The regulation of cyber warfare under contemporary international humanitarian law

D Van Zyl

Orcid.org 0000-0001-8401-4933

Dissertation accepted in fulfilment of the requirements for the degree *Master of Laws in International Aspects of Law* at the North-West University

Supervisor: Prof HJ Lubbe

Graduation ceremony: April/June 2022

Student number: 24977292

ACKNOWLEDGEMENTS

Firstly, I would like to thank my supervisor and mentor, Professor H.J. Lubbe Associate Professor at the North-West University, for providing me with guidance throughout the completion of this research, and moreover, for cultivating a deep love for Public International Law. Thank you for your continuous support over the span of five years.

I would also like to thank my editors for helping me to create a more rounded research paper.

Lastly, I would like to thank Dewald van Zyl, Erika van Zyl, Tanya van Zyl, Pieter Jansen van Rensburg, Pieter-Hendrik White and Francois van Niekerk for providing me with much needed emotional support, as doing research can be most lonesome. Thank you for your ongoing support and unwavering faith in me.

ABSTRACT

The purpose of this research paper is to establish whether International Humanitarian Law is applicable to armed conflicts that consist of a cyber element and if so, to what extent it would apply. This required an in-depth analysis into the prohibition on the use of force as well as the principles of International Humanitarian Law. The first step was to establish the current position regarding the prohibition on the use of force and International Humanitarian Law. Once this was clear, the next phase of the research was to apply these positions to cyber-attacks and situations of International armed conflict consisting of a cyber element. The Tallinn Manual 1.0 as well as 2.0, were utilised to a great extent in order to establish the position that the International experts, who composed these manuals, hold regarding the applicability of cyber-related conflict to customary international law. By applying cyber-attacks to the prohibition on the use of force it was found that where a cyber-attack reaches the level of damage that a kinetic attack can inflict, the attack will be prohibited by article 2(4). By applying armed conflicts consisting of a cyber-element to International Humanitarian Law, it was found that where such an armed conflict arises, International Humanitarian Law will apply. Contemporary International Humanitarian Law is shown to be applicable to cyber-related conflicts, however, due to the novelty of cyber space, certain uncertainties do exist on the scope of the application of International Humanitarian Law on cyber related conflicts. These uncertainties can possibly be clarified in the future through state practice and further research.

Key words

Armed attacks; Armed conflicts; Contemporary International Law; Cyber-attacks; Cyber operations; Cyber space; Cyber threats; Cyber warfare; Distinction; International Humanitarian Law; Kinetic warfare; Military necessity; pre-emptive action; Prohibition on the use of force; Proportionality; Self-defence; Unnecessary suffering.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

ARPA	Advanced Research Project Agency
ARPANET	Advanced Research Projects Agency Networks
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CFAA	Computer Fraud and Abuse Act of 1986
DDoS	Distributed Denial of Service Attack
ESD	Electronics Systems Division
IACs	International Armed Conflicts
ICC	International Criminal Court
ICJ	International Court of Justice
ICRC	International Committee of the Red Cross
IJRC	International Justice Resource Center
IHL	International Humanitarian Law
IP address	Internet Protocol Address
IRA	Irish Republican Army
MES	Military Electromagnetic Spectrum
NACDL	National Association of Criminal Defence Lawyers
NATO	North Atlantic Treaty Organisation
NCI	National Critical Infrastructure
NIACs	Non-International Armed Conflicts
UK	United Kingdom
UN	United Nations
UN Charter	United Nations Charter
UN	United Nations
USA	United States of America
VCLT	Vienna Convention on the Law of Treaties of 1969

Chapter 1: Introduction

On 27 April 2007, Estonia experienced a shutdown of internet systems designed to regulate civilian infrastructure, ranging from parliament websites to banks.[1] These shutdowns were the result of numerous cyber-attacks conducted in a single cyber operation, which at the time, was the largest non-kinetic operation to ever be conducted.[2][3] These cyber-attacks were targeted at Estonia's capital city, Tallinn, where a Soviet bronze statue was planned to be relocated.[4] This is relevant since the attacks are presumed to have been conducted by Russia as a show of discontent with the relocation of the bronze statue.[5] Russia's involvement, however, has not conclusively been established due to lack of attribution, and as such Estonia cannot hold Russia accountable for the attack on its civilian internet systems.[6] Even if Russia can be held accountable for the attack, uncertainty exits on how to respond to such an attack. The attack on Estonia will be discussed at length later on in chapter 2.

If the operation conducted on Estonia in 2007 was a kinetic armed operation, the position would be as follows. Contemporary international law prohibits the use of force between states and as such, if an armed operation on Estonia were to have a forceful effect, similar to what is meant in the prohibition on the use of force clause, it would be prohibited. Estonia would then have a right to repel the attack by way of self-defence. If the attack on Estonia has not yet taken place, the state might have a right to defend themselves pre-emptively, however, uncertainty exists whether pre-emptive action is permitted by contemporary international law. Applying the principle of the prohibition on the use of force to cyber space, it becomes clear that uncertainty exists

---

1 Tamkin 2017 https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/.

2 Cyber related concepts and terminology will be discussed at length in chapter 2.

3 Tamkin 2017 https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/.

4 Tamkin 2017 https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/.

5 Tamkin 2017 https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/.

6 Shakarian 2011 *Military Review* 63-68.

on whether cyber operations constitute forceful acts, and if so, whether it would be prohibited.

Where a kinetic armed conflict would arise between Estonia and Russia, International Humanitarian Law (IHL) would apply. IHL does not prohibit armed conflicts, but rather provides regulation to minimise damage and suffering of civilians and combatants, as well as civilian objects. This is done through the principles of IHL which are, distinction, military necessity, unnecessary suffering and proportionality. The distinction element requires combatants to distinguish between civilians and combatants, and to only attack combatants; military necessity requires combatants not to harm civilians and civilian objects if it isn't necessary to reach an intended goal; unnecessary suffering protects combatants against suffering that is unnecessary; and proportionality requires combatants to not cause harm to civilians and civilian infrastructure, if the harm endured is not in proportion to the military gains expected.

The principles of IHL have evolved to regulate all forms of kinetic armed conflicts and as such, the novelty of cyber related armed conflicts creates uncertainty on whether it is regulated to the same extent. Distinction, for example, requires combatants to visually differentiate between civilians and combatants, which would not be a problem in a kinetic armed conflict. In a cyber related conflict, however, cyber operations are conducted over computer systems, that are comprised of zeroes and ones, this means that combatants do not have the luxury to make a visual distinction between civilians and combatants. This causes the necessity for IHL to be interpreted to regulate cyber related armed conflicts, or new treaties must be created in order to regulate armed conflicts in cyber space.

As seen in this problem statement, force exerted through kinetic armed operations between states is adequately prohibited, and proper regulation of kinetic armed conflicts by IHL exists, however, uncertainty arises where force and armed conflicts arises in cyber space. In the light hereof the research question that this study will answer is whether contemporary international humanitarian law regulates cyber warfare and if so, to what extent it would apply. The aim of this research is to establish

that current international law is sufficient for regulating cyber warfare, and that interpreting the prohibition of the use of force clause, as well as IHL to include cyber space will not require creating new legislation and/or treaties, but that cyber warfare is already regulated in its entirety. This will be answered by reaching the objectives, provided in chapters 2, 3, and 4 of this study. The first objective is to form a basis of terminology and background of cyber space, to better understand its novel concepts. The second objective is to establish what force, in terms of the prohibition on the use of force clause, is and when such force is prohibited in the light of cyber space. The third objective is to identify when cyber operations are prohibited by the prohibition on the use of force clause. The fourth objective is to establish if a state may defend itself against a cyber operation and if so, in what manner may it defend itself. The fifth objective is to establish the nature of an armed conflict. The sixth objective is to establish whether armed conflicts can be cyber related and thus be regulated by IHL. The seventh objective is to establish the applicability of the principles of IHL in cyber space.

Chapter 2 provides a short background on the origin and expansion of cyber warfare, as well as to explain the relevant terminology that is used throughout this study. Cyberspace is a contemporary concept with new terminology and ideals that may be difficult to understand at first. As such, it is important to grasp the basic terminology relating to cyberspace before understanding its relevance to IHL.

In chapter 3, an in-depth analysis is conducted on cyber operations and its relevance to use of force under international customary law. It is necessary to establish whether cyber operations are regarded as force under article 2(4) and as such, prohibited. This section of the analysis begins by providing a short background on the creation and evolution of use of force up until the present day. This is followed by an in-depth analysis of article 2(4) and its relevance to cyber operations. The exceptions to the prohibition on the use of force, found in article 51, are analysed in the light of cyber operations to establish whether defence by way of cyber operations or against cyber operations is justifiable.

In chapter 4, an analysis of IHL in the light of cyber operations is conducted. This analysis starts by providing historical background of IHL. This explains the purpose of the need for armed conflict to be regulated. Following this historical background, the sources of IHL are discussed for purposes of providing an understanding of how the different sources of IHL work together in order to provide sufficient regulation of armed conflicts. Once this has been done, there is differentiation between International Armed Conflicts (IACs) and Non-International Armed Conflicts (NIACs). Both IACs and NIACs are discussed at length and compared to cyber operations for purposes of establishing applicability. Ultimately, the principles of IHL are analysed in the light of cyberspace to establish whether IHL is applicable to cyber warfare. This is done by conducting an in-depth analysis on the principles of distinction, military necessity, unnecessary suffering and proportionality respectively, and by comparing them to operations and attacks in cyberspace.

The motivation behind this study is that a legal uncertainty exists on whether international law must be supplemented in order to find applicability in cyber space. This uncertainty arises from the notion that force and harm arising in cyber space is intangible. The significance of this study is that cyber space is a part of most aspects of human society, regulating and controlling mechanised systems as well as social lives. As such, a harmful act in cyber space can cause physical damage to civilian infrastructure as well as harm to civilians.

This dissertation will be conducted by means of a literature review of primary and secondary sources, published on the topic. These include, but are not limited to, legislation, case law, books, journal articles, international instruments and relevant electronic resources.

Chapter 2: Cyber operations, cyber-attacks and cyber warfare

2.1 Introduction

Various names exist for military acts conducted in cyberspace which includes, cyber warfare, spectrum warfare, and electronic warfare.[7] This is because the Military Electromagnetic Spectrum (MES) underwent various evolutionary changes over the past century.[8] This evolution began with the weaponisation of radio waves in the 1920's, with the most recent evolutionary development of the MES being cyber warfare.[9] Cyberspace, cyber threats and all terminology relating to cyber warfare in general are concepts that may challenging to grasp, given that cyberspace is a novel field with very different concepts to what the physical world has to offer. This chapter will provide a comprehensive insight to navigate the challenging concepts throughout this dissertation, by explaining where cyber threats began and by reading the history leading up to creating legislation as well as about non-binding documents designed to provide regulation and clarification on cyberspace, cyber war and how contemporary international law applies to it. Once the history and origins of cyberspace has been discussed, an explanation on the Tallinn Manual follows in which the reason for its creation, its nature and purpose are discussed. This is necessary because throughout this study, the Tallinn Manual plays an integral part of the research as is discussed later on in this chapter at 2.3. Different forms of cyber-attacks that are relevant for this dissertation are considered in order to provide guidance to understand how cyber-attacks differ and how they can cause damage in the physical world. Lastly, the problem of attribution is discussed, because this problem is unique to cyberspace and sits at the root of most uncertainty in cyber law. With the conclusion of this chapter, cyber concepts and international law will be clear and navigation throughout this dissertation will be possible with relative ease.

---

7 Lehto Non-kinetic Warfare- The new game changer in the battle space 316.
8 Lehto Non-kinetic Warfare- The new game changer in the battle space 316.
9 Lehto Non-kinetic Warfare- The new game changer in the battle space 316.

2.2 History and timeline of cyber war

The history of warfare is filled with a series of frontiers that opened new ways to conducting warfare. For people living at the dawn of sailing, warfare at sea was unheard of and it would be unthinkable that entire battles could be conducted at sea. The same goes for aerial warfare, a battle conducted in the air was unfathomable to people in the 1700s. There is a total of four domains in which warfare can be conducted: land, sea, air and space.[10] Cyberspace is described as the fifth domain[11] that is not physical, but entirely virtual and that can be compared to sea, space and outer space due to the lack of territorial boundaries within these realms.[12] Like all domains, cyberspace can be utilised in warfare by attacking infrastructure that run on computer systems or conducting espionage by spying on the online activities of other states. Cyber warfare is conducted by performing a series of attacks or operations in cyberspace.

The first cyber threats were observed as early as the mid-1960s by university students who were given access to the computers of universities.[13] These students worked with the university computers and deciphered the coding behind the programming of these computers, which allowed them to access parts of the system that were thought to be inaccessible.[14] Cyber security and cyber threats, however, first appeared in 1972 with the precursor to the internet called The Advanced Research Projects Agency Networks (ARPANET).[15] A program, called the Creeper, was introduced to ARPANET, by the researcher, Bob Thomas. The Creeper moved around the system leaving messages that read, "I'm the Creeper, catch me if you can".[16] The inventor of e-mail, Ray Tomlinson, created a program called, The Reaper, that chased down The Creeper and

---

10 Buchan *Cyber Espionage and International Law* 1.
11 Buchan *Cyber Espionage and International Law* 1.
12 Schmitt *Tallinn Manual 2.0 on the International Law* 12.
13 Fox 2019 https://www.securitypursuit.com/blog-posts/history-matters-cyber-attacks-from-the-1960s.
14 Fox 2019 https://www.securitypursuit.com/blog-posts/history-matters-cyber-attacks-from-the-1960s.
15 Featherly 2021 https://www.britannica.com/topic/ARPANET.
16 Norman 2021 https://www.historyofinformation.com/detail.php?entryid=2860.

destroyed it.[17] Although unaware at the time, these two programs paved the way for computer viruses, cyber-attacks and anti-virus software to be developed.[18] Eventually, the ARPANET system was introduced to telephone cables that enabled the system to stretch throughout the world. Between 1972 and 1974, discussions on cyber security grew to such an extent that the USA air force, together with the Advanced Research Project Agency (ARPA) and the Electronics Systems Division (ESD), started researching cyber security on a national level.[19] By 1976, the term, cyber security, was a common term and research institutions, together with governments, implemented certain security measurements in order to protect themselves from potential malevolent cyber-attacks.[20]

In 1979 a teenager by the name of Kevin Mitnick became the first person to conduct a cyber-attack on an internet system. He hacked into a digital equipment corporation, called, "The Ark", that was developing operating systems.[21] The cyber-attack was conducted by copying data from "The Ark" onto Kevin's computer. This attack realised the fear of the capability of internet systems to be used as cyber-attacks in cyberspace.[22] Small-scale cyber-attacks continued to emerge throughout the 1980s with attacks on the Los Alamos National Laboratory in the USA[23] and attacks on AT&T[24] among others, whilst the Trojan Horse virus, created in 1975 by John Walker, also made its first appearance on computer systems. This malicious software disguises itself as a useful program on a computer system, but in actual fact contains coding that can be used to spy on the infected computer system or cause the system to malfunction.[25] Trojan Horses are used in cyber threats to disguise the attack from the user of the

---

17 Norman 2021 https://www.historyofinformation.com/detail.php?entryid=2860.
18 Norman 2021 https://www.historyofinformation.com/detail.php?entryid=2860.
19 Featherly 2021 https://www.britannica.com/topic/ARPANET.
20 Chadd 2020 https://blog.avast.com/history-of-cybersecurity-avast.
21 Hesseldahl 2015 https://www.vox.com/2015/3/26/11560712/why-kevin-mitnick-the-worlds-most-notorious-hacker-is-still-breaking.
22 Hesseldahl 2015 https://www.vox.com/2015/3/26/11560712/why-kevin-mitnick-the-worlds-most-notorious-hacker-is-still-breaking.
23 Baker and Hamilton 2000 https://fas.org/sgp/library/bakerham.html.
24 Lasar 2011 https://www.wired.com/2011/09/att-conquered-20th-century/.
25 Britannica, The Editors of Encyclopaedia 2018 https://www.britannica.com/technology/trojan-computing.

computer system.[26] At this stage in time, cyber threats were grouped into two categories, cyber network exploitations and cyber network attacks.[27]

Cyber network exploitations refer to offensive operations designed to monitor or collect information from an affected computer system,[28] while cyber network attacks refer to cyber-attacks that are designed to destroy or harm affected computer systems.[29] With the rising complexity of cyber threats, such as hacktivism, cyber terrorism, cyber war and cyber vandalism, these categories are unable to categorise all forms of cyber threats, as elements of both categories can exist simultaneously in a cyber threat.

During 1985, at the height of the Cold War, a new form of cyber threat emerged, called cyber espionage.[30] Cyber espionage is defined by Buchan as "…the non-consensual collection of confidential information that is under the control of another actor".[31] Cyber espionage poses states a particular concern given that state and non-state actors can benefit from information gathered from an affected party.[32] Cyber espionage is however discussed in more depth later on in this chapter at 2.4.i.

The first comprehensive legislation to come into effect, in terms of cyber security, was enacted in 1986 by the USA.[33] This act is called the *Computer Fraud and Abuse Act* (hereinafter the CFAA) and it primarily prohibits the unauthorised access to computer systems by third parties.[34] Consequentially, the CFAA was responsible for the conviction of Robert Morris, in relation to one of the first recorded cyber-attacks in history.[35] Morris disrupted the world's nascent cyber infrastructure by inserting a worm

---

26 Britannica, The Editors of Encyclopaedia 2018 https://www.britannica.com/technology/trojan-computing.
27 Buchan *Cyber Espionage and International Law* 1.
28 Buchan *Cyber Espionage and International Law* 1
29 Buchan *Cyber Espionage and International Law* 1.
30 Fox 2019 https://www.securitypursuit.com/blog-posts/history-matters-cyber-attacks-from-the-1960s.
31 Buchan *Cyber Espionage and International Law* 1.
32 Buchan *Cyber Espionage and International Law* 1.
33 NACDL 1986 https://www.nacdl.org/Landing/ComputerFraudandAbuseAct.
34 NACDL 1986 https://www.nacdl.org/Landing/ComputerFraudandAbuseAct.
35 Rowen B 2017 https://www.infoplease.com/world/cyberwar-timeline.

attack into the system, causing an overflow of internet traffic that slowed down computer functions all over the world to a point that rendered them unusable.[36]

In 2007, Estonia fell victim to a devastating cyber-attack, which marked the first recorded cyber-attack "…done in an overtly political manner".[37] For 24 hours the country's Internet system was intentionally overloaded by a Distributed Denial of Service Attack (DDoS attack) which is "…an orchestrated swarm of Internet traffic"[38] that froze all systems running through the Internet.[39] The DDoS attack had a similar outcome to the worm attack that Robert Morris was responsible for in 1988, however, the difference between the two was in the functionality of the attacks. The worm attack is a program that multiplies itself to a point where the computer system is overloaded, while the DDoS attack is a command directed at different computer systems to simultaneously send data to the targeted system in order to create the intended overload.[40] The DDoS attack is more effective, because cyber security measurements such as anti-virus programs cannot detect the DDoS attack.[41] After the attack on Estonia, the North Atlantic Treaty Organisation's (NATO) Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia, invited an independent International Group of Experts to develop a manual on the law regulating cyber warfare,[42] known as the Tallinn Manual on the International Law Applicable to Cyber Warfare[43] that will be discussed in more depth later on in this chapter at 2.3.

On 7 August 2008, a cyber-attack was launched on Georgia. The country was attacked by the Russian military whilst its internet systems suffered numerous coordinated cyber-attacks from an unknown source.[44] These cyber-attacks were beneficial to the

---

36 Rowen B 2017 https://www.infoplease.com/world/cyberwar-timeline.
37 Tamkin 2017 https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/.
38 Tamkin 2017 https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/.
39 Tamkin 2017 https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/.
40 Singer and Friedman *Cybersecurity and Cyberwar* 44.
41 Singer and Friedman *Cybersecurity and Cyberwar* 44.
42 Anon *Tallinn Manual 2.0 on the International Law* 91.
43 Anon *Tallinn Manual 2.0 on the International Law* 91.
44 Shakarian 2011 *Military Review* 63-68.

Russian military's attack by bringing the infrastructure of Georgia to a standstill. In both the Estonia and Georgia cases, it is alleged that the Russian government contracted various hacking groups to conduct these cyber-attacks on Russia's behalf,[45] however, there is no conclusive evidence to prove this.

