Bits Before Bombs:

Cyber-attack as a Breach of Article 2(4) of the UN Charter

Candidate number: 78

Word count: 11 718

JUS399 Master's Thesis
Faculty of Law

UNIVERSITY OF BERGEN

10.5.19

Table of contents

1 Introduction

1.1 Introduction to the problem, research question and relevance

This thesis analyses cyber-attacks as a means of war. More concretely, the issue raised in this thesis is if, and when, cyber-attacks can constitute a breach of "use of force" in Article 2(4) of the United Nations (UN) Charter. The thesis will focus on the application of cyber-attacks by States that target other States.

The UN Charter was created as a result of the Second World War, and thus the prohibition on the use of force was directed at classic and weapons known at the time. The breakthrough of the internet changed the rules for many industries, and war is no exception. With the development of cyber combat, far from the traditional concept of conventional weapons and explosives, cyberspace has become a new domain for military operations. Today, wars are fought at sea, on land, in the air, across space and in the emerging battleground of cyberspace. In modern society, we are heavily reliant on technology and the increased digitalisation of society means that vulnerability to hateful intrusions has also grown. This has made the use of digital weapons a rising global problem. The vulnerabilities can range between an individual level with stolen personal information to state-level with larger political motivated digital attacks.

Cyber-attacks can be a serious threat to national security, and as a result, States and academics are beginning to treat cyber-attacks as acts of war. However, cyber combat does not look like the historic perception of what constitutes war, and this creates an issue in regard to the regulations monitoring armed conflicts. Traditionally, the law of war has mainly been regulated by treaties, international customary law and fundamental principles. Key principles in humanitarian law include the need for military necessity,[1] a distinction between combatants and non-combatants[2] and proportionality between the harmed caused and the expected military advantage.[3]

[1] International Committee of the Red Cross (2009) Rule 70
[2] International Committee of the Red Cross (2009) Rule 1
[3] International Committee of the Red Cross (2009) Rule 14

With the rise of opportunities connected to technology, both practitioners and scholars acknowledge that cyber warfare plays by new rules. And the rules are not necessarily fair: cyber combat does not usually distinguish between States and private individuals or corporations as targets. The perpetrators of the attack often do not care about the harm caused. Further, the attacks are often even conducted by the military of another State and can be committed by anyone with internet access.

In February 2018, UN Secretary-General António Guterres stated that

> *"When one looks at today's cyberspace, it is clear that we are witnessing, in a more or less disguised way, cyberwars between States - episodes of cyberwar between States.*
>
> *The fact that is we have not yet been able to discuss whether or not the Geneva Conventions apply to cyberwar or whether or not international humanitarian law applies to cyberwar."*[4]

So far, no State has claimed to be targeted with "use of force" or be under "armed attack"[5] of the cyber forces from another State. This thesis questions if, and when, cyber-attacks become "use of force", as stipulated in the UN Charter?

1.2 Terminology

There is no definite legal definition of what a cyber operation or a cyber-attack is. However, there have been many attempts to define the term, both by the military of various States and by academics. The Tallinn Manual[6] defines overall cyber-operations as "[w]hether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects".[7] *Merriam Webster* defines a cyber-attack as "[a]n attempt to gain illegal access to a computer or computer system for the purpose of causing damage or harm".[8] Additionally, the United States Army defines it as "[t]he premeditated use of disruptive activities, or the threat thereof, against computer and/or networks, with the intention to cause harm or to further social, ideological, religious, political or similar objectives, or to intimidate

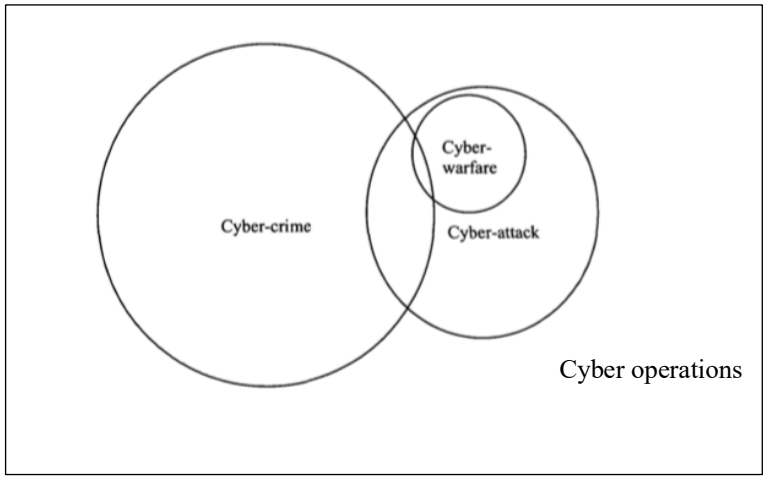
[4] Guterres (2018)
[5] UN Charter Article 51
[6] a non-binding, academic study on how international law applies to cyber operations, read more under section 1.4
[7] Tallinn Manual (2017) Rule 92
[8] Merriam Webster (undated A)

any person in furtherance of such objectives".[9] Meanwhile, the German Cyber Security Strategy defines a cyber-attack as "[a]n IT attack in cyberspace directed against one or several other IT systems and aimed at damaging IT security – confidentiality, integrity and availability – which may all or individually be compromised".[10] Lastly, Waxman defines cyber-attacks as "[e]fforts to alter, disrupt, or destroy computer systems or networks or the information or programs on them".[11]

It is clear that the definition laid out by the Tallinn Manual is not limited to software only. The definition by *Merriam Webster* does not seem to distinguish between unsuccessful and successful attempts, and it states that the attack has to have an intention behind it, without mentioning what these intentions may entail. The American definition goes further by laying out a set of intentions behind the attack. This way, the definition only applies to attacks falling within the mentioned intentions and, accordingly, delimitates towards other intentions. The definition laid out by Waxman, together with the United States Army definition, both open up for including threats and efforts at an attack. Finally, it is worth mentioning that cyber is highly influenced by geopolitics. Due to the variation in definitions of what a cyber-attack is, this thesis defines cyber-attack as the following.

There are three main segments of cyber operations: cyber-crime, cyber-attack and cyber warfare.[12] In order to properly define the segments, it is important to distinguish between them.

Figure 1: Cyber operations[13]



[9] US Army Training & Doctrine Command (2005) section VII-2
[10] German Federal Ministry of the Interior (2011) pp.14-15
[11] Waxman (2011) pp. 421-422
[12] Hathaway (2012) p. 834
[13] Inspired by Hathaway (2012) on pp. 833, but an additional layer has been added.

Cyber-crime is understood as the use of computer-based means to commit an illegal act conducted only by non-State actors.[14] For example, committing crimes by using a computer system, computer network or hardware device.[15] Cyber-crime thus comprises a broad variety of illegal activities, for instance, online piracy, storage and sharing of child pornography and computer intrusions. This means that cyber-crime is committed by individuals without any political or national purpose and are often illegal under national and/or international law.

Cyber-attacks may be conducted by either State or non-State actors. They must involve active conduct and aim to undermine the function of a computer network with a political or national security purpose.[16] It is clear from Figure 1 that some cyber-attacks are neither cyber-crime or cyber-warfare, and two scenarios fall within this category. The first scenario is when a cyber-attack outside the context of an armed attack, is carried out by a State actor, provided its effects do not rise to the level of an armed attack. It would still have to fulfil all elements of a cyber-attack, such as undermining the function of a computer network for a political or national security purpose. The Chinese governments attack on the Falun Gong website in 2011 falls into this category.[17] The second scenario is when a cyber-attack is conducted by non-State actors and it does not rise to the level of an armed attack and does not constitute a cyber-crime. This may be because the act is not criminalised under national or international law, or because they do not use computer-based means.[18] Since there are gaps in criminal law, this is possible. As this thesis limited to State vs. State actors, only the former scenario will be reviewed.

Cyber-warfare is distinctive because it must also constitute a cyber-attack. The overlap between cyber-attack and cyber-crime in the figure entails two types of attacks. First, cyber-attacks carried out by any actor in the context of armed conflict, provided that those actions could not be considered as cyber-crimes. This is either because they do not use computer-based means or they do not constitute war crimes or both. Second, a cyber-attack carried out by a State actor with effects equivalent to those of a conventional "armed attack".[19] In sum,

[14] Hathaway (2012) pp. 833-4
[15] Gordon (2006) p. 14
[16] Hathaway (2012) p. 836
[17] Hathaway (2012) p. 835
[18] Hathaway (2012) p. 835
[19] Hathaway (2012) p. 836

not all cyber-attacks are cyber-warfare and only cyber-attacks with effects equivalent to those of a conventional "armed attack", or occurring with the context of armed conflict, reaches the necessary threshold.

