MASTER'S THESIS IN INTERNATIONAL LAW AND HUMAN RIGHTS

Patrick Schubert

PROTECTION OF CIVILIAN DATA FROM CYBER ATTACKS IN ARMED CONFLICTS

Master´s Thesis in Public International Law
Master´s Programme in International Law and Human Rights
Supervisor: Mikaela Heikkilä
Åbo Akademi University 2022

ÅBO AKADEMI – FACULTY OF SOCIAL SCIENCES, BUSINESS AND ECONOMICS

Abstract for Master´s Thesis

Subject: Public International Law, Master´s Degree Programme in International Human Rights Law	
Author: Patrick Schubert	
Title of the Thesis: PROTECTION OF CIVILIAN DATA FROM CYBER ATTACKS IN ARMED CONFLICTS	
Supevisor: Mikaela Heikkilä	

Cyber operations targeting civilian data can in a present-day context operate in somewhat of a grey area. Because of this, states and non-state groups can attack civilian data during an armed conflict without consequens in most cases, which can rapidly cause more harm to the civilian population than the destruction of physical civilian objects. Since states have in many cases been reluctant to share their views on how international humanitarian law applies to the case of data as a civilian object, this thesis sets out to clarify whether data is protected from attack during an armed conflict.

The general protection of civilians and civilian objects seams to be unfit to deal with the notion of computer data being digital in nature, as opposed to material. It is therefore only in very specific contexts that civilian computer data will be protected from cyber operation, due to the consequences of the operation qualifying it as an attack. International humanitarian law, however, affords special protection to certain objects, persons and activities. Since these protections are in most cases applied in an overreaching manner some civilian data, falling witing the grasps of special protection, can be protected from attack.

Key words: Cyberspace, cyber attack, cyber operation, ICTs, civilian data, data, object, IHL, Tallinn manual 2.0, Special protection,

Date: 07.04.2022	Number of pages: 81 Number of words (excl. bibliography and annexes: 27339

The abstract is approved as a maturity test:

List of abbreviations

ICC	International Criminal Court
ICJ	International Court of Justice
ICRC	International Committee of the Red Cross
ICTY	International Crimes Tribunal of the former Yugoslavia
ICT	Information and Communication Technology
OED	Oxford English Dictionary
SCADA	Supervisory Control and Data Acquisition
UN	United Nations

Table of Contents

1. Introduction 1
1.1. Background 1
1.2. Research questions and structure 4
1.3. Method, sources and limitations 5
2. Technical and legal aspects related to cyberspace 11
2.1 Concepts and terminology 11
2.2 The Cyberspace 12
2.3 Data defined 15
2.4 The reach of international humanitarian law in cyberspace 16
2.5 Military operation and attacks in cyberspace 20
3. Data as an object of international humanitarian law 25
3.1 Civilian objects and military objectives 25
3.2 The qualifications of military objectives 28
3.3. Data in light of the definition of military objectives and civilian objects 33
3.3.1. Data as an object 33
3.3.2. The 'object' requirement 34
3.3.3. Interpretation and International Customary Law 36
3.3.4. State practice 39
3.3.5. Conclusions: Data an object? 45
4. Civilian data protected from attack through possible special protection 48
4.1. Special protection of international humanitarian law 48
4.2. Special protection afforded to medical personnel, objects and activities 48
4.3. Objects indispensable to the survival of the civilian population 51
4.4. Works and installations containing dangerous forces 53

4.5. Cultural property 54
4.6. The natural environment 56
4.7. Humanitarian relief operations 58
4.8. Journalists 59
4.9. Conclusion: The special protection of data 61
5. Conclusion 64
Bibliography 68

1. Introduction

1.1. Background

With the development of technology most societies have become thoroughly digitalized and therefore highly dependent on the access of data when conducting their day-to-day activities. Many everyday services access our personal information in the form of computer data even when accomplishing the most simple tasks, such as paying with a credit card, visiting a medical service or using electricity or water from the electrical grid or the water supply.[1] At the same time, the technological development has made states, non-state groups and international organizations both more dependent on constant access to data as well as more susceptible to cyber attacks through the use of cyberspace. This development has in turn resulted in states developing cyber military capabilities of their own both for defensive and offensive purposes. Among others the United States, the United Kingdom and Australia have publicly revealed that they have used cyber means and methods of warfare in the fight against the Islamic State.[2] The use of cyber operations during armed conflicts is already a reality and cyber operations will probably become an even more prominent part of the battlefield in the future.[3]

In the recent decades, cyber operations have been conducted as part of the military action in the Russian-Georgian war of 2008 as well as in the conflict between Russia and Ukraine since 2014.[4] More recently, in 2022 the tension between Russia and Ukraine has developed into a full scale invasion of Ukraine by Russian military forces, which have been followed by a constant onslaught of cyber attacks against the Ukrainian government.[5] Similarly, in the Russian-Georgian war of 2008 the alleged Russian cyber