In 2010, Stuxnet, the first cyber weapon able to inflict physical damage, emerged.[46] The Iranian nuclear plant, Natanz, was the target of this attack that reportedly destroyed a fifth of its nuclear centrifuge.[47] It is believed to have been orchestrated by the joint efforts of the US and Israel, that aimed to take control of the nuclear site's control systems.[48] Stuxnet is a worm designed to attack the Siemens program that automotive industrial machines function on, and then updates it with destructive instructions that destroy the functionality of the affected machinery.[49]

The same DDoS attack used in 2007 on Estonia, made another appearance in 2014 in the Ukrainian territory of Crimea, and similar to the 2008 cyber-attack on Georgia, was accompanied by a Russian-armed coalition.[50] These combined cyber and kinetic attacks resulted in the ongoing Russian occupation of the Crimean peninsula.[51] The DDoS attack that was used in Crimea is estimated to have been thirty-two times larger than the attack used in Estonia in 2007 and have temporarily disrupted internet connectivity throughout the Ukraine.[52]

2.3 Tallinn Manual and Tallinn Manual 2.0

Following the cyber-attack on Tallinn in Estonia, the North Atlantic Treaty Organisation (NATO) assessed the cyberspace capabilities of its member states as well as legislations regulating them.[53] Cyber security and infrastructure defence were focussed

---

45 Shakarian 2011 *Military Review* 63-68.
46 Rowen B 2017 https://www.infoplease.com/world/cyberwar-timeline.
47 Fildes *BBC News*.
48 Fildes *BBC News*.
49 Wolf "Cyber-Physical Systems" 5.
50 Shakarian 2011 *Military Review* 63-68.
51 Shakarian 2011 *Military Review* 63-68.
52 Shakarian 2011 *Military Review* 63-68.
53 Schmitt *Tallinn Manual on the International Law* 1.

on and found to be ineffective against cyber-attacks.[54] As a result, NATO established a cyber-security policy in relation to the Wales Summit in September 2014.[55] The adopted cyber-security policy aimed to bind all NATO states in accepting the evolving threat that cyberspace represents, and to recognise that international law applies to cyberspace.[56] Furthermore, NATO established the Cooperative Cyber Defence Centre of Excellence (CCDCOE) that aims to develop technological, strategic and legal advancements in cyberspace.[57] The CCDCOE invited an independent International Group of Experts to develop a manual on the law regulating cyber warfare.[58] The Tallinn Manual on the International Law Applicable to Cyber Warfare was completed and was first published in 2013 by the Cambridge University Press. The Tallinn Manual, a non-binding document designed to interpret existing law, applies to cyber warfare[59] and addresses cyber operations that are prohibited by article 2(4) of the United Nations Charter (UN Charter),[60] the prohibition on the use of force clause. The Tallinn Manual also encourages states to practice their right to self-defence afforded to them by article 51 of the UN Charter where a cyber-operation threatens a state's sovereignty and territorial integrity.[61]

In 2017, a follow-up manual to the Tallinn Manual, the Tallinn Manual 2.0 was published.[62] The Tallinn Manual 2.0 expanded on the work in the Tallinn Manual by discussing cyber operations that are not seen as force under article 2(4) or as armed attacks under article 51.[63] The Manual rather focuses on cyber operations that are encountered by states on a frequent basis and require cyber security systems rather than forceful self-defensive measurements.[64] Even though the Tallinn Manual is a non-

---

54 Schmitt *Tallinn Manual on the International Law* 1.
55 NATO 2014 https://www.nato.int/cps/en/natohq/official_texts_112964.htm.
56 NATO 2014 https://www.nato.int/cps/en/natohq/official_texts_112964.htm.
57 NATO 2021 https://ccdcoe.org/.
58 Schmitt *Tallinn Manual on the International Law* 1.
59 NATO Cooperative Cyber Defence Centre of Excellence Tallinn Manual https://ccdcoe.org/research/tallinn-manual/.
60 Schmitt *Tallinn Manual on the International Law* 42.
61 Schmitt *Tallinn Manual on the International Law* 42.
62 Anon *Tallinn Manual 2.0 on the International Law* 91.
63 Schmitt *Tallinn Manual 2.0 on the International Law* 1-2.
64 Schmitt *Tallinn Manual 2.0 on the International Law* 2.

binding document, legal experts, legislators and legal scholars regard it as an influential source in cyber-related issues.[65] The state practice on the regulation of cyber issues as well as the creation of cyber law by states necessitates an update to the Tallinn Manual and Tallinn Manual 2.0 and as a result, the CCDCOE have announced in 2021 that a five-year project will be conducted by the International Group of Experts, directed by Professor Michael Schmitt, who have directed both the Tallinn Manual and the Tallinn Manual 2.0.[66] The latest project will be an updated version on legislative matters concerning both the previous versions and will be titled, the Tallin Manual 3.0.[67]

The non-binding nature of the Tallinn Manual is necessary for the CCDCOE's intended purpose.[68] The CCDCOE is not intended to be a law-creating body, but rather to give legislators a well-researched source to base legislation on.[69] The International Group of Experts are invited by the CCDCOE to participate in the project in a non-representative manner; each expert contributes to the project in his or her personal capacity and does not represent any state or organisation.[70] The Tallinn Manual is scrutinised by representatives of states before being published in order to ensure that the findings of the International Group of Experts are not seen as findings that are out of touch with cyber incidents in practice.[71] The Tallinn Manual will continue to be a non-legally binding document that provides unbiased interpretations of legislation and international law in the context of cyberspace.[72]

---

65 Schmitt *Tallinn Manual 2.0 on the International Law* 2-3.
66 NATO 2021 https://ccdcoe.org/news/2021/the-ccdcoe-invites-experts-to-contribute-to-the-tallinn-manual-3-0/.
67 NATO 2021 https://ccdcoe.org/news/2021/the-ccdcoe-invites-experts-to-contribute-to-the-tallinn-manual-3-0/.
68 Schmitt *Tallinn Manual on the International Law* 1.
69 Schmitt *Tallinn Manual on the International Law* 1.
70 Schmitt *Tallinn Manual on the International Law* 1.
71 Schmitt *Tallinn Manual on the International Law* 1.
72 Schmitt *Tallinn Manual on the International Law* 1.

2.4 Cyber threats, cyber operations and cyber-attacks, meaning and forms

With the advent of the fifth domain of warfare, cyberspace, a number of new terms were created to ease the definition of acts and threats in cyberspace. This section is designed to explain the concepts of cyber threats, cyber operations and cyber-attacks as well as to differentiate between the numerous forms that exist. Cyber threats, cyber operations and cyber-attacks are closely associated with armed threats, armed operations and armed attacks respectively.[73] The difference between the wording armed and cyber can be defined as armed meaning traditional or kinetic[74] and cyber meaning threats, operations or attacks conducted in cyberspace.[75]

The term, cyber threat, similar to the term, armed threat, constitutes a threat of a cyber-related incident taking place and that the incident has not yet taken place, but is expected to.[76] A cyber threat has the potential to become a cyber-operation or cyber-attack, but there is also the possibility that the perceived cyber threat will not come to fruition.[77]

Cyber operations are operations conducted in cyberspace that can either arise from a perceived threat or can occur without the affected state having any prior notion of the operation taking place.[78] The effect of a cyber-operation can either rise to the level of damage for it to be prohibited by article 2(4), or it can fall short of the required level of damage to do so.[79] In short, a cyber-operation in and of itself is the process an attack follows rather than the attack itself.

Cyber-attacks are defined by the USA's Joint Chiefs of Staff's Lexicon of 2011[80] as:

---

73 Libicki "Correlations between cyberspace attacks and kinetic attacks" 200-202.
74 Libicki "Correlations between cyberspace attacks and kinetic attacks" 200-202.
75 Libicki "Correlations between cyberspace attacks and kinetic attacks" 200-202.
76 Libicki "Correlations between cyberspace attacks and kinetic attacks" 207.
77 Libicki "Correlations between cyberspace attacks and kinetic attacks" 207.
78 Roscini *Cyber Operations* 43-44.
79 Roscini *Cyber Operations* 44.
80 The Vice Chairman of the Joint Chiefs of Staff Memorandum for Chiefs of the Military Services Commanders of the Combatant Commands Directors of the Joint Staff Directorates. See Cartwright date unknown https://info.publicintelligence.net/DoD-JointCyberTerms.pdf 5.

> … a hostile act using computer or related networks or systems and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions [although the] intended effects of cyber-attack are not necessarily limited to the targeted computer systems or data themselves…

Cyber-attacks are in essence armed attacks that are conducted in cyberspace. A cyber-attack can rise to the level of a threat that is prohibited by article 2(4) or not.[81] The difference between cyber-attacks and cyber operations is that cyber operations, as discussed earlier, are the processes that lead up to attacks whilst a cyber-attack causes damage. This means that all cyber-attacks have elements of cyber operations, but not all cyber operations have elements of cyber-attacks. This is echoed in Rule 30 of the Tallinn Manual[82] stating that:

> A cyber-attack is a cyber-operation, whether offensive or defensive that is reasonably expected to cause injury or death to persons or damage or destruction to objects.

Cyber-attacks can be divided into different groups that form their own functions and can result in different magnitudes of harm not only in cyberspace, but in the physical world.[83] According to Singer and Friedman,[84] there are four different modes of cyber-attacks, namely, information gathering and espionage, disruption of services to hijack sites for propaganda or publicity, physical systems attack and propaganda and social media influence.

i) Information gathering and espionage involve passive recognisance and probing of public and private networks to search for useful data and weaknesses in systems.[85] Buchan[86] describes cyber espionage as follows:

> …the non-consensual collection of confidential information that is under the control of another actor.

---

81 Schmitt *Tallinn Manual 2.0 on the International Law* 340.
82 Schmitt *Tallinn Manual 2.0 on the International Law* 91.
83 Singer and Friedman *Cybersecurity and Cyberwar* 2.
84 Singer and Friedman *Cybersecurity and Cyberwar* 54-66.
85 Singer and Friedman *Cybersecurity and Cyberwar* 59.
86 Buchan *Cyber Espionage and International Law* 2.

There are two categories of cyber espionage, namely, political espionage and economic espionage. The circumstances in which an act of cyber espionage is conducted, will determine under which category it will be grouped.[87] Political espionage occurs when a state enhances its national security to collect information about this state in an unsolicited manner.[88] Non-state actors such as terrorist organisations are increasingly responsible for such a form of espionage although their aim may be different to that of a state.[89] Economic espionage occurs when states obtain trade secrets from foreign companies in an unsolicited manner in order to distribute these secrets to the state's domestic companies.[90] The aim of this form of espionage is to boost a state's economy.[91]

ii) Disruption of service used to hijack sites for propaganda or publicity is applied to hack a government website and place fake information on it.[92] Terrorist organisations such as Al-Qaeda are known to use these tactics for propaganda purposes.[93] Al-Qaeda published an online English magazine, called Inspire, to recruit American and European citizens into their ranks, mainly to become suicide bombers.[94]

iii) Physical systems attacks are aimed at disabling physical systems such as systems that operate bank teller machines or sewage plants etc.[95] These attacks are mostly conducted by Stuxnet, discussed earlier in the chapter, which can cause destruction in the physical world.[96]

iv) Propaganda and social-media influence are good examples of the Iranian protests in 2009 against an oppressive leader, and gave rise to the Arab spring.[97] These forms of cyber-attacks are very common since 2010 with the rise of Fake News.[98]

---

87 Buchan *Cyber Espionage and International Law* 2.
88 Buchan *Cyber Espionage and International Law* 2.
89 Buchan *Cyber Espionage and International Law* 2-3.
90 Buchan *Cyber Espionage and International Law* 3.
91 Buchan *Cyber Espionage and International Law* 3.
92 Singer and Friedman *Cybersecurity and Cyberwar* 208.
93 Singer and Friedman *Cybersecurity and Cyberwar* 105.
94 Singer and Friedman *Cybersecurity and Cyberwar* 105.
95 Singer and Friedman *Cybersecurity and Cyberwar* 69.
96 See para 2.2 above.
97 Grossman 2009 http://content.time.com/time/world/article/0,8599,1905125,00.html.
98 Singer and Friedman *Cybersecurity and Cyberwar* 214.

Propaganda and fear are distributed from unknown sources to the public, which is shown to have the tendency not to "fact check" information that is available on social media and believing it to be a credible source of information.[99] This has the effect that state and non-state actors can spread false information that is intended to contribute to their agenda relatively easily.[100]

2.5 Problem with attribution

With the 2007 cyber-attack on Tallinn, Estonia, the actor behind the cyber-attack was identified, although it is accepted to have been Russia. However, without definitive proof, Russia cannot be held accountable.[101] The in-effect to identify an actor behind an attack is a relatively new problem. With conventional warfare, the colour of soldiers' uniforms, the language they speak or the position of a state's military within another state's territory were clear indications of who was behind an attack and who could be held accountable.[102] There are no borders in cyberspace, there is no flag identifying where the attack comes from and there is only one language, coding.[103] This gives rise to the problem of attribution, meaning that there is no certain way to attribute an attack without someone taking responsibility for the action.[104]

Cyberspace consists of various connections between all "online" computers, where each computer can be identified with an identity code called an internet protocol (IP) address.[105] IP addresses can be traced from an action on the internet back to the computer that was commanded to conduct the action in the first place, meaning that most actions are traceable and can thus be attributed to the owner of the computer that conducted the attack.[106] The problem with this is that attacks such as the DDoS attack uses multiple computers to make the original IP address undetectable.[107] When

---

99 Singer and Friedman *Cybersecurity and Cyberwar* 214.
100 Singer and Friedman *Cybersecurity and Cyberwar* 214.
101 Shakarian 2011 *Military Review* 63-68.
102 Singer and Friedman *Cybersecurity and Cyberwar* 72.
103 Singer and Friedman *Cybersecurity and Cyberwar* 72.
104 Singer and Friedman *Cybersecurity and Cyberwar* 72.
105 Buchan *Cyber Espionage and International Law* 1.
106 Singer and Friedman *Cybersecurity and Cyberwar* 296.
107 Singer and Friedman *Cybersecurity and Cyberwar* 44.

the cyber-attack on Tallinn, Estonia, was examined, it was found that over a million computers were used to conduct the attack.[108] The scale of the attack is just so great that it is impossible to determine where the command comes from.[109] On a smaller scale such as cyber espionage, the IP address is traceable to the initiating party, however, third party hackers are often used to conduct cyber-attacks and as such, the identity of the party giving instructions to the third party remain un-identifiable.[110] Tracking IP addresses in cyberspace cannot be carried over into the physical world.[111]

There are three problems to take into account when dealing with the question of attribution: there are no geographical limitations in cyberspace; the owner of a captured computer is often oblivious that his/her computer is being used by a third party in an attack; where an attack in cyberspace is conducted, the attack can only be traced back to the computer/computers being used to launch the attack.

i) Geographical limitations have always been an identifying element for attribution, in establishing whether or not an attack by a foreign state is attributable to the state.[112] With the rise of cyberspace, geographical borders became obsolete in that there are no geographical borders in cyberspace.[113] For example, Iceland can conduct a cyber-attack on Norway by enlisting hackers situated in Russia, to attack Norway through computers situated in the Netherlands. The attributable party would be Iceland, however, the attack would seem to have come from the Netherlands. Ways of creating "borders" in cyberspace by means of firewalls are used by some states, such as China,[114] however, this form of creating borders can infringe on people's right to access information as guaranteed by article 19 of the Universal Declaration of Human Rights,[115] given that the government of a

---

108 Anon 2017 https://e-estonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/.
109 Singer and Friedman *Cybersecurity and Cyberwar* 76.
110 Singer and Friedman *Cybersecurity and Cyberwar* 76.
111 Singer and Friedman *Cybersecurity and Cyberwar* 76.
112 Singer and Friedman *Cybersecurity and Cyberwar* 72-76.
113 Singer and Friedman *Cybersecurity and Cyberwar* 72.
114 Chan 2018 https://www.bloomberg.com/quicktake/great-firewall-of-china.
115 Article 19 of the *Universal Declaration of Human Rights* (1948) and Resolution 59 of the UN General Assembly (1946).

state will then control all content online, and the citizens will not be able to access the internet freely.[116]

ii) The owner of a captured computer is often oblivious that his/her computer is being used by a third party in an attack.[117] It was found that 25% of the computers used in the cyber-attack on Tallinn Estonia was based in the USA.[118] The owners of these computers had no idea that their computers were used in the attack and likely never will.[119] This is because a compromised computer is not affected in any way. The attackers simply create a path for information to flow from their computer through the captured computer to the affected computer.[120]

iii) Where an attack in cyberspace is conducted, the attack can only be traced back to the computer/computers used to launch the attack.[121] By going back to the example given in (i), computers in the Netherlands conducted the attack on Norway. The Russian hackers who used these computers cannot be traced because the IP addresses they used were those of computers in the Netherlands meaning neither Russia nor Iceland was attributable. Even if it was possible to attribute the attack to the Russian hackers, Iceland would still be safe from attribution because the contract between them and the Russian hackers took place in the physical world.

Another problem that states, affected by a cyber-attack, face, is that programs designed to initiate a cyber-attack give no indication on what the intended outcome of the attack may be.[122] The program can either spy on government systems or destroy a power grid regulated by government systems. This uncertainty creates even more uncertainty on how to react appropriately against a particular cyber-attack.[123] An

---

116 Chan 2018 https://www.bloomberg.com/quicktake/great-firewall-of-china.
117 Singer and Friedman *Cybersecurity and Cyberwar* 113-115.
118 Anon 2017 https://e-estonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/.
119 Anon 2017 https://e-estonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/.
120 Singer and Friedman *Cybersecurity and Cyberwar* 113-115.
121 Singer and Friedman *Cybersecurity and Cyberwar* 74.
122 Singer and Friedman *Cybersecurity and Cyberwar* 76.
123 Singer and Friedman *Cybersecurity and Cyberwar* 76.

action in retaliation may be greater than necessary to repel the cyber-attack because the nature of the attack remains uncertain.[124]

The inability to establish to whom a cyber-attack may be attributed is not always a question of who the culprit is, but rather that there is no sufficient evidence in order to attribute an attack to a suspected party.[125] In most cases a state can reasonably guess who initiated a cyber-attack by the behaviour of another state.[126] To clarify this statement the cyber-attack on Georgia can be used where it was reasonably expected that Russia initiated the attack.[127] The reason for suspecting Russia is because, when the cyber-attack disabled the electricity network all over Georgia, a Russian kinetic attack invaded the country, leading to the suspicion of Russia's involvement in the cyber-attack due to the timing of the two attacks.[128] This assumption cannot be used as proof of a state's involvement and must thus be seen as speculation. However, at the rate at which cyberspace and its accompanying elements are evolving, a solution to this question may be close at hand. Furthermore, state practice on the matter can provide future procedures for states to follow in order to attribute another cyber-attack to a state where the attacker is unclear.

2.6 Conclusion

In this chapter, a historical timeline starting in the 1960s during which the evolution of cyber threats together with specific relevant cyber-attacks throughout history could be observed. The cyber-attack on Tallinn, Estonia, was one of the historical tipping points for cyber security and gave rise to the inception of the CCDCOE as well as the Tallinn Manual and Tallinn Manual 2.0. Out of this it can clearly be seen that cyber threats are evolving at a rate that has never in history been observed. It is also

---

124 UN A51 *Charter of the United Nations* (24 October 1945) https://www.un.org/en/about-us/un-charter/full-text.
125 Singer and Friedman *Cybersecurity and Cyberwar* 76.
126 Shakarian 2011 *Military Review* 63-68.
127 Shakarian 2011 *Military Review* 63-68.
128 Shakarian 2011 *Military Review* 63-68.

observed that international law, states and state organisations are assisting one another in creating a system where cyberspace can be regulated of which a good example is the Tallinn Manual. It is necessary to bear in mind that the Tallinn Manual is non-binding and serves primarily the purpose of advice on ideas that have been thoroughly researched by the independent group of legal experts who were tasked to create this manual. Cyber-attacks have been dealt with in detail in order to understand how the different types of attacks in cyberspace can affect the physical world. The problem with attribution is a relatively new problem pertaining to cyberspace. It is the lack of borders in cyberspace, the inability to realise when a computer is used in a cyber-attack and the fact that an IP-address is only traceable to the computer that have conducted the attack and not to the computers that captured them that attribution is so challenging in cyberspace. The scale on which cyber-attacks is conducted makes the task of attribution even harder because attacks are conducted by using multiple computers. The uncertainties regarding attribution in cyber warfare do not have a solution as of yet, however, the evolution of cyberspace has proved that problems are solved with increasing speed and as such a possible solution may be close at hand.

Chapter 3: Cyber operations/attacks and the prohibition on the use of force

3.1 Introduction

Use of force and its prohibition have been implemented by rulers of states and kingdoms since ancient times and have been developed to be relevant to all forms of attacks that a state may reasonably expect to face in times of war. With the advent of cyberspace, uncertainty arose on whether cyber-attacks can be prohibited by using force. In this chapter, the prohibition on the use of force, as well as self-defense is discussed in depth in the light of cyberspace and cyber operations. An historical overview is used to illustrate the evolution of use of force to better understand the uncertainty that cyber operations pose in this regard. An in-depth analysis is conducted into different forms of force to establish when force may be prohibited in terms of international customary law and whether cyber operations meet the requirements for prohibition. This will be done by comparing different viewpoints regarding the meaning of force and interpreting the Tallinn Manual in the light of these findings in order to establish whether cyber operations form part of the definition of prohibited force. Self-defense and pre-emptive self-defense are dealt with in depth as defensive measures against cyber operations. The meaning behind the term, armed attack, is defined and compared to cyber-attacks in order to establish a possible correlation between the two. The purpose of this chapter is to establish whether prohibition on use of force as well as limitations to the rule, applies to cyberspace and cyber-attacks.

3.2 Historical overview on the prohibition of use of force

All throughout human history, warfare was part of human interaction with one another. For centuries wars were fought without any regulations, regulating or prohibiting use of force between peoples.[129] Regulation of warfare eventually started to develop, and in Rome the concepts of just and unjust war began to rise.[130] This ancient form of

[129] Speier 1941 *American Journal of Sociology* 445.
[130] Nussbaum 1952 *University of Pennsylvania LR* 678.

regulation of use of force was called the *ius fetiale* that was established by the *fetiales*, a group of priests who was responsible for the upkeep of international relations in the Roman state.[131]

When Christianity was adopted by the Romans, it influenced among others, the doctrine of "Just Warfare".[132] Christian theologians such as St. Augustine, Chrysostom, Jerome, Oroeius, Salvian and St. Thomas Aquinas were the spear heads that drove this influence.[133] St. Thomas Aquinas stated in *Summa Theologica*[134] the three criteria for just warfare that he developed from Augustine's sermon on the son of the centurion. In Aquinas's objects he comes to the conclusion that all war is sin and an act against God and peace. He interrupted himself by stating that Augustine stated in the abovementioned sermon, "do violence to no man… and be content with your pay".[135] Aquinas concluded that, for Augustine to preach to soldiers to be content with their pay, means that soldiering is not a sin in itself.[136] Aquinas then developed the three requirements for a war to be just: the authority of a sovereign to wage war; the cause of war must be just and the just cause must have sprung from the right intentions.[137]

With the advance of independent European states, came the evolution of the doctrine of "Just Warfare".[138] "Wars were states of legal affairs rather than a matter of subjective moral judgement".[139] States did not have the moral authority to justify the actions of another in relation to warfare and as such "Just Warfare" as developed in ancient Rome ceased to exist.[140] This perspective on warfare was endorsed by the rising positivist movement, and by the Peace of Westphalia in 1648.[141] The Peace of

---

131 Britannica, The Editors of Encyclopaedia 2016 https://www.britannica.com/topic/fetial.
132 McGriffert 1909 *Harvard Theological Rev* 29.
133 McGriffert 1909 *Harvard Theological Rev* 29.
134 Aquinas *Summa Theologica* 1813.
135 Aquinas *Summa Theologica* 1813.
136 Aquinas *Summa Theologica* 1813.
137 Aquinas *Summa Theologica* 1813.
138 Von Elbe 1939 *American Journal of International Law* 665.
139 Von Elbe 1939 *American Journal of International Law* 665.
140 Von Elbe 1939 *American Journal of International Law* 665.
141 Gross 1948 *The American Journal of International Law* 20-41.

Westphalia that was signed by the Dutch, the Spanish and the Germans, after the conclusion of the eighty year war, established the European system of the balance of powers, which survived in Europe until its end with the outbreak of the 1st World War.[142]

When the 1st World War ended, an international institution was established to repair relations between states.[143] This institution was called the League of Nations and was established in 1919.[144] Under the 1919 Covenant of the League of Nations, a representative of each member state was selected to form part of the council.[145] Articles 8 and 9 of the Covenant dealt with armaments and reduced the manufacturing of weapons by all member states to the lowest possible level to ensure that the "evil effects" of private manufacturing of weapons for war are suppressed.[146] All member states were directed to raise all differences between states to the council for arbitration.[147] The Covenant did not revoke the right of states to wage war, but war was subject to limitations and would be conducted only as a last resort.[148] In 1928, the General Treaty for Renunciation of War was signed as an attempt to regulate the use of force by legal means, more commonly known as the Pact of Paris or the Kellogg–Briand Pact.[149] Article 1[150] of the Treaty enabled parties within the Treaty to "condemn recourse to war" as well as "renounce it".

> The High Contracting Parties solemnly declare in the names of their respective peoples that they condemn recourse to war for the solution of international controversies, and renounce it, as an instrument of national policy in their relations with one another.

---

142 Britannica, The Editors of Encyclopaedia 2021 https://www.britannica.com/event/Peace-of-Westphalia.
143 Britannica, The Editors of Encyclopaedia 2020 https://www.britannica.com/topic/League-of-Nations.
144 Britannica, The Editors of Encyclopaedia 2020 https://www.britannica.com/topic/League-of-Nations.
145 Article 3 of the *Covenant of the League of Nations*, 1924.
146 Articles 8 & 9 of the *Covenant of the League of Nations*, 1924.
147 Article 5 of the *Covenant of the League of Nations*, 1924.
148 Ridgley 1997 *The British Library Journal* 41-46.
149 Dugard *et al International Law* 730.
150 Article 1 of the *General Treaty for Renunciation of War*, 1928.