The small, overlapping area between all three kinds of attack in the figure will not be elaborated because this is scenarios carried out by a non-State actor.

1.3 Delimitation of the research question

The scope of this thesis will be delimited in several ways. Firstly, this study is limited to State vs. State cyber-attack scenarios only. The reason is that international armed conflicts (IACs) constitute a well-regulated area of international law and these rules have been further studied and developed, also when it comes to cyber operations.

Second, this thesis will be delimitated to the study of cyber-attacks, and therefore will not explore the legal area of cyber-defence or other forms of cyber operations. This is because it is not possible within the scope of this thesis to evaluate other forms of cyber operations.

This thesis will also focus on *jus ad bellum* and will not analyse *jus in bello*. This focus means that this thesis will not evaluate what would be the correct responses to the use of force conducted by cyber-attacks.

Finally, cyber-attacks are a fast-developing area and this thesis will, therefore, be limited to the knowledge that was available 20. April 2019.

1.4 Methodology

The main methodological challenge with this thesis is that there is currently no international law regulating the field of cyber operations. To attempt to overcome this gap, an international group of approximately twenty experts met at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) and created the Tallinn Manual – a non-binding, academic study on how international law applies to cyber operations. The Tallinn Manual was published by Cambridge University Press in 2013 and focuses especially on *jus ad bellum*. Accordingly, the Tallinn Manual is an essential source in this thesis. In February 2017, the Cambridge University Press published the Tallinn Manual 2.0. The successor is designed to expand the scope of the Tallinn Manual and is the version referred to in this thesis.

Building on the understandings of the Tallinn Manual 2.0, this thesis will also rely on extensive literature analysis. Cyber operations are a relatively new legal area with rapid developments and challenges, yet, there are already some prominent researchers in the field.

To finish, it is worth mentioning that this field is highly influenced by geopolitics and within a legal area in rapid development. The cyber strategies of each State are designed to ensure the States' interests and it is also possible to draw a line between the State's cyber strategy and their warfare history.

1.5 The structure of the thesis

Due to the complexities in this thesis in regard to the technical terms, it will start by giving an introduction to cyber operations. This will consist of an explanation of how a cyber-attack is carried out before it is explained who can be considered as involved when it is only state actors.

This thesis will then turn to the main focus, which is Article 2(4) of the UN Charter in regard to cyber-attack. First, there will be an examination of the concept "use of force" in Article 2(4) before moving on to an analysis of "use of force" in relation to cyber-attack. After this, there will be a concrete analysis of two cases where cyber-attack led to very different results. Finally, this thesis will try to explore what a cyber-attack might lead to in the future of warfare.

2 An introduction to cyber operations

2.1 How

There are different ways to conduct cyber-operations, both offensive and defensive. Most cyber agencies run by States, such as the Norwegian Cyber Defence,[20] use the Cyber Kill Chain framework. This model was developed by Lockheed Martin and functions as the methodology for identifying and understanding how an attacker will try to cause harm in order to prevent it. A Kill Chain is a "[s]ystematic process to target and engage an adversary to create desired effects".[21] The method gives the defender an advantage by knowing its opponent's next move.

The Kill Chain consists of seven steps, and in order to demonstrate the model properly, the explanation will in the following focus on the attacker's point of view.

First, in the reconnaissance stage, the attacker conducts research by assessing the potential target from outside the organisation.[22] This research is both technical and non-technical, and the attacker may visit websites such as conference proceedings and mailing lists for social relationships or information of a specific technology.[23] The attacker works to determine which target will return the most asset for the resources consumed in manipulating the target's systems.

Second, the weaponization stage. The attacker develops a malware that is specifically designed to exploit the vulnerabilities already discovered during the previous step.[24]

Third, the delivery stage involves transmitting the malware from the attacker to the targeted system for exploitation.[25] The most used delivery vector observed by Lockheed Martin for the years 2004-2010 are websites, USB removable data and email attachments,[26] and a cyber-attack is most likely to target an internal employee of an organisation.[27]

[20] See for instance Nikolaisen (2016)
[21] Hutchins (undated)
[22] Death (2018)
[23] Hutchins (undated)
[24] Hutchins (undated)
[25] Death (2018)
[26] Hutchins (undated)
[27] Death (2018)

Fourth, during the exploitation phase, the malware is delivered to the targeted victim and the execution can start.[28] The attacker takes advantage of the discovered vulnerabilities in the system to gain superuser access to the information system.[29]

Fifth, in the installation stage the malware installs itself onto the targeted information system,[30] and by doing this, it has created a backdoor. Now it can download additional software if network access is possible. This allows the malware to stay small and undetectable.[31]

Sixth, during the command and control (C2) stage, the attacker has put in place their management and communication code onto the targeted network.[32] This gives the attacker the possibility to have "hands on the keyboard" access inside the system,[33] just like regular employees.

Seventh, the action on objectives stage where an attacker can take actions to achieve their original goals.[34] This might include collecting and extracting information, destruction of the information systems[35] or DDoS, which is coordinated botnets ("zombie" computers) hijacked by viruses overwhelming servers by visiting the website multiple times.[36]

[28] Hutchins (undated)
[29] Death (2018)
[30] Hutchins (undated)
[31] Death (2018)
[32] Death (2018)
[33] Hutchins (undated)
[34] Hutchins (undated)
[35] Death (2018)
[36] Hathaway (2012) p. 837

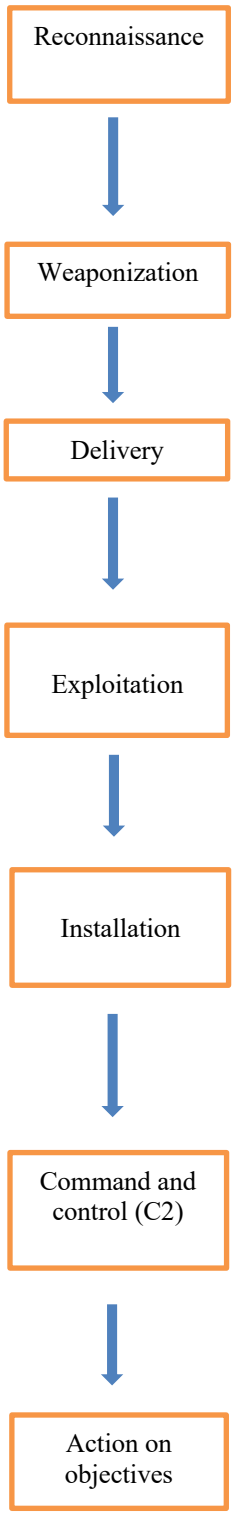


Figure 2: Cyber Kill Chain[37]

[37] Lockheed Martin (undated)

2.2 Who

During a cyber-attack, finding out who your enemy is could be one of the hardest tasks. The International Group of Experts agree that the customary international law of State responsibility undeniably extends to cyber activities.[38] As a result, three different scenarios referring to the right of States have been identified by various academics.

First, is the case of "uniformed" hackers. It is widely known that several States have developed their own cyber units within their national army. For instance, Norway has its own Cyber Defence,[39] China has a Strategic Support Force,[40] the US-appointed its first cyber warfare general almost a decade ago,[41] Israel is investing heavily in its Cyber unit in the Israeli Defence Force,[42] and in finally, Germany has its own Cyber unit.[43] This scenario will be included further in this thesis.