---

[1] Tim Mc Cormack 'International Humanitarian Law and the Targeting of Data' (2018) 94 INT'L L. STUD. 222 p. 223.
[2] Fleming, 'Director's Speech at Cyber UK18' GCHQ (12 April 2018) p. 1-6; Burgess 'Offensive Cyber and the People Who Do It' Australian Signals Directorate, speech given to the Lowy Institute (27 March 2019); Paul M. Nakasone, 'Statement of General Paul M. Nakasone, Commander, United States Cyber Command, before the Senate Committee on Armed Services' (14 February 2019).
[3] Gisel, Rodenhäuser and Dörmann, 'Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts' (2020) 913 International Review of the Red Cross 287 p. 288.
[4] Schmitt MN, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2ed Cambridge University Press 2017) rule 80, para 3.
[5] Alaz ab Mamoun 'Russia is using an onslaught of cyber attacks to undermine Ukraine's defence capabilities' (theconversation, 24 February 2022) <https://theconversation.com/russia-is-using-an-

operations against Georgia took down the country's websites and crippled communications of the Georgian government affecting civilians nationwide. In addition, these attacks were used to access and gather computer data from Georgian servers.[6]

While it is clear that international humanitarian law is applicable to cyber operations in these cases because of ongoing armed conflicts, it is still uncertain how international humanitarian law applies to cyber operations targeting civilian computer data.[7] Among other these uncertainties are reflective of how the principles of international humanitarian law apply to military action conducted through cyberspace, which have especially been observed at the political level in the UN Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security.[8] In the Open-ended working group, States where unable to codify anything conclusive, concluding that there are "questions relevant to how the principles of international humanitarian law, such as principles of humanity, necessity, proportionality, distinction and precaution, apply to ICT operations…. States noted that further study was required on these important topics in future discussions."[9]

The International Committee of the Red Cross (ICRC) has already in 2015 stated in its report on International humanitarian law and the challenges of contemporary armed conflicts, that the destruction or manipulation of civilian data could rapidly cause more harm to the civilian population than the destruction of physical civilian objects.[10] Attacks on civilian objects are prohibited according to the Articles of Chapter IV of Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (hereinafter Additional Protocol I) and

---

onslaught-of-cyber-attacks-to-undermine-ukraines-defence-capabilities-177638> accessed 1.3.2022; Tidy Joe 'Ukraine crisis: 'Wiper' discovered in latest cyber-attacks' (BBC, 25 February 2022) <https://www.bbc.com/news/technology-60500618> accessed 1.3.2022.

[6] David Hollis 'Cyberwar Case Study: Georgia 2008' (2010) Small War Journal, p. 1-4.

[7] *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, ICJ GL No 95, [1996] ICJ Rep 22 para 86; Tallinn Manual 2.0 (n 4) rule 80, para 3.

[8] Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security 'Chair's Summary' (10 March 2021) UN doc A/AC.290/2021/CRP.3 para. 8, 19.

[9] *Ibid* para. 18.

[10] International Committee of The Red Cross, 'International humanitarian law and the challenges of contemporary armed conflicts' (2015) 32IC/15/11, p. 43.

according to Customary International Humanitarian Law in both international and non-international armed conflicts.[11]

However, with regards to data, soft law instruments such as the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (hereinafter Tallinn Manual 2.0) has stated that the notion of objects according to customary international humanitarian law does not include data. Followingly, civilian data would fall outside of the principle of distinction and not be afforded the protection that is commonly related to civilian objects.[12] For the most part states have been reluctant to issue statements regarding the protection of data, probably since it would clearly restrict the conduct of legitimate cyber operations. However, if data was considered an object of international humanitarian law, states would have to distinguish between military and civilian targets in addition to factoring in the damage caused to civilian data in the proportionality calculations of an attack.[13]

The ICRC considers that because our societies are essentially dependent on data, the conclusion to not distinguish between different types of data, between civilian and military, would be inconsistent with the object and purpose of the norms of customary international humanitarian law.[14] The ICRC argues that civilian data such as "medical data, biometric data, social security data, tax records, bank accounts, companies' client files or election lists and records" are essential for the functioning of modern society.[15] Therefore, if data does not constitute an object of international humanitarian law, the destruction or manipulation of civilian data would not be prohibited by the principles of international humanitarian law. Thereby making data a legitimate target of military action, which could be attacked because it does not amount to an object that would engage

[11] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Protocol I) art. 48, 51-56; Jean-Marie Henckaerts, Louise Doswald-Beck and ICRC 'Customary International Humanitarian Law, Volume 1: rules' (Cambridge University Press, 2005) rule 7.
[12] Tallinn Manual 2.0 (n 4) rule 100 commentary para. 3-4.
[13] Michael N. Schmitt 'Wired warfare 3.0: Protecting the civilian population during cyber operations' (2019) 101 International Review of the Red Cross 333 p. 353.
[14] International humanitarian law and the challenges of contemporary armed conflicts (n 10) p. 43.
[15] International humanitarian law and the challenges of contemporary armed conflicts (n 10) p. 43.

the prohibition of attacks on civilian objects.[16] The exclusion of civilian data as a civilian object is to be regarded as a severe protection gap within international humanitarian law that can result in exploiting civilians during armed conflict. States could, for instance, execute military operations with the aim of gathering personal information of civilians that are stored in cyberspace because military operations against civilian data would not be prohibited.[17] According to the ICRC the "the replacement of paper files and documents with digital files in the form of data should not decrease the protection that IHL affords to them."[18]