Peaceful international relations ended once more with the outbreak of the Second World War in 1939. As a result of the horrific consequences of the war, the Charter of the United Nations (UN Charter) was adopted in 1945. This Charter established a framework to regulate use of force by members of the international community[151] that is still in force today. The Kellogg-Briand Pact also remains in force today although the UN Charter has absorbed most of its use.

3.3 Article 2(4) the prohibition on the use of force

The preamble of the UN Charter as well as article 1, 11, 33-38 and 99 of said Charter determines that all disputes should be settled peacefully.

Article 2(4) elaborates by prohibiting use of force, stating that:

> All members shall refrain 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.[152]

In the International Court of Justice (ICJ) judgement of 1986 between Nicaragua and the USA the court regarded the article 2(4) on prohibition of the use of force generally reflects customary international law[153] and as such, the prohibition is at the core part of *jus cogens.*[154] This means that there is no dispute on whether or not article 2(4) is enforceable, and that the question of what "force" is, referred to in terms of article 2(4), rather should be looked at.

States interpreted force in terms of article 2(4) depending on their influential and economical position in relation to other states. Waxman[155] was of the opinion that there were three such viewpoints, namely, the dominant viewpoint, the alternative viewpoint and the viewpoint focusing on the violation and defence of rights, specifically that it protects states' rights to freedom from interference. The first viewpoint that

---

151 Dugard *et al International Law* 701.
152 UN date unknown https://www.un.org/en/sections/un-charter/un-charter-full-text/ para 4.
153 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v USA) Merits* 1986 ICJ Reports 14 at 98-100 (hereinafter the *Nicaragua* judgment).
154 Roscini *Cyber Operations* 45.
155 Waxman 2011 *Int'l L Stud* 45-46.

Waxman identified, he called the dominant viewpoint.[156] The dominant viewpoint was favoured by the US and its allies, largely the NATO-member states, and it followed the interpretation that article 2(4) only applies to military attacks or armed force between states.[157] By reading the meaning behind the text in article 2(4), it is clear that the article supports this.[158] There is a counter argument, however, that article 51's distinctive constraints on "armed attacks", which will be dealt with in chapter 3.7, indicates that the drafters envisioned prohibited force to be broad.[159] When reading the document, "discussions of means", as Waxman put it, it indicates an intention to regulate armed force more strictly.[160]

The second viewpoint, the alternative viewpoint that Waxman identified, is a wider approach.[161] This viewpoint does not highlight the instrument utilised, but rather its purpose and general effect.[162] Force is seen as a form of coercion for example, military force is merely a branch of coercion, as such coercion is prohibited under this viewpoint.[163] The third world favoured this viewpoint interpreting force to include political and economic coercion, among other forms of pressure that endangers the sovereignty of states.[164] The critique against the alternative viewpoint is that, with a wider approach, it is difficult to draw lines between unlawful coercion, an example of which is the unlawful sanctions that were placed on Nicaragua by the USA,[165] and lawful pressure,[166] an example of which is the economic sanctions placed on South Africa in order to pressure it into abandoning the apartheid regime.[167] The Security Council under Chapter VII may implement enforcement measurements whenever it finds that a threat to the peace, a breach of the peace, or an act of aggression has

---

156 Waxman 2011 *Int'l L Stud* 45.
157 Waxman 2011 *Int'l L Stud* 45.
158 Waxman 2011 *Int'l L Stud* 45.
159 Waxman 2011 *Int'l L Stud* 46.
160 Waxman 2011 *Int'l L Stud* 46.
161 Waxman 2011 *Int'l L Stud* 46.
162 Waxman 2011 *Int'l L Stud* 46.
163 Waxman 2011 *Int'l L Stud* 46.
164 Waxman 2011 *Int'l L Stud* 46.
165 Case concerning the *Military and Paramilitary Activities in and Against Nicaragua* (*Nicaragua v United States of America*) (Merits) https://www.icj-cij.org/public/files/case-related/70/6505.pdf 5.
166 Waxman 2011 *Int'l L Stud* 46.
167 Dugard *et al International Law* 733.

occurred.[168] When the Council may implement enforcement measurements, they are economic or diplomatic in nature.[169] If these measurements are inadequate, the Council may use military enforcement in order to protect world peace.[170]

Waxman identified a third viewpoint focusing on the violation and defence of rights specifically that they protect states' rights to freedom from interference.[171] This viewpoint is favoured by the third world and might, as Waxman put it "…tie the concept of force to improper meddling or intrusion of the internal affairs of other states, rather than a narrow set of means".[172]

The ICJ takes a position that favours the dominant viewpoint in its judgement on the *Nicaragua* case[173] stating that:

> …the United States of America, by producing in 1983 a manual entitled *"Operaciones sicológicas en guerra de guerrillas"*, and disseminating it to *contra forces*, has encouraged the commission of acts contrary to general principles of humanitarian law; but does not find a basis for concluding that any such acts that may have been committed are imputable to the United States of America as acts of the United States of America…

In the *Operaciones sicológicas en guerra de guerrillas* Manual,[174] the USA argued that psychological warfare is an instrument equal to an act that is regarded as force in terms of article 2(4).[175] The Manual was published by the USA as its defence against Nicaragua.[176] The ICJ found that a narrow approach to the interpretation of

---

168 UN A39 *Charter of the United Nations* (24 October 1945) https://www.un.org/en/about-us/un-charter/full-text.

169 UN A41 *Charter of the United Nations* (24 October 1945) https://www.un.org/en/about-us/un-charter/full-text.

170 UN A42 *Charter of the United Nations* (24 October 1945) https://www.un.org/en/about-us/un-charter/full-text.

171 Waxman 2011 *Int'l L Stud* 46.

172 Waxman 2011 *Int'l L Stud* 46.

173 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v USA) Merits* 1986 ICJ Reports 14 at 98-100.

174 Galbán, Rodrigues and Fernández 2009 *Review of Medical Humanities* 1-22.

175 Galbán, Rodrigues and Fernández 2009 *Review of Medical Humanities* 1-22.

176 Galbán, Rodrigues and Fernández 2009 *Review of Medical Humanities* 1-22.

psychological warfare against article 2(4) does not amount to actions that are imputable towards the USA.[177]

In order to establish whether cyber operations can be included in the definition of force that article 2(4) prohibits, the definition of force must be interpreted in the light of cyber operations. Rule 11 of the Tallinn Manual contains the criteria for when cyber operations amount to a threat or a use of force.[178] Rule 11 states that, "…cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of using force".[179] Article 2(4) does not define force, however, in articles 41 and 46 in the preamble of the Charter, force appears with the adjective, armed.[180] The argument can be made that, if the writers wanted to express force as "armed force" in article 2(4), they would have done so expressly, which they have not, and that this eludes to a wider meaning of force in article 2(4).[181] A narrow reading of article 2(4) seems to be sustained by a teleological interpretation thereof.[182]

Rule 68 of the Tallinn Manual 2.0[183] states that:

> A cyber operation that constitutes a threat or use of force against the territorial integrity of political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful.

This rule echoes what article 2(4) of the UN Charter stipulates over all forms of force between states and applies its merit to cyber operations. Rule 68 draws a comparison between cyber operation-related force and article 2(4). Rule 68 of the Tallinn Manual does not, however, provide guidance towards when a cyber-operation can be considered as use of force under article 2(4). The legal experts tasked with compiling The Tallinn Manuals 1.0 and 2.0 faced differing opinions on the interpretation of article 2(4) as well as on its implementation. They differed mainly on the dominant viewpoint,

---

177 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v USA) Merits* 1986 ICJ Reports 14 at 98-100.
178 Roscini *Cyber Operations* 45.
179 Schmitt *Tallinn Manual on the International Law* Rule 11 on 45.
180 UN Charter Preamble UNTS Vol 16 1.
181 Roscini *Cyber Operations* 45.
182 Roscini *Cyber Operations* 45.
183 Schmitt *Tallinn Manual 2.0 on the International Law* Rule 68.

the alternative viewpoint and the viewpoint focusing on the violation and defence of rights, specifically that it protects states' rights to freedom from interference. According to Roscini, three conditions must be met in order for article 2(4) to apply to cyber operations, namely, cyber operations must be attributed to a state; cyber operations must amount to a threat or use of force and the threat or use of force must be exercised in the conduct of international relations.[184]

3.4 Forms of prohibited force

The next step is to establish whether the article 2(4) prohibition on the use of force is limited to armed force only and whether the indirect use of force is also considered as force under article 2(4). According to Dugard,[185] the traditional viewpoint is that armed force only is prohibited by article 2(4). Authorisation must first be given by the UN Security Council, alternatively, a state may act in self-defence to halt an attack by another state. There are, however, differing viewpoints on the matter, which will be examined later on in this chapter. Dugard further points out that developing countries, for example, maintain that economic coercion is a form of force that is just as destructive to political independence as armed force. With the 1945 drafting of the UN Charter in San-Francisco, certain states, mainly third world countries and states that follow the alternative viewpoint regarding the interpretation of article 2(4),[186] lobbied for economic coercion to be included into the definition of use of force and thus be prohibited by article 2(4).[187] Although the scale and effect of economic coercion can theoretically be of such a magnitude that the threshold for it to be considered as a use of force is met, it will seldom be to such an extent that it can be considered as unjust force.[188] This view is supported by the Declaration on Principles of International Law of 1970 stating that economic force aiming[189] "to coerce another state in order to obtain from it the subordination of the exercise of its sovereign rights",[190] is prohibited.

---

184 Roscini *Cyber Operations* 44.
185 Dugard *et al International Law* 733-734.
186 Waxman 2011 *Int'l L Stud* 46.
187 Schmitt *Tallinn Manual 2.0 on the International Law* 330.
188 *Nicaragua* judgment para 228.
189 Dugard *et al International Law* 733.
190 Resolution 2625 (XXV)

This viewpoint only carries weight if, firstly, economic force is viewed as an unlawful intervention and secondly, the unlawful intervention's aim is to undermine a state's sovereignty by way of subordination.[191] The view that economic coercion is prohibited by article 2(4) is not supported, though, it is accepted that economic coercion undermining the sovereignty of a state is not reconcilable with the principles of the UN Charter unless authorised by the Security Council under Chapter VII.

3.5 Cyber operations and the prohibition on the use of force

Economic coercion and cyber operations can, to some extent, be compared to one another. Both do not qualify as "armed" attacks. Like economic coercion, cyber-operations have the potential to be as destructive to political independence as an armed attack.

The prohibition on the use of force does not only apply to state-run armed forces, but also to intelligence agencies or private contractors whose actions can be attributed to a state.[192] Private entities can also conduct unlawful acts in their own capacity under international- and domestic law, however, not under article 2(4) because the requirement for concerning entities to be states is not met.[193] If such actions are sanctioned or funded by a state, that state would be attributable in the act and as such, article 2(4) will apply. Cyber operations that do not meet the requirements to be considered as force between states or that do not meet the threshold of damage to be considered as use of force under article 2(4) may constitute a violation of sovereignty under Rule 4 of The Tallinn Manual 2.0 or breech the prohibition of intervention in rule 66 of The Tallinn Manual.[194]

Consequently, the question of whether cyber operations qualify as "force" that is prohibited under article 2(4) must be explored. Cyber operations cannot sufficiently be identified or distinguished as a form of use of force by coercive intention,[195] because

---

191 Dugard *et al International Law* 733.
192 Schmitt *Tallinn Manual 2.0 on the International Law* 329.
193 Schmitt *Tallinn Manual 2.0 on the International Law* 329.
194 Schmitt *Tallinn Manual 2.0 on the International Law* 329.
195 Roscini *Cyber Operations* 46.

armed force is a form of extreme intervention.[196] Further confirmation that the requirement for use of weaponry in armed force is not conclusive, derives from the fact that situations where armed forces are involved without the use of weaponry i.e. a violation of airspace is regarded as violations of sovereignty, and not as a use of force under article 2(4).[197] Cyber operations that are non-destructive and psychological, designed to undermine confidence in a government, i.e. hacktivism, is not considered as use of force.[198]

In establishing whether article 2(4) is deemed to be applicable to cyber operations depends on which of the three analytic approaches are favoured.[199] The instrument-based approach is concerned with the instruments used to conducted an attack and is used to differentiate between economic and political coercion and armed force.[200] The target-based approach states that where a cyber operation is employed against national critical infrastructure (NCI), irrespective of their effects thereon, it is considered to be use of armed force.[201] The effects of the action in the effects-based approach is favoured because armed force has the potential to cause damage to both people and infrastructure.[202] For this reason it is clear that where a cyber operation causes, or has the potential to cause, damage equal to that of what a traditional kinetic operation can cause, it would be considered as use of armed force.[203] This approach to article 2(4) doesn't account for the fact that civilisation's reliability on cyberspace creates the possibility that similar harmful acts can be achieved without the presence of traditional damaging effects.[204]

The group of experts conjured out of these differing opinions a rule that predominantly follows the interpretation of the dominant viewpoint,[205] namely, that article 2(4) only

---

196 Roscini *Cyber Operations* 46.
197 Dörr 2012 *Max Planck Encyclopaedia of Public International Law* 611.
198 Schmitt *Tallinn Manual 2.0 on the International Law* 331.
199 Roscini *Cyber Operations* 46.
200 Roscini *Cyber Operations* 47.
201 Roscini *Cyber Operations* 47.
202 Roscini *Cyber Operations* 47-48.
203 Roscini *Cyber Operations* 47.
204 Roscini *Cyber Operations* 48.
205 Waxman 2011 *Int'l L Stud* 45.

applies to military attacks or armed force between states, as Waxman coined it. Rule 69 of the Tallinn Manual 2.0[206] states that:

> 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.

Rule 69 examines the term use of force found in Rule 68[207] and focuses on the effect rather than on the instrument used to create a forceful act. There are no criteria when an act can be seen as a use of force[208] and as such, the International Group of Experts used the judgment of the *Nicaragua* case to assist them in establishing the threshold for when an act can be classified as use of force.[209] The ICJ stated that when determining if a particular action equates to an armed attack, "scale and effect" must be considered.[210] The International Group of Experts is of the opinion that scale and effect are sufficient measurements to consider when establishing whether cyber operations specifically and any act in general reach the threshold of use of force.[211] Scale and effect successfully encompass the qualitative and quantitative measurements to consider when establishing whether a cyber-operation is considered as use of force.

The International Group of Experts came to the conclusion that not all forms of cyber operations are considered as use of force, however, the scale and effect of a cyber-operation must be considered when establishing whether a cyber-operation reaches the threshold to be considered as use of force.[212] The International Group of Experts also acknowledged that the difference between certain cyber operations that do not reach the level of force that is prohibited and those that do are in some cases so small that it does not need to be taken into account.[213] This means that the International Group of Experts concluded that the most efficient way to view cyber operations in the

---

206 Schmitt *Tallinn Manual 2.0 on the International Law*.
207 Schmitt *Tallinn Manual 2.0 on the International Law* 329.
208 Schmitt *Tallinn Manual 2.0 on the International Law* 329.
209 Schmitt *Tallinn Manual 2.0 on the International Law* 329.
210 *Nicaragua* judgment paras 188-190.
211 Schmitt *Tallinn Manual 2.0 on the International Law* 329.
212 Schmitt *Tallinn Manual 2.0 on the International Law* 332.
213 Schmitt *Tallinn Manual 2.0 on the International Law* 333.

light of article 2(4), is to view the act through a spectrum of differing magnitudes of scale and effect that can either reach the threshold of damage that is considered as use of force or not.

The question still begs as to what circumstances give rise to a cyber-operation that reaches the threshold to be considered as use of force. Michael N. Schmitt[214] defined eight factors that should be considered in order to pinpoint when scale and effects of cyber-operations that produce pre-judicial consequences of a non-physical nature reach the threshold to be considered as use of force resembling that of kinetic use of force.[215] They are severity, immediacy, directiveness, invasiveness, measurability of effects, military character, state involvement and presumptive legality.[216]

Severity is measured through the glass of a *de minimis* rule in that significant damage to people and property will result in a cyber-operation qualifying as a form of use of force.[217] Cyber operations that result in a mere inconvenience or irritation will not generally be classified by states as a form of use of force.[218] A cyber operation will more likely be considered as a form of use of force, where more consequences are inflicted on the national interest of the affected state.[219]

Immediacy of the effects resulting from a cyber-operation rises the likelihood of the affected state to interpret the cyber operation as a form of use of force.[220] Where the consequences of a cyber-operation manifest themselves immediately, less time is afforded to the affected state to resolve or prevent the intended outcome of the cyber operation by peaceful manner.[221] States will more likely classify a cyber operation as a form of use of force where the consequences are immediate and not lagged.[222]

---

214 Schmitt *Tallinn Manual 2.0 on the International Law* 333-336.
215 Roscini *Cyber Operations* 48.
216 Schmitt *Tallinn Manual 2.0 on the International Law* 334-336.
217 Schmitt *Tallinn Manual 2.0 on the International Law* 334-336.
218 Schmitt *Tallinn Manual 2.0 on the International Law* 334-336.
219 Schmitt *Tallinn Manual 2.0 on the International Law* 334.
220 Schmitt *Tallinn Manual 2.0 on the International Law* 334.
221 Schmitt *Tallinn Manual 2.0 on the International Law* 334.
222 Schmitt *Tallinn Manual 2.0 on the International Law* 334.

The directiveness factor characterises the causality between cause and effect.[223] Where cause and effect are loosely connected, a state is less likely to characterise a cyber-operation as a form of use of force.[224] Where the link between cause and effect is strong, the possibility of being classified as a form of use of force is greater.[225]

Invasiveness indicates the degree to which a cyber-operation encroaches upon the affected state or its cyber system, opposed to that state's interests.[226] Where the cyber system is more protected against cyber operations, intrusion will point to a larger likelihood that the intruding cyber operation is seen as a form of use of force (e.g., hacking a military database).[227] Where the focus of the attack is centralised to one state, perceived intent of the maliciousness of the attack increases.[228]

The measurability of effects factor refers to the intention of states to identify acts as a form of use of force when the repercussions are clear to the beholder.[229] Where the repercussions of a cyber-operation are clear, states can easily calculate the scale of the damage done and consequentially characterise the cyber operation in question as a form of use of force with more ease.[230]

The military character factor points to the causality between the cyber-operation in question and military operations.[231] The causality between the cyber operation and military operations escalates the plausibility of said cyber operation being characterised as a form of use of force.[232] This is echoed in the UN Charter preamble that reads as follows: "…armed force shall not be used, save in the common interest".[233]

---

223 Schmitt *Tallinn Manual 2.0 on the International Law* 334.
224 Schmitt *Tallinn Manual 2.0 on the International Law* 334.
225 Schmitt *Tallinn Manual 2.0 on the International Law* 334.
226 Schmitt *Tallinn Manual 2.0 on the International Law* 334.
227 Schmitt *Tallinn Manual 2.0 on the International Law* 334.
228 Schmitt *Tallinn Manual 2.0 on the International Law* 334-335.
229 Schmitt *Tallinn Manual 2.0 on the International Law* 334-335.
230 Schmitt *Tallinn Manual 2.0 on the International Law* 334.
231 Schmitt *Tallinn Manual 2.0 on the International Law* 334.
232 Schmitt *Tallinn Manual 2.0 on the International Law* 336.
233 UN Charter Preamble UNTS Vol 16 1.

The state involvement factor points to the extent to which a state is involved in a cyber-operation against another state and will influence the way in which the affected state will view the intended purpose behind the attack. Where the nexus between a state and a cyber-operation is closer, it is more likely for an affected state to view the cyber-operation as a form of use of force.[234]

The prohibitive nature of international law[235] provides for acts that are not stated to be prohibited, as a result of not being mentioned in international law and is therefore perceived to be legal acts. Where a cyber-operation falls into the category of presumptive legality, it is less likely for that cyber operation to be considered as a form of use of force by an affected state.[236]

3.6 Circumstances in which force is permitted without the authorisation of the UN

There are certain circumstances when force is allowed without the authorisation of the UN. As mentioned earlier, traditionally, armed force alone is prohibited by article 2(4). Authorisation must first be given by the UN Security Council,[237] however, states may act in self-defence to halt an attack by another state, though the act in self-defence may not be greater than needed to repel the attack.[238] A state may also use force on another state to intervene in a matter that is appalling.[239] The right to individual or collective self-defence, that all member states of the UN have a right to, is regulated by article 51 of the Charter of the United Nations.[240] Article 51[241] reads as follows:

> 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

---

234 Schmitt *Tallinn Manual 2.0 on the International Law* 336.
235 *S.S. 'Lotus', France v Turkey, Judgement, 1927* at 19.
236 Schmitt *Tallinn Manual 2.0 on the International Law* 336.
237 Dugard *et al International Law* 733-734.
238 Dugard *et al International Law* 733-734.
239 Dugard *et al International Law* 733-734.
240 Dugard *et al International Law* 736.
241 UN A51 *Charter of the United Nations* (24 October 1945) https://www.un.org/en/about-us/un-charter/full-text.

> 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.

Article 51 is a temporary measurement that[242] provides member states with a "safety net" in order to protect their territorial integrity and sovereignty until the Security Council can reach appropriate measurements to maintain international peace and security.[243] However, for a state to be able to act in self-defence under article 51, the affected state must be able to prove that it acted in self-defence against an armed attack from another state.[244]

3.7 Interpretation of article 51 and self-defence

By interpreting "armed attack" in the context of article 51, it is clear that the article intends armed attack to be equal to the scale and effect of a kinetic attack that is conducted on a state by another state, that is underway or have concluded, and threatens the territorial integrity and/or sovereignty of the affected state.[245] The problem with this interpretation is the phrase, "nothing…shall impair…"[246] as well as "…inherent right of individual of collective self-defence…"[247] This phrase indicates no limitations on pre-existing rights of self-defence were imposed by the Charter because of the inherent right that a state has to defend its territorial integrity and sovereignty.[248] Scholars who interpret the phrase in this way, are of the opinion that self-defence is presented in a declaratory manner in the event of an armed attack occurring, in terms of article 51.[249] Most scholars who agree with this interpretation, are supporters of the legality of anticipatory self-defence which will be dealt with later

---

242 Ruys *'Armed Attacks' and Article 51 of the UN Charter* 58.
243 Ruys *'Armed Attacks' and Article 51 of the UN Charter* 58.
244 Ruys *'Armed Attacks' and Article 51 of the UN Charter* 58.
245 UN A51 *Charter of the United Nations* (24 October 1945) https://www.un.org/en/about-us/un-charter/full-text.
246 UN A51 *Charter of the United Nations* (24 October 1945) https://www.un.org/en/about-us/un-charter/full-text.
247 UN A51 *Charter of the United Nations* (24 October 1945) https://www.un.org/en/about-us/un-charter/full-text.
248 Ruys *'Armed Attacks' and Article 51 of the UN Charter* 58.
249 Randelzhofer "Article 51" 788-806.

on in this chapter.[250] This view allows for a wider interpretation of article 51 where armed attack is extended to other forms of attack such as cyber-attacks.[251] However, according to Ruys,[252] even if "inherent" was considered to be customary law by the ICJ, the term "…if an armed attack occurs…"[253] cannot be interpreted as declaratory as well. Ruys uses article 31(1) Vienna Convention on the Law of Treaties of 1969 (VCLT) in defence of this statement by testing the term against the three elements of interpretation.[254] Article 31(1)[255] states that:

> 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.