Second, the law of State responsibility also applies to cyber-attacks conducted by a non-State actor if the State factually exercises "effective control" over that specific conduct of the non-State actor.[44] This includes individuals or corporations hired by States to conduct cyber-attacks on the State's behalf. However, when can the actions by individuals or corporations be associated with the State? According to the International Law Commission (ILC) treaty on the Responsibility of States for Internationally Wrongful Acts Article 8, "[t]he conduct of a person or group of persons shall be considered an act of a State under international law if the Person or group of persons, is in fact, acting on the instructions of, or under the direction or control of, that State in carrying out the conduct".[45]

In the *Nicaragua* case, the Court was able to clarify that when State A gives assistance to rebels seeking to overthrow the government of State B, this assistance to the rebels may be indirect use of force contrary to customary international law. The evaluation must be based on the kind of assistance provided by State A to the rebels.[46] In the *Nicaragua* case, the court considered it was sufficient that the United States armed and trained the rebels.[47] In the

[38] Tallinn Manual (2017) p. 80
[39] Forsvaret (undated)
[40] Lyall (2018)
[41] Beaumont (2010)
[42] VICE News (2018)
[43] DW News (2018)
[44] Tallinn Manual (2017) Rule 17
[45] International Law Commission Article 8
[46] *Nicaragua v. United States of America* para 228
[47] *Nicaragua v. United States of America* para 228

International Criminal Tribunal of Yugoslavia (ICTY), in the case of *Tadić*, the Court declared that "[t]he degree of control may (…) vary according to the factual circumstances of each case".[48] Further, the Court expressed in their concluding assessment that when the actions of individuals and corporations can be tied to the State, the State "has a role in organising, coordinating or planning the military actions of the military group, in addition to financing, training and equipping or providing operational support to that group (…) regardless of any specific instruction by the controlling State concerning the commission of each of those acts".[49] One example is the Russian Business Network, a firm specialising in identity thefts, malicious malware, phishing and botnet command-and-control, suspected of executing the attacks towards Georgia.[50] This scenario will also be developed further in this thesis.

The final scenario is not attributable to the state so it will not be developed further in this thesis. Briefly, it involves hackers whose conduct has been encouraged by State agents, for example, by emails, chat rooms and websites. This means that they are neither *de jure* nor *de facto* State organs. One example is from 2001 when a U.S. Navy spy plane collided with a Chinese jet fighter in the South China Sea, and websites appeared to be offering instructions to hackers on how they could cripple U.S. government computers.[51]

One of the main problems with cyber operations concerns the identification of the origin of the attack, and this is also one of the main obstacles when applying Article 2(4) of the UN Charter. For the purpose of this thesis, however, it will be assumed that a cyber operation has been attributed to a State actor, as demonstrated in this subchapter.

[48] *Prosecutor v. Tadić* para 117
[49] *Prosecutor v. Tadić* para 137
[50] Roscini (2010) p.100
[51] Roscini (2010) p.101

3 UN Charter Article 2(4) – "use of force"

3.1 General

Article 2(4) of the UN Charter states that

> *"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."*

The prohibition of using force is seen as a pillar in international law, and it calls for the Members of the UN to refrain from "threat or use of force" against the territorial integrity and political independence of any State, the values particularly protected by the Charter.[52] The UN Charter does not provide a definition or criteria of "threat or use of force" and therefore it is important to examine what lies in the wording of "force". The general criteria for the interpretation of treaties is described in the 1969 Vienna Convention on the Law of Treaties, and it states that a treaty shall be interpreted in "good faith" in accordance with the "ordinary meaning" to the terms of the treaty in the "context and light" of its "object and purpose".[53]

The wording of the term "force" is ambiguous, and in light of the literal criteria and context, the results are inconclusive. In *Black's Law Dictionary*, "force" is defined as "[p]ower, violence or pressure directed against a person or thing".[54] This definition implies that "force" can entail a variety of actions, including measures of economic and political coercion.[55] By looking at the context of the term, it is also used in the Preamble of the UN Charter, as well as in Articles 41 and 46 where it is preceded by the adjective "armed". On the other hand, in Article 44, the reference is clearly to armed force only because it is stated. This distinction between *armed force* and *force* in the UN Charter may imply that the drafters wanted to separate the two and that they, therefore, wanted to refer to a broader notion of force in Article 2(4).

However, the Preamble of the UN Charter states that its overall purpose is to "[s]ave succeeding generations from the scourge of war", not to ban all forms of coercion. This

[52] Asrat (1991) p. 47
[53] Vienna Convention Article 31(1)
[54] Garner (1999) p. 673
[55] Ziolkowski (2012) pp.7-8

supports a narrow understanding of the provision, resulting in a limitation to military force only. It strengthens this understanding of the term by examining several UN General Assembly resolutions, such as the Declaration on Friendly Relations, which states that political and economic coercion shall not be considered as an aspect of the use of "force", but rather of the principle of non-intervention in domestic affairs of another State.[56] Despite the fact that the resolutions are non-binding documents,[57] the various resolutions may be seen as relevant to the interpretation as "subsequent practice" of the UN Member States.[58] Further, a proposal by Brazil to extend the prohibition on force to also include economic coercion was explicitly rejected at the San Francisco Conference.[59] In sum, the ordinary meaning, drafting history and relevant UN documents imply that the "use of force" is limited to military force only.

Today it is principally undisputed that the prohibition on the use of force is considered *jus cogens*. The status means that no State can contract out of the obligation to refrain from the use of force.[60] The status as *jus cogens* was first confirmed in the International Court of Justice (ICJ) case *Nicaragua* in 1986. The case started in 1979 when the Sandinista National Liberation Front (the Sandinista) overthrew the regime, leading opponents of the new Sandinista regime to flee to the United States in order to organise themselves as the Nicaraguan Democratic Force (the Contras).[61] Two years later, the Sandinista supported armed groups in El Salvador and Ronald Reagan, the sitting President of the United States at the time, chose to stop all American aid to Nicaragua because the United States had good relations to El Salvador.[62] Further, Nicaragua allowed the Soviet Union to pass arms through their ports and territory on the way to El Salvador, which created another layer to the already tense Cold War. Nicaragua made a claim to the ICJ in April 1984.

The ICJ ruled, *inter alia*, that the United States had violated the prohibition of the use of force under customary international law and the obligation to refrain from intervention in Nicaragua's sovereignty.[63] In detail, the Court decided that the United States breached its obligation under international humanitarian law not to intervene in the affairs of another State

[56] UN General Assembly A/RES/25/2625 Declaration on Friendly Relations
[57] UN Charter Article 10
[58] Ziolkowski (2012) pp.7-8
[59] Documents of the United Nations Conference on International Organisation (1945) pp.334
[60] Weller (2015) p. 17
[61] Tsagourias (1996)
[62] Harris (2010) p. 727
[63] *Nicaragua v. United States of America* para. 292

by training, arming, equipping, financing and supplying the Contras,[64] but the actions were not together considered as “threat or use of force”. Although financial support given to the Contras by the United States was an established fact, the Court could not comply with itself that the United States “created” the Contras, nor that they gave “direct and critical combat support” in the sense that this support was identical to a direct intervention by the United States military forces, or that all operations carried out by the Contras reflected strategy and tactics constructed by the United States.[65] However, the Court found that certain attacks conducted by the United States in the Nicaraguan territory between 1983-1984 were clearly to be considered as use of force, such as laying out mines.[66]

It is generally accepted that Jean S. Pictet's "scope, duration and intensity" criteria can be used as a starting point for an analysis to identify and classify the degree of use of force. This was also confirmed by the ICJ when it stated that the *scale and effects* are to be considered when determining whether a use of force amounts to an armed attack,[67] and it drew a distinction between an armed attack and *a mere frontier incident*.[68] This means that the attack shall be evaluated after its scale and effects whether it is a “use of force” or if it reaches the threshold of an “armed attack”. Once the use of force reaches the threshold of an armed attack, it triggers the right to individual and collective self-defence.[69]

3.2 Cyber-attacks and “use of force”

This sub-chapter will build on the previous section to discuss how the UN Charter’s provisions on the use of force apply to cyber operations before it explores if and when a cyber operation reaches the threshold of use of force and becomes prohibited under Article 2(4).

According to the Tallinn Manual Rule 68, “a cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful”. As mentioned, this thesis will only address cyber-attack, but this understanding is still in line with the States obligations under Article 2(4) of the UN Charter.