1.2. Research questions and structure

This thesis sets out to explore the current *lex lata* of international humanitarian law with the aim to clarify the issues related to the protection of civilian computer data in armed conflicts. Interpreting the rules of international humanitarian law in relation to computer data has never been a more topical issue. Especially, considering the statement of the ICRC in 2019 in the International Humanitarian Law and the Challenges of Contemporary Armed Conflicts – Recommitting To Protection In Armed Conflict On The 70th Anniversary Of The Geneva Conventions rapport considering that: "data have become an essential component of the digital domain and a cornerstone of life in many societies".[19] Additionally, the ICRC considers that the destruction or manipulation of civilian data could rapidly cause more harm to the civilian population than the destruction of physical civilian objects.[20] The topic of this thesis will be studied in light of the following research question and the underlying sub questions:

1. *Does international humanitarian law afford protection of civilian data from military action, in the context of an armed conflict?*

---

[16] International humanitarian law and the challenges of contemporary armed conflicts (n 10) p. 43; International Committee of the Red Cross 'INTERNATIONAL HUMANITARIAN LAW AND THE CHALLENGES OF CONTEMPORARY ARMED CONFLICTS - Recommitting To Protection In Armed Conflict On The 70th Anniversary Of The Geneva Conventions' (2019) p. 28.
[17] International humanitarian law and the challenges of contemporary armed conflicts (n 10) p. 43.
[18] International humanitarian law and the challenges of contemporary armed conflicts - recommitting to protection in armed conflict on the 70th anniversary of the geneva conventions (n 16) p. 28.
[19] International humanitarian law and the challenges of contemporary armed conflicts - recommitting to protection in armed conflict on the 70th anniversary of the geneva conventions (n 16) p. 28.
[20] International humanitarian law and the challenges of contemporary armed conflicts (n 10) p. 43.

a. *Does data fall within the definition of a civilian object as considered by customary international law and Article 52 of Additional Protocol I?*
b. *In what cases, if any, is civilian data protected from military action pursuant to special protection regimes of international humanitarian law?*

The reason for examining the research questions in the following order is that the question of, whether data qualifies as an object or not, is central for the thesis as a whole. Additionally, the second sub-question as well as the main research question can only be fully examined, after concluding the current state of the law, *lex lata*, in relation to data as an object of customary international humanitarian law. After the quality of data has been established the thesis will answer the second sub-questions, which ultimately works in tandem with the first, in answering the research question in its entirety.

The thesis is divided into four main chapters. After the introduction, *Chapter 2* seeks to explain the difficult circumstances and terminology following the conduct of armed conflict in cyberspace. Followingly, C*hapter 3* will seek to establish whether civilian computer data do constitute a civilian object, *lex lata,* in international customary law treaty law. After the position of data in relation to international humanitarian law, *lex lata,* is confirmed, *Chapter 4* will further dive into the protection of civilian computer data and examine whether computer data can be protected from military action despite data falling outside/inside the scope of a civilian object. Since different special protection regimes are common in international humanitarian law it would be useful to clarify whether and when they extend to civilian computer data. Finally, in *Chapter 5* the author makes concluding remarks as to the practical nature of protection related to civilian computer data and the specific cases in which protection of data could be afforded as well as discusses the implications of the current *lex lata*.

1.3. Method, sources and limitations

This thesis will be performed on the basis of the legal dogmatic method. The legal dogmatic method can be described as: "research that aims to give a systematic exposition of the principles, rules and concepts governing a particular legal field or institution and analyses the relationship between these principles, rules and concepts with a view to

solving unclarities and gaps in the existing law."[21] Smits, recognizes three key characteristics for a legal dogmatic research approach. First and foremost, an internal perspective is characteristic for the dogmatic method, meaning that the author places themselves inside the legal system, analyzing the legal system itself.[22] Secondly, it is important that the research recognizes the law as a system. This second aspect thereby requires that all appropriate elements of the law are "fitted together into one working whole, resolving internal inconsistencies among seemingly contradictory materials."[23]

Lastly, the third characteristic is that a dogmatic research method systematizes present applicable law, *lex lata*.[24] *Lex lata,* being considered as "[t]he positive law currently in force, without modification to account for any rules subjectively preferred by the interpreter."[25] Considering the above mentioned characteristics of the legal dogmatic approach, this thesis will examine the research question against the sources of international law, as set forth by Article 38 (1) of the Statute of the International Court of Justice (ICJ) as:

> a) international conventions, whether general or particular, establishing rules expressly recognized by the contesting states;
> b) international custom, as evidence of a general practice accepted as law;
> c) the general principles of law recognized by civilized nations;
> d) judicial decisions and the teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law[26]

In answering the research question the author will review relevant conventions related to the *jus in bello* such as the 1949 Geneva Conventions as well as their additional

---

[21] Jan M. Smits 'WHAT IS LEGAL DOCTRINE? ON THE AIMS AND METHODS OF LEGAL-DOGMATIC RESEARCH' (2015) Maastricht European Private Law Institute Working Paper No. 2015/06 p. 5.
[22] Smits (n 21) p. 5.
[23] Smits (n 21) 6.
[24] Smits (n 21) 6.
[25] Aaron X. Fellmeth and Maurice Horwitz *Guide to Latin in International Law* (2009) Oxford University Press USA OSO, p. 167.
[26] United Nations, Statute of the International Court of Justice, 24 October 1945, 33 UNTS 993, art. 38(1).

protocols.[27] When interpreting treaty law, the author will primarily turn to generally agreed upon rules for treaty interpretation as those enshrined in the Vienna Convention on the Law of Treaties (hereinafter VCLT).[28] In addition, the author will whenever possibly refer to state praxis and position papers which might suggest emerging custom or state practice, to further the arguments made elsewhere in this thesis.