Firstly, he considers the ordinary meaning of the term, "if an armed attack occurs" in his analysis when he refers to the French version of article 51 and finds that the wording suggests armed attack to be a precondition when exercising self-defence.[256] Ruys comes to the conclusion that the drafters of the UN Charter would have stated explicitly that the term be interpreted broadly, or that they would have excluded the term all together.[257] Secondly, Ruys focuses on the contextual element of article 31(1).[258] He finds that when article 51 is read together with article 2(4), 39, 42 and 53, the meaning is clear that the authors wanted to create a complete ban on use of force that is unilateral and that the UN Security Council be tasked to implement this ban.[259] Thirdly, he interprets the term in the light of the object and purpose element.[260] He finds that the object of the UN Charter is to end use of force that is unilateral and

---

250 Ruys *'Armed Attacks' and Article 51 of the UN Charter* 58.
251 Ruys *'Armed Attacks' and Article 51 of the UN Charter* 58.
252 Ruys *'Armed Attacks' and Article 51 of the UN Charter* 59.
253 UN A51 *Charter of the United Nations* (24 October 1945) https://www.un.org/en/about-us/un-charter/full-text.
254 Ruys *'Armed Attacks' and Article 51 of the UN Charter* 59.
255 UN A31(1) *The Vienna Convention on the Law of Treaties* (23 May 1969) https://treaties.un.org/doc/publication/unts/volume%201155/volume-1155-i-18232-english.pdf.
256 Ruys *'Armed Attacks' and Article 51 of the UN Charter* 59.
257 Ruys *'Armed Attacks' and Article 51 of the UN Charter* 59.
258 Ruys *'Armed Attacks' and Article 51 of the UN Charter* 59.
259 Ruys *'Armed Attacks' and Article 51 of the UN Charter* 59.
260 Ruys *'Armed Attacks' and Article 51 of the UN Charter* 59-60.

to enforce these measurements through the UN Security Council.[261] Ruys[262] concludes by stating that:

> …all of the primary interpretative elements indicate that the phrase 'if an armed attack occurs' forms an integral part of, and essential condition for, the exercise of the right of self-defence.

The analysis that Ruys conducted indicates that article 51 should be interpreted narrowly and that the phrase, "if an armed attack occurs"[263] limits states' right of personal and collective self-defence to kinetic attacks as well as attacks that have already occurred. This is supported by US Govender Stassen in the drafting of the UN Charter and more specifically the wording of article 51.[264] He was asked what self-defensive measurements the US could take in the event of a foreign navy staring down a US republic, when the foreign navy have not yet attacked.[265] Govender Stassen[266] answered the question by stating that:

> … we could not under this provision attack the fleet, but we could send a fleet of our own and be ready in case an attack came.

Govender Stassen's reply correctly reflects the narrow reading of article 51 and in 1945, this would have been a favoured position to take in terms of self-defence against a foreign attack. However, this position in terms of self-defence is outdated and does not provide sufficient measurements to defend against cyber-attacks.

3.8 Pre-emptive self-defence

Pre-emptive self-defence is a term used to define situations where a state reasonably anticipates an attack from another state and proceeds to defend itself against the perceived threat.[267] Legal scholars are divided on this subject, arguing that not

---

261 Ruys *'Armed Attacks' and Article 51 of the UN Charter* 60.
262 Ruys *'Armed Attacks' and Article 51 of the UN Charter* 60.
263 UN A51 *Charter of the United Nations* (24 October 1945) https://www.un.org/en/about-us/un-charter/full-text.
264 Ruys *'Armed Attacks' and Article 51 of the UN Charter* 64.
265 Ruys *'Armed Attacks' and Article 51 of the UN Charter* 64.
266 Foreign Relations of the United States, Diplomatic Papers (1945) 659.
267 Dugard *et al International Law* 501.

interpreting article 51 to afford states an inherent right to self-defence, leaves states vulnerable to attacks.[268] The argument follows that when states perceive a threat or aggression, the narrow interpretations bar a state from acting in self-defence until the treat or aggression turns into an armed attack.[269] Aggression is a situation in which an armed attack has not yet occurred, however, the threat of an armed attack is present.[270] The UN Security Council may, in terms of Chapter VII of the UN Charter, take measures to deal with the aggression, however, aggression may not reach the threshold to be considered as an armed attack under article 51.[271] In the event where aggression becomes an armed attack, harm has already occurred against the state that could have been avoided if the state could defend itself in a pre-emptive manner.[272] The ICJ refrained from deciding on pre-emptive self-defence in the *Nicaragua* case, however, it acknowledged that the customary right to self-defence in article 51 is preserved.[273] This judgement strengthens the notion that anticipatory self-defence forms part of international law.[274]

For a cyber-operation to be regarded as an armed attack in terms of article 51, the scale and effect of the cyber operation must be equal to that of an armed attack and the cyber-operation must be conducted by one state to another.[275] The international Group of Experts who compiled the Tallinn Manual acknowledged that there are differences between an armed attack and aggression[276] and that the Tallinn Manual is only concerned with armed attacks.[277] The International Group of Experts used the ICJ note on the Nuclear Weapons Advisory Opinion to justify that the scale and effect of some cyber operations warrant them to be considered armed attacks.[278] It is commonly

---

268 Dugard *et al International Law* 501.
269 Dinstein *War, Aggression and Self-Defence* 166.
270 Dinstein *War, Aggression and Self-Defence*166.
271 UN A39-51 *Charter of the United Nations* (24 October 1945) https://www.un.org/en/about-us/un-charter/full-text.
272 Dinstein *War, Aggression and Self-Defence*166.
273 Dugard *et al International Law* 740.
274 Dugard *et al International Law* 740.
275 Schmitt *Tallinn Manual 2.0 on the International Law* 340.
276 Schmitt *Tallinn Manual 2.0 on the International Law* 340.
277 Schmitt *Tallinn Manual 2.0 on the International Law* 340.
278 Schmitt *Tallinn Manual 2.0 on the International Law* 340.

accepted that nuclear weapons are considered to be armed attacks despite not being kinetic weapons, however, their scale and effect rise to such a level that it is considered to be armed attacks.[279] Furthermore, the International Group of Experts refer to the word "armed" in article 51, stating that this may refer to the use of weaponry.[280] They decided to take the position that the effect of the weapon is what is meant rather than the weapon itself.[281] However, they acknowledged the view that "armed" refers to weaponry and for that reason, they came to the conclusion that a cyber-operation is not considered an armed attack unless cyber weaponry is used.[282] This means that cyber-operations conducted in order to gather intelligence, commit theft, as well as cyber operations that involve interrupting cyber services that are non-essential, brief or periodic, do not qualify as armed attacks.[283]

The question of whether cyber operations can be considered as armed attacks should not be the only focus. Cyberspace consists of internet networks stretched out over the entire world.[284] Transferring data across the planet is instantaneous leaving no time to consider whether a perceived cyber operation is a form of aggression or an armed attack. This instantaneous nature of cyberspace complicates the question of when self-defence can be instituted against an armed attack.[285] In some cases, the perceived state has only seconds to identify the cyber armed attack and implement self-defence, which has the effect that the intention as well as imminent outcome of the attack is unclear.[286] The only sufficient way for a state to defend itself from such an attack is to act pre-emptively, however, the difference between pre-emptive measurements and prohibited prevention is very little.[287] The ICJ has confirmed that pre-emptive action and anticipatory self-defence still form part of international law by endorsing the view that preserves the customary right of self-defence in the *Nicaragua* case.[288] However,

---

279 Schmitt *Tallinn Manual 2.0 on the International Law* 340.
280 Schmitt *Tallinn Manual 2.0 on the International Law* 340.
281 Schmitt *Tallinn Manual 2.0 on the International Law* 341.
282 Schmitt *Tallinn Manual 2.0 on the International Law* 341.
283 Schmitt *Tallinn Manual 2.0 on the International Law* 341.
284 Singer and Friedman *Cybersecurity and Cyberwar* 2.
285 Singer and Friedman *Cybersecurity and Cyberwar* 2.
286 Singer and Friedman *Cybersecurity and Cyberwar* 2.
287 Dever and Dever 2013 *Journal of Law and Cyber Warfare* 25-63.
288 Dugard *et al International Law* 740.

this can have the effect that the pre-emptive act of defence can be greater than needed to repel the attack because the scale and effect of such an attack would be unclear to the perceiving state.[289] However, pre-emptive action in terms of cyber-operations may not be in contrast with article 51. Where the act in self-defence is used to disable an intruding internet system, is non-destructive to the physical world and only disables an online system from attacking a state. The destructive consequences would not be physical and as such would not be considered to be in violation of article 51.[290] A response that causes physical damage would, however, constitute a violation in terms of article 51, and the effects of such a response may be greater than needed to repel a cyber-armed attack.[291]

3.9 Other forms of self-defence

There are other forms of self-defence, which are self-defence and accumulation of events, self-defence against terrorism, humanitarian intervention, collective self-defence, intervention in civil strife and civil wars, wars of national liberation and self-defence on the high seas.[292]

Self-defence and accumulation of events are situations where small-scale attacks, mostly guerrilla tactics, are used between neighbouring states.[293] The attacks does not amount to full-scale warfare, and not all attacks against a state is met with resistance.[294] However, states still retaliate by attacking neighbouring states in anticipation of an imminent small-scale attack on them.[295] This is thus seen as a leg of anticipatory self-defence, however, attacks from a neighbouring state must have already occurred in order to justify a reprisal as self-defence.[296] Generally speaking, these forms of self-defence are not justifiable under international law, as Dugard

---

289 Singer and Friedman *Cybersecurity and Cyberwar* 2.
290 Waxman 2011 *Int'l L Stud* 48.
291 Singer and Friedman *Cybersecurity and Cyberwar* 2.
292 Dugard *et al International Law* 736-765.
293 Dugard *et al International Law* 742.
294 Dugard *et al International Law* 742.
295 Dugard *et al International Law* 742.
296 Dugard *et al International Law* 742-743.

mentions, it is not justified under article 2(4).[297] This form of self-defence is, however, permitted by the Charter, because article 2(4) is punitive in purpose and the Charter is protective.[298] Dugard goes further in stating that the Security Council is known to accept accumulation of events as a form of self-defence in certain situations where reprisals did not cause significant loss to civilian life and infrastructure.[299] This goes to show that the principle of "reasonableness" is a contributing factor for the Security Council to include when deciding whether or not such a form of self-defence is included.[300]

Self-defence against terrorism was not part of international law prior to the 11 September 2001 attacks by Al-Qaeda on the USA.[301] Following these attacks, the UN Security Council adopted Resolutions 1368[302] and 1373[303] that recognise the inherent right of a state's right to self-defence in accordance with article 51, as well as condemning the terrorist attacks.[304] In accordance with these resolutions, the USA and its allies attacked Afghanistan that harboured the terrorist group and allowed them to use the state as their base from where they attacked.[305] The attack on Afghanistan was sanctioned by the Security Council on the basis that the State allowed Al-Qaeda sanctuary within its borders.[306] In the years that followed a number of states tried to justify their acts in relation to Resolutions 1369 and 1373, but did not succeed in justifying their acts as self-defence against terrorism.[307] Israel wanted to justify constructing a wall in the occupied Palestinian territories as an act of self-defence against terrorism, but the ICJ found that the acts against Israel by Palestine was not imputable, and that the occupied territories was part of Israel's territory.[308] Armed

---

297 Dugard *et al International Law* 743.
298 Dugard *et al International Law* 743.
299 Bowett *The Law of International Institutions* cited by Dugard *et al International Law* 504.
300 Dugard *et al International Law* 742.
301 Dugard *et al International Law* 763.
302 *Security Council Resolution* 1368 12 September 2001
303 *Security Council Resolution* 1373 on threats to international peace and security caused by terrorist acts 28 September 2001.
304 Dugard *et al International Law* 763.
305 Dugard *et al International Law* 763.
306 Dugard *et al International Law* 763.
307 Dugard *et al International Law* 764.
308 Dugard *et al International Law* 761.

activities in the Congo by rebellious groups from an opposing party in the Congo committed terrorist activities on civilians and infrastructure.[309] The ICJ abstained from recognising the Congo's counter attacks to these rebels in an act of self-defence stating that an act in self-defence against terrorism that is in accordance with Resolutions 1368 and 1373 is regarded as being in line with state practice. Acts carried out on non-state actors cannot be considered as being in line with state practice.[310] The ICJ goes further by stating that an act of self-defence against terrorists requires punitive action against terrorist bases or the state that is harbouring them, and that this goes beyond anticipatory self-defence.[311] Consequently, self-defence against terrorism should be utilised to prevent future terrorist actions only, or be sanctioned by the Security Council.[312]

Humanitarian intervention has been part of international law since before the drafting of the UN Charter in 1945,[313] however, with the drafting of the Charter, humanitarian intervention was not included as a form of self-defence.[314] This form of intervention takes place where states intervene in a matter to protect non-nationals where they are treated in such a way that it "shocks the conscience of mankind".[315] Only the Security Council, under Chapter VII of the Charter, may sanction a form of intervention in this regard. It has occurred that states acting against another state in protecting non-nationals succeeded in justifying their acts under Humanitarian Intervention.[316] In the International Criminal Tribunal for the Former Yugoslavia, it was found that the North Atlantic Treaty Organisation's (NATO) intervention in the aggrieved actions that took place in Kosovo was both illegal and justified.[317] Although the actions were prohibited by international law, the justification for acting to maintain world peace was sound.[318] The ICJ acknowledged the illegality of this form of intervention although it seems that

---

309 Dugard *et al International Law* 761.
310 Dugard *et al International Law* 761.
311 Dugard *et al International Law* 761.
312 Dugard *et al International Law* 761.
313 Dugard *et al International Law* 747.
314 Dugard *et al International Law* 747.
315 Dugard *et al International Law* 747.
316 Dugard *et al International Law* 747-748.
317 Dugard *et al International Law* 748.
318 Dugard *et al International Law* 749.

the court is willing to take into account the reasons behind such an act and where it is justified, the court is willing to acknowledge humanitarian intervention as an act of intervention.[319]

3.10 Conclusion

In conclusion, the prohibition of use of force clause as well as the exceptions found in article 51 have been examined in the light of cyber operations. It is found that the dominant viewpoint in which the literal meaning of the text behind article 2(4) is the most accepted interpretation of the article, and is most commonly used by law practitioners and scholars to interpret the meaning behind the prohibition on the use of force. However, the ICJ has noted in the *Nicaragua* case that the scale and effect of an attack rather than the weapon itself must be examined, in order to establish whether the act of force is prohibited by article 2(4). This has the effect that any form of attack, albeit kinetic operations, economic coercion or cyber operations, has the potential to rise to the magnitude of being considered force as prohibited in terms of article 2(4). The question of when an operation reaches the level of scale and effect to be considered as use of force was examined. It is found that where the scale and effect of an operation reach the level of destruction similar to that of a kinetic attack, the operation is prohibited in terms of article 2(4). Michael N. Schmitt[320] developed a set of factors that could help define when a cyber-operation is considered as use of force. Severity, immediacy, directiveness, invasiveness, measurability of effects, military character, state involvement and presumptive legality are examined to be sufficient factors to take into account when considering cyber operations as use of force. However, these factors are not a part of international law and will not be binding until there is state practice where these factors are used to consider whether a cyber-operation is considered use of force. The exceptions to article 2(4) was then discussed in the light of cyber operations. It is found that the wording of article 51 provides states with an unqualified right to self-defence, but that the wording in the event of

---

319 Dugard *et al International Law* 749.
320 Schmitt *Tallinn Manual 2.0 on the International Law* 333-336.

an armed attack limits that right to when an armed attack occurs or have concluded. Ruys analysed the wording in article 51 in the light of article 31(1) and found that the wording, in the event of an armed attack, places a qualifying element to a state's unqualified right to self-defence. There are still interpretations of article 51 that insist that armed attack is a lexical term that was carried over from previous legislation on the matter, and that the interpretation of the wording must not be read too narrowly. The ICJ made the uncertainty on the two schools of thought clear in their judgement on the *Nicaragua* case, deliberately deciding not to give judgement on whether or not pre-emptive action is recognised by international law, whilst noting that states have an unqualified right to self-defence. These differing opinions are relevant to the discussion of how the right to self-defence is implemented against a cyber-operation rising to the level of destruction to be considered as force. Due to the nature of cyber operations, the most effective way in which a state can practice its right to self-defence, is to act pre-emptively. This gives way to the problem of an act of self-defence being greater than intended to repel an attack on a state. Because of the speed in which cyber operations are conducted, the intention of an incoming attack is unclear, and the scale and effect of the imminent attack cannot be established until the attack have been carried out. It is uncertain how to prevent an attack without running the risk of the act in self-defence to be greater than needed to repel the attack. State practice may be the solution, however, there are currently not enough examples of state practice in this regard to give a definitive answer. The purpose of this analysis is to establish whether cyber operations form part of use of force and by doing so establishing possible shortcomings in interpretations of article 2(4) as well as of article 51. This analysis cannot begin to provide a solution to the problems in interpretations and as such cannot provide solutions to the problems that have been identified. Long overdue debates and legislation are needed to definitely establish whether or not pre-emptive action forms part of international law.

Chapter 4: Cyber warfare and international humanitarian law

4.1 Introduction

The Battle of Solferino between Franco-Italian and Austrian forces in 1859 sparked international movements that led to the inception of IHL.[321] Henry Dunant, a young Swiss banker, started a movement after having witnessed the death of thousands of wounded soldiers without receiving medical attention, which led to the eventual inception of the International Committee of the Red Cross (ICRC) based in Geneva Switzerland.[322] The ICRC is a non-governmental institution dedicated to assist in protecting and caring for affected persons of an armed conflict.

Following the inception of the ICRC, a host of first generation multilateral humanitarian treaties came into effect helping to shape IHL into what it represents today.[323] In 1899 and 1907, a series of treaties consisting of the "laws and customs of war" were adopted in The Hague, which is now known as The Hague Convention of 1899 and 1907.[324] The first Geneva Convention treaties, together with The Hague Conventions were the first multilateral humanitarian treaties that IHL consisted of.[325] In 1949 and 1977, another set of treaties was included into IHL with the second Geneva Convention relating to the protection of combatants and civilians in relation to armed conflicts.[326] The addition of the second Geneva Convention to IHL, morphed IHL into the international legal system as it currently exists.[327] IHL is enforceable by international criminal tribunals and the International Criminal Court (ICC), making it binding to all UN member states.[328]

IHL distinguishes between *jus ad bellum* (the right to wage war) and *jus in bello* (law governing the wage of war). *Jus ad bellum* and *jus in bello* determine when and how

---

321 ICRC 1998 https://www.icrc.org/en/doc/resources/documents/misc/57jnvr.htm.
322 ICRC 1998 https://www.icrc.org/en/doc/resources/documents/misc/57jnvr.htm.
323 ICRC 2016 https://www.icrc.org/en/document/history-icrc.
324 Sassòli *International Humanitarian Law* 8.
325 Sassòli *International Humanitarian Law* 8.
326 Sassòli *International Humanitarian Law* 8.
327 Sassòli *International Humanitarian Law* 9.
328 Gutiérrez Posse 2006 *International Review of the Red Cross* 68.

a state can respond to an armed attack.[329] IHL is a system of law that applies to instances of occupation and armed conflict and is also known as the law of armed conflict/war.[330] An inherent set of protective principles of IHL is extended to all combatants and civilians involved and/or affected by an international armed operation.[331] These principles are distinction, military necessity, unnecessary suffering and proportionality; they serve different purposes for regulation, however, they are integrated and must function as a whole. No distinction is made between civilians on either side of the conflict or the weaponry- and warfare methods used.[332]

There is a difference between International Armed Conflicts (IAC) and Non-International Armed Conflicts (NIAC).[333] IACs occur when an armed conflict arises between two or more states with the effect that the armed conflict in question takes place over national geographical borders, which creates an international element to the conflict. NIACs are armed conflicts that arises within the geographical borders of a single state of which a good example is civil war. This has the effect that there is no international element in this form of armed conflict. Contemporary IHL concerns itself with both IAC as well as NIAC through the Common Articles[334] found in the Additional Protocols.[335] The aim of IHL is to minimise the suffering and loss of civilian lives as well as damage to civilian objects inflicted through armed conflicts and situations of occupation[336] by regulating the activity of combatants during armed conflicts and circumstances of occupation.[337] The conduct of civilians and combatants can mostly be regulated through the principles of distinction, military necessity, unnecessary suffering and proportionality.

---

329 Sassòli *International Humanitarian Law* 18.
330 IJRC date unknown https://ijrcenter.org/international-humanitarian-law/.
331 Dugard *et al International Law* 765.
332 Dugard *et al International Law* 765.
333 IJRC date unknown https://ijrcenter.org/international-humanitarian-law/.
334 Common Articles of the Additional Protocols are articles that apply throughout all of the Addition Protocols, such as Common Article 3 which is article 3 in all of the Additional Protocols.
335 Dugard *et al International Law* 765.
336 IJRC date unknown https://ijrcenter.org/international-humanitarian-law/.
337 IJRC date unknown https://ijrcenter.org/international-humanitarian-law/.

The purpose of this chapter is to establish to what extent IHL regulates situations of armed conflict in order to test its applicability to situations where armed conflicts are cyber-attacks. This chapter starts by analysing the sources of IHL and their functions in order to establish a basis for the discussion of regulating armed conflicts. The distinction between NIACs and IACs is examined with particular focus on Common Articles 2 and 3 in order to discuss the necessity of distinction between them. Finally, the principles of IHL, as mentioned above, are discussed. Cyber operations are examined in the light of these elements to establish whether they can find applicability.

4.2 Sources of IHL

4.2.1 Treaties

4.2.1.1 Law of The Hague

As mentioned earlier, the law of The Hague or The Hague Convention is a body of law adopted in 1899 and in 1907 that constitutes laws and customs of war.[338] The Hague Convention establishes the rights and duties that belligerents have when participating in military operations, and limits their intentions for doing harmful acts.[339] The law of The Hague aims to balance military necessity and humanitarian considerations that will be discussed later on in this chapter.[340] There are four conventions that form The Hague Convention of which the fourth convention of 1907 is the most important for purposes of this discussion, and it relates to respect for laws and customs of war on land. Annexed hereto are The Hague Regulations that deal with the status of belligerents, conduct of hostilities, the prohibition of weapons "calculated to cause unnecessary suffering",[341] termination of hostilities and rules governing military occupation. Article 22 declares that the rights of belligerents[342] to adopt means of

338 Sassòli *International Humanitarian Law* 8.
339 Article 42-45 of The Hague Regulations of 1907
340 Sassòli *International Humanitarian Law* 36.
341 The Hague Regulations of 1907.
342 For purposes of convenience where belligerents appear in the text, it will refer to combatants.

injuring the enemy are not unlimited.[343] The Hague Regulations are generally accepted to form part of customary law.[344]

4.2.1.2 Prohibition of weapons that cause unnecessary suffering

The prohibition of weapons that cause unnecessary suffering did not enjoy any regulation before adopting The Hague Convention in 1907[345] that contains article 23(e) of The Hague Regulations[346] that is annexed thereto. Since adopting this treaty, the need for regulation of weapons that cause unnecessary suffering grew. In 1925 marked the Geneva Protocol was adopted, and with it, prohibitive measures against the use of poisonous gases and bacteriological weaponry used in warfare.[347] This was however supplemented in 1972 and 1993 by the Convention prohibiting the production and stockpiling of bacteriological weapons, and the Convention prohibiting the use of chemical weapons respectively.[348] The Hague Regulations as well as the 1972 and 1993 Conventions are still in effect.

