Department of Law at the Gothenburg University
Master of Laws Programme
Master thesis, 30 ECTS
Semester/Fall 2012

Cyber Warfare and the Concept of Armed Attack

Ebba Josefson

UNIVERSITY OF GOTHENBURG
SCHOOL OF BUSINESS, ECONOMICS AND LAW

Supervisor: Andreas Moberg
Examiner: Sara Stendahl

Special thanks to:

Maitre Ardavan Amir-Aslani – my employer in Paris 2012 who introduced me to this subject,

Andreas Moberg – my supervisor who patiently spent surprisingly many hours discussing international law with me,

Madelene Robinson-Geere and Alexandra Sterner – my friends who helped me refine this paper with wise comments and

Simon Lindqvist – my boyfriend who did not disturb me too much when I needed to work.

Table of contents

Preface

In 2010 a computer worm - Stuxnet - spread over the Internet and hence became known to the public. Until this day it is kept secret who is the author of Stuxnet and rumours are widespread. It is believed to have been created by the United States of America (hereinafter the U.S.) and Israel. Stuxnet is said to be part of an intelligence operation called Olympic games – an intelligence operation run by the American government. The Olympic games started during the Bush administration and was continued by the Obama administration.[1]

It is believed that the worm was originally planted in the computer network of the Iranian nuclear enrichment facilities, the Natanz plant, to slow down Iranian nuclear enrichment.[2] A slowdown desired by the U.S. to hinder Iran from developing nuclear weapons. After a programming error a member of staff brought the worm out of the system of the power plant and the worm was spread over the Internet.[3]

Stuxnet is interesting for a number of reasons. It is subject to rumour spreading as no one has, so far, accepted responsibility for being the author of the worm. No one has, so far, accepted responsibility for planting the worm in the Iranian nuclear network system. Stuxnet might be an example of a weapon in a new kind of warfare - cyber warfare. As previously stated, the information on Stuxnet is based on rumours and the public might never learn the full truth about Stuxnet but for me it will serve as a good hypothetical example for analysing international law on cyber warfare.

[1] Obama Order Sped Up Wave of Cyberattacks Against Iran, Sanger, The New York Times, June 1, 2012.
[2] Cyber Warfare and the Laws of War, Harrison Dinniss, pp 291-292 and Stuxnet virus: worm 'could be aimed at high-profile Iranian targets', Beaumont, The Telegraph, September 23, 2010.
[3] Obama Order Sped Up Wave of Cyberattacks Against Iran, Sanger, The New York Times, June 1, 2012.

1 Introduction

1.1 Aim

The growing number of states increasing their capabilities of using computer network attacks[4] as means of attacking another state[5] has made me believe that there is a growing need of a discussion on how to handle the use of computer network attacks between states in international law. Therefore the aim of this paper is to discuss questions such as – whether or not computer network attacks directed from one state to another can be comparable to the concept of "armed attack" in the Charter of the United Nations and customary international law. Why would it be desirable or worthwhile to include computer network attacks under the concept of "armed attack"? What would be the potential consequences of doing so? Can existing international law handle development of new technology and can it regulate new types of warfare and weapons such as computer network attacks?

I will focus on two concepts, namely, the "use of force" and "armed attack" in the Charter of the United Nations and customary international law. The concepts are closely related, which makes it hard to discuss one without the other. The main aim will be to discuss the relation between "armed attack" and "computer network attacks" and this because of the right to self-defence that follows with a recognized armed attack.[6] However, to discuss the meaning of an armed attack without discussing the concept of use of force seems meaningless to me since they are very closely interconnected.

In order to analyse if international law, generally regulating the use of force and armed attack, can be applicable to computer network attacks it will be necessary to discuss *why* the UN Charter and customary international law are relevant as laws

[4] Will be defined below.
[5] For further reading see for example World Wide Warfare - Jus ad bellum and the Use of Cyber Force, Roscini and Cyber Warfare and the Laws of War, Harrison Dinniss.
[6] For further reading on if a computer network attack can constitute use of force, see: Computer Network Attack and the Use of Force in International Law, Schmitt and The Law of Information Conflict, Wingfield and Tallinn Manual.

regulating resort to force – *jus ad bellum.*[7] It is also necessary to analyse the argumentation regarding the questions *why* it can or cannot be possible to apply general international law on the use of force and armed attack to computer network attacks.

The main questions of this paper will be:

1. What are the international treaty and customary law concepts of "use of force" and "armed attack" generally considered to comprise and why are these concepts relevant in a discussion on the development of international law governing resort to force?

2. What are the arguments in favour of or against applicability of the concept of "armed attack" in the Charter of the United Nations or customary international law to computer network attacks?

1.2 Scope and limitations

The main focus of this paper will be to discuss the argumentation on applicability of existing international regulation to computer network attacks. I will limit my analysis to the concepts of use of force and armed attack which are concepts found in the Charter of the United Nations and customary international law. International law covers a wide spectrum of regulations but due to the limited frames of this paper I have decided to limit my analysis to the most relevant laws governing resort to force, namely, the Charter of the United Nations and customary international law. To further narrow my analysis I will mainly concentrate on the concepts of "use of force" and "armed attack". Armed attack because of its inherent right to self-defence and the use of force because it is a fundamental principle of international law, to not use force against another state, therefore the need to discuss what these concepts comprise. Since the *threat* to use force normally is lawful if the *use* of the same kind of force would be lawful, I will not consider the extension of "threat" in any further aspect

[7] Law governing the resort to force between states.

than necessary for the understanding of this paper.[8] Neither will kinetic[9] attacks on cyber command centrals be included in the concept of computer network attacks.

This paper will focus on computer network attacks in *jus ad bellum* and not consider *jus in bello.*[10] The reason for this limitation is the limited frames of this paper and that my interest first fell on the perspective of jus ad bellum. Computer network attacks in jus in bello is an interesting subject in development that could be suitable for further research.[11]

Even though article 39 of the Charter, regulating the Security Council's right or duty to determine the existence of a threat to the peace or an act of aggression, is also closely related to article 2(4) and the prohibition of use of force and article 51 regarding armed attack, article 39 will only be considered when necessary in relation to 2(4) and 51. This because the aim of this paper is to discuss, among other things, when the right to act in self-defence for states comes about and not specifically the right to take measures for the Security Council. Neither will I in this paper specifically consider the aspects of "non-intervention" and lawful "counter-measures" in response to intervention. Consideration of these questions and aspects will only be taken when necessary for the understanding of the discussion of an armed attack and the use of force. To include both the Security Council's right to act and the concept of non-intervention more than serving as comparison in the analysis would be too comprehensive.

The main focus of this paper is computer network attacks carried out between *states*. I will therefore not to any greater extent consider, for example the War on Terror where non-governmental groups are authors of attacks, but foremost consider attacks attributable to states. Neither will I consider computer network attacks from or between individuals or entities for private gain, commonly called cyber criminality, more than to give examples of computer network attacks as such. Cyber criminality is

[8] Tallinn Manual, Chapter II, Section 1, Rule 12, para 3.
[9] "Involving or producing movement" – Cambridge Dictionaries Online or "producing or causing motion" – Oxford English Dictionary. For example the motion caused by the explosion of a bomb.
[10] The law of armed conflict or International Humanitarian law.
[11] For further reading on computer network attacks and jus in bello see for example: Tallinn Manual and Cyber Operations and the Jus in Bello, Schmitt.

an increasing problem for both private and public actors and is an interesting subject of its own. However due to the limits of this paper I need to keep cyber criminality almost fully outside the frames of this paper.[12]

Cyber operations are normally divided into three types: CNA (Computer Network Attack), CNE (Computer Network Exploitation) and CND (Computer Network Defence). Computer network attacks aim at " … disrupt, deny, degrade, or destroy … "[13] information in computers or computer networks while computer network exploitation aims at intelligence collection and gathering data. Computer network defence is prevention of the former two, for example through cyber operations or law enforcement.[14] I will concentrate on computer network attacks because computer network exploitation is mainly used for cyber espionage and similar activities and therefore considered as cyber criminality. Computer network defence will only be referred to in relation to the right to self-defence that follows with an armed attack. Hereinafter all sorts of cyber operations that are relevant for this paper to discuss will be referred to as *computer network attacks*.

Theories relevant to the paper will be considered in the analysis. Therefore I do not have a specific chapter dedicated to theories.

1.3 Method and material

This paper will be a study of the applicability of international law governing resort to force (jus ad bellum) to computer network attacks carried out *between states*. To perform this analysis I will examine international law, study state practice, case law, preparatory works and doctrine relevant to the subject.

[12] REMARKS BY THE PRESIDENT ON SECURING OUR NATION'S CYBER INFRASTRUCTURE and European Convention on Cybercrime and A/RES/55/63 and A/RES/64/25 and Asleep at the Laptop and The Cybercrime Wave That Wasn't and Global Project on Cybercrime and Börsen nästa mål för nätattackerna and Cyberattacker ett stort växande hot and Estonia fines man for "cyber war" and Europa går samman i Cyber Europe 2012 and Hot om stor aktion på fredag and The real Iranian threat: Cyberattacks.
[13] Cyberwarfare and International Law, Melzer, p 5.
[14] Ibid., pp 5-6.

There is a high availability of information concerning international law in general. Information on computer network attacks, on the other hand, is of more limited scale, although increasing.

As previously stated, the Charter of the United Nations and customary international law are relevant regulations. The Charter is relevant due to the fact that the concepts of use of force and armed attack are codified therein. There is preparatory work that can be of guidance for interpretation, which indicates the ideas and norms ruling at the time of the creation of the Charter. Customary international law is built on usus (state practice) and opinio juris and these concepts will be discussed further in relation to international law in general and to computer network attacks specifically. The concepts are of importance in the creation of customary law and important in the development of the concepts of use of force and armed attack.

The main source regarding case law is jurisprudence from the International Court of Justice (hereinafter the ICJ) because of its general acceptance as an international court and because the Court has treated relevant concepts for this paper in its judgments. It should be taken into consideration that the parties have to recognize the Court's jurisdiction and consent to be part of the proceedings, which is why the jurisprudence is of limited scale compared to the number of conflicts regarding resort to force.

The Advisory Opinions of the ICJ do not have any binding effect but the Court states that the Advisory Opinions have great legal weight and moral authority and after examining other sources such as doctrine I am prepared to acknowledge that this seems to be the general view.[15] Furthermore, UN-resolutions from the General Assembly and the Security Council seem to be generally accepted as reliable sources of international law and are applied as such.

The doctrine on computer network attacks in relation to international law is of special interest to comment. Many authors refer to each other and there seems to be a certain resemblance in their argumentation. Another matter to consider is that some of the authors that I have referred to in this paper have also participated in the creation of the

[15] ICJ website.

"Tallinn Manual" on cyber warfare. The Manual express consensus among its authors and is, at the moment, the most recent text on the subject.[16]

The Stuxnet worm will serve as an example throughout this paper to substantialize questions arising.

2 Computer network attacks

2.1 Computer network attacks – definition and overview of the concept

A computer network attack is an operation that occurs in cyberspace. A suggested definition of cyberspace is:

> "**cyberspace** — A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[17]

I will concentrate on computer network attacks that are wanted by the developer but unwanted by victim of such an attack. Computer network attacks are often developed to cause some kind of harm to its victim by interfering with or altering information in the attacked network or computer. A definition is given as follows:

> "**computer network attack** — Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[18]

This is the definition that will be used throughout this paper.

---

[16] Michael N. Schmitt, Heather Harrison Dinniss, Thomas C. Wingfield, Nils Melzer and Eric Talbot Jensen.
[17] Department of Defense Dictionary of Military and Associated Terms, p 77.
[18] Ibid., p 59 and Cyber Warfare and the Laws of War, Harrison Dinniss, p 4.