Following the sources of international law as considered by the ICJ, customary international law constitutes that of Article 38(1)(b) of the Statute of the International Court of Justice and is considered as "general practice accepted as law."[29] In more detail, it is considered that customary international law requires two elements to emerge, state practice and *opinio juris sive necessitatis*. As stated by the ICJ in the *Continental Shelf case*: "It is of course axiomatic that the material of customary international law is to be looked for primarily in the actual practice and opinio juris of States."[30]

State practice can consist of both physical and verbal acts of states as well as practice of executive, legislative and judicial organs of a state.[31] In addition, states have to act in accordance with their practice, for practice to be general as if it "occurred in such a way as to show a general recognition that a rule of law or legal obligation is involved."[32] In the customary international humanitarian law study by the ICRC, state military manuals

[27] Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (adopted 12 August 1949, entered into force 05 October 1950) 75 UNTS 31 (First Geneva Convention); Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (adopted 12 August 1949, entered into force 05 October 1950) 75 UNTS 85 (Second Geneva Convention); Geneva Convention Relative to the Treatment of Prisoners of War (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 135 (Third Geneva Convention); Geneva Convention Relative to the Protection of Civilian Persons in Time of War (adopted 12 August 1949, entered into force 05 October 1950) 75 UNTS 287 (Fourth Geneva Convention); Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Additional Protocol I); Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 609 (Additional Protocol II).
[28] Vienna Convention on the Law of Treaties (adopted 23 May 1969, entered into force 27 January 1980) 1155 UNTS 331.
[29] Statute of the International Court of Justice (n 26) art. 38(1)(b).
[30] International Court of Justice, *Continental Shelf case* (Libyan Arab Jamahiriya v. Malta) (Judgment) [1985], ICJ Reports 1985 para 27.
[31] ICRC Customary International Humanitarian Law Rules (n 11) p. xxxviii-xl.
[32] North Sea Continental Shelf cases (Federal Republic of Germany v Netherlands and Denmark) Judgment [1969] ICJ Rep 3 para 74.

were considered as verbal acts of state practice.[33] However, following the developments of international law as applicable to cyberspace, numerous states have issued public state position papers, voicing their view on the matter of how international law applies to acts in and throughout cyberspace. Therefore, this thesis uses state position papers and official statements of states as evidence of state practice in relation to the applicability of international law in cyberspace during armed conflicts.

Opinio juris is seen as the fact that practice of states is considered to be reflective of a legal conviction. The conviction has to be accepted or supported, or at least not objected to, by the international community in large. For customary international law to emerge there is a requirement for *opinio juris communis.*[34] The verbal accounts of states can count as both state practice as well as be reflective of a legal conviction of the state,[35] which is why state positions can be used to argue that an element of *opinio juris has* emerged. For a norm of customary international law to crystalize the ICJ considered in the *North Sea Continental Shelf case* that:

"State practice, including that of States whose interests are specially affected, should have been both extensive and virtually uniform in the sense of the provision invoked; -and should moreover have occurred in such a way as to show a general recognition that a rule of law or legal obligation is involved."[36]

The Rome Statute of the International Criminal Court (ICC) will be used in this thesis to further the argument that some international norms are indeed customary. This is primarily done due to the unique relationship between international criminal law and that of some rules of customary international humanitarian law. Additionally, with 123 ratifications, the Statute and its contents are widely ratified by states.[37]

---

[33]ICRC Customary International Humanitarian Law Rules (n 11) p. xxxviii-xl.
[34] Per Sevastik, Katrin Nyman-Metcalf, Sia Spiliopoulou Åkermark, Olle Mårsäter *En bok i folkrätt* (Norstedts Juridik, 2013) p. 39.
[35] ICRC Customary International Humanitarian Law Rules (n 11) p. xlvi.
[36] North Sea Continental Shelf cases (Federal Republic of Germany v Netherlands and Denmark) Judgment [1969] ICJ Rep 3 para 74.
[37] International Criminal Court 'The State Parties to the Rome Statute' (no date) <https://asp.icc-cpi.int/en_menus/asp/states%20parties/pages/the%20states%20parties%20to%20the%20rome%20statute.aspx> accessed 6 April 2022.

Considering the exceptional mandate of the ICRC "to work for the faithful application of international humanitarian law applicable in armed conflicts and... to prepare any development thereo"[38] the author will turn to the commentaries of the ICRC when interpreting the Geneva Conventions and their additional protocols.[39] With regards to non-international armed conflicts the International Crimes Tribunal of the former Yugoslavia (ICTY) has recognized that the practice of the ICRC is an important factor in the emergence of customary rules in non-international conflicts.[40] Additionally, reports, positions papers as well as any other relevant documents produced by the ICRC will be used to further argument made by the author that are based on the primary sources of law. In addition, the ICRC's study on customary international humanitarian law will be used when further analyzing and applying customary international humanitarian law throughout this thesis. Although criticized, *inter alia*, for placing to much emphasize on written materials of state opinions rather than operational practice,[41] the work is the most complete codification of the rules of customary international humanitarian law and relevant due to the ICRC's mandate, as mentioned above.