The Ottawa Convention was adopted in 1997 with the intention to ban production, use and transfer of land mines and anti-personnel weaponry.[349] According to Dugard,[350] this Convention is founded on three principles, firstly, the right to choose methods of warfare between parties in an armed conflict is not unqualified; secondly, to prohibit weaponry that causes unnecessary suffering in armed conflicts, and thirdly, a distinction must be made between civilians and combatants. The Convention on Cluster Munitions of 2010 is based on similar principles to those of the Ottawa Convention.[351]

The question of whether nuclear weapons is an accepted form of weaponry in armed conflicts, came into question in 1996.[352] The International Court of Justice (ICJ),

---

343 Article 22 of The Hague Regulations of 1907.
344 Sassòli *International Humanitarian Law* 36.
345 Dugard *et al International Law* 767.
346 Article 23(e) of The Hague Regulations of 1907.
347 Dugard *et al International Law* 767.
348 Dugard *et al International Law* 767.
349 Dugard *et al International Law* 767.
350 Dugard *et al International Law* 768.
351 Dugard *et al International Law* 767.
352 Dugard *et al International Law* 770.

requested by the General Assembly, composed an advisory opinion on the Legality of the Treaty or User of Nuclear Weapons.[353] The ICJ found that nuclear weaponry, irrespective of the potential to cause unnecessary suffering and excessive force, is not an unaccepted form of weaponry in terms of contemporary international law, as it cannot be entirely prohibited by international treaties.[354] It is however mandated to conclude negotiations before nuclear weaponry may be used in order to peruse alternative resolutions.[355] Certain states still endeavour to ban nuclear weaponry through domestic law and by entering into agreements with other states to ban the use of nuclear weapons such as the Treaty of Pelindaba, the African Nuclear-Weapons-Free Zone.[356]

4.2.1.3 Law of Geneva

The Geneva Conventions of 1949 are generally regarded as a regulating treaty that protects different categories of people.[357] The protection afforded by the Geneva Conventions is only applicable in circumstances of ICA, while Common Article 3 protects people in situations of NIAC.[358] The Law of Geneva consists of Conventions I and II that provide protection for shipwrecked, sick and wounded persons,[359] Convention III provides protection for prisoners of war[360] and Convention IV protects civilians of all sides of conflicts.[361] Annexed to the Geneva Conventions are the Additional Protocols.

Protocol I regulates principles of IAC,[362] Protocol II of NIAC[363] and Protocol III consists an additional protective emblem.[364] These Protocols are distinct from the Geneva

353 Dugard *et al International Law* 770.
354 Dugard *et al International Law* 770-771.
355 Dugard *et al International Law* 771.
356 Dugard *et al International Law* 771.
357 Sassòli *International Humanitarian Law* 36-37.
358 Sassòli *International Humanitarian Law* 37.
359 Convention I and II of the Geneva Conventions of 1949.
360 Convention III of the Geneva Conventions of 1949.
361 Convention IV of the Geneva Conventions of 1949.
362 Article 2 of the Additional Protocols to the Geneva Conventions of 12 August 1949.
363 Article 2 of the Additional Protocols to the Geneva Conventions of 12 August 1949.
364 Article 2 of the Additional Protocols to the Geneva Conventions of 12 August 1949.

Conventions and are considered international treaties of which only states and parties to the Geneva Conventions can become members.[365] These Additional Protocols are considered an extension of the Geneva Conventions that are only enforceable on states that are member parties.[366] The Additional Protocols are however largely incorporated into customary law that is enforceable upon all states.[367]

4.3 Armed conflicts and IHL (the scope of application)

The Hague Convention with its annexed Regulations of 1907,[368] Geneva Conventions of 1949[369] and the Additional Protocols I and II of 1977[370] are the most prominent IHLs in terms of armed conflicts and are collectively known as the law of armed conflict.[371] The regulations that make up the law of armed conflict can either regulate an armed conflict in its entirety or certain aspects may be applicable depending on its nature.[372] This means that the nature of an armed conflict must be determined before the applicable law can be established. Furthermore, the nature of involving an individual in an armed conflict must be determined to further establish the applicable law regulating it,[373] however this will be discussed later on in this chapter at 4.3.1. The question of to what extent the law of armed conflict applies to an armed conflict is not so obvious, due to the fact that there is no definition for armed conflicts in the Geneva Conventions.[374] It is implied that the authors of the Geneva Conventions deliberately refrained from including a definition of armed conflict in the Conventions[375] and as such created room for a wider interpretation of the nature of armed conflicts. Armed

365 Sassòli *International Humanitarian Law* 38.
366 The Preamble of the Additional Protocols to the Geneva Conventions of 12 August 1949.
367 Sassòli *International Humanitarian Law* 38.
368 The Hague Conventions (IV) Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land.
369 The Geneva Conventions of 12 August 1949.
370 Additional Protocols to the Geneva Conventions of 12 August 1949.
371 Solis *The Law of Armed Conflict* 149.
372 Solis *The Law of Armed Conflict* 149.
373 Solis *The Law of Armed Conflict* 149.
374 Solis *The Law of Armed Conflict* 150.
375 Solis *The Law of Armed Conflict* 150.

conflict is however defined by the Appeals Chamber of the International Criminal Tribunal for the former Yugoslavia[376] as:

> …a resort to armed forces between states or protracted armed violence between governmental authorities and organized armed groups or between such groups within a State.

This definition supports the implication, mentioned above, that the authors of the Geneva Conventions intended the interpretation of armed conflicts to be wide. Armed force between groups or organisations as well as between states may constitute an armed conflict.

Determining the nature of an armed conflict in modern times is particularly significant because the law of armed conflict applies to different forms of armed conflicts.[377] The first classification on the nature of an armed conflict known as the general nature from hereon for convenience sake, is when an IAC arises from a declaration of war between two states.[378] The general nature of an armed conflict is clear-cut, in that the law on armed conflicts apply to it in its entirety.[379] An example hereof is World War II where a formal declaration of war was given from the UK and its allies to Germany and its allies.[380] The law of armed conflict, however, did not exist as it does today, but had it existed, it would have applied to the Great War in its entirety. Armed conflicts that can be classified under the general nature of armed conflicts are not so common in modern times,[381] and as such the nature of armed conflicts is difficult to determine.[382] In the event where multiple parties to the Geneva Conventions are engaged in armed conflicts against one another, the nature of the armed conflict may be regulated by Common Article 2.[383] In instances of armed conflict as contemplated in Common Article

---

376 *Prosecutor v Tadic* Case no. IT-94-1-A Appeals Chamber of the International Criminal Tribunal Application Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction 2 Oct 1995 para 70 https://www.icty.org/x/cases/tadic/acdec/en/51002.htm.

377 Sassòli *International Humanitarian Law* 168.

378 Sassòli *International Humanitarian Law* 169.

379 Sassòli *International Humanitarian Law* 169.

380 History.com Editors 2020 https://www.history.com/this-day-in-history/britain-and-france-declare-war-on-germany.

381 Solis *The Law of Armed Conflict* 150.

382 Solis *The Law of Armed Conflict* 150.

383 Article 2 of the Geneva Conventions of 1949.

2, all Geneva Conventions and Additional Protocol I will apply[384] and will be considered IACs.

Where one or multiple parties to the Geneva Conventions are engaged in armed conflicts against a group that is not recognised as a state in terms of the requirements for statehood as set out in the Montevideo Convention,[385] then Common Article 3 and Additional Protocol II[386] apply and will be considered NIACs. NIACs can consist of situations where non-state actors are engaged in armed operations against one another,[387] no international law aspect will exist because the armed conflict does not transcend any state borders,[388] such as civil wars,[389] the domestic law of the appropriate state then applies.[390] In the event where party states to the Geneva Conventions are engaged in armed conflicts against non-state armed forces, the situation becomes less clear, and establishing the applicable law becomes difficult. The domestic law of the state in which the non-state armed forces reside cannot qualify as the regulating law because there is an international element present,[391] and the relevant state may have no affiliation with the non-state armed forces engaged in the conflict.[392] The distinction between IACs and NIACs is important in order to determine the nature of an armed conflict. As such, Common Article 2 and Common Article 3 must be further examined in order to identify sufficient guidelines for distinguishing between IACs and NIACs.

4.3.1 IACs and Common Article 2

Common Article 2 of the Geneva Conventions of 1949[393] reads as follows:

> In addition to the provisions which shall be implemented in peacetime, the present Convention shall apply to all cases of declared war or of any other armed conflict

---

384 Article 2 of the Geneva Conventions of 1949.
385 Article 1 of the Montevideo Convention on the Rights and Duties of States of 1934.
386 Article 3 of the Geneva Conventions of 1949.
387 Article 3 of the Geneva Conventions of 1949.
388 Sassòli *International Humanitarian Law* 169-170.
389 Sassòli *International Humanitarian Law* 169-170.
390 Solis *The Law of Armed Conflict* 153.
391 Article 2 of the Geneva Conventions of 1949.
392 Sassòli *International Humanitarian Law* 168.
393 Article 2 of the Geneva Conventions of 1949.

> which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them. The Convention shall also apply to all cases of partial or total occupation of the territory of a High Contracting Party, even if the said occupation meets with no armed resistance. Although one of the Powers in conflict may not be a party to the present Convention, the Powers who are parties thereto shall remain bound by it in their mutual relations. They shall furthermore be bound by the Convention in relation to the said Power, if the latter accepts and applies the provisions thereof.

With regard to Common Article 2, it is evident that this article applies in all cases where there is an armed conflict between multiple member states,[394] whether or not the states acknowledge them.[395] Occupation by one state of another with or without resistance will also constitute a situation where Common Article 2 will apply.[396] The article goes further in section 3 of the article[397] by addressing member states or non-member states that may be party to an armed conflict.[398] Common Article 2 places an obligation on member states to conduct themselves in their relationships with non-member states that does not comply with Common Article 2 as if they were member states to the Geneva Conventions.[399] This may constitute sanctions,[400] public statements condemning the non-member state's actions[401] as well as possible intervention of the armed conflict by member states.

In such an event, IAC Common Article 2 applies together with Additional Protocol I to the Geneva Conventions.[402] This is supported by article 1(3) of the Additional Protocols[403] by stating that:

> this Protocol, which supplements the Geneva Conventions of 12 August 1949 for the protection of war victims, shall apply in the situations referred to in Article 2 common to those Conventions.

---

394 Article 2 of the Geneva Conventions of 1949.
395 Solis *The Law of Armed Conflict* 150.
396 Solis *The Law of Armed Conflict* 150.
397 Article 2(3) of the Geneva Conventions of 1949.
398 ICRC *Commentary on the First Geneva Convention* para 344.
399 ICRC *Commentary on the First Geneva Convention* paras 344-350.
400 Solis *The Law of Armed Conflict* 151.
401 Solis *The Law of Armed Conflict* 151.
402 Solis *The Law of Armed Conflict* 151.
403 Article 1(3) of the Additional Protocols to the Geneva Conventions of 1949.

The applicability of the protocol differs from that of Common Article 2 in that the commission to treat non-member states as member states in armed conflicts does not carry over for the non-signatories of Additional Protocol I.[404] States that are members to the Geneva Conventions, but not signatories of the Additional Protocols such as the USA,[405] are not bound by the Additional Protocols.[406] This, however, does not mean that the regulations in the Additional Protocols do not apply to non-signatories; a majority of the regulations in the Additional Protocols are incorporated into IHL with Common Articles, which means that these regulations will find applicability through other authoritative instruments.[407]

4.3.2 Common Article 3 and NIACs

Before World War II and the inception of the United Nations, the general consensus among countries was that governing bodies of sovereign states should not be held accountable by other states for acts conducted within their own borders.[408] This form of non-regulation was established with the Peace of Westphalia[409] signed in October 1648 with the rise of the city-state.[410] This view changed partly during the Nuremburg Trials[411] held after the conclusion of World War II, due to the atrocious acts conducted by Germans in the concentration camps situated within the geographical jurisdiction of Germany.[412] With the drafting of the Geneva Conventions in 1949, the drafters were of the view that regulation of acts within the territorial jurisdiction of states should be regulated to a minimum extent.[413] These events gave rise to the issuance of Common Article 3.

---

404 Sassòli *International Humanitarian Law* 38.
405 Sassòli *International Humanitarian Law* 38.
406 Sassòli *International Humanitarian Law* 38.
407 Sassòli *International Humanitarian Law* 39.
408 Solis *The Law of Armed Conflict* 151.
409 Gross 1948 *The American Journal of International Law* 20–41.
410 Gross 1948 *The American Journal of International Law* 20-41.
411 Solis *The Law of Armed Conflict* 153.
412 Solis *The Law of Armed Conflict* 153.
413 ICRC *Commentary on the First Geneva Convention* paras 107-109.

Common Article 3 begins by stating that, where an armed conflict arises without the international element,[414] as described in Common Article 2, within the geographical area of a High Contracting Party to the Geneva Conventions, all parties to that conflict is "…bound to apply, as a minimum…"[415] the provisions as set out further in Common Article 3. Common Article 3[416] reads in its entirety as follows:

> In the case of armed conflict not of an international character occurring in the territory of one of the High Contracting Parties, each Party to the conflict shall be bound to apply, as a minimum, the following provisions:
>
> 1) Persons taking no active part in the hostilities, including members of armed forces who have laid down their arms and those placed *hors de combat* by sickness, wounds, detention, or any other cause, shall in all circumstances be treated humanely, without any adverse distinction founded on race, colour, religion or faith, sex, birth or wealth, or any other similar criteria.
>
>   To this end, the following acts are and shall remain prohibited at any time and in any place whatsoever with respect to the above-mentioned persons:
>
>   *a)* violence to life and person, in particular murder of all kinds, mutilation, cruel treatment and torture;
>
>   *b)* taking of hostages;
>
>   *c)* outrages upon personal dignity, in particular humiliating and degrading treatment;
>
>   *d)* the passing of sentences and the carrying out of executions without previous judgment pronounced by a regularly constituted court, affording all the judicial guarantees which are recognized as indispensable by civilized peoples.
>
> 2) The wounded and sick shall be collected and cared for. An impartial humanitarian body, such as the International Committee of the Red Cross, may offer its services to the Parties to the conflict.
>
>   The Parties to the conflict should further endeavour to bring into force, by means of special agreements, all or part of the other provisions of the present Convention.
>
>   The application of the preceding provisions shall not affect the legal status of the Parties to the conflict.

This article describes armed conflicts in situations where they occur within the territorial borders of a single state, thereby excluding the international element from Common Article 2, armed conflicts. The High Contracting Party, as the drafters of the

---

414 Article 3 of the Geneva Conventions of 1949.
415 Article 3 of the Geneva Conventions of 1949.
416 Article 3 of the Geneva Conventions of 1949.

Geneva Conventions put it, enters into an armed conflict with hostile groups[417] that are not affiliated with another state within its territory.[418] These forms of armed conflicts may eventually be declared as a belligerency by other states allowing the state that is a party to the armed conflict to act upon the rights of a belligerent.[419] This has the effect that the hostile groups may be seen as an international entity due to the scale of damage[420] that they inflict, and enables the state that is a party to the armed attack to denounce any act of the hostile group,[421] thus freeing themselves from any responsibility regarding the acts of the hostile groups. Recognising a hostile group as a belligerent, however, has lost its applicability in modern times.[422] The position currently held is that Common Article 3 applies to all armed conflicts that qualify as NIACs and is supplemented by Additional Protocol II to the Geneva Conventions.[423]

Additional Protocols II defines in article 1(2)[424] forms of internal conflicts that do not constitute NIACs.

> This Protocol shall not apply to situations of internal disturbances and tensions, such as riots, isolated and sporadic acts of violence and other acts of a similar nature, as not being armed conflicts.

Distinction between Common Article 3 NIACs and other forms of internal conflicts has been established by the International Criminal Tribunal for the former Yugoslavia[425] wherein the Tribunal applied a test as set out by the Appeals Chamber to establish whether there is an armed conflict as described by Common Article 3.[426] This test focuses on two aspects, namely, "…the intensity of the conflict and the organization

---

417 Article 3 of the Geneva Conventions of 1949.
418 Article 3 of the Geneva Conventions of 1949.
419 Solis *The Law of Armed Conflict* 153.
420 Solis *The Law of Armed Conflict* 153.
421 Solis *The Law of Armed Conflict* 153.
422 Sassòli *International Humanitarian Law* 117.
423 Article 1 of the Additional Protocols II to the Geneva Conventions of 1949.
424 Article 1 of the Additional Protocols II to the Geneva Conventions of 1949.
425 *Prosecutor v Tadic* Case no IT-94-1-A Opinion and Judgement 7 May 1997 para 562 https://www.icty.org/x/cases/tadic/tjug/en/tad-tsj70507JT2-e.pdf.
426 *Prosecutor v Tadic* Case no IT-94-1-A Opinion and Judgement 7 May 1997 para 562 https://www.icty.org/x/cases/tadic/tjug/en/tad-tsj70507JT2-e.pdf.

of the parties to the conflict".[427] These two aspects form a threshold for when internal conflicts become NIACs, thus serving as the minimum requirements to be classified as a NIAC.[428]

Where this test is conducted and existence of an NIAC is established, Common Article 3 must be observed by the parties to the NIAC and all other articles that the Geneva Conventions consist of may be ignored.[429] This has the effect that, in NIACs only the domestic law of a state that is a party to the armed conflict, Common Article 3 and human rights law will apply.

There has always been uncertainty on the application of the law of war on counter-terrorist operations.[430] Terrorist groups are non-state actors and thus cannot be a party to the Geneva Conventions.[431] Common Article 3 may apply to terrorist groups where their acts reach a scale of violence,[432] and the group has a form of organisation to be considered as an international entity,[433] as discussed above. To assist in establishing when a certain law applies to the conduct of terrorist groups, the scale of violence and how the group is organised must be viewed on a spectrum.[434] On the one side of the spectrum are groups that have no organisational elements and the violence that they cause is minimal to non-existent.[435] On the other side of the scale is a highly organised group with a scale of violence inflicted equal to a state in wartime.[436] The aforementioned group will not be considered an international entity and will be viewed as a criminal group bound under the domestic law of the country in which they reside whilst the latter will be viewed as an international entity bound by Common Article 3 and Additional Protocol II. A good example of a terrorist group that is viewed as an

---

427 *Prosecutor v Tadic* Case no IT-94-1-A Opinion and Judgement 7 May 1997 para 562 https://www.icty.org/x/cases/tadic/tjug/en/tad-tsj70507JT2-e.pdf.
428 *Prosecutor v Tadic* Case no IT-94-1-A Opinion and Judgement 7 May 1997 para 562 https://www.icty.org/x/cases/tadic/tjug/en/tad-tsj70507JT2-e.pdf.
429 Pictet (ed) *Commentary, IV Geneva Convention* cited by Solis *The Law of Armed Conflict* 154.
430 Solis *The Law of Armed Conflict* 159.
431 Roscini *Cyber Operations* 152.
432 Roscini *Cyber Operations* 152-153.
433 Roscini *Cyber Operations* 153-154.
434 Solis *The Law of Armed Conflict* 160-161.
435 Solis *The Law of Armed Conflict* 160-161.
436 Solis *The Law of Armed Conflict* 160-161.

international entity is the Taliban.[437] They recently terminated their control of Afghanistan and, although they are not recognised by the UN as the state's legitimate government,[438] the UN implored them to abide by international law and international standards.[439]

4.3.3 In the context of cyber space

In the context of cyber-operations, the question of what armed conflicts are, must be answered in order to establish whether cyber-operations can be classified as such. By interpreting the definition of an armed conflict, as contemplated by the Appeals Chamber of the International Criminal Tribunal for the former Yugoslavia as mentioned at 4.3.2, Kittichaisaree[440] came to the following conclusion with regard to cyber-attacks:

> To state the obvious, the law of armed conflict applies whenever there is an armed conflict. Only those activities amounting to, connected to, or conducted in the context of an armed conflict are governed by this body of law. Thus, not all cyber-operations or cyber-attacks are so governed

This may not be the case for all cyber-operations. When examining the ICRC's updated Commentary to the First Geneva Convention of 1949 in 2016,[441] it is clear that, in their view cyber-operations have the potential to cause IHL to be applicable in a situation where cyber-operations are conducted by one state on another, and where the operation coincides with a kinetic attack.[442] Cyber-operations will amount to an armed conflict where they cause similar damage to that of a kinetic operation that constitutes an armed attack.[443] In the event where a cyber-operation does not reach the level of damage associated with armed conflicts, but disrupts infrastructure, be it civilian or

---

437 A terrorist organisation operating mainly in the Middle East that is driven by extremist Sunni Islam religious practices.

438 Nichols 2021 https://www.reuters.com/world/asia-pacific/exclusive-taliban-names-afghan-un-envoy-asks-speak-world-leaders-2021-09-21/.

439 United Nations Security Council The situation in Afghanistan Security Council meeting S/PV.8834 SC/14603 16 August 2021.

440 Kittichaisaree *Public International Law of Cyberspace* 204.

441 ICRC *Commentary on the First Geneva Convention* para 255.

442 ICRC *Commentary on the First Geneva Convention* para 254.

443 ICRC *Commentary on the First Geneva Convention* para 254.

military infrastructure, the position is unclear.[444] State practice may be the solution to this uncertainty, however, it is clear that the potential is there for cyber-operations to initialise armed conflicts.

4.4 Principles of IHL

4.4.1 Distinction

Article 48 of the Additional Protocol I[445] reads as follows:

> In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.