The word “attack” in “computer network attack” is, in my opinion, used because it refers to an unauthorised entrance to, or use of, a computer network. It can also refer to an authorised entrance or use to such extent that the network becomes overloaded with information, with the result that, for example, a website goes down. This latter form of attack is commonly called DDoS (Distributed Denial of Service) or DoS (Denial of Service). A computer network attack can also, for example, have the construction of a worm or virus. A *worm* is malicious malware that, unlike a virus, does not need a host program to multiply and spread itself, nor does it need human intervention for spreading. A worm can spread by copying itself through Internet, for example via email. The worm causes harm by changing or modifying files or at least by slowing down the infected network.[19]

Computer network attacks are often associated with hackers and the hacker culture and the image of teenagers sitting in a dark room avoiding daylight and social contact in real life. Hackers are programmers with developed knowledge about entering closed computer networks and systems with the purpose of obtaining classified information.[20] But these kids or hackers are not the only ones constructing computer worms or hacking networks. Computer network attacks are also developed by military services on behalf of governments. For example, an American general has admitted that the USA has used computer network attacks against Afghanistan since 2010.[21]

It is a logic question to ask what the purpose would be of engaging in a computer network attack. The purpose can be everything from the sole purpose of causing damage, to collapsing bank systems or nuclear facilities to paralyse another state. Some use computer network attacks for espionage, such as industrial or governmental espionage. This kind of attack is difficult to detect since it is normally in the interest of the attacker to keep it secret from the victim. A recent example of such an attack is the hacking of the email account of the President of the European Council Herman

[19] Internets mörka sidor Om cyberhot och informationskrigföring, Heickerö, p 37 and Cyber Warfare and the Laws of War, Harrison Dinniss, p 296 and Svenska hackare En berättelse från nätets skuggsida, Goldberg and Larsson, p 304.
[20] Internets mörka sidor Om cyberhot och informationskrigföring, Heickerö, p 26.
[21] Cyberattacker ett stort växande hot, Olsson, SvD, 2012-10-08 and Cyber Warfare and the Laws of War, Harrison Dinniss, p 53-57.

Van Rompuy on the 18th of July 2011 where the hackers for 14 minutes could enter his email account.[22] The purpose of such an attack may be political. One state's government may want to know the standpoint of another government in negotiations before a transnational meeting.[23] Another purpose can be to find internal military strategies or similar information. Another example of computer network attacks used for political reasons is the use of DDOS attacks on governmental or other important websites. Estonia was in 2007 subject to DDOS[24] attacks from Russian hackers who were believed to be organised by the Russian government. However, the Russian government has denied all responsibility of organising the attacks.[25] More recent examples of DDOS attacks are the continuous attacks on Sweden and Swedish governmental websites during September and October 2012.[26] These attacks were organised by the hacker organisation "Anonymous" and directed at Sweden and the Swedish government as a revenge action to a raid that the Swedish police made on PRQ, a web hotel, and because of the Swedish police's investigation of Julian Assange, editor-in-chief and founder of Wikileaks. The attacks caused overload on many governmental websites out of which many went down entirely for some time.

2.2 Computer network attacks as modern warfare - From bow and arrow to cyber warfare

War has existed for millennia and war technology is in constant development.[27] Beginning with land war and war at sea, new technology made it possible with war in or from the air. The next great evolution was when space war was developed where bombs could be controlled through satellites. All of these warfare types were based on physical attack or with a physical result, for example an explosion. Today we have reached cyber warfare, through advanced computer technology where the attack takes place in cyberspace, although still sometimes with physical result. This new type of

[22] Cyberattacker ett stort växande hot, Olsson, SvD, 2012-10-08.
[23] Ibid.
[24] Distributed Denial of Service.
[25] Cyber Warfare and the Laws of War, Harrison Dinniss, p 289 and Estonia hit by "Moscow cyber war", BBC News and Estonia fines man for "cyber war", BBC News.
[26] Börsen nästa mål för nätattackerna, Wadendal, SvD, 2012-10-05 och Hot om stor aktion på fredag, SvD, 2012-10-03.
[27] For further reading see: The Law of Information Conflict, Wingfield.

warfare includes, for example Internet espionage, sabotage or misleading information. All these methods have been used in every type of warfare, but are now concentrated on being exercised through networks and computers.

Another aspect of computer network attacks is that they are not as expensive for the attacking state as classic warfare on land, sea, air and in space.[28] Schmitt refers to cyber warfare as "war on the cheap".[29] However, it might be expensive to prevent these types of attacks. Entire computer network systems must be protected from attacks that the victim does not know the construction of or where in the system they will enter.

Today we are not only talking about weapons of mass destruction but also "mass *disruption* weapons".[30] Computer network attacks will be more advanced in the future and states have developed cyber commands, for example the U.S., United Kingdom, China and South Korea.[31] The U.S. Army Cyber Command states that: "This represents the next evolutionary step in U.S. Army cyberspace".[32] Sweden is developing a cyber command[33] and NATO considers computer network attacks as new threats to the organisation[34] by stating that "Cyber attacks continue to pose a real threat to NATO and cyber defence will continue to be a core capability of the Alliance".[35]

2.3 Why are computer network attacks between states a legal issue

Law affects society and society affects law. Development of new techniques will change societies and the way people interact, which will sometimes force legal changes. International law is being affected by the societies we live in and the norms

[28] Internets mörka sidor Om cyberhot och informationskrigföring, Heickerö, pp 30-31.
[29] Computer Network Attack and the Use of Force in International Law, Schmitt, p 897.
[30] REMARKS BY THE PRESIDENT ON SECURING OUR NATION'S CYBER INFRASTRUCTURE and The real Iranian threat: Cyberattacks, Goldman, CNN Money, November 5, 2012.
[31] Cyber Warfare and the Laws of War, Harrison Dinniss, p 53, footnote 78 and World Wide Warfare - Jus ad bellum and the Use of Cyber Force, Roscini, pp 97-98.
[32] http://www.arcyber.army.mil
[33] Hemligt förband ska skydda från it-hot, Olsson, SvD, 2012-12-04.
[34] Internets mörka sidor Om cyberhot och informationskrigföring, Heickerö, pp 17, 29-30.
[35] http://www.nato.int/cps/en/natolive/topics_78170.htm

and values ruling at the time being in these communities.[36] These norms and values also differ from community to community. Internet has for quite some time become part of many peoples day-to-day life in many communities and it is hard to imagine that we would stop using it. Internet has changed our way of communicating and is part of globalisation. It has affected young generations and is now something that kids learn how to use at a young age.[37] This means, as far as I believe, that the new generation in high technological countries will grow up considering Internet and computers as part of their daily life. The growing dependency on the Internet and computer networks, not necessarily connected to the Internet, for infrastructures, such as water distribution or electrical power transmission, will make societies more vulnerable for computer network attacks.[38]

I believe that the growing dependency on the Internet and computer networks for societies will affect the way we see international law. When computer network attacks become more frequent between states, to paralyse or injure one another, there will soon have to be a decision about if a state can lawfully defend itself against a computer network attack. I believe this is also why a growing number of authors and experts are interested in the subject.

Computer network attacks are new tools in modern warfare. Computer network attacks have existed for some time but were not specifically taken into consideration in the creation of, for example the UN Charter. This means that there are no specific laws in international law that are pointing out exactly how computer network attacks shall be handled or laws to fall back on saying that war can or cannot be started through or because of a computer network attack. This is not an entirely lawless legal area since there are principles, customary law and treaties that may be used for analogies.[39] Treaties, such as the UN Charter, are regulating resort to force but are based and created on the thought that war takes place on land, at sea or in air. International law has not been fully able to keep up with the technological evolution.

[36] Computer Network Attack and Use of Force in International Law, Schmitt, p 910.
[37] Färre svenskar skaffar Facebook, Karlsson, Göteborgs Posten, 2012-10-17 and Teknikfrälst innan han kan gå, Karlsson, Göteborgs Posten, 2012-10-17 and Svenskarna och Internet 2012, Findahl, p 6.
[38] Cyber Warfare and the Laws of War, Harrison Dinniss, p 5.
[39] Tallinn Manual, p 24, part A, para 2.

International law is unique in the way it is created. Sovereign states have to agree on laws they want to create and follow. This may be a time-consuming process, which sometimes may not even come to a final result. It is not guaranteed that new laws will be able to cover all the new technological aspects of the cyber domain even though laws are often generally constructed to be able to cover many different scenarios.

The subject of computer network attacks in international law is relevant because of the discrepancy resulting from the lack of legal regulation and the fact that computer network attacks are already considered a method of warfare. Another verification of the legal issue concerning computer network attacks is that new literature is constantly written on the subject and that a group, put together by NATO, is working on a manual on cyber warfare.[40]

3 Computer network attacks as an "armed attack"

3.1 The concepts of "use of force" and "armed attack" in the UN Charter and customary international law

To be able to compare a computer network attack with an "armed attack" I have to begin with discussing what is considered to be an "armed attack" in general. I also have to comment on the concept "use of force" to understand how these two concepts and international law have developed.

Many authors,[41] discussing computer network attacks in relation to international law, refer to the Charter of the United Nations and customary international law by building their argumentation around these laws and the concept "armed attack". Why do so many authors refer to these sources? Melzer concludes that the UN Charter is considered to be one of the most important sources of international law in jus ad

[40] Tallinn Manual.
[41] See for example Nils Melzer, David E. Graham, Michael N. Schmitt, Heather Harrison Dinniss and Marco Roscini.

bellum.[42] This conclusion is probably the point of view of many educated women and men in international law.

What can be of guidance is the Advisory Opinion on Nuclear Weapons,[43] especially the sequence where the ICJ discuss the relevant applicable law for the use of nuclear weapons:

> " … the Court concludes that the most directly relevant applicable law governing the question of which it was seised, is that relating to the use of force enshrined in the United Nations Charter … ".[44]

A reason for why the ICJ comes to this conclusion may be that the ICJ is an institution of the United Nations. Although free to use other sources of law such as international customary law, the Charter is the keystone of the organisation of which the ICJ is part. However, it is still a fact that the Charter of the United Nations is one of the most accepted Charters regarding relations between states.

International law is a kind of its own and its creation is different from that of national law. It rests on a belief that there is a common interest to follow the rules of international law and if there is no such interest there is no international law. There is no institution above sovereign states, which makes the enforcement process difficult. Questions that have ensued recently, for example about computer network attacks as part of warfare, will have to be discussed and developed in the international community for new international principles to be established through state practice, international jurisprudence and doctrine as well as international treaty law.[45] Political interests can shape and affect the development of international law. There are few institutions where questions like these about computer network attacks carried out between states can be discussed and one of the few institutions that can give a judgment on the legal aspects is the ICJ.[46]

[42] Cyberwarfare and International Law, Melzer, p 6.
[43] Advisory Opinion on the Threat or use of Nuclear Weapons.
[44] Ibid., para 34.
[45] Cyberwarfare and International Law, Melzer, p 6.
[46] ICJ website and A/RES/42/22, 18 November 1987, General Assembly, article 32.

One of the difficulties with international law governing resort to force is to find what is regarded as a legitimate or illegitimate use of force in the international society today. Part of this problem is that the "use of force" and "armed attack" are not defined in treaty law.[47] There are two main bodies of international law regulating the use of force and armed attack, namely, international treaty law and customary international law. The main treaty on the subject is the Charter of the United Nations, especially article 2(4) and the concept "use of force":

> "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."

As well as article 51 and the concept "armed attack":

> "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security."

The Charter does not specify what an "armed attack" is or when self-defence is considered to be lawful or unlawful more than in the case of that an armed attack occurs. Customary international law helps to clarify these concepts further. Here we find principles developed over time concerning the use of force and armed attacks that give guidance on how the concepts should be interpreted, for example state practice (usus) and opinio juris.[48] Due to the special character of international law, what is a lawful resort to force can change over time by, for example state practice. There are

[47] The Law of Information Conflict, Wingfield, p 73.
[48] Ibid., p 73 and Nicaragua case, para 184.

rulings from the ICJ and doctrine on the subject that will be relevant to analyse further.[49]

The prohibition of the use of force in the Charter of the United Nations expressed in article 2(4) can be seen as a codification of the principle considered as jus cogens in customary international law.[50] When considering the concept of the use of force in the Charter scholars are discussing if the concept should be interpreted in a restrictive or permissive context.[51] This discussion occurs, for example when new war technology is developed or when a state uses other means than armed force against another state. It is not certain if the wording of the Charter can cover new war technology or other means that are not directly identified as armed force. Some commentators argue for a more *restrictive* interpretation of the concept "use of force", meaning that not every governmental interference of a state in another state should be covered by the concept, but foremost armed or military force.[52] These commentators, for example, argue that economic coercion should not be covered by the use of force.[53] Brownlie seems to draw the line at economic coercion but argues that operations with weapons that do not have a kinetic or similar effect might be seen as a use of force firstly, if the means are generally referred to as "weapons" or "warfare" and secondly, if they are used to destroy life or property. Schmitt acknowledges the second criterion.[54] Brownlie gives examples of situations like releasing water with the risk to flood a valley or a village.[55] On the other hand Brownlie also argues that the interpretation of the concept use of force does not have to be restrictive since the justification of the use of force only lies in the given exceptions in the Charter and therefore those are the

[49] Statue of ICJ, article 38.
[50] Nicaragua case, para 190 with reference to the International Law Commission, (paragraph (1) of the commentary of the Commission to Article 50 of its draft Articles on the Law of Treaties, ILC Yearbook, 1966-11, p. 247).
[51] Cyber Warfare and the Laws of War, Harrison Dinniss, p 58.
[52] The Law of Information Conflict, Wingfield, p 87 and Cyberwarfare and International Law, Melzer, p 7.
[53] The Law of Information Conflict, Wingfield, pp 87-90 and Textbook on International Law, Dixon, p. 310 and Cyberwarfare and International Law, Melzer, p. 7 and International Law and the Use of Force by States, Brownlie, pp 362-363 and Warfare - Jus ad bellum and the Use of Cyber Force, Roscini, p 105.
[54] International Law and the Use of Force by States, Brownlie, pp 362-363 and "Attack" as a Term of Art in International Law, Schmitt, p 288.
[55] International Law and the Use of Force by States, Brownlie, pp 362-363.

ones that need to be restrictively interpreted.[56] Brownlie is therefore asking for a more restrictive interpretation of armed attack. Schmitt refers to a restrictive point of view where positivists argue that in accordance with the Vienna Convention:

> "A treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose."[57]

According to Schmitt the positivist believe that "force" in 2(4) means armed force interpreted in accordance with the preamble of the Charter that refers to "armed force".[58] Schmitt on the other hand refers to the positivist view of interpreting the Charter as failing to reflect the full purpose of the Charter,[59] namely, maintaining international peace and security. The reason being that they do not reflect the reality of the world today where the threat to peace might lie in new technology rather than traditional weapons.[60] However, in the end Schmitt comes to the conclusion that the restrictive approach is the strongest and that the use of force is commonly thought to include armed force and exclude economic coercion, but with this not saying that the use of force only means "armed force".[61] I understand the restrictive utilisation of the use of force as a way to protect it from being stretched to cover all types of attacks or interventions.[62] It is a way to avoid undermining the concept and to only use it in the worst and most apparent cases.