[64] *Nicaragua v. United States of America* para. 292
[65] Harris (2010) p. 733
[66] *Nicaragua v. United States of America* para. 228
[67] *Nicaragua v. United States of America* para. 195
[68] *Nicaragua v. United States of America* para. 195
[69] UN Charter Article 51

Following the wording of Article 2(4), in order for this Article to apply to cyber-attack, three conditions must be met.[70] First, the cyber-attack needs to be attributed to a State. As mentioned in section 2.1, this must either be cyber units within a national army, or individuals or corporations hired by States to conduct a cyber-attack on the State's behalf. This excludes private individuals encouraged by State agents. Second, the cyber-attack must reach the threshold of either a "threat" or "use of force". Finally, the threat or use of force must be put to use in the manner of "international relations".[71] This requires that the threat or use of force must not only be conducted by a State actor, but also against another State. Accordingly, States are not prohibited by Article 2(4) to threaten or resort to a cyber-attack against individuals or groups not connected to a State. This also applies if they amount to a threat or use of force, as long as such attacks do not affect another State's territorial integrity or political independence.[72] The territorial integrity is tied to any intervention, direct or indirect, in the affairs of a State, meanwhile, political independence is connected with people's right to self-determination, freedom and independence.[73]

Further, the International Group of Experts elaborated on this when by stating that cyber-attack "constitutes a use of force when its scale and effects are comparable to non-cyber-attacks rising to the level of a use of force".[74] This means that one must look at conventional attacks that reach the required threshold to understand which criteria a cyber-attack has to meet to be considered as use of force.

Since the "use of force" is traditionally limited to military force only, it must first be examined if and when a cyber-attack becomes the use of military force.

A natural understanding of the term "military forces" is the armed forces of a State. This is in line with *Merriam Webster*'s definition.[75]

Further, the *Black's Law Dictionary* states that "armed" implies"[e]quipped with a weapon" or "[i]nvolving the use of a weapon",[76] and this would be in line with the ordinary meaning of the expression. There is no binding definition of "weapon" in the *jus ad bellum* instruments,

[70] Roscini (2014) p. 44
[71] UN Charter Article 2(4)
[72] Roscini (2014) p. 44
[73] UN General Assembly A/RES/25/2625 Declaration on Friendly Relations
[74] Tallinn Manual (2017) Rule 69
[75] Merriam Webster (undated B)
[76] Garner (1999) p. 123

but the *Black's Law Dictionary* states that is "[a]n instrument used or designed to be used to injure or kill someone".[77] The International Committee of the Red Cross (ICRC) defined that weapons are "[m]eans to commit acts of violence against human or material enemy forces".[78] What is common for both definitions is that they state that it must be involved in an instrument meant to create violent consequences.

The question is then, is Article 2(4) limited to military armed force, or does it extend to cover physical force of a non-military nature? To illustrate what is meant here, one may imagine the White Nile section of the River Nile. The Nile has been essential for life in these countries for centuries and is still important today in order to avoid drought. It starts in the Victoria Lake in Uganda, continues through South Sudan and Sudan before it enters Egypt and finally flows into the Mediterranean Sea. But, imagine that Uganda decides to create a dam in order to make the river stop, leaving Egypt without the Nile. It is reasonable to assume that the action has intentions to influence the territorial integrity of Egypt, but it is clear that there was no military use of force involved.

Randelzhofer argues that this kind of situation can only be accepted within narrow limits and acknowledges that physical force can affect a State just as severely as the use of military force.[79] Nonetheless, the purpose behind Article 2(4), as stated in the article itself, is to ban means of coercion. This is further confirmed in the Preamble of the UN Charter where it is stated that the purpose is to "[s]ave succeeding generations from the scourge of war".[80] The illegal use of force would also, under normal circumstances, follow from other rules, such as the principles of territorial integrity or non-intervention.

However, the ICJ gave a clear statement that Article 2(4) of the UN Charter in its Advisory Opinion on the *Legality of the Use of Nuclear Weapons*: "[weapons] does not refer to specific weapons. They apply to any use of force, regardless of the weapons employed.". The ICJ also expressed that a weapon does not have to be explosive, which would be the case of most biological weapons.[81] In sum, this means that a weapon, independent of composition, can be used as a military force. This is supported by the fact that several States have included cyber

[77] Garner (1999) p. 1730
[78] Henckaerts (2013) p. 49
[79] Randelzhofer (2002) p. 119
[80] UN Charter Preamble
[81] ICJ Reports *Legality of the Threat or Use of Nuclear Weapons* (1996), para 39

operations as a part of their national military strategy, as previously mentioned in section 2.1. It is therefore acceptable to say that a cyber-attack can be considered as a weapon.

After the turn of the millennium, the debate about when cyber-attack should be considered to reach the threshold of "use of force" started to grow. Three approaches are developed by researchers in order to address the issue and attempt to make cyber-attack conform to *jus ad bellum* norms. Whether or not cyber-attack is considered as "use of force" depends ultimately on which of the three analytical approaches is applied.

The instrument-based approach focuses on the means used to conduct an act and has traditionally been employed to distinguish armed force from economic and political coercion.[82] However, this approach has received criticism for being centred on instruments that are defined by their physical characteristics. Further criticism is levelled at this approach because under this view, it has been claimed that the approach cannot be applied on digital codes and that it would lead to the conclusion that cyber-attack never can be considered as "use of force" under Article 2(4)[83] and that a cyber-attack will only be considered as "use of force" if it uses traditional military weapons.[84]

The target-based approach argues that cyber-attacks reach the threshold of the use of armed force when they are conducted against national critical infrastructure, whatever their effects may be.[85] This means that a cyber-attack only needs to deliver malware, as explained in step 3 in Figure 2 and penetrate a critical system to justify a conventional military response.[86] Further, this approach is in line with Article 2(4) of the UN Charter by focusing on the targeted infrastructure. This will be important for both the territorial integrity and political independence of the attacked State. Nonetheless, this approach has been criticised for being overinclusive in that it would also qualify as a use of force those cyber operations that only cause inconvenience or merely aim to collect information whenever they target a national critical infrastructure. Further, there is no generally accepted definition of what constitutes a national critical infrastructure.[87]

[82] Hathaway (2012) p. 845
[83] Handler (2012) pp. 226-7
[84] Hollis (2007) p. 1043
[85] Roscini (2014) p. 47
[86] Hathaway (2012) pp. 846-7
[87] Roscini (2014) p. 47

Finally, the approach with the most support is the effects-based approach. It classifies a cyber-attack as an armed force based on the gravity of its actions.[88] Thus, any cyber-attack that causes or is reasonably likely to cause the damaging consequences normally produced by kinetic weapons would be a use of armed force.[89] This understanding is in line with the *scale and effects* statement in the *Nicaragua* case and Rule 69 in the Tallinn Manual.[90]

In the absence of a conclusive definite threshold, the International Group of Experts has taken notice of the effects-based approach. The Tallinn Manual states that this approach was chosen because it is intended to identify cyber-attack that are analogous to other non-kinetic or kinetic actions that the international community would describe as use of force.[91] On this basis, the effects-based approach will be used further in this thesis.

The effects-based approach was originally developed by Michael Schmitt, and he further developed factors to be used by States while they make use of force assessments. Both the Group of Experts and Schmitt have highlighted that the following factors are not formal legal criteria, but they can contribute to the evaluation of the *scale and effect* of a cyber-attack, as stated in the *Nicaragua* case and the Tallinn Manual.

a) *Severity*. A cyber-attack that "[s]eriously injures or kills a number of persons or that causes significant damage to, or destruction of, property" would satisfy the requirement of scale and effects.[92] Smaller inconvenience or irritation will, however, never reach the threshold. Between these two extremes, the more consequences infringe on critical national interest, as stated in Article 2(4), the more they will contribute to the portrayal of a cyber-attack as use of force. It is in line with international customary law that the scope, intensity and duration of the consequences have a great impact on this factor also while evaluating the cyber-attack.[93] In line with the *Nicaragua* case, the severity of a cyber-attack is the most significant factor in the analysis.