In addition to the ICRC study on customary international humanitarian law the Tallinn Manual 2.0 will be used throughout the thesis, in providing valuable insights on the discussion on cyber operations and the applicability of international law to their use in armed conflicts. Although the Tallinn Manual 2.0 is a soft law instrument and cannot be considered a primary source of law it will be considered as "teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law."[42] The Tallinn Manual 2.0 is the product of two separate international groups of experts, who have sought to codify the legal principles governing cyber operations in

---

[38] Statutes of the International Red Cross and Red Crescent Movement adopted by the 25th International Conference of the Red Cross at Geneva in 1986, amended in 1995 and 2006, art 5(2)(c), 5(2)(g).
[39] International Committee of the Red Cross, *Commentary on the additional protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, (1987).
[40] Prosecutor v. Dusko Tadic aka "Dule" (Decision on the defence motion for interlocutory appeal on jurisdiction), No. IT-94-AR72 International Criminal Tribunal for the former Yugoslavia (2 October 1995) para 109.
[41] John B. Bellinger, III and William J. Haynes II, 'A US government response to the International Committee of the Red Cross study Customary International Humanitarian Law' (2007) 886 International Review of the Red Cross 443 p. 445.
[42] Statute of the International Court of Justice (n 26) art. 38(1)(d).

relation to different legal regimes of international law. The goal of the Manual is to be an objective statement of *lex lata* as of date of adoption in June 2016, it does not venture into policy questions or statements reflecting *lex ferenda.*[43] Although the Tallinn Manual 2.0 has received some criticism, it is mostly with regards to the fact that the Manual does not express the views of states.[44] However, the Tallinn Manual 2.0 is not an international agreement of states or international organizations, rather it should and will be regarded as a product of the international experts that participated in the drafting of the manual in their personal capacity.[45] Finally the author will turn to relevant academic literature to support the findings of this thesis, although non-binding, scholarly work is crucial in understanding the legal issues in connection to cyberspace and the conflict that can be fought within it.

This thesis presupposes two factors. First and foremost, that there is an ongoing armed conflict either international or non-international in character to which the states are party to. Secondly, that the cyber operations that have been conducted are attributable to a state or to a non-state group. Therefore, this thesis does not deal with issues arising from either the threshold of an armed conflict or the issue of attribution in cyberspace. Finally, this thesis does not deal with the issues arising from the dual use characteristics of either cyberspace or the internet since the dual use nature of cyberspace and the internet has been thoroughly analyzed and discussed elsewhere by scholars.[46]

[43] Tallinn Manual 2.0 (n 4) p. 2-3.
[44] Jensen Eric Talbot 'The Tallinn Manual 2.0: Highlights and Insights' (2017) 48 Georgetown Journal of International Law 735 p. 777-778.
[45] Tallinn Manual 2.0 (n 4) p. 2-3.
[46] Se for instance: Droege C, 'Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians' (2012) 94 International Review of the Red Cross 533 or Gisel, Rodenhäuser and Dörmann (n 3).

2. Technical and legal aspects related to cyberspace

2.1 Concepts and terminology

The ICRC position paper on International Humanitarian Law and Cyber Operations during Armed Conflicts (2019) begins with providing the definition for cyber operations during armed conflicts as: "operations against a computer, a computer system or network, or another connected device, through a data stream, when used as means and methods of warfare in the context of an armed conflict."[47] In many cases however, the means of using cyber technology is combined with activities such as crime, warfare and attacks that when conducted through cyberspace are coupled with the 'cyber' prefix, resulting in cyber warfare or cyber crime, for instance. However, it is important to pay explicit attention since the meaning of the words themselves can have a different contextual meaning in the international legal sphere as opposed to in the day-to-day context, as seen in the case of cyber warfare and cyber crime above. For instance, a cyber attack generally refers to a "cyber operation against a particular object or entity, and in the military sense it usually indicates a military operation targeting a particular person or object… the term as used in the *jus in bello* indicates a particular type of military operation that involves the use of violence".[48] As can be derived from the previous quote and the definition of cyber operation of the ICRC above, terminology plays a vital part in understanding the legal issues faced in this thesis and in cyberspace for that matter.

The issue of terminology is common when encountering novel areas of the law and it was also seen as a particular obstacle that the drafters of both editions of the Tallinn Manual had to overcome.[49] Since it is vital to avoid confusion about some of the most central

[47] ICRC, 'International Humanitarian law and cyber operations during armed conflicts ICRC position paper submitted to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, November 2019' (2020) 913 International Review of the Red Cross 481 p. 483.
[48] Tallinn Manual 2.0 (n 4) p. 4.
[49] In the drafting of both editions of the Tallinn Manual, terminology posed a particular obstacle. Many words and phrases have a common meaning as well as having specific military or legal meanings. In addition to the example presented in the text if the word 'attack' is coupled with the word 'armed' in the jus ad bellum, it refers to a cyber operation that justifies a response in self defence according to article 51 of the UN charter. See Tallinn Manual 2.0 (n 4) p. 4-5; Schmitt MN, Tallinn Manual on the International Law Applicable to Cyber Warfare (Cambridge University Press 2013) p. 7.

terms and concepts of this thesis, this chapter will seek to discuss the meaning of some terms and concepts in relation to cyberspace. Therefore, this chapter will begin with defining cyberspace and discussing the legal implications of cyberspace with regards to the specialized regime of international humanitarian law. After ascertaining the basic legal and technical understanding of cyberspace, the chapter will discuss how military action is perceived when conducted in cyberspace in the *jus in bello*. Finally, the remainder of this chapter will seek to clarify digital computer data and how it is used throughout this thesis, since it has such a central role in understanding both the questions and conclusions reached.