Other scholars advocate a wider or permitting interpretation of the concept use of force where it would be possible to consider also economic and similar interference as the use of force. Wingfield argues, contrary to other commentators, that the lack of the word "armed" in 2(4) means that also economic coercion can constitute a use of force and support his argument with the fact that *the travaux préparatoires*[63] does *not*

[56] International Law and the Use of Force by States, Brownlie, pp 432-433.
[57] Vienna Convention on the Law of Treaties, article 31(1).
[58] For further reading on this discussion see: Computer Network Attacks and the Use of Force in International Law, Schmitt.
[59] Charter of the United Nations, article 1.
[60] Computer Network Attack and Use of Force in International Law, Schmitt, pp 901-902.
[61] Ibid., p 908.
[62] Ibid., pp 928-929 footnote 123.
[63] Preparatory work of the UN Charter.

state that the use of force should *only* be interpreted as armed force.[64] For example, both Wingfield and Brownlie believe that the use of biological and chemical weapons can constitute a use of force and an armed attack.[65] Schmitt refers to the expression "other manner" in 2(4) as covering all other forms of force.[66] If these interpretations of the use of force are correct, it is proof of the international law's ability to adjust to new types of weapons and warfare and that the interpretation of the use of force and armed attack matters in the development of international law on resort to force. The wider interpretation of the use of force can take into account changes of norms and values in the international society - norms and values that can have developed or changed over time, for example, because of technological evolution.

What the restrictive and permissive proponents have in common is that many of them interpret the Charter with an instrument-based approach, meaning that the *tool*, either economic or armed force, is the relevant basis for interpretation of the use of force. The Instrument-based approach was used in 1945, which was logical at the time of creation of the Charter, as it was most likely that the use of force at the time would consist of armed force.[67] Over time, development of technology etcetera has led to a discussion of the use of force mainly based on an effects-based approach, which will be discussed further below.

In my understanding there is not yet a universal agreement on what the concept of use of force is meant to include or exclude. There are several indicative principles and many commentators have strong arguments on the interpretation in both a restrictive and permissive direction. This question will probably be discussed more in the future but I am not certain whether there will be a universal conclusion to the interpretation of the use of force. What is clearer to me, is the conclusion made by the ICJ in the *Nicaragua case:*

[64] The Law of Information Conflict, Wingfield, pp 88-89 and International Law and the Use of Force by States, Brownlie, p 362.
[65] International Law and the Use of Force by States, Brownlie, p 362 and The Law of Information Conflict, Wingfield, pp 112-113.
[66] Computer Network Attack and Use of Force in International Law, Schmitt, p 901.
[67] Ibid., p 909.

> "The essential consideration is that both the Charter and the customary international law flow from a common fundamental principle outlawing the use of force in international relations."[68]

The ICJ has had an important role in the interpretation of the concepts of use of force and armed attack. In the *Nicaragua case*, the ICJ concludes that it can apply customary international law norms independently from treaty norms with the same or similar content and that " … customary international law continues to exist alongside treaty law".[69] The Court makes this statement because the U.S. argues that the UN Charter is a codification of customary international law and that customary international law should therefore not be applied, neither should treaty law because of a multilateral treaty reservation between Nicaragua and the U.S.[70] The Court explains that the multilateral treaty reservation does not hinder the Court from applying customary international law. This because customary law does not cease to exist because of codification and the Court further determines that the wording in article 51 of the Charter regarding "inherent right" to self-defence refers to a right in accordance with customary international law.[71] When discussing the "inherent" right to self-defence, the Court states that:

> " … the Charter, having itself recognized the existence of this right, does not go on to regulate directly all aspects of its content. For example, it does not contain any specific rule whereby self-defence would warrant only measures which are proportional to the armed attack and necessary to respond to it, *a rule well established in customary international law*."[72] (Emphasis added).

This is strong proof that there are differences in the two bodies of law and that the interpretation of the concepts use of force and armed attack not necessarily have exactly the same contents in both international customary and treaty law. The Court's statement shows, in my opinion, that the customary international law and the international treaty law are two different bodies of law independently applicable to

[68] Nicaragua case, para 181.
[69] Ibid., para 176.
[70] Ibid., para 172 -176.
[71] Ibid., para 176 and 193.
[72] Ibid., para 176.

disputes of international law even though they may sometimes have the same or similar contents. The Court makes a similar statement in the *Congo v. Uganda case* where it clarifies that the provisions of the Declaration on Friendly Relations " … are declaratory of customary international law".[73]

Also the Security Council of the United Nations separates customary and treaty law and an example of this is found when the Security Council unanimously condemns the Israeli military attack on the Iraqi nuclear reactor Osirak as " … in clear violation of the Charter of the United Nations and the norms of international conduct … ".[74] A treaty or a resolution may be seen as a codification of customary international law norms but the codification as such does not exclude the possibility to apply the norms of the customary international law independently.

In the *Nicaragua case*, the Court continues by saying that one way of defining a principle of customary international law, such as the principle of prohibition of the use of force, as opinio juris is by the consent of states to resolutions of the General Assembly of the UN, such as the Declaration of Friendly Relations[75].[76] The principle of non-use of force in customary international law can therefore be used, independently from the Charter of the United Nations, as a source of international law. A conclusion I have drawn from this is that even though a principle has been codified in a resolution or treaty it does not lose its power as an independent principle of international law and the codification itself can instead be proof of the general acceptance of this principle as opinio juris. It might be important to define customary international law and treaty law as two different bodies of law as there might be differences in the outcome of the analysis of the two. This distinction is important in order to be able to analyse if it is possible to define a computer network attack as an armed attack under one, neither or both bodies of law.

[73] Congo v. Uganda case, para 162 and A/RES/25/2625 Declaration on Friendly Relations.
[74] S/RES/487 (1981), para 1.
[75] A/RES/25/2625 Declaration on Friendly Relations.
[76] Nicaragua case, para 191.

Concerning the concept of "armed attack" found in article 51 of the Charter there is no precise definition of the concept.[77] The ICJ itself expresses this in the *Nicaragua case:*

> " … a definition of the 'armed attack' which, *if found to exist*, authorizes the exercise of the 'inherent right' of self-defence, is not provided in the Charter, and is not part of treaty law."[78] (Emphasis added).

A few paragraphs later the Court states that there is a general agreement on acts that can constitute an armed attack referring to the resolution on Definition of Aggression, which will be discussed further below.[79] Apparently a definition of the concept of armed attack is discussable. In a dictionary the term "armed" is defined as: "Furnished with arms or armour; fully equipped for war"[80] or "using or carrying weapons".[81] These are only suggested definitions but they do not help clarifying the concept of armed attack in any further extent.

However, the ICJ defines a difference between the use of force and an armed attack in the *Nicaragua case* by saying that an armed attack constitutes " … the most grave forms of the use of force … "[82] and that an act has to be of " … such *gravity* as to amount to' (inter alia) an actual armed attack conducted by regular forces … "[83](emphasis added). Later in the judgement the ICJ concludes that:

> "While an *armed attack* would give rise to an entitlement to collective self-defence, a *use of force* of a *lesser degree of gravity* cannot … produce any entitlement to take collective counter- measures involving the use of force."[84] (Emphasis added).

[77] The Law of Information Conflict, Wingfield, p 73.
[78] Nicaragua case, para 176.
[79] Ibid., para 195.
[80] Oxford English Dictionary.
[81] Cambridge Dictionaries Online.
[82] Nicaragua case, para 191.
[83] Ibid., para 195.
[84] Ibid., para 249.

This conclusion is also acknowledged by Wingfield stating that the interpretation of the concept of armed attack is more restrictive than that of the use of force,[85] while Schmitt believes that the use of force is to be found between economic coercion and armed force.[86]

Further, the Court explains that an attack has to reach a certain level of *scale* and *effects* to be considered as an armed attack, this in comparison to " … a mere frontier incident … "[87] that may reach the level of intervention. The scale and effects criteria are in the *Nicaragua case* applied to a situation where an act is carried out by armed bands or irregulars, but as long as this act:

> " … because of its scale and effects, would have been classified as an *armed attack* rather than as a mere frontier incident had it been carried out by regular armed forces."[88] (Emphasis added).

The Court does not clearly make out the difference between when an act constitutes an "intervention", a "use of force" or an "armed attack", but points out the two criteria as guidance. A clearer line would have been preferable, since acts that constitute an armed attack, are followed by the right to use force in self-defence while interventions are not. What is clear is that the Court concludes that the concept of "armed attack" exists, not only in the Charter, but also in customary international law.[89]

Brownlie believes that the use of force needs to be of a certain gravity to be differentiated from "frontier incidents" but that the more important question is if there was "intent" to attack.[90] The intent or objective of an act may, beside the criterion of gravity, also be considered as criterion for deciding if an act is an armed attack. In addition to this both Wingfield and Graham have put forward "scope, duration and

[85] The Law of Information Conflict, Wingfield, p 47, 76-77.
[86] Computer Network Attack and Use of Force in International Law, Schmitt, p 914.
[87] Nicaragua case, para. 195.
[88] Ibid., para 195.
[89] Ibid., para. 195.
[90] International Law and the Use of Force by States, Brownlie, p 366.

intensity" as criteria to define armed attack, although Wingfield states that these criteria can also be used to define the use of force.[91]

The ICJ statement that a principle of customary international law expressed in a resolution from the General Assembly could be considered, as opinio juris, must,[92] in my opinion, also be applicable to the Declaration on the Definition of Aggression.[93] The Court points out that the declaration reflects customary international law.[94] However, it is interesting to note that Schmitt finds it "suspect" that the Court refers to non-binding General Assembly resolutions as proof of opinio juris.[95]

According to article 1 of the resolution an "aggression" is the use of armed force from one state against another. What complicates the utilization of the resolution is that it aims only at defining the concept "aggression", used in article 39 of the Charter, which gives the Security Council right to take measures if it identifies a threat to or breach of the peace or an act of aggression. One of the main purposes of the resolution is that the General Assembly:

> "Calls the attention of the Security Council to the Definition of Aggression, as set out below, and recommends that it should, as appropriate, take account of that Definition as guidance in determination, in accordance with the Charter, the existence of an act of aggression."[96]

The resolution does not literally aim at defining the concepts "use of force" or "armed attack" in 2(4) or 51 of the Charter and not once in the document is the concept of "armed attack", mentioned. According to article 2 together with article 3 of the resolution, it covers also use of armed force that does not reach "sufficient gravity". I believe that this wording aims at covering also acts of armed force, which are not of such gravity to reach the level of armed attack, but are acts that reach the level of being a threat or breach of the peace, which will enable the Security Council to take

[91] The Law of Information Conflict, Wingfield, p 80 and Cyber Threats and the Law of War, Graham, p 90.
[92] Footnote 76 and Nicaragua case, para 191 and 195.
[93] A/RES/29/3314 Definition of Aggression.
[94] Nicaragua case, para 195.
[95] Computer Network Attack and Use of Force in International Law, Schmitt, p 920.
[96] A/RES/29/3314 Definition of Aggression.

measures. According to Graham the resolution does not give an exact answer as to what constitutes an armed attack, however it does give examples of " … state actions that are deemed to qualify as such [armed attack], and these have gained extensive international acceptance".[97]

I do not fully agree with Graham in his analysis. The Definition of Aggression aims at, as its title indicates, giving a definition of aggression and therefore also includes acts that do not reach a level of an armed attack. The Court confirms that the acts referred to in article 3(g) of the Definition of Aggression, such as sending of armed bands or irregulars, can constitute an armed attack, under customary international law.[98] Although I agree that the resolution can of course be of guidance, to identify an armed attack, it does *not* give a clear difference between a situation considered as an armed attack or an act of aggression. Such a definition would be desirable as it is when an armed attack occurs that states have the right to self-defence while an act of aggression allows for the Security Council to take measures.