Article 48 points out that distinction in armed conflicts consists of two elements:[446] firstly, to distinguish between civilians and combatants,[447] and secondly, to only target combatants.[448] The first element, called the distinction element for convenience sake, is based on the concept that wars are fought by soldiers and not civilians.[449] This has not always been the case, historically, when an armed conflict arose between tribes, nations or empires, the civilians were considered instruments that could be used to instil fear and low morality in opposing combatants.[450] When wars where won, the victor had complete power over the civilians of the conquered state, which often led to enslavement and genocide.[451] Laws of distinction between combatants and civilians began to emerge in the sixteenth century[452] and appeared in customary law for the first time in 1868 with the preamble of the St. Petersburg Declaration.[453] After the atrocities conducted on civilians in World War II, distinction was formally introduced in

---

444 ICRC *Commentary on the First Geneva Convention* para 254.
445 Article 48 of the Additional Protocols I to the Geneva Conventions of 1949.
446 Article 48 of the Additional Protocols I to the Geneva Conventions of 1949.
447 Article 48 of the Additional Protocols I to the Geneva Conventions of 1949.
448 Article 48 of the Additional Protocols I to the Geneva Conventions of 1949.
449 Roscini *Cyber Operations* 177.
450 Solis *The Law of Armed Conflict* 251.
451 Solis *The Law of Armed Conflict* 251.
452 Neff *War and the Law of Nations* 85.
453 Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight, Saint Petersburg, 29 November/ 11 December 1868.

customary international law with article 48.[454] Article 48 states that distinction must be made between civilians and combatants as well as civilian objects and military objects.[455] The distinction between civilians and combatants are regulated by Article 48, read together with article 44(3) of Additional Protocol I.[456]

> In order to promote the protection of the civilian population from the effects of hostilities, combatants are obliged to distinguish themselves from the civilian population while they are engaged in an attack or in a military operation preparatory to an attack. Recognizing, however, that there are situations in armed conflicts where, owing to the nature of the hostilities an armed combatant cannot so distinguish himself, he shall retain his status as a combatant, provided that, in such situations, he carries his arms openly:
>
> *a)* during each military engagement, and
>
> *b)* during such time as he is visible to the adversary while he is engaged in a military deployment preceding the launching of an attack in which he is to participate.
>
> Acts which comply with the requirements of this paragraph shall not be considered as perfidious within the meaning of Article 37, paragraph 1 *c)*.

This requires military personnel to visually distinguish themselves form civilians by mainly wearing a uniform that identifies the person as a combatant and not a civilian.[457] This visual distinction requirement was not always complied with as was seen in the USA-Somali war of 1992.[458] In these wars, USA combatants could not distinguish between civilians and combatants[459] and were forced to rely on article 44(3)'s recognition[460] that visual differentiation cannot at all times be attained.[461] By interpreting article 44(3), it is clear that combatants who cannot be visually differentiated from civilians, retain their combatant status through their actions.[462] An example hereof is found in the book, Black Hawk Down,[463] where a situation is described in which a USA helicopter was shot down in the USA-Somali conflict. The wounded soldiers from the wrecked helicopter were held up in a nearby house, fighting

---

454 Solis *The Law of Armed Conflict* 251.
455 Article 48 of the Additional Protocols I to the Geneva Conventions of 1949.
456 Article 44(3) of the Additional Protocols I to the Geneva Conventions of 1949.
457 Article 44(3) of the Additional Protocols I to the Geneva Conventions of 1949.
458 Solis *The Law of Armed Conflict* 255.
459 Corn 1998 *The Army Lawyer* 35, 38 cited by Solis *The Law of Armed Conflict* 255.
460 Corn 1998 *The Army Lawyer* 35, 38 cited by Solis *The Law of Armed Conflict* 255.
461 Article 44(3) of the Additional Protocols I to the Geneva Conventions of 1949.
462 Article 44(3) of the Additional Protocols I to the Geneva Conventions of 1949.
463 Bowden *Black Hawk Down* 90.

off Somali military forces. There was an unarmed woman who no one shot at; she was screaming and pointing at where the wounded soldiers were situated before returning to cover. As she disappeared, an attack by the Somali forces was unleashed upon the location that she pointed out. After the attack subsided, she reappeared from cover and pointed out another location where wounded US soldiers were taking cover. When the woman reappeared a third time, she was shot and killed by one of the US soldiers. Even though visually, the woman appeared to be an unarmed civilian, her actions of identifying the location where the wounded US soldiers were situated, gave her the status of a combatant and thus a legitimate target for the US combatants. In terms of Article 51(3) of Additional Protocol I,[464] the status of a civilian shall cease to exist when that civilian directly partakes in the military conflict.

> Civilians shall enjoy the protection afforded by this Section, unless and for such time as they take a direct part in hostilities.

When articles 44(3), 48, and 51(3) of the Additional Protocol I are read together, it is clear that, where the actions of a perceived civilian positions them that they directly partake in the armed conflict,[465] that person will have the status of a combatant[466] for as long as the opposing combatants can observe that their actions, to directly partake in the armed conflict, continue.[467]

Similarly, to civilians, civilian objects also enjoy the right to be distinguished from military objects and be protected under article 48 of the Additional Protocols I.[468] Civilian objects are defined by article 52 of the Additional Protocols I as "…all objects which are not military objectives".[469] This is seen in the obligation placed on combatants by the term military necessity[470] that will be discussed later in this chapter at 4.4.2 to limit attacks to military objectives only.[471] This means that all objects are

---

464 Article 51(3) of the Additional Protocols I to the Geneva Conventions of 1949.
465 Article 51(3) of the Additional Protocols I to the Geneva Conventions of 1949.
466 Article 44(3) of the Additional Protocols I to the Geneva Conventions of 1949.
467 Article 51(3) of the Additional Protocols I to the Geneva Conventions of 1949.
468 Article 48 of the Additional Protocols I to the Geneva Conventions of 1949.
469 Article 52 of the Additional Protocols I to the Geneva Conventions of 1949.
470 Sassòli *International Humanitarian Law* 351-352.
471 Sassòli *International Humanitarian Law* 351-352.

protected from attacks during armed conflicts unless the object is used for military purposes.

For distinction to be complied with during an attack conducted in cyberspace, it must be established that cyber-attacks can be directed in such a way as to target combatants and military objects only in compliance with article 48 of the Additional Protocols I.[472] The combatants in cyberspace must also be able to distinguish themselves as combatants in terms of article 44(3) of the Additional Protocols I.[473]

The question whether distinction can be made between civilians and combatants in cyberspace, may lie in the principle of civilians gaining combatant status due to their direct involvement in a military operation.[474] This may have specific relevance to cyberspace because, similarly to situations as mentioned above, no distinction can be made between combatants and civilians in the cyber realm other than their actions.[475] Using the example of the civilian woman who gained combatant status in the US-Somali war, as described in Black Hawk Down,[476] if for example, a similar situation occurred in cyberspace, where the civilian woman is a hacker using malware to pinpoint US military facilities in Somalia and then relaying this information to the Somali military in order to conduct attacks on them, her direct actions would allow US combatants to act against her as if she was a combatant. Nothing other than a combatant's action in cyberspace can currently distinguish the said combatant from a civilian.[477] This has the effect that there must be a general rule by which all people interacting at any given time in the cyber realm, must be seen as civilians until their actions indicate otherwise.[478] This is in line with article 51 of the Additional Protocols I[479] by guaranteeing civilian safety from military operations and limiting the status of civilians by their conduct in relation to the armed operation in question.

---

472 Article 48 of the Additional Protocols I to the Geneva Conventions of 1949.
473 Article 44(3) of the Additional Protocols I to the Geneva Conventions of 1949.
474 Article 51(3) of the Additional Protocols I to the Geneva Conventions of 1949.
475 Article 44(3) of the Additional Protocols I to the Geneva Conventions of 1949.
476 Bowden *Black Hawk Down* 90.
477 Kittichaisaree *Public International Law of Cyberspace* 214.
478 Kittichaisaree *Public International Law of Cyberspace* 215-216.
479 Article 51 of the Additional Protocols I to the Geneva Conventions of 1949.

Distinguishing between civilian and military objects in cyberspace can be more complicated than distinguishing between civilians and combatants. The cyber-space is a network created by and reliant on civilian infrastructure.[480] Military documents, systems for national defence of states, Twitter, Facebook and all other websites, documents and information available on the internet exist in the cyber-space. An attack in cyberspace will inevitably be conducted on systems that are used by a military as well as by civilians.[481] These types of systems are coined as "dual-use objects" in terms of Rule 101 of the Tallinn Manual 2.0.[482] The amount of military information present in a given dual-use object in relation to civilian information may differ from hour to hour.[483] This complicates the decision for combatants to target military objects as contemplated in article 48,[484] however, the task is not impossible.[485] Extreme care must be taken[486] in order to ensure that any damage conducted through an intended attack on military objects in cyber-space is in proportion to the intended outcome for purposes of necessity[487] and that the attack will not be seen as indiscriminate as regulated by unnecessary suffering[488] (both military necessity and unnecessary suffering will be discussed later in this chapter at 4.4.2 and 4.4.3 respectively.)

Another issue with distinction between civilian and military objects is whether data is seen as objects in terms of the Law of War.[489] In any cyber-attack, data will be manipulated, deleted or damaged in order to reach the intended military objective.[490] As an example, Ireland uses an internet provider that is called the IRA, to run their automated weapons factory. An attack on the IRA service provider would be effective to shut the factory down. However, other civilians and companies may also make use of the IRA internet service provider, which would mean that the attack would damage

---

480 Schmitt *Tallinn Manual 2.0 on the International Law* 445.
481 Schmitt *Tallinn Manual 2.0 on the International Law* 445.
482 Schmitt *Tallinn Manual 2.0 on the International Law* 445.
483 Schmitt *Tallinn Manual 2.0 on the International Law* 445.
484 Article 48 of the Additional Protocols I to the Geneva Conventions of 1949.
485 Kittichaisaree *Public International Law of Cyberspace* 215.
486 Kittichaisaree *Public International Law of Cyberspace* 216.
487 Kittichaisaree *Public International Law of Cyberspace* 216.
488 Roscini *Cyber Operations* 285.
489 Schmitt *Tallinn Manual 2.0 on the International Law* 416.
490 Kittichaisaree *Public International Law of Cyberspace* 206.

civilian data as well. For purposes of distinction, data may be seen as objects and an attack may still be conducted on military data to the detriment of civilian data where the damage from the attack is proportional to the intended outcome of the military objective.[491]

In the view of the International Group of Experts who compiled the Tallinn Manual 2.0, the majority of the experts is of the opinion that data cannot be considered an object for purposes of article 48 because of its intangible nature.[492] According to them, data does not coincide with the ordinary meaning of an object and is not in line with the 1987 ICRC commentary on the Additional Protocols.[493] They acknowledge in Rule 92 that data alteration could be seen as an attack on civilian objects, if it causes damage equal to that of an armed attack or if the functionality of cyber infrastructure is altered.[494]

It is clear that the law of armed conflict places an obligation on combatants to distinguish between civilians and combatants, as well as, civilian objects and military objects, and to only target combatants and military objects. This principle is not altered or loosely implemented in relation to distinction in cyberspace. However, the notion that distinction between combatants and civilians in cyber-space is not ascertainable except for actions of individuals interacting with the cyber realm, complicates the principle of distinctions in this regard. Similarly, the task of distinguishing between civilian and military objects is complicated by dual-use objects.

The fact that the actions of individuals in cyberspace constitute the only ground for proper distinction between civilians and combatants in cyberspace, all individuals interacting with the cyber realm must be regarded as civilians until their actions indicate that their conduct allows them to be classified as combatants, as contemplated in article 48 read together with article 51 of the Additional Protocols. This is in essence

---

491 Kittichaisaree *Public International Law of Cyberspace* 215.
492 Schmitt *Tallinn Manual 2.0 on the International Law* 437.
493 Schmitt *Tallinn Manual 2.0 on the International Law* 437.
494 Schmitt *Tallinn Manual 2.0 on the International Law* 437.

how the general rule as contemplated at 4.4.1 above guarantees the principle of distinction between civilians and combatants in cyber-space.

For purposes of distinction between civilian and military objects in cyberspace, the complicated principle of a dual-use object complicates the application of distinction in cyberspace. Distinction in this regard does not require combatants to refrain from attacking civilian objects. Proportionality and military necessity must be given priority in taking the decision to attack an object in cyberspace. This must coincide with extreme care on the part of the combatant.

4.4.2 Military necessity

Article 35 of the Additional Protocols I[495] curtails the basic rules when it comes to the methods and means of warfare, and states as follows:

1. In any armed conflict, the right of the parties in the conflict to choose methods or means of warfare is not unlimited.
2. It is prohibited to employ weapons, projectiles and material and methods of warfare of a nature to cause superfluous injury or unnecessary suffering.
3. It is prohibited to employ methods or means of warfare that are intended, or may be expected, to cause widespread, long-term and severe damage to the natural environment.

This article which is named "The Basic rules"[496] has been created to establish the fundamental position in customary international law that the means by which an armed conflict is conducted, is not unlimited.[497] This is echoed by The Hague Regulations of 1907 in article 22[498] where it is stated that, "The right of belligerents to adopt means of injuring the enemy is not unlimited."[499] Military necessity appears to be an exception to the basic rules found in article 35 of the Additional Protocols I and article 22 of The Hague Regulations 1907.

---

495 Article 35 of the Additional Protocols I to the Geneva Conventions of 1949.
496 Article 35 of the Additional Protocols I to the Geneva Conventions of 1949.
497 ICRC *Commentary on the First Geneva Convention* para 1382.
498 Article 22 of The Hague Regulations of 1907.
499 Article 22 of The Hague Regulations of 1907.

Military necessity does not appear in the Geneva Conventions or the Additional Protocols,[500] however, article 23(g) of The Hague Regulations of 1907[501] states as follows:

> Art. 23. In addition to the prohibitions provided by special Conventions, it is especially forbidden… (g) To destroy or seize the enemy's property, unless such destruction or seizure be imperatively demanded by the necessities of war

According to article 23(g), military necessity constitutes an exception to destruction of an enemy's property. Although this reference to military necessity is only limited to the destruction of an enemy's property, it is interpreted to include all acts conducted by combatants in armed conflicts.[502]

The *Kriegsraison* is a German term that had its roots in Prussian military society;[503] the complete term reads as follows: "*Kriegsraison geht vor Kriegsmanier"* ("the necessities of war take precedence over the rules of war").[504] This interpretation of military necessity allowed commanders as well as individual combatants to do whatever necessary to win the armed conflict.[505] The law of war was seen as a "… reciprocity of mutual agreement…"[506] and not as the "…*lex scripta*".[507] This interpretation only ceased to exist during the Nuremburg Trials after the conclusion of World War II.[508]

Another interpretation for necessity is the doctrine of "A state of necessity".[509] This differs from the *Kriegsraison* in that the law of war does not apply to situations where a state of emergency is called.[510] The governing body of a state can, upon its interpretation of a necessary action,[511] commit acts that are prohibited by IHL.[512] As

---

500 Solis *The Law of Armed Conflict* 258.
501 Article 23(g) of The Hague Regulations of 1907.
502 Solis *The Law of Armed Conflict* 258.
503 Solis *The Law of Armed Conflict* 265.
504 ICRC *Commentary on the First Geneva Convention* para 1386.
505 ICRC *Commentary on the First Geneva Convention* para 1386.
506 Morgan *The German War Book* 53-55 cited by Solis *The Law of Armed Conflict* 266.
507 Morgan *The German War Book* 53-55 cited by Solis *The Law of Armed Conflict* 266.
508 ICRC *Commentary on the First Geneva Convention* para 1386.
509 ICRC *Commentary on the First Geneva Convention* para 1387.
510 ICRC *Commentary on the First Geneva Convention* para 1387.
511 ICRC *Commentary on the First Geneva Convention* para 1387.
512 ICRC *Commentary on the First Geneva Convention* para 1387.

the doctrine of *Kriegsraison*, state of necessity is not compatible with the Geneva Convention, the Martens-clause or the Additional Protocols.[513]

Military necessity in terms of IHL means a balance between two principles, unnecessary suffering and proportionality.[514] This allows for military necessity to be taken into account without infringing the laws of war.[515] This has the effect that IHL cannot be eroded through non-compliance, and the protection to civilians and objects remain guaranteed.[516] In the event where IHL does not provide clarification on the prohibitive nature of acts conducted during armed conflicts, the parties in the conflict are free to act within the confines of customary international law.[517] This is guaranteed by the article 1(2) of the Additional Protocols I,[518] Martens-clause that reads:

> In cases not covered by this Protocol or by other international agreements, civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience.

With regard to the principle of military necessity in cyberspace, there is very little literature that is substantial in establishing to what extent this principle may apply in the cyber realm. The International Group of Experts who composed the Tallinn Manual 1.0. referred to military necessity only once in the discussion on rule 83 of the Tallinn Manual 1.0 regarding the protection of the natural environment.[519] In this discussion the International Group of Experts concluded that the environment must be seen as an object, thus it enjoys the same protection that civilian objects have and cannot be subjected to wantonness.[520] They go further by explaining that the term, "wantonness", refers to "…destruction is the consequence of a deliberate action taken maliciously…"[521] thus, wantonness is an action that is inconsistent with the principle of

---

513 ICRC *Commentary on the First Geneva Convention* para 1388.
514 ICRC *Commentary on the First Geneva Convention* para 1389.
515 ICRC *Commentary on the First Geneva Convention* para 1389.
516 ICRC *Commentary on the First Geneva Convention* para 1389.
517 Article 1(2) of the Additional Protocols I to the Geneva Conventions of 1949.
518 Article 1(2) of the Additional Protocols I to the Geneva Conventions of 1949.
519 Schmitt *Tallinn Manual on the International Law* Rule 83 231.
520 Schmitt *Tallinn Manual on the International Law* Rule 83 231-232.
521 Schmitt *Tallinn Manual on the International Law* Rule 83 232.

military necessity.[522] Other that the conclusion that the environment is seen as an object, rule 83 as well as its discussion is of no relevance to this dissertation. However, it establishes an important objective for purposes of military necessity in its relation to cyberspace. In this discussion of rule 83, military necessity is utilised to establish the validity of rule 83 as if it should be obvious that it applies to the cyber realm unequivocally. Out of this application of military necessity and lack of literature on its application to the cyberspace, the assumption can be made that the principle of military necessity is applicable to cyberspace in its entirety. This assumption may change in the future, depending on state practice and the issuance of possible future legislation on the matter.

It is thus evident that military necessity constitutes an exception on the general rules found in article 35 of the Additional Protocols I in that civilians and civilian objects may be attacked or allowed to be damaged if the outcome of the attack is necessary to reach a military objective. The advantages gained from such a military objective must also be in relation to the destruction or damage of civilians and/or civilian objects. Further, military necessity must be in line with the principles of IHL and must strike a balance between unnecessary suffering and proportionality. For purposes of the application of military necessity in cyberspace, an assumption is made that this principle applies unequivocally based on the lack of literature and its application in the discussion of the protection of the natural environment found in the Tallinn Manual 1.0.

4.4.3 Unnecessary suffering

Unnecessary suffering is defined by article 35(2) of the Additional Protocols I,[523] which reads as follows:

> It is prohibited to employ weapons, projectiles and material and methods of warfare of a nature to cause superfluous injury or unnecessary suffering.

---

522 Schmitt *Tallinn Manual on the International Law* Rule 83 232.
523 Article 35(2) of the Additional Protocols I to the Geneva Convention of 1949.

The questions arising from article 35(2) are what the nature of "…weapons, projectiles and material and methods of warfare…"[524] means, and how "unnecessary suffering" can be calculated.[525]

Unnecessary suffering in terms of IHL, is an obligation as well as a right placed on combatants rather than civilians.[526] Suffering of combatants is not prohibited by article 35(2), but rather the use of weapons that cause excess suffering.[527] Weaponry is the main instrument used to cause suffering in armed operations, yet,[528] weapons are allowed to be used in armed conflicts.[529] Similar to all other elements of conflicts, weaponry is restricted by IHL. The Convention on Prohibition or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects of 1980 (the Conventional Weapons Convention)[530] aims to reduce unnecessary suffering prevalent in modern weapons[531] and together with article 23(e) of The 1907 Hague Regulations forbid employing weapons that cause unnecessary suffering.[532] Article 36 of the Additional Protocols I[533] places a further element to the restriction of these types of weapons by directing states, making or using weapons, to determine whether or not their use would be in line with Additional Protocol I.

The obligation placed on states by article 36 can be difficult to establish. The ICJ aids by determining when suffering of combatants become unnecessary through using weaponry by defining unnecessary suffering in the Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons.[534] On the meaning of unnecessary suffering,

---

524 Solis *The Law of Armed Conflict* 270.
525 Solis *The Law of Armed Conflict* 270.
526 ICRC *Commentary on the First Geneva Convention* para 1410.
527 ICRC *Commentary on the First Geneva Convention* para 1411.
528 Solis *The Law of Armed Conflict* 270.
529 Solis *The Law of Armed Conflict* 270.
530 Green *Essays on the Modern Law of War* cited by Solis *The Law of Armed Conflict* 270.
531 The Preamble to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects as Amended on 21 December 2001.
532 Article 23(e) of The Hague Regulations of 1907.
533 Article 36 of the Additional Protocols I to the Geneva Convention of 1949.
534 Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, ICJ GL No 95, [1996] ICJ Rep 226, ICGJ 205 (ICJ 1996), 8th July 1996, United Nations [UN]; International Court of Justice [ICJ].

the ICJ explains it as "a harm greater than that unavoidable to achieve legitimate military objectives".[535] In term of this wording, it can be interpreted that the ICJ views unnecessary suffering as a pendulum. The scale of suffering in and of itself is not in question, rather the scale of suffering in relation to the military necessity establishes whether or not suffering can be considered as necessary.[536]

In relation to unnecessary suffering and cyber operations, one of the biggest concerns is that of prohibition of indiscriminate attacks.[537] Cyber operations are proven to be precise methods of attack that can target a specific intended object without causing damage to civilians and/or civilian infrastructure.[538] However, as discussed earlier, cyberspace is a dual-use object that holds civilian and military data.[539] Where an attack is directed against military objectives, sharing internet usage with civilian data, an attack on the military objectives may cause civilian data to be damaged as well, and is thus considered as an indiscriminate attack.[540] A good example of this is where a military objective shares a power grid with a hospital that is regulated through the internet, with a hospital. If the power grid of the military objective is targeted in order to disable it, the hospital will inevitably be affected as well. The much-needed life support machinery among others may become disabled, causing damage to civilians, and depending on the military gains from the attack, will be disproportionate. This attack can be regarded as indiscriminate damage. Another example of a cyber-operation that caused indiscriminate damage is the 2017 cyber-attack on the Ukraine by Russia for which they have not claimed responsibility as yet.[541] The cyber-attack was targeted at Kiev, the capital city of Ukraine, on the day before the country

---

535 Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, ICJ GL No 95, [1996] ICJ Rep 226, ICGJ 205 (ICJ 1996), 8th July 1996, United Nations [UN]; International Court of Justice [ICJ] 35.

536 Solis *The Law of Armed Conflict* 271-272.

537 International Humanitarian Law and the Challenges of Contemporary Armed Conflicts: Recommitting to Protection in Armed conflict on the 70th Anniversary of the Geneva Conventions 28.

538 Kittichaisaree *Public International Law of Cyberspace* 206.

539 Cross reference to dual use weapons.

540 Kittichaisaree *Public International Law of Cyberspace* 214.

541 Perlroth, Scott and Frenkel 2017 https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html#.

celebrated the eleventh year since their split from the Soviet Union and the adoption of a new constitution. The attack not only affected Ukraine, but it also affected American and Danish businesses such as Maersk and Merck, as well as a Cadbury factory in Australia.[542]

These two examples outline the current questions that need answering in order to establish whether the indiscriminate nature of cyber-attacks can be regulated in order to be in line with the Law of Armed Conflict. The first uncertainty is whether cyber weapons can be manipulated to limit its spread as seen in the 2007 Ukraine attack.[543] Malware can be inserted into a system and will spread to other systems, similar to a virus, and cause damage irrespective of whether the system is a targeted military objective or a civilian chocolate factory.[544] There is uncertainty whether such weaponry can in future be manipulated to attack the military objective only, and even if the indiscriminate spread of cyber weaponry can be regulated, the question, as to what extent it would be justified, comes into play.[545] Will it be justified to attack the power grid for purposes of disabling a military objective, if a hospital relies on the same power grid to function? Only continuous testing of cyber weaponry by states, in line with article 36 of the Additional Protocols I,[546] will establish whether these weapons can be altered to regulate their indiscriminate spread through internet systems. As for the question of justifiability of a cyber-attack, the principle of proportionality must be considered.