2.2 The Cyberspace

Although a majority of people are connected to cyberspace on a daily basis through the use of connected devices (smartphones, computers, tablets), it is important to clarify the meaning of the word itself. The prefix, cyber, comes from the Greek verb *kyberno* which means to steer or to govern.[50] In language, the use of the cyber prefix in conjunction with nouns such as war or terrorism transports these nouns into the virtual arena which makes up cyberspace.[51] The actual word cyberspace was first used in 1984 by the writer William Gibson and is credited to him and his book Neuromancer. In the book, Gibson defines cyberspace as:

"a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphical representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data".[52]

---

[50] Andrew Liaropoulos 'Power and Security In Cyberspace: Implications for The Westphalian State System' (2011) p. 541.
[51] Breno Pauli Medeiros and Luiz Rogério Franco Goldoni 'The Fundamental Conceptual Trinity of Cyberspace' (2020) 42(1) Contexto Internacional 31 p. 33.
[52] Christensson Per 'Cyberspace Definition' (TechTerms.com, 2006) https://techterms.com/definition/cyberspace> accessed 26 November 2021.

Gibson's perception of cyberspace was not far from the current understanding of cyberspace after all, today cyberspace does indeed share some of the same characteristics that he envisioned. The global aspect of cyberspace has time after time been acknowledged, especially by military manuals, because it opens up for attacks at physical infrastructure within the borders of a state even without access to said states territory.[53] This follows from the fact that cyberspace is virtually "created by the connection of physical systems and networks, managed by rules set in software and communications protocols."[54] Rattray's perception of cyberspace points out that there are different layers, which are inherent to cyberspace as a whole. He distinguishes both the physical and non-physical layers of cyberspace.[55]

The Tallinn Manual 2.0 furthers this definition, by adding a layer to the ones suggested by Rattray. According to the Tallinn Manual 2.0 cyberspace is made up of three layers: a physical, a logical and a social layer. Naturally, the physical layer consists of physical objects or hardware such as cables, routers, servers and computers. The logic level, however, comprises of connections, which exist between different network devices and facilitates the exchange of data between devices on the physical layer through applications and protocols. Lastly, the social layer consists of the users who engage in activities in cyberspace.[56] At this point, it is important to state that cyberspace should not be equated with the internet. The internet is part of cyberspace, but cyberspace is vastly more widespread than just the internet which could be perceived as comprising only of the physical and logical layers of cyberspace.[57] As for cyberspace, the Tallinn manual 2.0, defines cyberspace as "[t]he environment formed by physical and non-physical components to store, modify, and exchange data using computer networks".[58]

---

[53] Breno Pauli Medeiros and Luiz Rogério Franco Goldoni 'The Fundamental Conceptual Trinity of Cyberspace' (2020) 42(1) Contexto Internacional 31 p. 35.
[54] Gregory J Rattray 'An environmental approach to understanding cyberpower.' In Franklin D Kramer, Stuart H Starr and Larry K Wentz (eds), Cyberpower and National Security (Washington, DC: National Defense University Press 2009) p. 254
[55] Gregory J Rattray 'An environmental approach to understanding cyberpower.' In Franklin D Kramer, Stuart H Starr and Larry K Wentz (eds), Cyberpower and National Security (Washington, DC: National Defense University Press 2009) p. 254.
[56] Tallinn Manual 2.0 (n 4) p. 12.
[57] Inglis C. 'Cyberspace - Making Some Sense of It All' (2016) 15(2) Journal of Information Warfare 17, p. 17.
[58] Tallinn Manual 2.0 (n 4) p. 564.

For some scholars, cyberspace has emerged as a fifth domain of warfare, in addition to the four formerly recognized domains, land, air, sea and space.[59] However, there is one major difference in characteristics of cyberspace which is the fact that it is totally man made, as opposed to the naturally occurring domains.[60] Considering that cyberspace should essentially be understood as, "the sum of technology, people, and procedures that employ the Internet to achieve actions ranging from personal communications, the conduct of business and government, to the coordination and support of processes and activities that rely on data and synchronization delivered by and through the Internet",[61] the reach of state sovereignty in cyberspace has to be considered. Since the physical layer or cyber infrastructure, located within a state's territory falls within the territory of the state where it resides it also falls within that state's sovereignty.[62] However, how do the virtual elements and actors of cyberspace fair in light of state sovereignty?

The Tallinn Manual 2.0, states that "no state may claim sovereignty over cyberspace *per se*… because much of cyber infrastructure comprising cyberspace is located in the sovereign territories of States."[63] However the manual still considers that all layers of cyberspace are encompassed by the principle of sovereignty.[64] Consider the social layer of cyberspace, which encompasses individuals and groups conducting cyber activities, states can exercise their sovereignty over these actors, through the use of various jurisdictions. A state can exercise jurisdiction over both cyberinfrastructure and its nationals located within its territory.[65] In addition, according to the active nationality principle, states can exercise jurisdiction over their nationals regardless whether on domestic territory or abroad.[66] Therefore all actors of the social layer fall within state sovereignty, even when cyber activities "cross multiple borders, or occur in international