An interesting reflection is that the French version of the declaration is called "Définition d'agression" and that the French version of the Charter's article 51 refers to "agression armée" as for the English "armed attack". I am neither an English nor French native speaker, however there appears to be a slight difference in the English versions' use of "aggression" and "armed attack", at least that it could be subject for argumentation. This is avoided in the French versions by using the same wording in the declaration and articles of the Charter.

As previously mentioned[99] the Charter allows an *inherent* right to self-defence, which by some has been interpreted as referring to a right developed in customary law that has been acknowledged in the Charter.[100] As the ICJ points out the French version of article 51 refers to a "droit naturel" (natural right), which implies that the right to self-defence existed before the Charter was written.[101] However, proponents of a restrictive interpretation argue that the right to self-defence now applies only to

[97] Cyber Threats and the Law of War, Graham, p 90.
[98] Nicaragua case, para 195.
[99] See footnote 71-72.
[100] International Law, Cassese, p 359 and Nicaragua case para 176.
[101] Nicaragua case, para 176.

member states being the victim of an armed attack.[102] While the wording of article 51 states that the right to self-defence arises when an armed attack "occurs" the customary international law goes beyond that and gives guiding principles about the lawfulness of self-defence.[103]

Old principles formulated in the *Caroline case*[104] suggest that the right to self-defence only arises when " … 'necessity of that self-defense is instant, overwhelming, and leaving no choice of means, and no moment of deliberation'".[105] This is more commonly expressed as that an *imminent threat* must be at hand.[106] This is part of the discussion in international law about anticipatory self-defence concerning if self-defence can be lawful not only as "preventive" but also "pre-emptive" self-defence.[107] It is not agreed upon at what moment self-defence is lawful and there are authors proposing that self-defence might be launched in advance of an armed attack occurs and others saying that this is an unlawful use of force.[108] Among the authors proponents of anticipatory self-defence there are different opinions on how far the right can be extended in advance of the armed attack.[109] [110]

Other principles developed in customary international law are the principles of "necessity" and "proportionality" regulating the lawful use of force - self-defence.[111] The principle of necessity requires that the use of force in self-defence " … be needed to successfully repel an imminent attack or defeat one that is under way."[112] seen

[102] Cyber Warfare and the Laws of War, Harrison Dinniss, p 83.
[103] International Law and the Use of Force by States, Brownlie, pp 366-368.
[104] For further reading, see: AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS and Computer Network Attack and Use of Force in International Law, Schmitt, p 930, footnote 124 or Tallinn Manual, Chapter II, Section 2, Rule 15, para 2.
[105] Cyber Threats and the Law of War, Graham, p 90 and AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS, DoD, p 16.
[106] Cyber Threats and the Law of War, Graham, p 90 and Nicaragua case, para 194 and Textbook on International Law, Dixon, p 315.
[107] International Law, Cassese, pp 357-358.
[108] The Law of Information Conflict, Wingfield, pp 46-47.
[109] Cyber Warfare and the Laws of War, Harrison Dinniss, p 83 and Tallinn Manual, Chapter II, Section 2, Rule 15, para 4.
[110] For further reading on anticipatory self-defence: International Law, Cassese, Chapter 18.2.3.
[111] For further reading: The Law of Information Conflict, Wingfield, pp 41-46 and Cyber Threats and the Law of War, Graham, p 90.
[112] Tallinn Manual, Chapter II, Section 2, Rule 14, para 2 – 4.

from the victim's point of view. Proportionality " … limits the scale, scope, duration, and intensity of the defensive response to that required to end the situation that has given rise to the right to act in self-defence."[113] The use of force does not have to be of the same type as the attack. The requirement of necessity and proportionality of lawful self-defence is acknowledged in the *Corfu Channel case,* the *Nicaragua case, Oil Platforms case* and in the *Congo v. Uganda case* as well as in the *Advisory Opinion on the use of Nuclear Weapons*.[114] In the *Nicaragua case* the Court points out both the principles and that these are to be applied in addition to the Charter:

> " … the Charter, having itself recognized the existence of this right, does not go on to regulate directly all aspects of its content. For example, it does not contain any specific rule whereby self-defence would warrant only measures which are *proportional* to the armed attack and *necessary* to respond to it, *a rule well established in customary international law*."[115] (Emphasis added).

All these principles provide guidance for defining an armed attack but there is still no clear definition. In resolutions from the Security Council the Council declares that a state is the object of an armed attack but does not clarify when or how the attacks reached the level of an armed attack.[116] Wingfield suggests that the period of time and intensity must be of importance and also suggests that the requirement of necessity and proportionality is applicable to all the use of force and that states can use necessary and proportional force as a response to a use of force not amounting to an armed attack, although maybe not self-defence amounting to a level of armed force.[117] Others, on the other hand, propose that the use of force in self-defence is strictly associated with the occurrence of an armed attack. Wingfield claims that the victim-state in that case only has ineffective means of response against the use of force from

[113] Tallinn Manual, Chapter II, Section 2, Rule 14, para 5.
[114] Corfu Channel case, p. 35 (only regarding proportionality) and Nicaragua case, para 176, 194, 237 and Oil Platforms case, para 73-77 and Congo v. Uganda case, para 147 and Advisory Opinion on the Threat or Use of Nuclear Weapons, para 41-43.
[115] Nicaragua case, para 176.
[116] S/RES/0661 (1990), Iraq v. Kuwait and The Law of Information Conflict, Wingfield, p 111.
[117] The Law of Information Conflict, Wingfield, p 41 and 47-51. For further reading, see: The Law of Information Conflict, Wingfield and Computer Network Attack and Use of Force in International Law, Schmitt.

the other state and that the commentators often cannot argue in a satisfactory way in favour of their positioning.[118]

To briefly summarise the analysis above - the UN Charter and customary international law are two different bodies of law governing resort to force and the concepts of use of force and armed attack exist in both of them. Even though the content of the concepts may be similar in both bodies of law there might be differences nonetheless. While the Charter is applicable to the states that are members of the UN, customary international law is applicable to those, which are not members. However, principles of customary law, not codified in the Charter, are applicable to all states.

In regard to the use of force the most central question is if the concept should be interpreted in a restrictive or permissive way and if the term covers only armed force or if other forms of force are included as well, for example economic coercion. Even though there is no clear definition of the concept of armed attack a few criteria put forward to decide if an act is an armed attack are: scale and effect, sufficient gravity, intention and scope, duration and intensity. Means referred to as weapons or warfare can also serve as criteria.

Interpretation of the concepts use of force and armed attack can be based on both an instrument-based and an effects-based approach. Examples of effects are fatalities or large-scale destruction of property. There are examples of other forms of force that generally are considered to be able to amount to an armed attack, namely biological and chemical weapons. The ability to apply the concepts use of force and armed attack to such means shows the international law's ability to adjust to new types of warfare and that law governing resort to force has an ability to develop over time.

According to customary international law a threat must be imminent for the right to self-defence to be used in anticipation of an armed attack and the self-defence must be necessary and proportionate.

[118] The Law of Information Conflict, Wingfield, p 49.

After this general overview of the concepts of use of force and armed attack I will now turn to the question if these concepts can be applied to computer network attacks.

3.2 Computer network attacks as an "armed attack" in the UN Charter and customary international law

The main question of this paper is to analyse arguments in favour of and against the application of the concept of "armed attack" in the UN Charter and customary international law to computer network attacks. I will therefore below analyse a few relevant sources.

The suggestion that a computer network attack might be seen as a breach of the principle of "non-intervention" in a state's internal or external affairs, recognised in the Charter of the United Nations, the General Assembly's Declaration on Inadmissibility of Intervention and customary international law, is not too difficult to agree on.[119] However, a breach against this principle is not followed by a right to armed self-defence, for the victim-state, according to international law. A breach of the principle of non-use of force, on the other hand, is for the victim-state followed by a right to self-defence if an armed attack occurs, according to article 51 in the UN Charter and customary international law.[120] This might be one of the reasons why some authors and states advocate that a computer network attack could possibly be comparable to an armed attack.

The phenomenon of computer network attacks shares a few similarities with nuclear weapons. Nuclear weapons were weapons of new technology with powers beyond the weapons already known of, at the time, and that changed the terms of warfare. Perhaps can the conclusion, given by the ICJ in the Advisory Opinion on Nuclear Weapons, referred to above,[121] stating that the UN Charter is the most relevant applicable law concerning use of nuclear weapons, also be applicable to computer

[119] Tallinn Manual, Chapter II, Rule 10, para 6-10 and Computer Network Attack and the Use of Force in International Law, Schmitt, p 919 and 923.
[120] For further reading on the question if there is a right to self-defence against use of force not amounting to an armed attack, see: The Law of Information Conflict, Wingfield.
[121] See footnote 44.

network attacks. If the Charter is applicable to nuclear weapons then perhaps it is also applicable to computer network attacks due to the similarities just mentioned, and if not directly applicable, it may at least be of guidance.

In the Advisory Opinion, the ICJ concludes that no rule *specifically* prohibits or authorizes the threat or use of *nuclear weapons* in international customary or treaty law.[122] In paragraph 39 of the Advisory Opinion the Court clarifies that the articles regarding the use of force and armed attack of the Charter of the United Nations are *not* specifying what kind of weapon must be used to be applicable. According to Roscini, the airplanes used in the attack against the U.S. on September 11, 2001, must have been considered as weapons, since the Security Council in two resolutions[123] following the attacks, recognized and reaffirmed the inherent right to self-defence in accordance with the Charter.[124] Computer network attacks constitute a great example of when the wording of the Charter becomes subject for discussion. Even though, at the time of creation, the intention of the wording of the Charter was clear,[125] it is not clear today.

Roscini is of the opinion that weapons do not have to have kinetic effect and is certain that, for example biological weapons, are covered by 2(4) and refers to the *Nicaragua case* and the Court's conclusion that arming and training the Contras was to be seen as a use of force.[126] According to Wingfield commentators from both the restrictive and emancipated interpretation of when a use of force as self-defence is lawful have interpreted "armed force" as also including " … non-military physical force and indirect force … ".[127] In the Tallinn Manual it is expressed that the weapon employed is not a decisive matter and that it is state practice that the use of biological weapons can amount to an armed attack. According to the experts of the manual the same arguments are applicable to computer network attacks.[128]

---

[122] Advisory Opinion on the Threat or use of Nuclear Weapons, para 105.
[123] S/RES/1368 (2001) 12 September and S/RES/1373 (2001) 28 September.
[124] World Wide Warfare - Jus ad bellum and the Use of Cyber Force, Roscini, p 115.
[125] Cyber Warfare and the Laws of War, Harrison Dinniss, p 77.
[126] Nicaragua case, para 228 and World Wide Warfare - Jus ad bellum and the Use of Cyber Force, Roscini, p 106.
[127] The Law of Information Conflict, Wingfield, pp 50, 99-102.
[128] Tallinn Manual, Chapter II, Section 2, Rule 13 commentaries.

At the time being computer network attacks are not mentioned in the non-exhaustive list in article 3 of the Declaration on Definition of Aggression, but according to article 4, the Security Council may determine that other acts can constitute aggression under the provisions of the Charter. However, it is probable that a computer network attack could amount to the level of an *aggression* followed by the right for the Security Council to take measures according to the statement in the Definition of Aggression article 3(b), saying that an aggression is the use of *any weapons* against the territory of another state (as also pointed out in the Advisory Opinion on Nuclear Weapons). The group of experts of the Tallinn Manual have agreed that this is an expression of customary international law and that computer network attacks can constitute a use of force. The fact alone that a computer is used for launching the attack is not a relevant fact.[129] As long as the computer network attack is directed at another state and is directed at the territory of that state it can constitute an act of aggression. There has to be a cross border incident and as concluded in the Tallinn Manual computer network attacks sent *from one state to another* that reach the level of armed attack, fulfil this criterion. If the attack is sent from within the same state's territory it is instead a matter of national law.[130]

The type of weapon employed in an attack does not appear to be of great importance when deciding if a computer network attack can constitute an armed attack and as the cross-border criterion is fulfilled, if the attack is sent from one state to another, the issue is to know when or how the act reaches the *level* of an armed attack. As mentioned above much of the argumentation on the use of force and armed attack has previously focused on an instrument-based approach where the tool used, either economic or armed force, was in centre of discussion. However, now it appears more important to consider an effects-based approach, where the effect rather than the tool is important. As Schmitt concludes the international law is shaped and affected by the ruling norms of societies and the global community.[131] The Charter was constructed in the perspective of the existing norms at the time and it will be interpreted in relation to existing norms today.