[88] Hathaway (2012) p. 847
[89] Roscini (2014) p. 47
[90] Tallinn Manual (2017) Rule 69: "A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force".
[91] Tallinn Manual (2017) p. 333
[92] Tallinn Manual (2017) p. 341
[93] Common Article 3 to the Geneva Conventions

b) *Immediacy*. If the consequences of an act are revealed sooner, then, States have fewer opportunities to seek peaceful solutions of a dispute. Therefore, States harbour a greater concern for immediate consequences than those that are delayed or build slowly over time. For this reason, States are more likely to characterise a cyber-attack that produces immediate results as a use of force than cyber-attack that take weeks or months to achieve their intended effects.[94]

c) *Directness*. The more times passes between the initial act and its consequences, the less likely it is that States will deem the actor in violation of the prohibition on the use of force.[95] In armed conflicts, cause and effect are highly related to one another. For instance, a bomb explosion directly harms people and objects. Meanwhile, with economic sanctions, it may take weeks or longer to have an effect on market forces and so on. This means that cyber-attack with a direct effect is more likely to be labelled as the use of force.[96]

d) *Invasiveness*. This factor refers to the degree to which cyber-attack intrude into the target State. This means that the more secure a targeted system is, the greater is the concern as to its penetration. The degree to which the intended effects of a cyber-attack are limited to a particular State increases the perceived invasiveness of those attacks.[97] One example is domain names, which is a visible marker in cyberspace of belonging (e.g. "forsvaret.no"). Cyber-attack directly targeted towards the domain name of a specific State or State organ will be considered as more invasive.

e) *Measurability of effects*. This factor developed from the greater willingness of States to characterise actions as the use of force if the consequences are visible.[98] Ordinarily, the armed forces of a State carry out operations that are easy to label as the use of force and the effects of the operations are mainly measurable. However, with cyber-attack, this factor is less apparent. Consequently, a cyber-attack that can be evaluated in specific terms (e.g. number of servers disabled, the percentage of confidential files stolen) is more likely to be characterised as the use of force.[99]

[94] Tallinn Manual (2017) p. 334
[95] Tallinn Manual (2017) p. 334
[96] Tallinn Manual (2017) p. 334
[97] Tallinn Manual (2017) p. 335
[98] Tallinn Manual (2017) p. 335
[99] Tallinn Manual (2017) p. 335

f) *Military character*. If there is a connection between the cyber-attack in question and military operations, it enhances the likelihood of characterisation as a use of force.[100] This also has support in the UN Charter, where both the Preamble and several articles[101] refer to the use of [armed] force as in the use of military force. Traditionally, the use of force has also been understood to imply force engaged by armed forces. For instance, a cyber-attack conducted to cripple a military's communication system, and because of this, the State has reduced or lost its ability to conduct and sustain military operations.[102]

g) *State involvement*. The clearer the nexus between a State and cyber-attack, the more likely it is that other States will characterise them as uses of force by that State.[103]

h) *Presumptive legality*. International law is often positive: acts that are not forbidden are allowed. This means that in absence of a treaty or accepted international customary law, the act is presumptively legal. At this point, international law does not prohibit propaganda nor mere economic pressure *per se*. Therefore, these acts are presumptively legal.

These factors are not exhaustive. To evaluate whether a cyber-attack reaches the threshold of use of force, States may also look to other factors, such as the political environment, the identity of the attacker, whether the cyber-attack portends future use of military force, the nature of the target, and any record of cyber-attack by the attacker in the past.[104]

Since cyber-attack consists of a broad variety of actions, ranging from simply gathering information and surveillance to disrupting, deleting and completely crashing networks and destroying other connected equipment, this thesis will in the following try to draw out the lower threshold of what constitutes a use of force within cyber-attacks by looking at the different typologies.

[100] Tallinn Manual (2017) p. 336
[101] For example, UN Charter Article 44
[102] Tallinn Manual (2017) p. 336
[103] Tallinn Manual (2017) p. 336
[104] Tallinn Manual (2017) p. 337

3.3 Evaluation of the threshold

3.3.1 Cyber-attack causing physical damage to property, loss of life, or injury to persons or reasonably likely to do so

The primary effects of cyber-attack are those on the targeted computer, network or system, such as alteration of software, a Distributed Denial-Of-Service (DDoS) attack, deletion or other cyber-attacks. Further, the secondary effects are those on the infrastructure operated by the targeted system or network, including both total destruction and incapacitation. Finally, tertiary effects are those on persons affected by the destruction or incapacitation of the attacked infrastructure of the system.[105] It is important to note that it does not matter that these are not direct consequences because the ICJ stated in *Nicaragua* that "[i]ntervention that uses military armed force can occur either directly or indirectly".[106] This understanding is in line with the definition laid out in this thesis - extending a cyber-attack to also include damage to other objects.

As previously mentioned, it is clear that a cyber-attack that "seriously injures or kills a number of persons or that cause significant damage to, or destruction of, property" would satisfy the requirement of *scale and effects.*[107] This raises the question of whether a minor injury or a smaller number of killed persons or lesser destruction of property reaches the threshold.

The first known case of physical damage due to a cyber-attack is the Stuxnet case. Between June 2009 and May 2010, the Stuxnet malware targeted the computer systems of five facilities located in Iran. The worm affected specific industrial control systems which use a type of software for management of large-scale industrial systems.[108] In this case, the targeted industrial system was the uranium centrifuges at a nuclear plant in Natanz, Iran. The malicious worm was designed to force a change in the centrifuges' rotor speed, causing the speed to greatly increase and then rapidly decrease, which led to excessive vibrations or distortions, which again led to damage in the centrifuges.[109]

[105] Roscini (2014) p. 53
[106] *Nicaragua v. United States of America* para. 205
[107] Tallinn Manual (2017) p. 341
[108] Ziolkowski (2012) p. 4
[109] Lilienthal (2015) p. 396

When analysing if the Stuxnet-case can be identified as "use of force" is seems adequate to build on the *scale and effects* evaluation with the factors developed by the International Group of Experts in order to adapt it to a cyber-attack instead of conventional weapons.

a) *Severity*. The damage was imposed on Iran's nuclear program and resulted in such damage that it was set back several years. A cyber-attack creating physical damage on a nuclear plant is reasonably likely to be considered as a breach of the territorial integrity of the attacked State. Further, since it was a target of the weapon programme of Iran, which is undeniable of national interest and a core of their defence system, it also implies that the acts reach the threshold of use of force towards Iran's political independence. On the other hand, the scope of the actual damage on the centrifuges appears to have been minor and no personnel were harmed.[110]

b) *Immediacy*. Stuxnet consisted of several waves over a 10-month period, and according to this factor, it is unlikely to be viewed as a use of force.[111] Further, once a system was infected by the malware, it is believed that the damage took weeks or even months to evolve.[112]

c) *Directness*. It is beyond doubt a direct connection between Stuxnet and the damaged centrifuges in the Iranian nuclear plant.

d) *Invasiveness*. Stuxnet targeted highly secure and sensitive computer systems[113] and the cyber-attack represent a critical intrusion on both Iranian territorial and political sovereignty.

e) *Measurability of effects*. The effects of Stuxnet on the centrifuges of the nuclear plant appear both identifiable and measurable. Accordingly, this makes it easier to label as a use of force.

f) *Military character*. The Stuxnet was targeted at a nuclear plant. The plant provides uranium to be used for energy, but also for nuclear weapons. This

[110] Holloway (2015)
[111] Falliere (2011) p. 8
[112] Foltz (2012) p. 44
[113] Foltz (2012) p. 44-5

means that Stuxnet targeted one of the core elements of the Iranian military, which insinuates that it is a breach of political independence.

g) *State involvement*. No one has taken responsibility for the Stuxnet-case. Although not confirmed, it is widely believed that Israel and the United States were behind the attack.[114] The vague connection between the cyber-attack and the attacker suggests that it cannot be considered to reach the threshold of use of force.

h) *Presumptive legality*. The existing sanctions towards Iran are worth taking into account. First, the sanctions prohibit Iran from importing or exporting nuclear-related materials and technology. If such technology or material is discovered outside Iran, they can be lawfully seized and destroyed.[115] Second, Iran had been operating its centrifuges for years prior to Stuxnet,[116] which was in violation of several UN Security Council Resolutions.[117] Because of this, the cyber-attack on the nuclear plant may be argued as presumed legal.

By analysing these factors, in light of the effects-based approach, the *scale and effects* of the Stuxnet-case are considered to reach the threshold of "use of force" in Article 2(4) of the UN Charter.

3.3.2 Cyber-attack severely disrupting critical infrastructure

There is a disagreement in academia on whether disruptive operations, meaning those attacks that render ineffective or unusable infrastructures without physically damaging them, can also be seen as "use of force" under the UN Charter. The International Group of Experts consists of experts from various geopolitical backgrounds, and due to the internal disagreements amongst the group members, the Tallinn Manual focuses mainly on physical damage.