---

[59] Wolff Heintschel von Heinegg 'Territorial Sovereignty and Neutrality in Cyberspace' (2013) 89 International Law Studies 123, p. 123; David J. Betz and Tim Stevens 'Cyberspace and the State: Toward a Strategy for Cyber-power' (2011) 51 Adelphi Series 9, p. 35.
[60] David J. Betz and Tim Stevens 'Cyberspace and the State: Toward a Strategy for Cyber-power' (2011) 51 Adelphi Series 9, p. 35.
[61] Inglis C. 'Cyberspace - Making Some Sense of It All' (2016) 15(2) Journal of Information Warfare 17, p. 17.
[62] Tallinn Manual 2.0 (n 4) p. 11.
[63] Tallinn Manual 2.0 (n 4) p. 13.
[64] Tallinn Manual 2.0 (n 4) p. 12.
[65] Nottebohm Case (Lichtenstein v Guatemala) (Judgment) [1955] ICJ Rep 4, p. 23.
[66] Tsagourias N and Russell B 'Research Handbook on International Law and Cyberspace' (Edward Elgar Publishing 2015) p. 19.

waters, international airspace, or outer space, all are conducted by individuals or entities subject to the jurisdiction of one or more States."[67] This also holds true for any objects that are within state sovereignty but whether applications, data and internet protocols of the logic layer suffice as objects will further be explored in chapter 3, explicitly with regards to data.[68]

2.3 Data defined

At its most basic level digital data is formed by the complex succession of 1s and 0s. This is commonly known as binary, which computers through software and protocols can interpret and turn into something that users can perceive, like the text of this thesis for example. However, it should be noted that data is not only limited to documents of text stored on computers. The binary code can constitute anything from computer code for an application on a smartphone or a military missile system, both are just as much data as the protocols of a credit card company which handles transactions when made by the card's user.[69] Simply put, data are information, and because all computers use binary data on a rudimental level it can be created, processed, saved, and stored. In addition, this allows for data to be transferred between computers either through network connections or with a media device, since data itself does not deteriorate over time or because it is used.[70]

The binary code of otherwise unreadable data is what the so-called logic layer of cyberspace is composed of, which *inter alia* is recognized in the Tallinn Manual 2.0.[71] The Tallinn Manual 2.0 has defined data as "[t]he basic element that can be processed or produced by a computer to convey information. The fundamental digital data measurement is byte."[72] Some scholars have argued that data should be categorized into different types of data depending on how it functions. According to Dinniss data should

[67] Tallinn Manual 2.0 (n 4) p. 12.
[68] Tallinn Manual 2.0 (n 4) p. 12.
[69] Mc Cormack (n 1) p. 223.
[70] Christensson Per 'Data Definition' (TechTerms.com, 2006) <https://techterms.com/definition/data> accessed 26 November 2021.
[71] Tallinn Manual 2.0 (n 4) p. 12.
[72] Tallinn Manual 2.0 (n 4) p. 564.

not be understood as a single entity, but distinguished as two types of data, operation-level data and content-data.[73] Operation-level data is what gives data logic and is essentially composed of program data or 'code'. It is what gives hardware functionality as well as the ability to perform pre-determined tasks.[74] Content-level data on the other hand, does not have functionality on the logic layer of cyberspace but is simply information or text "such as the text of this Article, or the contents of medical databases, library catalogues."[75]

This thesis does not strictly adopt to consequentially use either data as such or content-level and operational-level data, as suggested by Dinniss.[76] For example, in chapter 3, the more general term data or computer data will be used, as it succeeds to encompass both content-level data and operational-level data. However, in chapter 4 it sometimes proves useful to distinguish between different types of data since special protection might be afforded only to one of the different types of data. When using content-level data and operational-level data, this thesis adopts the definition presented above as suggested by Dinniss.[77]

2.4 The reach of international humanitarian law in cyberspace

It is now generally accepted that international law applies to cyber operations and to cyberspace by both states and academia. The United Nations Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security (UNGGE) has been the primary forum for state cooperation when discussing how international law pertains to information and communication technologies (ICT). The discussions on information security started after the Russian Federation submitted the first resolution on the subject to the UN General Assembly in 1998, which eventually led to the creation of the UNGGE.[78]

---

[73] Heather A Harrison Dinniss, 'The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives' (2015) 48 Isr L Rev 39 p. 41.
[74] Dinniss (n 73) p. 41.
[75] Dinniss (n 73) p. 41.
[76] Dinniss (n 73) p. 41.
[77] Dinniss (n 73) p. 41.
[78] Gisel, Rodenhäuser and Dörmann (n 3) p. 292.

In the 2013 report of the UNGGE, it reaffirmed that both international law and the UN Charter is applicable to cyberspace and any acts conducted therein.[79] The group further concluded that both "[s]tate sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory."[80] Later in the 2015 report as well as in the final report of the UNGGE in 2021 it was affirmed that international humanitarian law and especially the principles of humanity, necessity, proportionality and distinction are applicable to the use of ICTs by states in situations of armed conflict.[81]

Since the object and purpose of international humanitarian law is to regulate military action in future conflicts while allowing for military necessity, international humanitarian law treaties are adopted with the development of means and methods of warfare in mind.[82] Therefore, as early as in the 1868 Declaration of St. Petersburg, it was stated that the principles establish therein should be respected by "future improvements which science may effect in the armament of troops".[83] Similarly, even though the use of offensive cyber capabilities is not specifically mentioned in any of the 1949 Geneva Conventions or their additional protocols, Article 36 of Additional Protocol I requires that any weapon, means or methods of warfare used in an armed conflict is subject to international humanitarian law. This is because states party to Additional Protocol I are required to, in their development of new means and methods of warfare, ensure that their uses are in compliance with international humanitarian law, however this obligation does not extend