[129] Tallinn Manual, Chapter II, p 45.
[130] Ibid., Chapter II, Section 2, Rule 13.
[131] Computer Network Attack and Use of Force in International Law, Schmitt, p 910.

Jurisprudence from the ICJ is seen as part of the international law governing jus ad bellum and it is natural that principles pointed out in the Court's judgments are applied by authors, discussing computer network attacks as part of warfare. The effects-based approach might be derived from the principles pointed out by the ICJ about *scale* and *effects* in the *Nicaragua case* to define an attack as an armed attack if carried out by non-regular forces.[132] The situation resembles a possible computer network attack, because computer network attacks are not performed by the sending of regular forces but rather by cyber commands, probably situated far from where the attacks have effect.

This might be part of the answer to the question *why* it is necessary to compare the effects of a computer network attack with the effect of a bomb or other weapons with kinetic effect. Melzer considers it uncontroversial that a computer network attack can be equated with a use of force when the effects are on the same level as attacks of kinetic or similar force.[133] As discussed above, some authors support the restrictive interpretation of the concepts use of force and armed attack and refer to *the travaux préparatoires* of the Charter of the United Nations, considering that, for example economic coercion is not included in the concept of use of force.[134] Although Brownlie agrees on this, he also considers it possible that the *travaux préparatoires* did not exclude " … force other than armed force … "[135] from being included in the concept use of force and he believes that it is necessary to decide if the use of weapons without kinetic or similar effect will be defined as a use of force, for example biological and chemical weapons.[136] Zemanek argues that it is a matter of *result*, for example fatalities or large-scale destruction of property that distinguishes an armed attack from other attacks.[137] Dinstein also has a results-based approach to the question if a computer network attack may be seen as an armed attack.[138]

[132] Nicaragua case, para 195.
[133] Cyberwarfare and International Law, Melzer, p 7.
[134] Ibid., p 7 and International Law and the Use of Force by States, Brownlie, p 362-363 and World Wide Warfare - Jus ad bellum and the Use of Cyber Force, Roscini, p 105.
[135] International Law and the Use of Force by States, Brownlie, p 362.
[136] Ibid., p 362.
[137] World Wide Warfare - Jus ad bellum and the Use of Cyber Force, Roscini, pp 114-115 footnote 134.
[138] Cyber Warfare and the Laws of War, Harrison Dinniss, p 60.

Using the argument of scale and effects as criteria can be a way to make computer network attacks come closer to the concepts use of force and armed attack and the interpretation that the concepts only contain military or armed force because of the similar *physical* effects, instead of being compared to economic coercion without obvious physical effects. Schmitt has developed a test with 6 criteria for differentiating acts of the use of force from economic coercion, which could be useful. Especially since the experts of the Tallinn Manual have come to consensus about that economic coercion cannot constitute a use of force. The adjusted criteria are now incorporated in the Manual.[139]

It is worthwhile to note that the experts of the Tallinn Manual also classify *scale* and *effect* as criteria useable for determining if a computer network attack can constitute a use of force.[140] It is also expressed in the Tallinn Manual that considering computer network attacks as possibly amounting to an armed attack and a use of force, depending on its scale and effects, is in line with both the Charter and customary international law.[141] However, even though effect can serve as a criterion, it is still preferable to analyse every case separately and to see to the, as Schmitt describes it, " … qualitative nature of an action's consequences … " rather than specifying general conditions for measuring the effect (Schmitt- quantitative standards).[142]

It is hard to foresee all possible effects caused by a computer network attack but still the experts of the Manual agreed that only foreseeable effects would serve as fulfilling the criterion of effects.[143] A computer worm might be programmed to change the normal functions of a program but if the worm escapes to another program, network or computer, for example via Internet or by someone spreading it purposely, the effects might be graver than the attacker had planned in the first place.

[139] Tallinn Manual. Chapter II, Section 1, Rule 11 commentaries and for further reading on Schmitt's test: Computer Network Attack and Use of Force in International Law, Schmitt and The Law of Information Conflict, Wingfield.
[140] Tallinn Manual, Chapter II, Section 1, Rule 11, para 1.
[141] Ibid., Chapter II, Section 2, Rule 13 commentaries.
[142] "Attack" as a Term of Art in International Law, Schmitt, p 288.
[143] Tallinn Manual, Chapter II, Section 2, Rule 13, para 10.

An example is the Stuxnet worm, which was spread over the Internet, which led to it being exposed.[144]

There is consensus among experts of the Tallinn Manual that computer network attacks can constitute an armed attack and the relevant criteria to decide when these acts amount to armed attack are *scale* and foreseeable *effects.*[145] What the experts ask themselves is if a number of computer network attacks, not individually reaching the level of an armed attack, but accumulated can constitute an armed attack.[146] Their answer is *yes*, a fact that is interesting put in relation to the information shared in an article on the Iranian cyber-threat.[147] In the article a massive disturbance attack on U.S. banks' websites is attributed to Iran with " … mounting belief -- if not direct evidence … "[148] and the author cites Leon Panetta, Secretary of Defense (U.S.), saying that " … United States reserves the right to respond to a cyberattack with 'kinetic force'".[149] The last phrase of the article is a question " … how far will the U.S. let them keep going forward before this becomes a declaration of war?'".[150] The question seems just, after the conclusion made by the experts of the Tallinn Manual that many attacks accumulated can constitute an armed attack. It is the victim-state, which has the burden of proof that it is under an armed attack and that the self-defence is lawful.[151] As stated in the *Nicaragua case* " … it is the State which is the victim of an armed attack which must form and declare the view that it has been so attacked."[152] Likewise, Iran declared that it was under attack when the Stuxnet worm became known.[153] This shows how urgent it is to find a solution in the international community to the question on how to handle computer network attacks.

---

[144] Obama Order Sped Up Wave of Cyberattacks Against Iran, Sanger, The New York Times, June 1, 2012.
[145] Tallinn Manual, Chapter II, Section 2, Rule 13 and para 3, 10 and Chapter II, Rule 11, para 1.
[146] Ibid., Chapter II, Section 2, Rule 13 commentaries.
[147] The real Iranian threat: Cyberattacks, Goldman, CNN Money, November 5 2012.
[148] Ibid.
[149] Ibid.
[150] Ibid.
[151] Oil Platforms case, para 57 and Cyber Warfare and the Laws of War, Harrison Dinniss, p 77 and International Law and the Use of Force by States, Brownlie, p 214.
[152] Nicaragua case, para 195.
[153] Cyber Warfare and the Laws of War, Harrison Dinniss, p 57, footnote 96.

Another possible comparison with the Advisory Opinion on Nuclear Weapons can be made with the discussion in paragraph 47 where the ICJ clarifies that if a *use* of a weapon is unlawful, the *threat* of the use of such a weapon is also unlawful. This is acknowledged in the Tallinn Manual.[154] This could be put in contrast with the fact that it has been discussed in the U.S. if U.S. officials should make public announcements about development of offensive cyber weapons.[155] In an article it is mentioned that *if* the U.S. declares that it has offensive cyber weapons it could lead to an *arms race* on cyber weapons.[156] Such an arms race would in itself be contrary to the purpose of the Declaration on the Non-Use of Force,[157] especially articles 19 and 20 demanding that states should prevent arms race and contribute to relaxation of international tension. On the other hand, such a public discussion about cyber capabilities may lead to an international discussion on how the international community should handle computer network attacks in the perspective of international law.

As mentioned above,[158] Brownlie has expressed that if computer network attacks are commonly referred to as types of "weapons" and "warfare", this serves as one criterion for considering computer network attacks as a use of force and in the long run perhaps as an armed attack. Brownlie's second criterion is that if computer network attacks can destroy life and property they should be considered as a use of force. Roscini believes that a computer network attack can be equated with a use of force and that large-scale computer network attacks can amount to an armed attack. His main argument is that since the Charter and customary international law can cover nuclear weapons, they are flexible enough to cover also computer network attacks.[159] Schmitt believes that a computer network attack can possibly constitute an armed attack if it results in fatalities or that property is destroyed at a large scale.[160] Roscini refers to Brownlie's criteria and is convinced that both these criteria fit computer

[154] Tallinn Manual, Chapter II, Section 1, Rule 12 commentaries.
[155] U.S. Suspects Iran Was Behind a Wave of Cyberattacks, Shanker and Sanger, The New York Times, October 13, 2012.
[156] Cyberwarfare Emerges From Shadows for Public Discussion by U.S. Officials, Shane, The New York Times, September 26, 2012.
[157] General Assembly Resolution A/RES/42/22.
[158] See footnote 54.
[159] World Wide Warfare - Jus ad bellum and the Use of Cyber Force, Roscini, p 130.
[160] Computer Network Attack and Use of Force in International Law, Schmitt, p 934.

network attacks well, especially associating this kind of attack with a new form of warfare or weapons. I have found that a few authors in the daily press already refer to computer network attacks as warfare and weapons and perhaps is this criterion for defining a new technology as a use of force or an armed attack already fulfilled.[161]

So far, I have found that Roscini is the sole author agreeing with Brownlie that referring to computer network attacks as weapons and warfare is a suitable criterion, admitting that my research is of limited scale. Computer network attacks can, in my opinion, possibly fit into both of Brownlie's criteria depending on the type of attack. Apparently, these attacks are already referred to as weapons and part of warfare[162] and may result in destruction of property (for example the destruction of centrifuges in the Iranian nuclear enrichment facilities because of Stuxnet)[163] and may cause death if, for example, disrupting systems controlling traffic lights or air traffic. The experts of the Tallinn Manual have expressed that the object targeted of the attack serves as criterion for defining a computer network attack as an armed attack. If the objects are humans or property the attack is an armed attack if, at the same time, the scale and effects criteria are fulfilled and the act is a trans-border operation.[164]

As mentioned above[165] "scope", "duration" and "intensity" were pointed out as criteria to define an armed attack. According to Graham these criteria can be used together with three different approaches (effects-based, instrument-based or "strict liability") to define an armed attack. Graham refers to the effects-based approach or consequence-based approach as the approach used by the U.S. and continues by concluding that proponents of the three different approaches agree that a "cyber attack" can be seen as an armed attack.[166] Wingfield gives an example where one state completely cuts of the telecommunications of another state through a computer

[161] The Real Iranian threat: Cyberattacks, Goldman, CNN Money 2012-11-05 and U.S. Suspects Iran Was Behind a Wave of Cyberattacks, Shanker and Sanger, The New York Times 2012-10-13 and Cyberwarfare Emerges From Shadows for Public Discussion by U.S. Officials, Shane, The New York Times 2012-09-26 and A New Kind Of Warfare, The New York Times 2012-09-09 and Obama Order Sped Up Wave of Cyberattacks Against Iran, Sanger, The New York Times 2012-06-01.
[162] Ibid.
[163] Obama Order Sped Up Wave of Cyberattacks Against Iran, Sanger, The New York Times 2012-06-01 and Cyber Warfare and the Laws of War, Harrison Dinniss, pp 81, 291-292.
[164] Tallinn Manual, Chapter II, Section 2, Rule 13, para 18.
[165] See footnote 91.
[166] Cyber Threats and the Law of War, Graham, p 91-92.

network attack and refers to this as the " … electronic equivalent of an armed attack … ".[167] Wingfield also applies the criteria of scope, duration and intensity by exemplifying that computer network attacks causing repeated train crashes or one significant attack paralyzing the stock exchange for a considerable time would amount to an armed attack with a following right to self-defence.[168] Opposing, some of the experts of the Tallinn Manual do not find the latter computer network attack as constituting an armed attack because they do not consider such a financial loss as destruction of property.[169]

Zemanek, to whom Roscini refers, believes that it is not the question about what type of weapon that matters, but the question of *intent* and result.[170] Roscini states that the attacker must have intention to harm the victim.[171] Schmitt concludes that computer network attacks that destroy property or result in fatalities and were sent with *intention* to do so will probably be seen as an armed attack. He identifies a more difficult question on how to handle computer network attacks that do not cause fatalities or destroy property.[172] Although a few of the Tallinn Manual experts consider *intention* as a criterion for deciding if a computer network attack can constitute an armed attack the majority of experts does not consider intention relevant.[173] It appears that there is no general consensus regarding *intention* as criterion for deciding if a computer network attack can constitute an armed attack.