Modern society is becoming heavily digitised and private individuals, corporations and government agencies all rely on efficient and secure computer systems. Article 2(4) contains attacks on territorial integrity and political independence of States, and this speaks for including a cyber-attack affecting a State's security, public safety, national economic security,

[114] Fruhlinger (2017)
[115] Foltz (2012) p. 45
[116] Foltz (2012) p. 45
[117] Amongst others, UN Security Council Resolutions 1737 (2006), 1747 (2007), 1803 (2008), and 1929 (2010)

the safe and reliable functioning of critical infrastructure and the availability of key resources.[118]

There is no general agreement on what "critical infrastructure" entails. The UN General Assembly has stated that "[e]ach country will determine its own critical information infrastructures".[119] This has led to the different States creating their own understanding of what is critical and which sectors that are included in the definition is based on the country's distinctiveness.

For example, the 2001 US PATRIOT Act defines it as "[s]ystems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters".[120] Meanwhile, the Cyber Security Strategy for Germany defines critical infrastructure as "[o]rganisations or institutions with major importance for the public good, whose failure or damage would lead to sustainable supply bottlenecks, considerable disturbance of public sector or other dramatic consequences", and further identifies the following areas: energy, information technology and telecommunications, health, transport, food, water, finance and insurance, State and administration, media and culture.[121] By comparing these definitions, the common figure is that critical infrastructures are vital for national security, including governmental, societal and individual security.

The case of Estonia provides a good framework for understanding this. In 2007, a Soviet war monument in Tallinn was supposed to be moved to a military cemetery. The statue symbolises the victory over Nazi-Germany, and for many Russians, it is a beloved symbol of wartime sacrifice. However, the Estonians mostly see the statue as a symbol of foreign occupation and suppression. The statue was originally scheduled to be moved on 9. May, the "Russian Victory Day",[122] but due to the fear of riots, the move was brought forward. In Tallinn, this led to a riot from several thousand protesters belonging to Estonia's large population of ethnic Russians, and in Moscow, a youth movement attacked the Estonian

[118] Roscini (2014) p. 55
[119] UN General Assembly Resolution 58/199 of 23 December 2003
[120] 2001 US PATRIOT Act, section 1016
[121] German Federal Ministry of the Interior (2011) p. 15
[122] Russia celebrate the victory over the Nazis

embassy, resulting in protests by NATO, the United States and the European Union.[123] The riots towards the embassy gave in under Western pressure, but the number of cyber-attacks toward Estonia emerged.

Estonia is considered to be one of the most networked countries in Europe and more than 355 government agencies use a joint system called X-road. The initial cyber-attack consisted of DDoS directed at public and private internet providers, highly affecting the X-road system.[124] These attacks were, however, un-coordinated and simple to overcome. The second phase consisted of millions of emails sent to Parliament representatives, causing the server to crash and leaving the government and government agencies without communication facilities for days.[125] The third phase completely shut down the internet in Estonia, including everything from news organisations, political parties to banks and companies in the public and private sector. On the 10th May, Estonia was near a digital collapse.[126] The last large attack took place five days later, with a bot-network consisting of 85 000 "zombie-computers" exercising a DDoS towards the Computer Emergency Response Team Estonia.[127] The attack on Estonia has later been called Web War I because it this was the first time a country has been attacked throughout its whole cyber domains at the same time, and there has never before been a need for an equally active cyber defence.[128]

As stated previously, when analysing if the Stuxnet-case can be identified as "use of force" the evaluation will build on the *scale and effects* assessment with the factors developed by the International Group of Experts.

a) *Severity*. The cyber-attack in Estonia did not inflict any loss of life or injury to persons. Further, there were no physical damages on infrastructure or other objects. However, there were economic losses due to the lack of internet access for the largest banks. It is also likely that the attack led to an economic loss for small and medium businesses that is more dependent on online-based communication and trade,[129] in addition to impacting ordinary people and leaving them without living expenses. Once an attack creates repercussions for

[123] The Economist (2007)
[124] E-Estonia (undated)
[125] The Economist (2007)
[126] Shackelford (2009) p. 205
[127] Infosec (undated)
[128] Blank (2008) p. 227
[129] Tikk (2010) p. 19

ordinary people, it is likely to be considered as an influence on the political independence of the targeted State. The media in Estonia was also cut-off from reporting the attacks, both internally and externally, leading to social consequences for Estonians. This implies that the consequences of severity were extensive and might be severe enough to characterise it as "use of force".

b) *Immediacy*. Most of the consequences appeared immediately after the attacks began. With the computers flashing in front of them, the IT-workers were able to watch how their computer system was taken over, minute by minute.[130] The continued attacks had greater scope, intensity and duration and led to severe consequences, as described. Some attacks lasted only for an hour or so, while others continued for up to between 5 and 10 hours.[131] Immediately after the attack, the larger economic consequences were not visible, however, the social consequences for the smaller businesses and citizens were visible soon after the attack.

c) *Directness*. All crashed websites and network systems were a direct result of the cyber-attack. The attacks consisted of hacking directly into the servers[132] of the various government agencies where they deleted and posted Russian propaganda messages.[133] As the bank services also were targeted, the banks had to upgrade their network defence systems. Since there were no other contributing factors, the attack led directly to the bank's expenditures on upgrading the network defence system. There is direct causation between the attacks and the consequences mentioned in this evaluation.

d) *Invasiveness*. As mentioned, Estonia is one of the most advanced network-countries in Europe and their dependency on the internet made them extremely vulnerable during the attack. The attacks penetrated, in varying degrees, well-secured domains belonging to government agencies and both private and public companies and is likely a breach of territorial integrity. Testimonials

[130] Davis (2007)
[131] Davis (2007)
[132] As previously explained in section 2.2
[133] Davis (2007)

from hackers on Russian forums[134] indicate that these attacks were well-planned, well-organised and more than just a *mere frontier incident*.[135]

e) *Measurability of effects*. During the attacks, the Estonian cyber defence had an overview over what was affected, for how long, how the attacks were exercised and the number of attacks targeted at Estonia. This makes it easy to evaluate the number of destroyed or infected data. On the other hand, it is harder to measure the social and economic consequences. Some of the targeted banks have their losses, but it is hard to say the exact number of transactions lost by both banks and businesses. Because the banks were also attacked, it is likely that the citizens were unable to use their bank cards to buy daily essentials and, even worse, they were unable to get an update on why this was because the news channels were also affected. Thus, the cyber-attack did have an effect on the self-determination of the citizens of Estonia and their political independence.

f) *Military character.* The cyber-attack was launched towards both private and public targets, amongst other the Computer Emergency Response Team Estonia, a section of the Cyber Security Intelligence of Estonia. Since Estonia is a highly digitised country and very reliant on technology, this implies that the cyber-attack can be seen as a breach of political independence because the cyber-attack targeted the core of the Estonian cyber military.

g) *State involvement*. It is confirmed that the cyber-attacks mostly originated from sources outside Estonia, and the cyber-attacks were tracked to originate from as many as 178 different countries.[136] Therefore, a State connection with the attacks must be evaluated. It is clear that the action of a "group acting on the instructions of, or under the direction or control of, that State" is attributable to the State.[137] Encouragement to carry out attacks was discovered on Russian chat forums where nationalistic and political hackers posted instructions on

[134] Davis (2007)
[135] *Nicaragua v. United States of America* para. 195
[136] Cooperative Cyber Defence Centre of Excellence (CCDCOE) (2010) p. 23
[137] International Law Commission Article 8, *Nicaragua v. United States of America* para. 228; *Prosecutor v. Tadić* para. 117

how to conduct a cyber-attack and what the prioritised targets were.[138] This could, however, be private individuals without a connection to the Russian State. On the other hand, the targets in the second and third phase were well-constructed and organised and required significantly more financial support and knowledge. It is few, if any, independent groups that have these kinds of financial assets, which implies a close connection with the Russian government.[139] Further, the Estonian government claimed that they could trace the attacks to Russian IP-addresses.[140] Combined, this suggests close ties to the Russian authorities. Still, it is not proven beyond reasonable doubt and because of this, the cyber-attack cannot definitely be tied to Russia.

h) *Presumptive legality*. In the beginning, the attacks appeared more as criminal acts and spreading of propaganda and are therefore not restricted by international law. However, during the continued attacks, the cyber-attacks gained a stronger character of power and started to attack the websites of the Estonian Parliament, President and Prime Minister. These attacks on central figures in Estonian politics is a clear violation of political independence and speaks strongly for the cyber-attack to amount to "use of force".