Ultimately, it has been established that suffering of civilians and/or combatants would be unnecessary where the suffering endured is greater that the military gains that coincide with it. In the modern era, weapons have the potential to cause mass suffering and as such, taking caution against attacks that is unnecessary is particularly important. Categorically, the Conventional Weapons Convention, as well as, The Hague

---

542 Perlroth, Scott and Frenkel 2017 https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html#.
543 Kittichaisaree *Public International Law of Cyberspace* 219.
544 Singer and Friedman *Cybersecurity and Cyberwar* 43.
545 Kittichaisaree *Public International Law of Cyberspace* 219.
546 Article 36 of the Additional Protocols I to the Geneva Convention of 1949.

Regulations, endeavours to restrict unnecessary suffering by forbidding weapons that are found to cause unnecessary suffering. Article 36 of the Additional Protocols I places a further obligation on states to test weaponry that they employ and/or create to not cause unnecessary suffering. If such a weapon is found to cause unnecessary suffering, it will be prohibited or must be altered and restricted.

Because cyberspace is a dual-use object, precision-targeted attacks have the potential to cause indiscriminate suffering as discussed in the two examples given above at 4.4.3. The questions arising from this are whether cyber weapons can be altered to minimise its spread through cyberspace, and whether a cyber-attack that causes indiscriminate suffering is justified. The question of whether cyber weapons can be altered, can be answered through continuous testing of cyber weaponry by states as contemplated by article 36 of the Additional Protocols I. The question of to what extent indiscriminate attacks are justified, can find applicability in the principle of proportionality.

4.4.4 Proportionality

Together with unnecessary suffering, proportionality is a term closely associated with military necessity.[547] The concept is initially referenced to in Article 22 of The Hague Regulations of 1907[548] by limiting the right of belligerents to injure the enemy.[549] Although proportionality is not explicitly mentioned, it can be interpreted that a belligerent must take account of civilians and civilian infrastructure.[550] In terms of the law of war, proportionality is defined in two sections of the Additional Protocols I of 1977,[551] firstly, article 51.5(b)[552] reads as follows:

> 5. Among others, the following types of attacks are to be considered as indiscriminate:
> b) an attack which may be expected to cause incidental loss of civilian life, injury to

---

547 Cross reference to military necessity.
548 Article 22 of The Hague regulations of 1907.
549 Article 22 of The Hague regulations of 1907.
550 Solis *The Law of Armed Conflict* 273.
551 Additional Protocols I to the Geneva Conventions of 1949.
552 Article 51.5(b) of the Additional Protocols I to the Geneva Conventions of 1949.

> civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.

Secondly, article 57.2(b)[553] states:

> 2. With respect to attacks, the following precautions shall be taken: *b)* an attack shall be cancelled or suspended if it becomes apparent that the objective is not a military one or is subject to special protection or that the attack may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.

Article 51.5(b) places a protective element on civilians and civilian objects by stating that an attack that may cause injury or death to civilians and/or damage to civilian objects, is "excessive"[554] when compared against the perceived military necessity. There is uncertainty as to what is meant by excessive.[555] Article 57.2(b) constitutes a precaution on the side of the belligerent to "…cancel or suspend…"[556] an attack with an outcome that can be interpreted as military necessity when the perceived injury or death of civilians and/or damage to civilian objects is excessive.[557] Proportionality is defined in the Law of Armed Conflict by combining these two articles.[558]

Regarding the question of what "excessive" entails in relation to both articles 51.5(b) and 57.2(b) it is worth noting the commentary on the Additional Protocols of 8 June 1977 more specifically paragraphs 1978 and 1979:[559]

> **1978** Such criticisms are justified, at least to some extent. Putting these provisions into practice, or, for that matter, any others in Part IV, will require complete good faith on the part of the belligerents, as well as the desire to conform with the general principle of respect for the civilian population.
>
> **1979** Comments were also made in various quarters that paragraph *5(b)* authorized any type of attack, provided that this did not result in losses or damage that were excessive in relation to the military advantage anticipated. This theory is manifestly incorrect. In order to comply with the conditions, the attack must be directed against

---

553 Article 57.2(b) of the Additional Protocols I to the Geneva Conventions of 1949.
554 Article 51.5(b) of the Additional Protocols I to the Geneva Conventions of 1949.
555 Solis *The Law of Armed Conflict* 274.
556 Article 57.2(b) of the Additional Protocols I to the Geneva Conventions of 1949.
557 Article 57.2(b) of the Additional Protocols I to the Geneva Conventions of 1949.
558 Henckaerts and Doswald-Beck *Customary International Humanitarian Law* cited by Solis *The Law of Armed Conflict* 274.
559 ICRC *Commentary on the First Geneva Convention* paras 1978 & 1979.

> a military objective with means which are not disproportionate in relation to the objective, but are suited to destroying only that objective, and the effects of the attacks must be limited in the way required by the Protocol; *moreover,* even after those conditions are fulfilled, the incidental civilian losses and damages must not be excessive. Of course, the disproportion between losses and damages caused, and the military advantages anticipated raises a delicate problem; in some situations, there will be no room for doubt, while in other situations there may be reason for hesitation. In such situations the interests of the civilian population should prevail, as stated above.

By regarding paragraph 1979 first, it can be understood that excessive, as contemplated in article 52.5(b), will only come into effect where the attack meets the requirements of military necessity in that the attack must be in proportion to the objective in question, and that the objective is targeted.[560] The element of unnecessary suffering must also be met through the appropriate use of weaponry.[561] After these requirements have been met, proportionality must be regarded by not allowing injury or death of civilians and/or damage of civilian objects to be excessive in relation to military necessity and/or unnecessary suffering. The paragraph goes further by stating that "excessive" would mean that there is disproportion between the injury or death of civilians and/or the damage of civilian objects, and the military advantages that is gained through the attack in question.[562] For combatants engaged in an armed operation, this decision is complex and difficult to make at a whim, and thus paragraph 1978 states that in practice, belligerents must act in complete good faith and have comfort that their decisions are made with the best interest of the civilian population in mind.[563] This eludes that there is no threshold for an excessive attack in the light of article 52.5(b), but an objective decision must rather be taken regarding the proportionality between civilian loss of life, injury and/or damage to civilian objects and the military gains acquired through the attack in question. Where the balance between the two appears to be highly disproportionate, the proportionality requirements have not been met.

---

560 ICRC *Commentary on the First Geneva Convention* para 1979.
561 ICRC *Commentary on the First Geneva Convention* para 1979.
562 ICRC *Commentary on the First Geneva Convention* para 1979.
563 ICRC *Commentary on the First Geneva Convention* para 1978.

For purposes of the cyberspace, it is worth referring to the example of a power grid supplying electricity to a hospital as well as a military objective.[564] The question arising from this example is whether a cyber-attack that causes damage to civilians and/or civilian infrastructure, can be justified. By examining proportionality and articles 51(5)(b) and 57(2)(b), it is clear that when damage to civilians and/or civilian infrastructure is excessive, a cyber-attack will be unjustified.[565] Whether an attack is labelled as excessive, will be determined by the objective observation of civilian injury, loss of life and/or damage to civilian objects compared to the military necessity of conducting the attack. This is echoed by Rules 114 to 120 of the Tallinn Manual 2.0[566] Schmitt[567] states in relation to Rule 114 to 120 as follows:

> …. an attacker to take steps to minimise civilian harm regardless of whether expected collateral damage is excessive in relation to the military advantage anticipated.

This would imply that, where the military necessity to disable a military objective by attacking the power grid, would be necessary enough to the observer to justify the loss of life support systems by a hospital on the same grid causing the death of civilians in intensive care, would be proportionate.

Ultimately, as in kinetic armed operations, distinction must be made between the actual military objective and the collateral damage incidental to the attack. The military objective must be necessary and in line with the Law of Armed Conflict. The attack on a military objective may not be excessive, causing unnecessary suffering and the collateral damage to civilians must be in proportion to the outcomes of military necessity. Where a cyber-operation, in conjunction with a kinetic operation or not, meets the requirements as set out above, it will be in line with the Law of Armed Conflict and thus be regulated by IHL.

---

564 Cross reference to example.
565 Schmitt *Tallinn Manual 2.0 on the International Law* 476.
566 Schmitt *Tallinn Manual 2.0 on the International Law* Rules 114 to 120.
567 Schmitt *Tallinn Manual 2.0 on the International Law* 476.

4.5 Conclusion

The objective of this chapter was to establish to what extent contemporary IHL regulates situations of armed conflict, in order to test its applicability to situations where armed conflicts include a cyber-attack. This chapter started with discussing the sources of IHL in order to form a basis from which to better understand later discussions of more integrated matters. The discussion on armed conflicts is instituted by firstly establishing what actions constitute an armed conflict. It was established that the general rule is that states declare war on one another, which applies the Law of Armed Conflicts in its entirety. This form of armed conflicts is less applicable in modern times. The most effective means used in establishing whether an act constitutes an armed conflict, is to distinguish between IACs and NIACs. Common Articles 2 and 3 together with the Additional Protocols establish how IACs and NIACs can be distinguished from one another. In terms of establishing when cyber operations constitute an armed attack, irrespective whether it is an IAC or an NIAC, can be answered by the definition of an armed conflict as given by the Appeals Chamber of the International Criminal Tribunal for the former Yugoslavia. The scale of damage and organisational formation of a group engaged in an armed conflict must be equal to that of a state in an armed conflict in order to be classified as such. As Kittichaisaree mentions, the Law of Armed Conflict will be applicable whenever an armed conflict arises. This draws the conclusion that, where an armed group conducting a cyber-attack in conjunction with armed attacks causes the scale of damage and consists of the organisational formation to constitute an armed conflict, irrespective of whether it is an IAC or an NIAC, the Law of Armed Conflicts will be applicable.

The next factors that were taken into account were the principles of IHL that are distinction, military necessity, unnecessary suffering and proportionality. Regarding the element of distinction, article 48 of the Geneva Conventions provides two factors for combatants to abide by in order to successfully distinguish between combatants and civilians. Firstly, combatants must distinguish between civilians and combatants and secondly, only target combatants. The first factor also requires combatants to distinguish between civilian objects and military objects. In terms of article 44(3) of

the Additional Protocols I, combatants must ensure that they are distinguished from civilians to prevent confusion as to who the targets are. Article 44(3) is not always complied with as can be seen in the example given out of the book, Black Hawk Down, and as such, the actions of perceived civilians can also alter their status to that of combatants in terms of article 51(3) of the Additional Protocols I. For purposes of distinction in cyber-space, the position is the same, however, distinguishing between civilians and combatants in cyberspace is complicated. This alludes to the need that a further general rule must be included for situations where distinction must be made between civilians and combatants in cyberspace. All must be viewed as civilians until their actions in cyberspace give them the status of combatants. Where distinction is made between civilian objects and military objects in cyberspace, the situation may be more complicated. Dual-use objects, in terms of Rule 101 of the Tallinn Manual 2.0, refer to the fact that both civilians and combatants are active in cyberspace and that an attack on military objects can potentially harm civilian objects as well. As such, extreme care must be taken by combatants to minimise damage to civilian objects. Where an attack in cyberspace will inevitably cause damage to civilian objects and that damage is not in proportion to the military objective at hand, such an attack must be halted. Another problem with distinction of objects in cyberspace is whether data can be regarded as objects. Whilst the International Group of Experts who compiled the Tallinn Manual 2.0 is of the opinion that data is intangible and is thus not in line with the definition of an object, they acknowledge in Rule 92 of the Tallinn Manual 2.0 that data alerting attacks that cause damage equal to that of what a kinetic attack can cause or that damages cyber infrastructure must be regulated by the Law of Armed Conflict. For purposes of distinction, the data may be regarded as objects that can be damaged by armed conflicts when the damage caused is of the same magnitude as the damage that kinetic armed attacks are capable of.

Military necessity is regarded an exception to the general rule found in article 35 of the Additional Protocols I in that it allows for the death or injury to civilians and/or destruction to civilian objects when it is necessary to reach an intended military objective. The intended advantage gained from such a military objective must be in

proportion with the destruction or damage of civilians and/or civilian objects. Furthermore, military necessity must be in line with the principles of IHL and thus must strike a balance between unnecessary suffering and proportionality. This allows for military necessity to be taken into account without infringing on the laws of armed conflict. Where IHL does not provide clarification on the prohibitive nature of acts conducted during armed conflicts, the parties in conflict are free to act within the confines of customary international law as guaranteed by article 1(2) of the Additional Protocols I. Only military necessity is acceptable in terms of the Law of Armed Conflict thus excluding *Kriegsraison* and a state of necessity out of its meaning. An assumption is made in relation to the applicability of military necessity in cyberspace that it applies unequivocally based on the lack of literature and its application in the discussion on the protection of the natural environment found in the Tallinn Manual 1.0.

Regarding the principle of unnecessary suffering, article 35(2) of the Additional Protocols I constitutes two questions, firstly, what the nature of "…weapons, projectiles and material and methods of warfare…" means, and secondly, to what extent suffering must be endured for it to become unnecessary. The Conventional Weapons Convention together with article 23(e) of the 1907 Hague Regulations forbids the employment of weapons that cause unnecessary suffering. Article 36 further places an obligation on states employing and creating weapons to test whether or not their use would be in line with the Additional Protocols. The test for this article 36 obligation is set out in the Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons. On the meaning of unnecessary suffering, the ICJ stated that harm greater than what is unavoidable to gain military objectives is unnecessary. This entails that unnecessary suffering must be viewed on a pendulum. Where suffering is greater than needed to achieve the intended goal, it will be unnecessary. In relation to cyber-attacks one of the biggest concerns is indiscriminate attacks. Cyberspace is a dual-use object where precision targeted attacks have the potential to cause indiscriminate suffering. The questions arising from this is whether cyber weapons can be altered to target specific objects only, and to what extent an indiscriminate act will be justified. The question of whether cyber weapons can be altered may be answered through continuous testing

of article 36 of the Additional Protocols together with state practice. The question of to what extent indiscriminate attacks are justified, can find applicability in the principle of proportionality.

Regarding the principle of proportionality, Article 51.5(b) places a protective element on civilians and civilian objects by stating that an attack that may cause injury or death of civilians and/or damage to civilian objects, is "excessive" when compared to the perceived military necessity. Article 57.2(b) constitutes a precaution on the side of the combatant to cancel or suspend an attack with an outcome that can be interpreted as military necessity when the perceived injury or death of civilians and/or damage to civilian objects is excessive. Proportionality is defined in the Law of Armed Conflict by combining these two articles. The commentary on the Additional Protocols of 8 June 1977 paragraph 1979 states that excessive in the context of proportionality would mean that the damage done to civilian objects and/or death/injury to civilians would be disproportionate to the advantages gained through the conclusion of the military objective. Paragraph 1978 goes further by stating that in decision making, combatants must act in good faith with the best interests of the civilian population in mind. This requires combatants to make an objective decision with the information available in order to establish whether proportionality is met. This is echoed in Rules 114 to 120 of the Tallinn Manual 2.0 eluding that proportionality regarding cyber-attacks would ultimately be reliant on an objective decision of whether or not the damage to civilian objects, death and/or injury to civilians are in proportion to the military objective in mind.

Contemporary IHL applies to all instances of armed conflict, whether an IAC or a NIAC. It was established that a conflict between different states or groups of combatants with a level of organisational capability and potential to cause damage equal to that of what a state in armed conflict can inflict, will be classified as an armed conflict. Weaponry that has the potential to cause damage and suffering equal to that of what kinetic weaponry can inflict, will be regulated under IHL irrespective of whether or not it is in fact a kinetic weapon. In the light of the abovementioned, a conclusion is drawn that cyber-attacks that cause a level of damage equal to that of a kinetic attack, utilised

by one state on another, or by a group with the level of organisational capability to be considered as a state on another group or state, will be considered an armed conflict and IHL will thus be applicable.

Chapter 5: Conclusion

At the start of this study, a historical overview of cyberspace and cyber-attacks was provided in order to establish the progression of attacks in cyberspace from the first recorded cyber-related attacks in the 1960s up until the present day. In this overview, the first discussion of the cyber-attack on Tallinn, Estonia of which the significance could not be overstated, was conducted. The cyber-attack gave rise to a number of institutions established to regulate cyber-related attacks including the CCDCOE and the Tallinn Manual. The historical overview of cyber-related attacks further emphasised the rate at which this form of attacks is being developed, indicating that proper regulation needs urgent attention.

The research question of this study was to establish whether contemporary IHL regulates cyber warfare and if so, to what extent it would apply. The prohibition on the use of force as well as the principles of IHL have particularly been focused on in order to establish its applicability in cyberspace. The aim of this research was to establish that current international law is sufficient for regulating cyber warfare and that interpreting the prohibition of the use of force clause as well as IHL to include cyber space will not require creating new legislation and/or treaties, but that cyber warfare is already regulated in its entirety. Seven objectives have been reached in order to ultimately reach the aim of this study. The first objective was to form a basis of terminology and background of cyber space, to better understand its novel concepts. The second objective was to establish what force, in terms of the prohibition on the use of force clause is, and when such force is prohibited in the light of cyber space. The third objective was to identify when cyber operations are prohibited by the prohibition on the use of force clause. The fourth objective was to establish if a state may defend itself against a cyber operation and if so, in what manner may it defend itself. The fifth objective was to establish the nature of an armed conflict. The sixth objective was to establish whether armed conflicts can be cyber related and thus be regulated by IHL. The seventh objective was to establish the applicability of the principles of IHL in cyber space.

Chapter 2 established important cyber-related terminology in order to provide a platform from which novel definitions and wording could be discussed and understood. On chapter 2.4, the difference between cyber threats, cyber-attacks and cyber operations has been discussed in the context of their proper use throughout this study. Cyberspace has been explained and interpreted as the fifth domain in which warfare is conducted together with sea, air, land and space. In chapter 2.5, the problem of attribution with relation to cyberspace has been discussed at length. The novelty of cyberspace together with the lack of borders, the inability to realise when a computer is used in a cyber-attack and the fact that an IP address is only traceable to the computer that has conducted the attack and not to the computers that captured them, make attribution in cyberspace challenging. The problem with attribution is that there is no clear-cut solution, and state practice can be the answer to this uncertainty.

In chapter 3, the prohibition of use of force clause found in article 2(4) and the exceptions found in article 51 have been discussed and examined in the light of cyber-space. Regarding the prohibition on the use of force clause, the objective was to establish what force is and whether cyber operation can be included into the definition of force. In paragraph 3.3, it was found that the dominant viewpoint is the preferred method of interpretation for purposes of article 2(4) by law practitioners and scholars. By using this method of interpretation, the literal meaning of the text behind article 2(4) is used to establish what the lawmakers envisioned. Through the lens of the dominant viewpoint interpretation of article 2(4), a note by the ICJ, in the *Nicaragua* case, was made that scale and effect of an attack rather than the weapon itself must be examined in order to establish whether the act of force is prohibited by article 2(4). In the light of the above, a conclusion is drawn that all forms of attacks can potentially rise to the magnitude of being considered force as prohibited in terms of article 2(4), which is also true for cyber-attacks. If the potential exists for a cyber-attack to rise to a level of magnitude to be considered as prohibited force, categorically, the question of when an operation reaches the level of scale and effect to be considered use of force has to be examined. The answer to this question has a comparative element to it. If the scale and effect of an operation reach the comparative level of destruction of

a kinetic attack, the operation will be prohibited in terms of article 2(4). The next objective was to identify when cyber operations are prohibited by article 2(4). In paragraph 3.5, a set of factors, developed by Schmitt, that could help in this regard was introduced and includes severity, immediacy, directiveness, invasiveness, measurability of effects, military character, state involvement and presumptive legality. Although these factors are regarded to be sufficient when considering cyber operations as use of force, it is important to keep in mind that they are not a part of international law and will not be binding until there is sufficient state practice in this regard.

In chapter 3.7, the objective was to establish whether a state may defend itself against a cyber operation and if so, in what manner may it do so. The exceptions to article 2(4), found in article 51, were examined in the light of cyber operations. The wording of this article provides states with an unqualified right to self-defence, however, in the event of an armed attack the unqualified right of states is limited to instances when an armed attack occurs or is concluded. Through Ruys's analysis of the wording found in article 51, examined through the lens of article 31(1), he found that the wording in the event of an armed attack, places a limitation to an otherwise unqualified right to self-defence. On the other hand, interpretations of article 51 view the phrase, armed attack, as a lexical term, carried over from previous legislation and that a narrow reading thereof is insufficient. The uncertainty created by the two schools of thought in this regard was made clear in ICJ's judgement on the *Nicaragua* case, in which the ICJ deliberately decided not to give judgement on the question of whether pre-emptive action is recognised under international law, however, noting the unqualified right to self-defence that states have. This is relevant for purposes of self-defence in cyberspace. The speed at which cyber operations are conducted, limits them to pre-emptive action only when the acting state practises its right to self-defence. This has the effect that an act of self-defence to repel an attack on a state may be greater than intended. There is uncertainty on how to prevent an attack without running the risk of self-defence being greater than needed to repel the attack. State practice may be the solution, however, the position currently held is that there is no state practice, and it

may only be solved in the future. With that in mind, the applicability of the use of force is guaranteed and has been proven to regulate operations in cyberspace.

In chapter 4, the first discussion regarding IHL was an analysis of its sources in order to supply a basis from which IHL as a whole can be understood. This part of the discussion provided a comprehensive background of the topics of The Hague Conventions and its regulations, the prohibition of weapons that causes unnecessary suffering, and the Law of Geneva in order to accomplish its intended purpose.

In chapter 4.3, the objective was to establish what constitutes an armed conflict and whether cyber related conflicts can be included into its definition, and thus regulated by IHL. An in-depth discussion on armed conflicts was conducted in order to comprehend the IHL applicable thereto for purposes of applying it to armed conflicts consisting a cyber-element. In this discussion it was established that the general rule regarding armed conflicts, is providing a formal declaration of war by a state entering into an armed conflict with another state albeit less applicable in modern times. The distinction between IACs and NIACs is the most effective means of establishing whether or not an act constitutes an armed conflict, which is provided for in Common Articles 2 and 3 together with the Additional Protocols. By applying the discussion of armed conflicts to cyberspace, the question of when cyber operations constitute an armed attack was asked in paragraph 4.3.3. The Appeals Chamber of the International Criminal Tribunal for the former Yugoslavia provided an answer in this regard by stating that the scale of damage and organisational formation of a group, engaged in an armed conflict, must be equal to that of a state in an armed conflict for it to be classified as such. The conclusion then is that, irrespective of whether or not a cyber-attack is accompanied with an armed kinetic attack, when the damage inflicted and organisational formation of a group conducting a cyber-attack are comparable to that of a state conducting a kinetic attack, the law of armed conflicts will be applicable.