Can we already talk about opinio juris or usus regarding computer network attacks in international law? In the *Nicaragua case* the ICJ discusses how customary international law is created, when trying to determine if there is customary law regarding counter-measures against intervention. The Court expresses an opinion that states do not have to follow rules strictly, but they should in their practice at least act in accordance with the rule, for the rule to be seen as a customary rule. Moreover, it is

[167] The Law of Information Conflict, Wingfield, pp 91-92.
[168] Ibid., pp 101-102.
[169] Tallinn Manual, Chapter II, Section 2, Rule 13, para 9.
[170] World Wide Warfare - Jus ad bellum and the Use of Cyber Force, Roscini, pp 114-115 footnote 134.
[171] World Wide Warfare - Jus ad bellum and the Use of Cyber Force, Roscini, p 116.
[172] Computer Network Attack and Use of Force in International Law, Schmitt, p 913, 929 and "Attack" as a Term of Art in International Law, Schmitt, p 288.
[173] Tallinn Manual, Chapter II, Section 2, Rule 13, para 11.

the Court's opinion that as long as states in general act in consistency with a rule, an act inconsistent with the same rule should be seen as a breach of the rule and not as a change of, or a new rule.[174] Applied to computer network attacks these statements from the ICJ might show that even though a few states act as and proclaim that computer network attacks, according to them, should be seen as an armed attack, it is not certain that the ICJ would consider it as a change of or a new rule of customary international law.

Schmitt states that there is neither opinio juris nor state practice yet regarding computer network attacks as an armed attack or a use of force.[175] What should be taken into consideration is that Schmitt's essay was written 1999 and a lot has happened since then. The most recent text on the subject mentions that opinio juris regarding computer network attacks is scarce and that state practice is not yet well developed.[176] Roscini refers to D'Amato who said that by now computer network attacks would be prohibited in customary international law.[177] Also Roscini is of a different opinion than Schmitt. Roscini means that usus can be expressed not only through "physical" state practice but also through verbal acts such as statements of various kinds and that new rules of customary international law can develop over a short period of time.[178] The ICJ confirms in the *North Sea Continental Shelf cases* that *time* is not a single matter, for determining if there is state practice, stating as follows:

> " … an indispensable requirement would be that within the period in question, *short though it might be*, State practice, including that of States whose interests are *specially affected*, should have been both extensive and virtually uniform in the sense of the provision invoked;- and should moreover have occurred in such a way as to show a general recognition that a rule of law or legal obligation is involved."[179](Emphasis added).

---

[174] Nicaragua case, para 186.
[175] Computer Network Attack and the Use of Force in International Law, Schmitt, pp 919, 921 and Warfare - Jus ad bellum and the Use of Cyber Force, Roscini, p 123 footnote 179.
[176] Tallinn Manual, pp 19-20.
[177] World Wide Warfare - Jus ad bellum and the Use of Cyber Force, Roscini, p 123 footnote 178.
[178] Ibid., pp 123-124.
[179] North Sea Continental Shelf, para 174.

There are signs that, put together, might be indicating on a process of how computer network attacks should be handled. Slowly states are positioning themselves, for example by making cyber warfare part of their military strategies, as Canada, U.S., Russia and United Kingdom have done.[180] Documents and regulations are pointing out how nations or groups of nations should act facing computer network attacks. For example, the cyber strategy of NATO,[181] or that the U.S. has in the Nuclear Posture Review declared that " … These forces are enabled by U.S. capabilities to protect its assets in cyberspace and outer space … ".[182] The fact that the U.S., since 2010, has a cyber command indicates that the U.S. is preparing for cyber war. Other states that have cyber units as part of their armies are China, Germany, Iran and Israel.[183] The Russian military has expressed that it will consider computer network attacks on the Russian Federation as military means.[184] Also Sweden is developing a cyber command that will be ready for operative function next year.[185] Roscini uses this as proof that these states consider the use of computer network attacks as possibly breaching the prohibition of use of force.[186] The Vienna Convention on the Law of Treaties mentions that practice can be considered when interpreting, for example the UN Charter and the concept of armed attack.[187] These are all signs that state practice is being developed and it is foremost states, that have the capabilities of engaging in a computer network attack, that are relevant to consider to find state practice,[188] as pointed out in the citation just above (*specially affected*). However, in the *Anglo-Norwegian Fisheries case* the Court states that even though a few states have adopted a rule, it will not for sure be seen as a rule of international law if other states have adopted another rule.[189]

---

[180] Tallinn Manual, pp 16-17 and World Wide Warfare - Jus ad bellum and the Use of Cyber Force, Roscini, p 107 footnote 103.
[181] http://www.nato.int/cps/en/natolive/topics_78170.htm
[182] Nuclear Posture Review Report, p 33.
[183] World Wide Warfare - Jus ad bellum and the Use of Cyber Force, Roscini, pp 97-98 and U.S. Suspects Iran Was Behind a Wave of Cyberattacks, Shanker and Sanger, The New York Times, October 13, 2012.
[184] World Wide Warfare - Jus ad bellum and the Use of Cyber Force, Roscini, p 109.
[185] Hemligt förband ska skydda från it-hot, Olsson, SvD, 2012-12-04.
[186] World Wide Warfare - Jus ad bellum and the Use of Cyber Force, Roscini, pp 106-107.
[187] Article 31 para. 3(b).
[188] World Wide Warfare - Jus ad bellum and the Use of Cyber Force, Roscini, p 125.
[189] Anglo-Norwegian Fisheries case, p 131/19.

The number of states does not matter according to Cassese, concluding that only two countries (the U.S. and USSR) constructed state practice for outer space, and this in a short period of time.[190] The U.S. is one of the states that already has, in many ways declared its point of view concerning computer network attacks and will probably play an important role in the development of state practice.[191] A reason for this might be, in my opinion, that the U.S. is aware of its status as one of the leading states in cyber technology and that, at an early stage, it wants to be part of developing customary international law regarding computer network attacks in the direction preferable for the U.S. – in order to be able to defend itself against computer network attacks.

For an act to be seen as opinio juris the ICJ describes that it is not sufficient with only state practice but it is also needed that states believe that they are bound to act this way.[192] In the *North Sea Continental Shelf cases* the Court concludes that:

> " … in order to achieve this result, two conditions must be fulfilled. Not only must the acts concerned amount to a settled practice, but they must also be such, or be carried out in such a way, as to be evidence of a belief that this practice is rendered obligatory by the existence of a rule of law requiring it. The need for such a belief, i.e., the existence of a subjective element, is implicit in the very notion of the opinio juris sive necessitatis. The States concerned must therefore feel that they are conforming to what amounts to a legal obligation. The frequency, or even habitual character of the acts is not in itself enough."[193]

As both Schmitt and the other authors of the Tallinn Manual conclude opinio juris on computer network attacks is not yet well developed and I find it hard to say if any state yet believes that it is conforming to a legal obligation regarding considering

[190] International Law, Cassese, p 158.
[191] For example Nuclear Posture Review Report, p 33 and REMARKS BY THE PRESIDENT ON SECURING OUR NATION'S CYBER INFRASTRUCTURE and AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS, DoD, p 18 and Computer Attacks on Critical National Infrastructure, Jensen, p 229.
[192] Nicaragua case, para 207.
[193] North Sea Continental Shelf cases, para 77.

computer network attacks as an armed attack. This question will probably be discussed more in the near future.

Above[194] I have referred to the *Caroline case* in the aspect of when the right to self-defence arises and that the victim must face an *imminent threat* to lawfully defend oneself in anticipation of an armed attack. Brownlie states that since the invention of long-range missiles " … the difference between attack and imminent attack may now be negligible … ".[195] This can be compared to the instant set off of a computer network attack. There is not much time for a reaction in anticipatory self-defence. In an article, published in the New York Times, U.S.'s Defense Secretary Leon E. Panetta was referred to have said, in a speech about the U.S. cyber capabilities that:

> "'If we detect an *imminent threat* of attack that will cause significant, physical destruction in the United States or kill American citizens, we need to have the option to take action against those who would attack us to defend this nation when directed by the president. For these kinds of scenarios, the department has developed that capability to conduct effective operations to counter threats to our national interests in cyberspace.'"[196] (Emphasis added).

I do not believe that it is a coincidence that Mr Panetta uses the word *imminent* in his speech when talking about the cyber threat against U.S., in my opinion, this is a way to implement the thought that this kind of threat is a serious and real threat that the U.S. must be able to defend itself from.

In the *Nicaragua case* the court makes an interesting statement while discussing if there is a similar right to self-defence in case of an unlawful intervention as in the case of an armed attack:

> "… under international law in force today - whether customary international law or that of the United Nations system - States do *not have a right* of

[194] See footnote 104.
[195] International Law and Use of Force by States, Brownlie, p 368.
[196] U.S. Suspects Iran Was Behind a Wave of Cyberattacks, Shanker and Sanger, October 13, 2012.

'collective' *armed response to acts which do not constitute an 'armed attack'*."[197](Emphasis added).

This statement from the Court might, in my opinion, be a strong reason for why many authors are proponents to that computer network attacks should possibly be considered as armed attack in article 51 of the Charter of the United Nations and customary international law. The Court refers to the "collective" right to self-defence but it is not meant to be any difference in the sense of the right to collective or individual self-defence. If the criterion to defend oneself with armed response is that the attack needs to be considered as an armed attack, it is not hard to understand that states that believe they face computer network attacks, of great sophistication and with devastating effects, have an interest in defending themselves in any way possible, including with armed force. It will, for these states, be necessary to convince the international community that computer network attacks must be considered as armed attack if they want to be able to defend themselves, in accordance with international law.

As Melzer points out the purpose of the Charter of the United Nations is to keep the peace and security and I can agree with him that it would be unsatisfactory if states can avoid the prohibition of the use of force in the Charter by using means, having the same effects as armed force, but not falling under the wording of the Charter because of its new technology and not being defined as armed attack in a traditional meaning.[198] Before summarizing my conclusions I would like to point out some potential consequences of considering a computer network attack as an armed attack.

3.3 Consequences

The primary consequence of defining a computer network attack as an armed attack is that the right to self-defence with use of force arises. The self-defence must follow the principles of necessity and proportionality established in customary international

[197] Nicaragua case, para 211.
[198] Cyberwarfare and International Law, Melzer, p 8.

law.[199] However, the self-defence does probably not have to be of the same kind, as that of the attack. Kinetic force can be used in self-defence against a computer network attack and vice versa.[200] The experts of the Tallinn Manual agreed that the victim of a computer network attack that amounts to an armed attack will have the right to use force in self-defence, those which are members of the Charter, according to the Charter and non-members according to customary international law.[201]

The threat must be imminent in order for the self-defence to be launched in anticipation of a computer network attack considered as an armed attack.[202] The majority of the experts of the Tallinn Manual concludes that *time* is not the relevant factor to decide if self-defence in anticipation of an imminent attack is justifiable, but the fact that a failure to act may result in loss of opportunity to act in self-defence for the victim-state.[203] A requirement of *immediacy* is put forward by the experts of the Tallinn Manual to distinguish self-defence from retaliation. The latter is *not* accepted in customary international law and a distinction is therefore necessary. Immediacy refers to an on-going attack or when further attacks are expected to follow.[204] The question of imminence and immediacy is relevant to computer network attacks due to the fact that the time for the sending of a computer network attack is almost negligible and the victim might not even be aware of the reason causing damage to its property or from where the attack originates. The attack must generally be attributable to a state for a right to self-defence.