In sum, the cyber-attack on Estonia did not cause physical damage to property, loss of life, or injury to persons, but it did influence the Estonian society in other ways. The attacks did result in direct and partly measurable damages and did have an invasion-like character in the highly digitised Estonian society. Further, several of these factors are close to or clearly a breach of the territorial integrity and/or political independence of Estonia. By evaluating these factors, it is reasonable to say that the cyber-attack on Estonia can be considered as "use of force" under the UN Charter.

[138] Landler (2007)
[139] Cooperative Cyber Defence Centre of Excellence (CCDCOE) (2010) p. 23
[140] BBC News (2007)

4 Virtual warfare in the future

Most of the available literature on cyber warfare focuses on cyber-attacks consisting of virtual attacks only. It is possible to imagine that an attack involving cyber activities carried out in combination with traditional use of kinetic armed force, known as hybrid warfare, can be likely than a solo cyber-attack.[141] This sort of combined attack is more likely because a solo cyber-attack amounting to an armed attack, like a "Cyber Pearl Harbour", would lead to a large-scale self-defence response from the attacked State.[142] It would, therefore, be more likely that, if a State had decided to go to war, it would seek to maximise the effect by also using other means of attack alongside a cyber-attack.[143]

Since the late 2010s, Russia has attempted to conduct this form of hybrid warfare in order to achieve its national strategic goals and make itself more prominent in the international arena.[144] The Russian government has officially stated that it does not engage in offensive cyber activities and the official doctrinal statement on the role of the Russian military in cyberspace focus on prevention of information warfare.[145] However, former and current Russian Chiefs of the General Staff have given statements about the military strategy saying otherwise. They have both stated that Russia has conducted hybrid warfare by focusing on introducing harmful software, working on domestic and foreign public opinion using the media and Internet and by disrupting information systems[146] in combination with conventional attacks.

One relevant example is the conflict between Georgia and Russia in 2008. At the beginning of August, after months of back-and-forth accusations and a series of clashes between Georgian military troops and the South Ossetian militia, President Saakashvili of Georgia ordered his troops to capture the South Ossetian capital of Tskhinvali. In response, Russia moved its troops to the Georgian border and started to conduct air strikes on the Georgian troops in South Ossetia as well as Abkhazia. NATO, the United States and the United Kingdom called for a ceasefire, but the conflict continued for five days, resulting in Russia taking control over

[141] For instance, read Park (2017) or Gill (2013)
[142] UN Charter Article 51
[143] Gill (2013) pp. 462-3
[144] Connell (2017)
[145] Unknown author. *The Military Balance* (2017) pp. 183-236
[146] Bartles (2016) p. 30

Tskhinvali and moving their troops close to Tbilisi, the capital of Georgia.[147] At the same time, supportive patriot hackers and/or Russian State agencies (there was no clear evidence as to who was responsible) exercised attacks on Georgian government websites, leading to inconveniences for the Georgian public and some government agencies.[148] In this case, the cyber-attack did not cause any appreciable damage, but it is easy to imagine that if the cyber-attack had been more large-scale and targeted at the communication system of the Georgian military or degrading the Georgian military weapons, it could reach the threshold of "use of force", if not also constitute an "armed attack", under the UN Charter. This case is a clear example of how cyber capabilities can be used alongside traditional kinetic weapons as means in an armed attack.

In the case of Estonia previously mentioned in this thesis, where Russia was assumed to be the attacker, it is possible to imagine that the cyber-attack could be combined with a conventional attack. Estonia was paralysed and left without methods of communication and became an easy target. NATO has stated that Article 5 of the North Atlantic Treaty can be invoked over cyber-attacks,[149] resulting in NATO defending the attacked State against its attacker.[150] For an attacker, there would be no point in risking this response from NATO without trying to maximise the result of the initial attack by conducting a hybrid attack. As a consequence, it can be seen as highly likely that this method of warfare will become more prevalent in the future when more States gain the capacity to effectively make use of cyber as a complement to traditional means and integrate it as a part of their operational practice.

[147] Pruitt (2018)
[148] Gill (2013) p. 461
[149] Fifth Domain (2017)
[150] North Atlantic Treaty Article 5

Bibliography

Literature

Asrat (1991) — Asrat, Belatchew. *Prohibition of force under the UN Charter. A study of art. 2 (4),* Uppsala: Iustus institution, 1991

Bartles (2016) — Bartles, Charles K. "Getting Gerasimov Right" in *Military Review* (2016), February issue, pp. 30-38

BBC News (2007) — BBC News. *The cyber raiders hitting Estonia.* (2007) http://news.bbc.co.uk/2/hi/europe/6665195.stm [Quoted 1.5.19]

Beaumont (2010) — Beaumont, Peter. *US appoints first cyber warfare general*. (2010), https://www.theguardian.com/world/2010/may/23/us-appoints-cyber-warfare-general [Quoted 1.3.19]

Blank (2008) — Blank, Stephen. "Web War I: Is Europe's First Information War a New Kind of War?" in *Comparative Strategy* (2008) volume 28 issue 3. P. 227-247

Connell (2017) — Connell, Michael and Sarah Vogler. *Russia's Approach to Cyber Warfare.* (2017), http://www.dtic.mil/docs/citations/AD1032208 [Quoted 27.4.19]

Cooperative Cyber Defence Centre of Excellence (CCDCOE) (2010) — Cooperative Cyber Defence Centre of Excellence (CCDCOE). *International Cyber Incident*, Tallinn, Estonia, 2010

Davis (2007) — Davis, Joshua. *Hackers Take Down the Most Wired Country in Europe.* (2007), https://www.wired.com/2007/08/ff-estonia/ [Quoted 19.4.19]

Death (2018) — Death, Darren. *The Cyber Kill Chain Explained*. (2018) https://www.forbes.com/sites/forbestechcouncil/2018/10/05/the-cyber-kill-chain-explained/ [Quoted 5.3.19]

DW News (2018) — DW News. *German cyber defense lends military and commerce.* (2018), https://www.dw.com/en/german-cyber-defense-blends-military-and-commerce/a-45636325 [Quoted 1.3.19]

The Economist (2007) — The Economist. *A cyber-riot.* (2007), https://www.economist.com/europe/2007/05/10/a-cyber-riot [Quoted 18.4.19]

E-Estonia (undated) — E-Estonia. *X-road.* (undated), https://e-estonia.com/solutions/interoperability-services/x-road/ [Quoted 18.4.19]

Falliere (2011) — Falliere, Nicolas; Liam Murchu and Eric Chien. *W32. Stuxnet Dossier.* (2011) https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf [Quoted 27.4.19]

Fifth Domain (2017)	Fifth Domain. *NATO Might Trigger Article 5 for Certain Cyberattacks.* (2017), https://www.fifthdomain.com/home/2017/06/01/nato-might-trigger-article-5-for-certain-cyberattacks-cycon-tallinn/. [Quoted 27.4.19]
Foltz (2012)	Foltz, Andrew C. "Stuxnet, Schmitt analysis, and the Cyber "use-of-force" debate" in *JFQ* (2012) issue 67, 4th quarter, p. 40-49
Forsvaret (undated)	Forsvaret. *Cyberforsvaret.* (undated) https://forsvaret.no/cyberforsvaret [Quoted 28.4.19]
Fruhlinger (2017)	Fruhlinger, Josh. *What is Stuxnet, Who Created It and How Does It Work?* (2017), https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html [Quoted 25.3.19]
Garner (1999)	Garner, Bryan. *Black's Law Dictionary*, 8. edition, Bryan Garner (ed.), St. Paul: Thompson West, 1999
German Federal Ministry of the Interior (2011)	German Federal Ministry of the Interior. *Cyber Security Strategy for Germany*, Berlin: Beauftragter der Bundesregierung für Informationstechnik, 2011
Gill (2013)	Gill, Terry D. and Paul A. L. Ducheine. "Anticipatory Self-defence in the Cyber Context" in *International Law Studies*, (2013), Volume 89 p. 438-471

Gordon (2006) — Gordon, Sarah and Richard Ford. “On the Definition and Classification of Cybercrime” in *Journal of Computer Virology* (2006) volume 2, issue 1, p. 13-20

Guterres (2018) — Guterres, António. *Address at the Opening Ceremony of the Munich Security Conference*. (2018), https://www.un.org/sg/en/content/sg/speeches/2018-02-16/address-opening-ceremony-munich-security-conference [Quoted 27.4.19]