In chapter 4.4, an in-depth analysis was conducted on the principles of IHL and its applicability in cyberspace. Distinction, military necessity, unnecessary suffering and proportionality were discussed at length and their applicability tested in cyberspace.

The objective here was to establish whether the principles of IHL is applicable in cyberspace.

The first of these four principles, discussed in paragraph 4.4.1, is the principle of distinction. Article 28 of the Geneva Conventions provides combatants with a dual obligation to firstly, distinguish between civilians and combatants, and secondly, to only target combatants. This distinction also requires combatants to distinguish between civilian and military objects. Article 44(3) of the Additional Protocols I places a further obligation on combatants to sufficiently distinguish themselves from civilians as to not cause confusion when distinction between civilians and combatants must be made. Compliance with article 44(3) is not always met and as such article 51(3) of the Additional Protocols I allows for the actions of civilians to determine their status as combatants. This is made apparent in the example given in chapter 4 out of the book, Black Hawk Down. The position remains the same regarding the applicability of the principle of distinction in cyberspace, however, distinguishing between civilians and combatants in cyberspace is near impossible, because combatants cannot make an objective decision regarding distinction on actors that cannot be seen. Only the actions of an actor in cyber space can be observed to distinguish him/her as a combatant and not a civilian. This necessitates a further general rule regarding distinction in cyberspace. All actors in cyberspace must be viewed as civilians, until their actions distinguish them as combatants. Taking into account the distinction of civilians and military objects; the position may be more complicated. Cyberspace consists of dual-use objects, as contemplated by Rule 101 of the Tallinn Manual 2.0, objects that both civilians and combatants use at any given time. The solution regarding these dual-use objects may lie in the fact that extreme care, from the side of combatants, must be taken to minimise damage to civilian objects. The solution may also lie in the fact that the inevitability of damage caused to civilian objects in armed conflicts is allowed, where the damage done is in proportion to the military objective at hand. The position that both extreme care and proportionality by combatants in armed conflicts are adhered to, must be properly upheld when distinction between civilian and military objects is made, provides for utmost objectivity in decision making and the best

protection for civilian objects in cyberspace that is currently available. The problem with dual-use objects in cyberspace is not the only obstacle that is encountered when distinguishing between civilian and military objects. There is also uncertainty on whether data can be regarded as objects in cyber space. According to the International Group of Experts who compiled the Tallinn Manual 2.0, data is intangible and thus not in line with the definition of an object. However, in Rule 92, they acknowledge that data-altering attacks that cause damage equal to that of what a kinetic attack is capable of, that cause damage to cyber infrastructure, must enjoy regulation under the law of armed conflicts. For this reason, it is assumed that, for purposes of distinction, data is seen as objects and thus enjoy protection under the law of armed conflict.

The applicability of the principle of military necessity, was discussed in paragraph 4.4.2. Military necessity can be viewed as an exception to the general rule found in article 35 of the Additional Protocols I, because it allows for death and/or injury to civilians and damage to and/or destruction of civilian objects where the intended military objective is necessary to achieve, provided that the military gains are in proportion to the death, injury, damage and/or destruction suffered in order to obtain that goal. Military necessity must furthermore strike a balance between unnecessary suffering and proportionality in order for it to be in line with the principles of IHL. Where no clarification in this regard is provided for in IHL, parties are free to act within the parameters set by customary international law. This, however, is only applicable to military necessity and as such, both *kriegsraison* and a state of necessity are excluded from the law of armed conflict and thus unacceptable. With regard to the applicability of the principle of military necessity in cyberspace, an assumption is made that this principle applies unequivocally in cyberspace. This assumption is based on the lack of literature and its application, together with the discussion on the protection of the natural environment, found in the Tallinn Manual 1.0.

In paragraph 4.4.3 a discussion on the applicability of the principle of unnecessary suffering to cyberspace was conducted. Article 35(2) of the Additional Protocols I provides for two questions in this regard. Firstly, what the nature of "…weapons,

projectiles and material and methods of warfare…" entails, and secondly, to what extent suffering must be endured for it to become unnecessary. Weapons that cause unnecessary suffering, are prohibited by the Conventional Weapons Convention, together with article 23(e) of the 1907 Hague Regulations. Furthermore, an obligation is placed on states, employing and/or creating weaponry by article 36 to test weaponry against the requirements as set out in the Additional Protocols. The Advisory Opinion on the Legality of the Threat of Use of Nuclear Weapons sets out the test the states must conduct in this regard. In terms of the test, unnecessary suffering must be viewed on a pendulum, where suffering and the intended goal are weighed against one another. Where suffering is greater than necessary to achieve the intended goal, it will be unnecessary. In the light of cyber-attacks, the greatest challenge to overcome, is indiscriminate attacks. Due to the dual-use object nature of cyberspace, precision-targeted attacks have the potential to cause indiscriminate suffering. A possible solution hereto is altering cyber weapons to exclude their potential to cause indiscriminate attacks, however, such alteration has as of yet not been accomplished. Only continuous testing in terms of article 36 of the Additional Protocols together with state practice, may provide a solution hereto, whilst the justification of indiscriminate attacks in cyberspace can find applicability through the principle of proportionality.

In paragraph 4.4.4, the element of proportionality was discussed and applied to cyberspace. It was found that article 51.5(b) places a protective element on civilians and civilian objects by declaring that an attack that may cause injury or death to civilians and/or damage to civilian objects, is "excessive" when compared against the perceived military necessity. Precaution on the side of the combatant is provided by article 57.2(b) to suspend attacks out of military necessity where the perceived injury, death, damage to and/or destruction of civilians and/or civilian objects are excessive. By combining articles 51.5(b) and 57.2(b) the definition of proportionality is ascertained. Excessive in this context, according to the commentary on the Additional Protocols, paragraph 1979 of 1977, entails that injury, death, damage to, and/or destruction of civilians and/or civilian objects are disproportionate to the military advantages gained. According to paragraph 1978, combatants must act in good faith,

with the best interest of the civilian population in mind. Combatants must accordingly make sound objective decisions on the information available to them for the principle of proportionality to be met. This is in line with Rules 114 to 120 of the Tallinn Manual 2.0 that implies that objective decision making on the side of combatants is relied upon with regard to the principle of proportionality in cyberspace.

Throughout this study, the view of IHL through the lens of cyberspace became clear. The uncertainty of whether cyber warfare is regulated by contemporary IHL is apparent, but without a doubt regulation of cyber warfare is guaranteed in contemporary IHL. The scope of application is also, to a great extent guaranteed, however, some irregularities do exist, such as the question of attribution, the uncertainty of the applicability of pre-emptive action and the problem with the indiscriminate nature of attacks conducted in cyberspace. However, these uncertainties have existed long before the problem statement of this study became relevant. Cyber warfare's entry into the regulatory sphere of IHL merely emphasised the need for proper regulation on long standing uncertainties. Proper state practice on these questions may be the solution, and future studies on the scope of applicability of cyber warfare by contemporary IHL may provide solutions to these uncertainties. The future of this study may be found in the proper utility of the Tallinn Manuals by legislators of domestic law in order to establish proper legal recourse on a local level with respect to cyber warfare. Further study on the need to recognise pre-emptive action as a form of self-defence against cyber-attacks, without the retaliating defensive attack being greater than needed to repel it, may have the outcome that a state’s unequivocal right to self-defence may be guaranteed. This study was timely and significant because it established that regulation of cyber warfare by contemporary IHL is guaranteed, and the current scope of application in this regard has been set. In the words of Kittichaisaree, "To state the obvious, the law of armed conflict applies whenever there is an armed conflict."

Bibliography

Literature

Anon *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*

Anon *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge 2017)

Aquinas *Summa Theologica*

Aquinas St. T *Summa Theologica* (Christian Classics Westminster 1981)

Bowden *Black Hawk Down*

Bowden M *Black Hawk Down: A Story of Modern War* 2nd ed (Grove Press New York 2010)

Bowett *The Law of International Institutions*

Bowett DW *The Law of International Institutions* (Stevens London 1963)

Buchan *Cyber Espionage and International Law*

Buchan R *Cyber Espionage and International Law* (Hart Oxford 2019)

Corn 1998 *The Army Lawyer*

Corn MGS "International and Operational Law Note, Principle 2: Distinction" 1998 *The Army Lawyer* 73

Dever and Dever 2013 *Journal of Law and Cyber Warfare*

Dever J and Dever J "Cyberwarfare attribution, preemption, and national self defense" 2013 *Journal of Law and Cyber Warfare* 25-63

Dinstein *War, Aggression and Self-Defence*

Dinstein Y *War, Aggression and Self-Defence* 3rd ed (Cambridge University Press Cambridge 2001)

Dörr 2012 *Max Planck Encyclopaedia of Public International Law*

Dörr O "Use of Force, Prohibition of" 2012 *Max Planck Encyclopaedia of Public International Law* Vol X 611

Dugard *et al International Law*

Dugard J *et al International Law: A South African Perspective* 5th ed (Juta Cape Town 2019)

Fildes *BBC News*

Fildes J "Stuxnet worm 'targeted high-value Iranian assets'" *BBC News* (23 September 2010)

Galbán, Rodrigues and Fernández 2009 *Review of Medical Humanities*

Galbán LYP, Rodrigues LC and Fernández MM "Essential concepts and characteristics of present-day psychological warfare" 2009 *Review of Medical Humanities* 1-22

Green *Essays on the Modern Law of War*

Green LC *Essays on the Modern Law of War* 2nd ed (Nijhoff Brill 1998)

Gross 1948 *The American Journal of International Law*

Gross L "The Peace of Westphalia 1648-1948" 1948 *The American Journal of International Law* 20-41

Gutiérrez Posse 2006 *International Review of the Red Cross*

Gutiérrez Posse HDT "The relationship between international humanitarian law and the international criminal tribunals" 2006 *International Review of the Red Cross* 65-86

Henckaerts and Doswald-Beck *Customary International Humanitarian Law*

Henckaerts JM and Doswald-Beck L *Customary International Humanitarian Law* (Cambridge University Press Cambridge 2009)

ICRC *Commentary on the First Geneva Convention*

ICRC *Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field* 2nd ed (Cambridge University Press Cambridge 2016) available at https://www.cambridge.org/core/books/commentary-on-the-first-geneva-convention/4C3F3D571C1F6DB5E88004AF7540665C

Kittichaisaree *Public International Law of Cyberspace*

Kittichaisaree K *Public International Law of Cyberspace* (Springer Cham 2017)

Kittichaisaree *Public International Law of Cyberspace*

Kittichaisaree K *Public International Law of Cyberspace* (Springer Cham 2017)

Lehto 2020 *Non-kinetic Warfare- The new game changer in the battle space*

Letho M *Non-kinetic Warfare- The new game changer in the battle space in the Cyber Warfare and Security Conference* (12-13 March 2020 Norfolk, Virginia, Old Dominion University, USA) 316-325

Libicki "Correlations between cyberspace attacks and kinetic attacks"

Libicki MC "Correlations between cyberspace attacks and kinetic attacks" Paper delivered at the *12th International Conference on Cyber Conflict* (CyCon) (26-29 May 2020 Estonia) 199-213

McGriffert 1909 *Harvard Theological Rev*

McGriffert AC "The influence of Christianity upon the Roman Empire" 1909 *The Harvard Theological Review* 28-49

Morgan *The German War Book*

Morgan JH *The German War Book* (John Murray London 1915)

Neff *War and the Law of Nations*

Neff SC *War and the Law of Nations: A general History* (Cambridge University Press Cambridge 2005)

Nussbaum 1952 *University of Pennsylvania LR*

Nussbaum A "The significance of Roman Law in the history of International Law" 1952 *University of Pennsylvania Law Review* 678-687

Pictet (ed) *Commentary, IV Geneva Convention*

Pictet JS (ed) *Commentary, IV Geneva Convention:* Relative to the Protection of Civilian Persons in Time of War (ICRC Geneva 1958)

Randelzhofer "Article 51"

Randelzhofer A "Article 51" in Simma B *et al* (eds) *The Charter of the United Nations: A Commentary* (Oxford University Press Oxford 2021) 788-806

Ridgley 1997 *The British Library Journal*

Ridgley G "The Covenant of the League of Nations" 1997 *The British Library Journal* 41-46

Roscini *Cyber Operations*

Roscini M *Cyber Operations and the use of force in International Law* (Oxford University Press Oxford 2014)

Ruys *'Armed Attacks' and Article 51 of the UN Charter*

Ruys T *'Armed Attacks' and Article 51 of the UN Charter: Evolutions in Customary Law and Practice* (Cambridge University Press Cambridge 2010)

Sassòli *International Humanitarian Law*

Sassòli M *International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare* (Edward Elgar Cheltenham 2019)

Schmitt *Tallinn Manual on the International Law*

Schmitt MN *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press Cambridge 2013)

Schmitt *Tallinn Manual 2.0 on the International Law*

Schmitt MN *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press Cambridge 2017)

Shakarian 2011 *Military Review*

Shakarian P "The 2008 Russian cyber-campaign against Georgia" 2011 *Military Review* 63-68 available at https://www.questia.com

Singer and Friedman *Cybersecurity and Cyberwar*

Singer PW and Friedman A *Cybersecurity and Cyberwar: What everyone needs to know* (Oxford University Press Oxford 2014)

Solis *The Law of Armed Conflict*

Solis GD *The Law of Armed Conflict: International Humanitarian Law in War* 2nd ed (Cambridge University Press Cambridge 2020)

Speier 1941 *American Journal of Sociology*

Speier H "The social types of war" 1941 *American Journal of Sociology* 445-454

Von Elbe 1939 *American Journal of International Law*

Von Elbe J "The Evolution of the concept of Just War in international law" 1939 *The American Journal of International Law* 665-688

Waxman 2011 *Int'l L Stud*

Waxman MC "Cyber-attacks as 'force' under UN Charter article 2(4)" 2011 *International Law Studies* 43-57 available at https://scholarship.law.columbia.edu/faculty_scholarship/847

Wolf "Cyber-Physical Systems"

Wolf M "Cyber-Physical Systems" in Wolf M (ed) *High-Performance Embedded Computing: Architectures, Applications, and Methodologies* 2nd ed (Morgan Kaufmann Publishers 2014) 391-413

Case law

S.S. 'Lotus', France v Turkey, Judgement, 1927

Prosecutor v Tadic Case no IT-94-1-A

The Republic of Nicaragua v The United States of America, 1986

Legislation

Computer Fraud and Abuse Act, 1986

International instruments

Additional Protocols I to the Geneva Conventions, 1949

Chapter VII: Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression Charter of the United Nations (2001)

Charter of the United Nations (24 October 1945)

Convention I and II of the Geneva Conventions, 1949

Convention III of the Geneva Conventions, 1949

Convention IV of the Geneva Conventions, 1949

Foreign Relations of the United States, Diplomatic Papers (1945)

General Treaty for Renunciation of War, 1928

Protocol I and II Additional to the Geneva Conventions of 12 August 1949 (1977)

Resolution 59 of the UN General Assembly (1946)

Security Council Resolution 1368 (12 September 2001)

Security Council Resolution 1373 (28 September 2001)

The Hague Regulations, 1907

Threats to international peace and security caused by terrorist acts (2001)

Universal Declaration of Human Rights (1948)

Internet sources

Anon 2017 https://e-estonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/

Anon 2017 "How Estonia became a global heavyweight in cyber security" https://e-estonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/ accessed 19 June 2021

Baker and Hamilton 2000 https://fas.org/sgp/library/bakerham.html

Baker HH and Hamilton LH 2000 *Science and Security in the Service of the Nation: A review of the security incident involving classified hard drives at Los Alamos National Laboratory* https://fas.org/sgp/library/bakerham.html accessed 21 June 2021

Britannica, The Editors of Encyclopaedia 2016 https://www.britannica.com/topic/fetial

Britannica, The Editors of Encyclopaedia 2016 *"Fetial" Encyclopaedia Britannica* https://www.britannica.com/topic/fetial accessed 21 June 2021

Britannica, The Editors of Encyclopaedia 2018 https://www.britannica.com/technology/trojan-computing

Britannica, The Editors of Encyclopaedia 2018 *"Trojan" Encyclopedia Britannica* https://www.britannica.com/technology/trojan-computing accessed 29 November 2021

Britannica, The Editors of Encyclopaedia 2020 https://www.britannica.com/topic/League-of-Nations

Britannica, The Editors of Encyclopaedia 2020 *"League of Nations" Encyclopedia Britannica* https://www.britannica.com/topic/League-of-Nations accessed 22 June 2021

Britannica, The Editors of Encyclopaedia 2021 https://www.britannica.com/event/Peace-of-Westphalia

Britannica, The Editors of Encyclopaedia 2021 *"Peace of Westphalia" Encyclopedia Britannica* https://www.britannica.com/event/Peace-of-Westphalia accessed 29 November 2021

Cartwright date unknown https://info.publicintelligence.net/DoD-JointCyberTerms.pdf

Cartwright JE date unknown *Joint Terminology for Cyberspace Operations* (Department of Defence Washington DC) https://info.publicintelligence.net/DoD-JointCyberTerms.pdf accessed 21 June 2021

Chadd 2020 https://blog.avast.com/history-of-cybersecurity-avast

Chadd K 2020 *The history of cybersecurity* https://blog.avast.com/history-of-cybersecurity-avast accessed 24 July 2021

Chan 2018 https://www.bloomberg.com/quicktake/great-firewall-of-china

Chan E "The Great Fire Wall of China" *Bloomberg News* (6 November 2018) https://www.bloomberg.com/quicktake/great-firewall-of-china accessed 24 July 2021

Featherly 2021 https://www.britannica.com/topic/ARPANET

Featherly K 2021 *ARPANET* (*Advanced Research Projects Agency Network*): *United States Defense Program Britannica* https://www.britannica.com/topic/ARPANET accessed 17 July 2021

Fox 2019 https://www.securitypursuit.com/blog-posts/history-matters-cyber-attacks-from-the-1960s

Fox S 2019 *History matters: cyber-attacks from the 1960s* https://www.securitypursuit.com/blog-posts/history-matters-cyber-attacks-from-the-1960s accessed 18 July 2021

Grossman 2009 http://content.time.com/time/world/article/0,8599,1905125,00.html

Grossman L 2009 *Iran protests: Twitter, the medium of the movement* http://content.time.com/time/world/article/0,8599,1905125,00.html accessed 27 May 2020

Hesseldahl 2015 https://www.vox.com/2015/3/26/11560712/why-kevin-mitnick-the-worlds-most-notorious-hacker-is-still-breaking

Hesseldahl A 2015 *Why Kevin Mitnick, the world's most notorious hacker, is still breaking into computers* https://www.vox.com/2015/3/26/11560712/why-kevin-mitnick-the-worlds-most-notorious-hacker-is-still-breaking accessed 17 July 2021

History.com Editors 2020 https://www.history.com/this-day-in-history/britain-and-france-declare-war-on-germany

History.com Editors 2020 *Britain and France declare war on Germany* (5 November 2009) https://www.history.com/this-day-in-history/britain-and-france-declare-war-on-germany accessed 29 November 2021

IJRC date unknown https://ijrcenter.org/international-humanitarian-law/

International Justice Resource Center (IJRC) date unknown *International Humanitarian Law (IHL)* https://ijrcenter.org/international-humanitarian-law/ accessed 18 June 2020

ICRC 1998 https://www.icrc.org/en/doc/resources/documents/misc/57jnvr.htm

ICRC 1998 *The battle of Solferino* (24 June 1895) https://www.icrc.org/en/doc/resources/documents/misc/57jnvr.htm accessed 29 November 2021

IJRC 2015 https://www.icrc.org/en/document/international-humanitarian-law-and-challenges-contemporary-armed-conflicts

IJRC 2015 *International humanitarian law and the challenges of contemporary armed conflicts* https://www.icrc.org/en/document/international-humanitarian-law-and-challenges-contemporary-armed-conflicts accessed 29

ICRC 2016 https://www.icrc.org/en/document/history-icrc

ICRC 2016 *History of the ICRC* (29 October) https://www.icrc.org/en/document/history-icrc accessed 16 October 2021

Lasar 2011 https://www.wired.com/2011/09/att-conquered-20th-century/

Lasar M 2011 *How AT&T Conquered the 21st Century Wired* https://www.wired.com/2011/09/att-conquered-20th-century/ accessed 9 October 2021

NATO 2021 https://ccdcoe.org/news/2021/the-ccdcoe-invites-experts-to-contribute-to-the-tallinn-manual-3-0/

NATO Cooperative Cyber Defence Centre of Excellence 2021 *Tallinn Manual The CCDCOE Invites Experts to Contribute to the Tallinn Manual 3.0* https://ccdcoe.org/news/2021/the-ccdcoe-invites-experts-to-contribute-to-the-tallinn-manual-3-0/ accessed 18 July 2021

NATO 2014 https://www.nato.int/cps/en/natohq/official_texts_112964.htm

North Atlantic Treaty Organization (NATO) 2014 *Wales Summit Declaration* (5 September 2014) https://www.nato.int/cps/en/natohq/official_texts_112964.htm accessed 18 July 2021

NATO 2021 https://ccdcoe.org/

NATO 2021 Cooperative Cyber Defence Centre of Excellence https://ccdcoe.org/ accessed 17 July 2021

NACDL 1986 https://www.nacdl.org/Landing/ComputerFraudandAbuseAct

National Association of Criminal Defence Lawyers (NACDL) 1986 *Computer Fraud and Abuse Act*, *1986* (CFAA) https://www.nacdl.org/Landing/ComputerFraudandAbuseAct accessed 17 July 2021

Nichols 2021 https://www.reuters.com/world/asia-pacific/exclusive-taliban-names-afghan-un-envoy-asks-speak-world-leaders-2021-09-21/

Nichols M 2021 *Exclusive: Taliban names Afghan U.N. envoy, asks to speak to world leaders* Reuters (21 September) https://www.reuters.com/world/asia-pacific/exclusive-taliban-names-afghan-un-envoy-asks-speak-world-leaders-2021-09-21/ accessed 6 November 2021

Norman 2021 https://www.historyofinformation.com/detail.php?entryid=2860

Norman JM 2021 *History of Information* https://www.historyofinformation.com/detail.php?entryid=2860 accessed 17 July 2021

Perlroth, Scott and Frenkel 2017 https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html#

Perlroth N, Scott M and Frenkel S 2017 *Cyberattack hits Ukraine then spreads internationally* https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html# accessed 05 June 2020

Rowen B 2017 https://www.infoplease.com/world/cyberwar-timeline.

Rowen B 2017 The roots of this increasingly menacing challenge facing nations and businesses Infoplease https://www.infoplease.com/world/cyberwar-timeline accessed 05 December 2021.

Tamkin 2017 https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/

Tamkin E 2017 *10 Years after the landmark attack on Estonia, is the world better prepared for cyber threats?* https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/ accessed 02 June 2020

UN date unknown https://www.un.org/en/sections/un-charter/un-charter-full-text/

United Nations (UN) date unknown *UN Charter* https://www.un.org/en/sections/un-charter/un-charter-full-text/ accessed 07 April 2020

UN 1945 https://www.un.org/en/about-us/un-charter/full-text

United Nations (UN) 1945 *Charter of the United Nations* (24 October) https://www.un.org/en/about-us/un-charter/full-text accessed 27 June 2021