What are the consequences of basing the decision on if a computer network attack can be seen as an armed attack on an effects-based approach? Schmitt, referring to the effects as a consequence-based approach, believes that such an approach will constitute a new normative standard that will be difficult for the international community to adopt, according to Harrison Dinniss.[205] Schmitt states that " … it would prove extraordinarily difficult to quantify or qualify consequences in a

[199] Tallinn Manual, Chapter II, Section 2, Rule 14.
[200] Computer Attacks on Critical National Infrastructure, Jensen, p 230 and Tallinn Manual, Chapter II, Section 2, Rule 14, para 5.
[201] Ibid., Rule 13, para 1 and 3.
[202] Ibid., Rule 14 and 15.
[203] Ibid., Rule 15, para 4.
[204] Ibid., Rule 15, para 8-10.
[205] Cyber Warfare and the Laws of War, Harrison Dinniss, p 60.

normatively practical manner".[206] I believe that Schmitt is expressing hesitation toward using a consequence- or effects-based approach because there will still be no clear definition of effect and it will be difficult to draw the line between effects that reach the level comparable to an armed attack and effects that do not. There will still be a grey zone. As Schmitt states:

> "It eases the evaluative process by simply asking whether force has been used, rather than requiring a far more difficult assessment of the consequences that have resulted."[207]

For example the effects of the Stuxnet worm were said to be a "slow down" of the Iranian nuclear enrichment program, which was said to be set back by 18 months, and that Iran had to change approximately 1000 IR-1 centrifuges because the worm was programmed to change the speed of the rotation of the centrifuges, which was causing damage to them.[208] If this attack could be attributed to a state, would these effects suffice, for Stuxnet to be qualified as an armed attack? There is destruction but no fatalities. I am not in a position to answer this, however in the Tallinn Manual Stuxnet is at least declared as a use of force,[209] also acknowledged by Harrison Dinniss.[210] Some of the experts even consider it amounting to armed attack.[211]

Schmitt concludes that an effects-based approach is a new normative standard of interpreting the use of force, which might lead to unpredictability and inconsistency compared to the instrument-based approach commonly applied earlier.[212] A new standard might need new consent,[213] which I interpret, as there is a need for a new treaty. On the other hand, it would be possible to argue that it is as inconsistent, not to exclude means, not covered by the wording of the Charter.

---

[206] Computer Network Attack and Use of Force in International Law, Schmitt, p 911.
[207] Ibid., p 911.
[208] Cyber Warfare and the Laws of War, Harrison Dinniss, p 292 and The New York Times, Obama Order Sped Up Wave of Cyberattacks Against Iran, Sanger, June 1, 2012.
[209] Tallinn Manual, Chapter II, Rule 10, para 9.
[210] Cyber Warfare and the Laws of War, Harrison Dinniss, pp 81-82.
[211] Tallinn Manual, Chapter II, Section 2, Rule 13, para 13.
[212] Computer Network Attack and the Use of Force in International Law, Schmitt, p 917.
[213] Ibid., p 921.

If it is *not* possible to equate a computer network attack with an armed attack, it would most possibly at least reach a level of threatening peace and security followed by the possible countermeasures from the Security Council according to article 39 of the Charter.

Potential consequences of Stuxnet might be that if Stuxnet is seen as an armed attack on Iran and can be attributable to the U.S., Iran has an inherent right to self-defence according to article 51 UN Charter. This means that it might be possible for Iran to defend itself, for example with armed force. However, the self-defence has to be necessary and proportionate. On the other hand, the U.S. might claim that Stuxnet was an act of anticipatory self-defence against an Iranian nuclear weapons threat. These are interesting thoughts but will only serve as example of a possible international computer network conflict.

3.4 The attribution problem

I would like to point at the attribution problem associated with computer network attacks - the problem with attributing the attack to a state. This is one of the most difficult problems concerning computer network attacks because the more sophisticated the attack is, the more difficult it is to trace its origin. Even if it would be clear that a computer network attack could be considered as an armed attack the victim would still have to know who the attacker is, to be able to defend itself. The attacker will try to cover traces as effectively as possible to minimise the risk of detection.[214]

Perhaps guidelines can be found in International Humanitarian Law (IHL) concerning defining military targets? At least attacks from state agents *de jure* and *de facto* might possibly be attributable to a state.[215] According to IHL, persons that are combatants, members of organized armed groups and civilians directly participating in the hostilities are considered to be military targets.[216] This might be one way of

[214] Internets mörka sidor Om cyberhot och informationskrigföring, Heickerö, p 32.
[215] Cyberwarfare and International Law, Melzer, p 24.
[216] Ibid., p 29.

attributing programmers of a computer network attack to a state and therefore attribute the attack to that state. In the Tallinn Manual principles of guidance for attribution have been put forward.[217] For example the Experts express that a single individual can cause an attack attributable to a state as long as it was under the direction of that state.[218]

Graham is advocating "imputed" [219] responsibility instead of "conclusive" [220] responsibility.[221] In my opinion, this is a dangerous way of attributing a computer network attack to a state, possibly with grave consequences if the attribution is incorrect and a right to self-defence of armed force follows the attack. For example, in computer network attacks like DDOS it is common that botnets[222] are used and computers from many states can be involved. The owners of most of the computers are not even aware that their computer is used in the botnet. Would it be reasonable that the attack would be attributed to all states where computers are involved in the botnet? To me this does not seem reasonable. If a sole person, without any connection to the government of that state, direct a computer network attack on another state, it would seem more reasonable that this would be a question of national criminal law. However, there may be a question, of international character, on which state can prosecute such a crime. Roscini mentions that some authors are of the point of view that a state should be able to defend itself without firstly attributing the attack to another state but Roscini directly rejects this idea by saying that it is illogical and ask himself to whom a victim would direct its self-defence.[223]

In the Tallinn Manual a majority of the experts shares the opinion that even a computer network attack from non-state actors,[224] for example terrorist groups, can be

---

[217] Tallinn Manual, Chapter I, Section 2, Rule 6-8 and 11.
[218] Ibid., Chapter II, Section 2, Rule 13, para 15.
[219] That attacks; launched from within the state's territory, from the state's citizens or any non-state actor can be attributable to the state.
[220] Absolute responsibility.
[221] Cyber Treats and the Law of War, Graham, p 93.
[222] "A group of compromised computers controlled by a master computer …". Cyber Warfare and the Laws of War, Harrison Dinniss, p 293.
[223] World Wide Warfare - Jus ad bellum and the Use of Cyber Force, Roscini, p 119.
[224] For further reading see: Cyber Warfare and the Laws of War, Harrison Dinniss, chapter 3.2.

seen as armed attack with a right to self-defence for the victim-state.[225] This is partly due to the development of international law after 9/11 – 2001 and the Al Qaeda attack on the U.S., where the right to self-defence was acknowledged in resolutions from the Security Council.[226] A general right to self-defence against attacks from non-state actors is probably not fully accepted in the international community and a proof of this is that a minority of the experts were not prepared to acknowledge such a rule.[227] The ICJ did not accept such a rule when the attack came from within the territory of the state in the Advisory Opinion on the Palestinian Wall.[228]

4 Conclusion

The Preamble of the Charter of the United Nations demonstrates the background and purpose of the Charter. Reading it I believe that war should be avoided in any way possible rather than finding new excuses to go to war. However, it would also be unsatisfactory if states would not be allowed to defend themselves against attacks that do not fit into the template of the Charter.

I have in my research on computer network attacks in international law found that many states strive for defining their actions against computer network attacks as a lawful use of force in self-defence of an armed attack. To reach this right to self-defence many arguments have been put forward.

In chapter 3.1 I have concluded what the concepts of use of force and armed attack generally are considered to comprise. Many of the arguments for what the concepts are understood to include have also been applied to whether a computer network attack can be considered as an armed attack or not. By concluding that the UN Charter and customary international law are two different bodies of law and the concepts of use of force and armed attack exist in both of them I have found that a certain flexibility of the interpretation of the concepts have helped developing

[225] Tallinn Manual, Chapter II, Section 2, Rule 13, para 16 (both).
[226] Ibid., Rule 13, para 16 (both) and S/RES/1373 (2001) and S/RES/1368 (2001).
[227] Tallinn Manual, Chapter II, Section 2, Rule 13, para 16-17.
[228] Advisory Opinion on the Palestinian Wall, para 139.

international law on resort to force by making it applicable to new technologies and new types of warfare. Even though the content of the concepts may be similar in both bodies of law there may be differences nonetheless. While the Charter is applicable to the states that are members of the UN, customary international law is applicable to non-member states. However, principles of customary law, not codified in the Charter, are applicable to all states.

One of the arguments for applying the concept of armed attack to computer network attacks, borrowed from both the Advisory Opinion on Nuclear weapons and the Definition of Aggression, is that the weapon used is not of decisive matter. The Charter and customary international law and the concepts of use of force and armed attack have previously been applied to nuclear weapons, biological weapons and similar weapons that do not directly fall under the wording of the Charter. The ability to apply the concepts of use of force and armed attack to such means shows international law's ability to adjust to new types of warfare and societal norms at the time being and that the law governing resort to force develops over time, alongside with society. Even acts performed by non-regular forces have been declared as possibly reaching the level of an armed attack as long as the scale and effects are comparable with an armed attack and it is a cross border incident. In my opinion, cyber commands may be equated with non-regular forces. Their actions can probably have similar effects as an armed attack if, for example, disrupting traffic lights, which result in fatalities or large-scale destruction.

I believe that international law will develop from an instrument-based approach to an effects-based approach in order to be able to interpret the concepts of use of force and armed attack in regards to computer network attacks. However, a difficulty with the effects-based approach will be to foresee all potential effects of computer network attacks.

The general scale and effects criteria are among the strongest criteria put forward by authors for applying the concept of armed attack to computer network attacks. When the scale and effects of a computer network attack are of such gravity as to amount to an armed attack most authors find it logical that the victim-state has a right to defend itself with armed force or with computer network attacks. If the object of a computer

network attack is humans or property and the result is fatalities or destruction of property the act can amount to an armed attack. Some authors propose that economic coercion can reach the level of an armed attack and that a computer network attack, with an effect like a stock market crash, may be an armed attack. However, since it is difficult to foresee all potential effects and compare them to other effects it is best to consider every case separately.

As there is no clear definition of the concept of armed attack a few other general criteria have been put forward and been applied to computer network attacks in order to decide if an act is considered as an armed attack. These criteria are: sufficient gravity, intention and scope, duration and intensity. After conducting this research I have found that there is no consensus about intention as criterion while scope, duration and intensity as well as the criterion of sufficient gravity still seem to have certain importance when considering a computer network attack as an armed attack. Also the criterion that if computer network attacks are referred to as weapons or warfare have been applied by some authors.

In regard to the use of force the most central question is whether the concept should be interpreted in a restrictive or permissive way - if the term covers only armed force or if other forms of force are included as well, for example economic coercion. This question is also key when arguing *against* the application of the concept of armed attack to computer network attacks, namely, that the concept should be interpreted in a restrictive way and exclude every use of force that is not directly understood as armed force. The restrictive interpretation reserves the right to self-defence to the worst cases to avoid stretching the meaning of the concepts. Against this argument it is argued that the travaux préparatoires of the Charter did not exclude other forms of force than armed force.

Many states already have cyber commands or cyber units and military strategies concerning computer network attacks and I believe that this can indicate on a development of state practice considering computer network attacks as a use of force and an armed attack. I would not, with my knowledge, say that the state practice is very well developed but I believe that it will develop increasingly the coming years as more states develop cyber capabilities and therefore also become states with specially

affected interests.[229] Regarding opinio juris I find it hard to state if this is developed or not regarding computer network attacks as an armed attack. I believe that the U.S. will play an important part in the development of customary international law on computer network attacks because the U.S. is a leading country in computer network technology and has already stated that, in military strategies and public announcements from President Obama, that it will defend itself from computer network attacks.

According to customary international law a threat must be imminent in order to have the right to use self-defence in anticipation of an armed attack. The self-defence must be necessary and proportionate to the threat perceived. These principles will also be applied to computer network attacks if they are considered as an armed attack. However it will be difficult to estimate what is necessary and proportionate self-defence against an attack that is hard to detect and difficult to attribute to another state and an attack of which the effects are difficult to foresee.

I can conclude that in this paper I have been referring to sources in general positive to the possibility to apply the concepts of use of force and armed attack in the UN Charter and customary international law to computer network attacks. Opposing arguments are mainly found in the general restrictive view of the use of force and armed attack. Maybe we can expect an Advisory opinion from the ICJ or resolution from The General Assembly or Security Council regarding computer network attacks in a not too distant future.[230]

A problem with international law, significant regarding computer network attacks, is that it is constructed to only concern state actors while non-governmental groups are excluded form this part of law. This is problematic as these groups may also use, and already do use, computer network attacks for whatever purpose they might have.[231] However, the applicability of international law to non-state actors is already discussed in the international community. We might see a change in the treatment and the right to act towards these groups as international law develops. To illustrate the presence of

[229] See footnote 179 and North Sea Continental Shelf, para 174.
[230] UN Charter, article 96.
[231] For example the group Anonymous's attacks on Sweden in October 2012, see footnote 26.

non-state actors I would like to quote the Anonymous with a quote taken from a film published just before the group's attacks on Sweden:

" … WE ARE LEGION
WE DO NOT FORGIVE
WE DO NOT FORGET
EXPECT US."[232]

[232] The Anonymous, YouTube film published October 3, 2012.

5 Bibliography

5.1 Doctrine

AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS, MAY 1999, US Department of Defense Office of General Counsel, www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf, accessed 2012-11-29, 15.27.

A New Kind of Warfare, The New York Times, September 9, 2012.