Handler (2012) — Handler, Stephanie Gosnell. “The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare” in *Stanford Journal of International Law* (2012), volume 48, p. 209-237

Harris (2010) — Harris, David. *Cases and Materials on International Law*, 7. edition, London: Thomas Reuters, 2010

Hathaway (2012) — Hathaway, Oona et. al. “The Law of Cyber-Attack” in *California Law Review* (2012), volume 100, p.817-885

Henckaerts (2013) — Henckaerts, Jean-Marie and Louise Doswald-Beck. *Customary International Humanitarian Law.* Cambridge: Cambridge University Press, 2013

Hollis (2007) — Hollis, Duncan B. “Why States Need an International Law for Information Operations” in *Lewis and Clark Law Review* (2007), volume 11, issue 4, p. 1023-1061

Holloway (2015) — Holloway, Michael. *Stuxnet Worm Attack on Iranian Nuclear Facilities.* (2015) http://large.stanford.edu/courses/2015/ph241/holloway1/ [Quoted 25.3.19]

Hutchins (undated) — Hutchins, Eric; Michael Cloppert and Rohan Amin. *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.* (undated) https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf [Quoted 5.3.19]

Infosec (undated) — Infosec. *Estonia: To Black Out an Entire Country – part one.* (undated) https://resources.infosecinstitute.com/estonia-to-black-out-an-entire-country-part-one/ [Quoted 18.4.19]

International Committee of the Red Cross (2009) — International Committee of the Red Cross. *Customary International Humanitarian Law*, 3. Edition, Cambridge: Cambridge University Press, 2009

Landler (2007)	Landler, Mark and John Markoff. *Digital Fears Emerge After Data Siege in Estonia.* (2007), https://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all& [Quoted 19.4.19]
Lilienthal (2015)	Lilienthal, Gary and Ahmad Nehaluddin. "Cyber-Attack as Inevitable Kinetic War" in *Computer law & security review*, (2015) volume 31, issue 3, pp. 390-400
Lockheed Martin (undated)	Lockheed Martin. *The Cyber Kill Chain*. (undated) https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html [Quoted 8.5.19]
Lyall (2018)	Lyall, Nicholas. *Chinas cyber militias*. (2018), https://thediplomat.com/2018/03/chinas-cyber-militias/ [Quoted 1.3.19]
Merriam Webster (undated A)	Merriam Webster. *Cyberattack.* (undated A), https://www.merriam-webster.com/dictionary/cyberattack [Quoted 27.4.19]
Merriam Webster (undated B)	Merriam Webster. *Military.* (undated B), https://www.merriam-webster.com/dictionary/military [Quoted 30.4.19]

Nikolaisen (2016) Nikolaisen, Per-Ivar. -*Er det IS eller Russland? Slik øver norske cybersoldater.* (2016), https://www.tu.no/artikler/er-det-is-eller-russland-slik-over-fremtidens-norske-cybersoldater/276500 [Quoted 4.3.19]

Park (2017) Park, Donhgui, Julia Summers and Michael Walstrom. *Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks*. (2017), https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/ [Quoted 27.4.19]

Pruitt (2018) Pruitt, Sarah. *How a Five-Day War with Georgia Allowed Russia To Reassert its Military Might.* (2018)*,* https://www.history.com/news/russia-georgia-war-military-nato [Quoted 19.4.19]

Randelzhofer (2002) Randelzhofer, Albrecht. «Article 2(4)» in *The Charter of the United Nations: A Commentary*, Simma, Bruno et al (eds.), Oxford: Oxford University Press, 2002, p. 112-136

Roscini (2010) Roscini, Marco. «World Wide warfare – jus ad bellum and the use of cyber force" in *Max Planck Yearbook of the United Nations Law,* (2010) volume 14, p. 85-130

Roscini (2014)	Roscini, Marco. *Cyber Operations and the Use of Force in International Law*. Oxford: Oxford University Press, 2014
Shackelford (2009)	Shackelford, Scott. "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law" in *Berkeley Journal of International Law* (2009) volume 27, issue 1, p. 192-251
Tallinn Manual (2017)	Schmitt, Michael N. (ed.) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 4. edition, Cambridge: Cambridge University Press, 2017
Tikk (2010)	Tikk, Eneken; Kadri Kaska and Liis Vihul. *International Cyber Incidents: Legal considerations*, Tallinn: Cooperative Cyber Defence Centre of Excellence, 2010
Tsagourias (1996)	Tsagourias, Nicholas. *The Nicaragua Case and the Use of Force: The Theoretical Construction of the Decision and its Deconstruction*. (1996) https://academic.oup.com/jcsl/article/1/1/81/784716 [Quoted 27.4.19]
Unknown Author. *The Military Balance* (2017)	Unknown Author. "Chapter 5. Russia and Eurasia", *The Military Balance.* (2017), Volume 117, p. 183-236
US Army Training & Doctrine Command (2005)	US Army Training & Doctrine Command. *Critical Infrastructure Threats and Terrorism: Cyber Operations and Cyber Terrorism Handbook*, DCSINT Handbook No. 1.02, 2005

VICE News (2018) — VICE News. *How Israel is becoming the world's top cyber superpower.* (2018), https://news.vice.com/en_ca/article/evmyda/how-israel-is-becoming-the-worlds-top-cyber-superpower [Quoted 1.3.19]

Waxman (2011) — Waxman, Matthew C. «Cyber-attacks and the Use of Force: Back to the Future of Article 2(4)" in *Yale Journal of International Law* (2011), volume 35, issue 2, p. 421- 459

Weller (2015) — Weller, Marc. «Introduction: International Law and the Problem of War» in *The Oxford Handbook of the Use of Force in International Law*, Marc Weller (ed), Oxford: Oxford University Press, 2015

Ziolkowski (2012) — Ziolkowski, Katharina. *Stuxnet - legal considerations.* Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2012

International sources of law

Law

2001 US PATRIOT Act — United States of America: *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* (USA Patriot Act) [United States of America], 26 October 2001

Treaties and resolutions

Common Article 3 to the Geneva Conventions	International Committee of the Red Cross (ICRC), *Geneva Convention Relative to the Treatment of Prisoners of War (Third Geneva Convention)*, 12 August 1949, 75 UNTS 135
ICJ Reports *Legality of the Threat or Use of Nuclear Weapons*	*Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion*, I.C.J. Reports 1996, p. 226, International Court of Justice (ICJ), 8 July 1996
International Law Commission	UN General Assembly, Report of the International Law Commission, 23 July 1999, A/54/10
North Atlantic Treaty	North Atlantic Treaty, 4 April 1949
UN Charter	United Nations, *Charter of the United Nations*, 24 October 1945, 1 UNTS XVI
UN General Assembly A/RES/25/2625 Declaration on Friendly Relations	United Nations General Assembly A/RES/25/2625 of 24 October 1970 *Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations*

UN General Assembly Resolution 58/199 of 23 December 2003	United Nations General Assembly Resolution 58/199 of 23 December 2003 *Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures*
United Nations Security Council S/RES/1737 (2006)	United Nations Security Council, Security Council resolution 1737 (2006) [Non-proliferation], 23 December 2006, S/RES/1737 (2006)
United Nations Security Council S/RES/1747 (2007)	UN Security Council, Security Council resolution 1747 (2007) [Non-proliferation], 24 March 2007, S/RES/1747 (2007)
United Nations Security Council S/RES/1803 (2008)	UN Security Council, Security Council resolution 1803 (2008) [on further measures against Iran in connection with its development of sensitive technologies in support of its nuclear and missile programmes], 3 March 2008, S/RES/1803 (2008)
United Nations Security Council S/RES/1929 (2010)	UN Security Council, Security Council resolution 1929 (2010) [on measures against Iran in connection with its enrichment-related and reprocessing activities, including research and development], 9 June 2010, S/RES/1929 (2010)
Vienna Convention	United Nations, *Vienna Convention on the Law of Treaties*, 23 May 1969, United Nations, Treaty Series, vol. 1155, p. 331

Case law

Nicaragua v. United States of America	*Nicaragua v. United States of America*; *Merits* International Court of Justice (ICJ), 27 June
Prosecutor v. Tadić	*Prosecutor v. Tadić* Case. No IT-94-1A, ICTY App. Ch. (July 15, 1999)

Other documents

Documents of the United Nations Conference on International Organisation	6 U.N.C.I.O. Docs. 331, 334-35 (1945)

List over figures