevens & Sons Limited. Lacey, W. M. (2009). The Making of Peace. Cambridge University Press.

Lepard, B. D. (2010). Customary International Law, A New Theory with Practical Applications. Cambridge University Press.

Sten Schaumburg-Müller & Jens Evald. (2004). Retsfilosofi, Retsvidenskab & Retskildelære. Jurist- og Økonomforbundets Forlag.

Articles

Dhanapala, J. (7. April 2007). GLOBALIZATION AND THE NATION STATE. The Colorado Journal of International Environmental Law and Policy, s. 1-8.

Dinstein, Y. (2002). Computer Network Attacks and Self-Defence. International Law Studies.

Greig, D. W. (April 1991). Self-Defence and the Security Council: What Does Article 51 Require? The International and Comparative Law Quarterly, s. 366-402.

M. Halberstam. (1996-1997). The right to self-defense once the security council takes action. Michigan Journal of International Law.

Reisman, W. M. (1. January 2006). The Past and Future of the Claim of Preemptive Self-Defense. THE AMERICAN JOURNAL OF INTERNATIONAL LAW.

Remus, T. (2013). Cyber-attacks and International law of armed conflicts; a "jus ad bellum" perspective. Journal of International Commercial Law and Technology Vol. 8, No.3 (2013).

Schmitt, M. N. (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press.

Sharp, W. G. (1999). Cyberspace and the use of force. Falls Church.

Simma, B. (1999). NATO, the UN and the Use of Force: Legal Aspects. European Journal of International Law, s. 1-22.

Waxman, M. C. (16. March 2011). Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4). Yale Journal of International Law.

Case Law

Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, 1996, International Court of Justice , p. 226 (International Court of Justice 8. July 1996).

Application Instituting Proceedings for the Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua vs. the United States of America) (International Court of Jutice April. 9 1984).

Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda) (International Court of Justice 19. December 2005).

Case Concerning Military and Paramilitary Activities in and Against Nicaragua (International Court of Justice 27. June 1986). The Caroline Case (1837).

Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, (International court of Justice 9. July 2004).

The Oil Platforms Case (Iran v. US), 161 (International Court of Justice 6. November 2003).

Judgement of the International Military Tribunal for the Trial of Major German War Criminals, Nuremberg Trial Proceedings Vol. 1, Indictment, Appendix C (International Military Tribunal for the Trial of Major German War Criminals 30. September 1946).

Judgment in the Case Concerning Military and Paramilitary in and Against Nicaragua (Nicaragua vs. the United States of America) (International Court of Justice 27. June 1986).

Judgment of the International Military Tribunal for the Trial of German Major War Criminals (Nuremberg Judgment) (International Military Tribunal for the Trial of German Major War Criminals 30. September 1946).

Resolutions

General Assembly. (1970). Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations. Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations. United Nations.

General Assembly. (1974). United Nations General Assembly Resolution 3314 (XXIX). Definition of Aggression. United Nations General Assembly Resolution 3314 (XXIX). Definition of Aggression. United Nations.

General Assembly. (1987). : Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations, General Assembly Resolution 42/22, 1987. : Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations, General Assembly Resolution 42/22, 1987. United Nations.

General Assembly. (2003, December 8). General Assembly resolution ES-10/14. United Nations General Assembly. (2005). World Summit Outcome. United Nations.

United Nations Secretary General. (2004). The Secretary-General's High-level Panel Report on Threats, Challenges and Change, A more secure world: our shared responsibility. United Nations.

United Nations Secretary General. (2005). In larger freedom: towards development, security and human rights for all. United Nations General Assembly.

United Nations Security Council. (2001). Resolution 1373. United Nations Security Council. United Nations Security Council. (2001). Security Council Resolution 1368. United Nations.

Reports

Committee on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy. (2010). Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy. National Research Committee.

Council of Europe Treaty Office. (2001). Convention on Cybercrime, CETS No.: 185. Council of Europe Treaty Office.

Council on Foreign Relations. (12. June 2013). The Dilemma of Humanitarian Intervention. Hentet fra Council on Foreign Relations: http://www.cfr.org/humanitarian-intervention/dilemma-humanitarian-intervention/p16524?cid=rss-fullfeed-the_dilemma_of_humanitarian_in-061213

National Research Council. (2010). Letter Report on the Committee on Deterring Cyber-Attacks: Informing Strategies and Developing Options for U.S. Policy. The National Academic Press.

The International Law Commission. (2001). The International Law Commission's Articles on State Responsibility on groups of State and non-State actors, whose conduct can be attributed to a State. The International Law Commission.

United States Military Doctrine. (2012). Information Operations, Joint Publication 3-13.

Websites

BBC. (u.d.). 1981: Israel bombs Baghdad nuclear reactor. Hentet fra www.news.bbc.uk.: http://news.bbc.co.uk/onthisday/hi/dates/stories/june/7/newsid_3014000/3014623.stm

Princeton. (u.d.). www.princeton.edu. Hentet fra www.princeton.edu: http://www.princeton.edu/~achaney/tmve/wiki100k/docs/Kellogg-Briand_Pact.html

Sanger, D. E. (25. September 2010). www.nytimes.com. Hentet fra Iran Fights Malware Attacking Computers: http://www.nytimes.com/2010/09/26/world/middleeast/26iran.html?_r=0

Stanford University. (4. February 2000). "Just War Theory". Hentet fra Stanford Enclyclopedia of Philosophy: http://plato.stanford.edu/entries/war/#2

Stanford University. (31. May 2003). Stanford Enclyclopedya of Philosophy. Hentet fra Stanford Enclyclopedya of Philosophy: http://plato.stanford.edu/entries/sovereignty/

The Bush Doctrine Preemptive Strikes Against Threats To America's Security. (u.d.). Hentet fra http://www.thebushdoctrine.com/

Morozov, E. (17. April 2009). www.newseek.com. Hentet fra Newsweek: http://www.newsweek.com/nato- hammers-out-strategy-cyberattack-77499

The White House. (2002). The National Security Strategy of the United States of America. Washingtoon: The White House.

The White House. (u.d.). www.whitehouse.gov. Hentet fra Cyber-Security: http://www.whitehouse.gov/issues/foreign-policy/cybersecurity

U.S Department of State. (u.d.). Office of the Historian. Hentet fra www.history.state.gov: http://history.state.gov/milestones/1921-1936/kellogg

Other

Kellogg, F. B. (15. March 1928). Special Supplement to Foreign Affairs, vol. 6, no. 3. Kellogg speech of March 15, 1928 before the Council on Foreign Affairs. Special Supplement to Foreign Affairs, vol. 6, no. 3. Kellogg speech of March 15, 1928 before the Council on Foreign Affairs. Council on Foreign Affairs.

World Affairs. (u.d.). Hentet fra http://affairs1490.rssing.com/chan-26037939/all_p1.html