Asleep at the Laptop, PREET BHARARA, The New York Times, Published: June 3, 2012, http://www.nytimes.com/2012/06/04/opinion/preventing-a-cybercrime-wave.html?_r=0, accessed 2012-12-10, 22.57.

”Attack” as a Term of Art in International Law: The Cyber Operations Context, Michael N. Schmitt, NATO CCD COE Publications, 2012, https://www.usnwc.edu/Academics/Faculty/Michael-Schmitt.aspx, accessed 2012-12-06, 14.24.

Börsen nästa mål för nätattackerna, Ia Wadendal, Svenska Dagbladet, 2012-10-05, http://www.svd.se/nyheter/inrikes/natattackerna-har-tjuvstartat_7557320.svd, accessed 2012-10-05, 15.45.

Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right to Self-Defense, Eric Talbot Jensen, Stanford Journal of International Law 38:207, 2002.

Computer Network Attack and the Use of Force in International Law – Thoughts on a Normative framework, Michael n. Schmitt, Columbia Journal of Transnational Law, [37:885 1999], 1999, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1603800, accessed 2012-12-07, 13.46.

Cyberattacker ett stort växande hot, Tobias Olsson, Svenska Dagbladet, 2012-10-08, http://www.svd.se/nyheter/inrikes/cyberattacker-ett-stort-vaxande-hot_7561104.svd, accessed 2012-10-08, 12.14.

Cyber Operations and the Jus in Bello: Key issues, Michael N. Schmitt, Naval War College International Law Studies, 2011, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1801176, accessed 2012-12-10, 21.00.

Cyber Threats and the Law of War, David E. Graham, JOURNAL OF NATIONAL SECURITY LAW & POLICY [Vol. 4:87 2010], http://www.google.fr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CFUQFjAB&url=http%3A%2F%2Fwww.jnslp.com%2Fwp-content%2Fuploads%2F2010%2F08%2F07_Graham.pdf&ei=3LbZT4P2L5Sh8gOk0YT7AQ&usg=AFQjCNF26YPFlXDYuN3aH9oZsM9eVRhJkw, or http://www.jnslp.com/2010/08/13/cyber-threats-and-the-law-of-war/, accessed 2012-10-09, 13.47.

Cyber Warfare and the Laws of War, Heather Harrison Dinniss, Cambridge University Press, 2012.

Cyberwarfare and International Law, Melzer Nils, UNIDIR Resources, Ideas for peace and security, 2011.

Cyberwarfare Emerges From Shadows for Public Discussion by U.S. Officials, Scott Shane, The New York Times, September 26, 2012.

Department of Defense Dictionary of Military and Associated Terms, 8 November 2010 (As Amended Through 15 August 2012), Joint Publication 1-02.

Estonia fines man for ”cyber war”, BBC News, http://news.bbc.co.uk/2/hi/technology/7208511.stm, Last Updated: Friday, 25 January 2008, 10:31 GMT, accessed 2012-10-17, 11.40

Estonia hit by ”Moscow cyber war”, BBC News, http://news.bbc.co.uk/2/hi/europe/6665145.stm, Last Updated: Thursday, 17 May 2007, 15:21 GMT 16:21 UK, accessed 2012-10-17, 11.44.

Europa går samman i Cyber Europe 2012, ENISA powered by CISION, 4 okt, 2012 09:00 CET, http://www.cisionwire.se/enisa---european-network-and-information-security-agency/r/europa-gar-samman-i-cyber-europe-2012,c9312812, accessed 2012-10-19, 11.22.

Färre svenskar skaffar Facebook, Caroline Karlsson, Göteborgs Posten, 2012-10-17, http://www.gp.se/nyheter/sverige/1.1098828-farre-svenskar-skaffar-facebook, accessed 2012-10-17, 13.18.

Global Project on Cybercrime (Phase 2) 1 March 2009 – 31 December 2011 Final project report, Council of Europe, Strasbourg, 9 April 2012 Provisional, http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/default_en.asp, accessed 2012-12-11, 10.04.

Hemligt förband ska skydda från it-hot, Tobias Olsson, Svenska Dagbladet, 2012-12-04, http://www.svd.se/nyheter/inrikes/hemligt-forband-ska-skydda-fran-it-hot_7723550.svd, accessed 2012-12-04, 11.44.

Hot om stor aktion på fredag, Svenska Dagbladet, 2012-10-03. http://www.svd.se/nyheter/inrikes/hot-om-stor-natattack-pa-fredag_7552202.svd, accessed 2012-10-05, 15.54.

International Law, Antonio Cassese, Oxford University Press, 2nd Edition, 2005.

International Law and the Use of Force by States, Ian Brownlie, Oxford University Press, 2002.

Internets mörka sidor Om cyberhot och informationskrigföring, Roland Heickerö, Bokförlaget Atlantis AB, 2012.

Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, I.C.J. Reports 2004, p. 136.

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1.C.J. Reports 1996, p. 226.

Nuclear Posture Review Report, April 2010, Department of Defense, United States of America, https://www.google.com/search?q=Barack+Obama%27s+2010+Nuclear+Posture+Review&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:sv-SE:official&client=firefox-a, accessed 2012-10-17, 13.34.

Obama Order Sped Up Wave of Cyberattacks Against Iran, The New York Times, DAVID E. SANGER, June 1, 2012. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=1&pagewanted=all, accessed 2012-09-07, 10.34.

Stuxnet virus: worm 'could be aimed at high-profile Iranian targets', Claudine Beaumont, The Telegraph, 23 September 2010, http://www.telegraph.co.uk/technology/news/8021102/Stuxnet-virus-worm-could-be-aimed-at-high-profile-Iranian-targets.html#, accessed 2012-10-17, 15.29

Svenska hackare En berättelse från nätets skuggsida, Daniel Goldberg and Linus Larsson, Norstedts, 2012.

Svenskarna och Internet 2012, Olle Findahl, .se Stiftelsen för Internetinfrastruktur, version 1.0, 2012.

Tallinn Manual on International Law Applicable to Cyber Warfare, Prepared by the International Group of Experts at the Invitation of The NATO Cooperative Cyber Defence Center of Excellence, General Editor Michael N. Schmitt, Cambridge University Press, 2013.

Teknikfrälst innan han kan gå, Caroline Karlsson, Göteborgs Posten, 2012-10-17.

Textbook on International Law, Martin Dixon, Oxford University Press, 2007 6th edition.

The Cybercrime Wave That Wasn't, DINEI FLORÊNCIO and CORMAC HERLEY, The New York Times, Published: April 14, 2012, http://www.nytimes.com/2012/04/15/opinion/sunday/the-cybercrime-wave-that-wasnt.html, accessed 2012-12-10, 23.02.

The Law of Information Conflict – National Security Law in Cyberspace, Thomas C. Wingfield, Aegis Research Corporation, 2000.

The real Iranian threat: Cyberattacks, David Goldman, CNN Money, 5 November 2012, http://money.cnn.com/2012/11/05/technology/security/iran-cyberattack/index.html?hpt=hp_c4, accessed 2012-11-23, 21.10.

U.S. Suspects Iran Was Behind a Wave of Cyberattacks, Thom Shanker and David E. Sanger, The New York Times, October 13, 2012. http://www.nytimes.com/2012/10/14/world/middleeast/us-suspects-iranians-were-behind-a-wave-of-cyberattacks.html?pagewanted=2, accessed 2012-11-12, 11.37.

World Wide Warfare - Jus ad bellum and the Use of Cyber Force, Marco Roscini, A. Von Bogdandy and R. Wolfrum, (eds.), Max Planck Yearbook of United Nations Law, Volume 14, 2010, p. 85-130, Koninklijke Brill N.V. 2010.

5.2 Legal texts

Charter of the United Nations.

Convention on Cybercrime, Council of Europe, Budapest, 23.XI.2001.

A/RES/25/2625, 24 October 1970, Resolution adopted by the General Assembly [Adopted on a Report from the Sixth Committee (A/8082)], 2625 (XXV). Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, http://www.un-documents.net/a25r2625.htm, accessed 2012-10-29, 09.30.

A/RES/29/3314, 14 December 1974, Resolution adopted by the General Assembly, [Adopted without a vote on a Repoort from the Sixth Committee], 3314 (XXIX). Definition of Aggression, United Nations, http://www.un-documents.net/a29r3314.htm, accessed 2012-10-29, 09.50.

A/RES/36/103, 9 December 1981, Resolution adopted by the General Assembly 36/103. Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States.

A/RES/42/22, 18 November 1987, General Assembly, Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations.

A/RES/55/63, 22 January 2001, Resolution adopted by the General Assembly, [on the report of the Third Committee (A/55/593)] Combating the criminal misuse of information technologies.

A/RES/64/25, 14 January 2010, Resolution adopted by the General Assembly [on the report of the First Committee (A/64/386)] 64/25. Developments in the field of information and telecommunications in the context of international security.

S/RES/487, Resolution 487 (1981) of 19 June 1981, Adopted by the Security Council at its 2288th meeting on 19 June 1981.

S/RES/0661 (1990), Resolution 661 (1990) of 6th August 1990, Adopted by the Security Council at its 2933rd meeting on 6 August 1990, The situation between Iraq and Kuwait.

S/RES/1368 (2001), Resolution 1368 (2001), Adopted by the Security Council at its 4370th meeting, on 12 September 2001.

S/RES/1373 (2001), Resolution 1373 (2001), Adopted by the Security Council at its 4385th meeting, on 28 September 2001.

The North Atlantic Treaty (1949), Washington D.C. - 4 April 1949

The Statute of the International Court of Justice, http://www.icj-cij.org/documents/index.php?p1=4&p2=2&p3=0#CHAPTER_II, accessed 2012-12-04, 12.44.

Vienna Convention on the Law of Treaties 1969, Done at Vienna on 23 May 1969. Entered into force on 27 January 1980. United Nations, Treaty Series, vol. 1155, p. 331, United Nations 2005.

5.3 Case law

Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgment, I.C.J. Reports 2005, p. 168.

Caroline case, 1837.

Corfu Channel case, Judgment of April 9th, 1949: I.C.J . Reports 1949, p. 4.

Fisheries case, Judgment of December 18th, I95I: I.C.J. Reports 1951, p. 116.

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986, p. 14.

North Sea Continental Shelf, Judgment, I.C.J. Reports 1969, p. 3.

Oil Platforms (Islamic Republic of Iran v. United States of America), Judgment, I.C.J. Reports 2003, p. 161

5.4 Websites

Cambridge Dictionaries Online, http://dictionary.cambridge.org/dictionary/british/kinetic?q=kinetic, accessed 2012-12-11, 10.38.

International Court of Justice, ICJ http://www.icj-cij.org/jurisdiction/index.php?p1=5&p2=1, accessed 2012-10-10, 14.21 and http://www.icj-cij.org/jurisdiction/index.php?p1=5&p2=2, 2012-12-20, 17.04.

NATO
http://www.nato.int/cps/en/natolive/topics_78170.htm, accessed 2012-10-19, 11.02.

NATO Cooperative Cyber Defence Centre of Excellence
http://www.ccdcoe.org/cycon/272.html, accessed 2012-10-17, 09.30.

Oxford English Dictionary,
http://www.oed.com.ezproxy.ub.gu.se/view/Entry/103498?redirectedFrom=kinetic#eid, accessed 2012-12-18, 14.21.

REMARKS BY THE PRESIDENT ON SECURING OUR NATION'S CYBER INFRASTRUCTURE, East Room, THE WHITE HOUSE, Office of the Press Secretary, May 29, 2009, http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure, accessed 2012-11-29, 13.32.

U.S Army Cyber Command, U.S 2nd Army
http://www.arcyber.army.mil, accessed 2012-10-19, 10.21.

Youtube, Anonymous, film published October 3, 2012,
http://www.youtube.com/watch?v=LPzdbDSk6Hg, accessed 2012-12-20, 16.32.

For further reading:

- On the question regarding computer network attack as ”use of force”:
  - Computer Network Attack and Use of Force in International Law, Schmitt
  - Cyberwarfare and International Law, Melzer.
  - Tallinn Manual.

- On the question regarding right to self-defence in response to use of force not amounting to armed attack:
  - The Law of Information Conflict, Wingfield
  - Computer Network Attack and Use of Force in International Law, Schmitt, footnote 123.
  - ”Attack” as a Term of Art in International Law, Schmitt.

- On the question regarding Security Council’s possibility to engage countermeasures in case of computer network attack:
  - Computer Network Attack and Use of Force in International Law, Schmitt.

Proof of Registration

I was registered on the course Master thesis, 30 ECTS for the first time during the fall semester 2012. The first lecture that I attended was on August 29, 2012. I have not been reregistered or participated in any examinations previous to the current one.

Sincerely,

Ebba Josefson