[79] UNGA 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (24 June 2013) UN Doc A/68/98 para 19.
[80] UNGA 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (24 June 2013) UN Doc A/68/98 para 20.
[81] UNGA 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (22 July 2015) UN Doc A/70/174 para. 28-29; UNGA 'Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security' (14 July 2021) UN Doc A/76/135 para. 71(f); se also the view of ICRC in International humanitarian law and the challenges of contemporary armed conflicts - recommitting to protection in armed conflict on the 70th anniversary of the geneva conventions (n 16) p. 26-29.
[82] Gisel, Rodenhäuser and Dörmann (n 3) p. 298.
[83] Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight. Saint Petersburg, (adopted 11 December 1868, entered into force 11 December 1868).

to non-international armed conflict.[84] The applicability of international humanitarian law to cyber means and methods of warfare was reaffirmed by the ICJ in the 1969 advisory opinion on the Legality of the Threat or Use of Nuclear Weapons, when stating that the principles and rules of international humanitarian law applicable to armed conflict "applies to all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future."[85]

Several states have also recognized the applicability of international law as well as international humanitarian law specifically, to cyber means and methods of warfare in the context of an armed conflict, through public declarations of position papers on the issue. For instance, the United Kingdom stated in 2021 that "IHL applies to operations in cyberspace conducted in the furtherance of hostilities in armed conflict just as it does to other military operations."[86] Similarly Australia held that "[e]xisting international law provides the framework for state behaviour in cyberspace. This includes, where applicable, the law regarding the use of force, international humanitarian law, international human rights law, and international law regarding state responsibility."[87] Several other states have made similar declarations of their national positions on how international law applies to cyberspace and the activities committed therein, inter alia:

[84] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Protocol I) art. 36.
[85] *Legality of the Threat or Use of Nuclear Weapons* Advisory Opinion (n 7) para 86.
[86] Foreign, Commonwealth & Development Office 'Policy paper: Application of international law to states' conduct in cyberspace: UK statement' (Gov.uk, 3 June 2021) <https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement> accessed 17.1.2022 para 22.
[87] Commonwealth of Australia, Department of Foreign Affairs and Trade 'Australia's International Cyber Engagement Strategy' (2017) p. 90.

Estonia,[88] France,[89] Finland,[90] Germany,[91] Israel,[92] Italy,[93] Japan,[94] Netherlands,[95] Norway,[96] Russia[97] and Switzerland.[98]

State position papers are thereby in line with the conclusion of the Tallinn Manual 2.0, which considers that international humanitarian law is applicable to cyber operations whenever an armed conflict is present, either international or non-international in

[88] UNGA 'Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266' (13 July 2021) UN Doc A/76/136* p. 23.

[89] Ministère des Armées de France, 'INTERNATIONAL LAW APPLIED TO OPERATIONS IN CYBERSPACE' (2019) <https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf> accessed 19 January 2022 p. 12.

[90] Ministry for Foreign Affairs 'International law and cyberspace Finland's national positions' (2020) <https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727> accessed 19 January 2022 p. 7.

[91] Ministry of Foreign Affairs 'On the Application of International Law in Cyberspace Position Paper' (2021) <https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf> accessed 19 January 2022 p. 1.

[92] Mission of Israel to the UN in Geneva 'Application of International Law to Cyberspace' (https://embassies.gov.il/ 25 October 2021) <https://embassies.gov.il/UnGeneva/priorities-statements/ScienceTechnologyDevelopment/Pages/Israel-approach-on-the-Application-of-International-Law-to-Cyberspace.aspx> accessed 19 January 2022.

[93] Ministry of Foreign Affairs and International Cooperation 'ITALIAN POSITION PAPER ON 'INTERNATIONAL LAW AND CYBERSPACE' (2021) <https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf> accessed 19 January 2022 p. 9.

[94] Ministry of Foreign Affairs of Japan 'Basic Position of the Government of Japan on International Law Applicable to Cyber Operations' (2021) <https://www.mofa.go.jp/files/100200935.pdf> accessed 19 January 2022 p. 6.

[95] Government of the Kingdom of the Netherlands 'Appendix: International law in cyberspace' <https://www.government.nl/binaries/government/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace/International+Law+in+the+Cyberdomain+-+Netherlands.pdf> accessed 19 January 2022 p. 5.

[96] Norwegian Government Security and Service Organisation 'NORWEGIAN POSITIONS ON SELECTED QUESTIONS OF INTERNATIONAL LAW RELATING TO CYBERSPACE' (2021) <https://www.regjeringen.no/contentassets/a8911fc020c94eb386a1ec7917bf0d03/norwegian_positions.pdf> accessed 19 January 2022 p. 9.

[97] UNGA 'Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266' (13 July 2021) UN Doc A/76/136* p. 79-80.

[98] Federal Department of Foreign Affairs 'Switzerland's position paper on the application of international law in cyberspace' (2021) <https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf> accessed 19 January 2022 p. 8.

nature.[99] Since this thesis assumes the existence of an armed conflict the requirements for an armed conflict to emerge will not be discussed further.[100]

States that have joined the Paris Call for Trust and Security in Cyberspace have also reaffirmed the applicability of international humanitarian law as well as international law to cyberspace.[101] Although the Paris call is not a legal framework, the declaration made by states at the time of joining the Paris Call serves as proof of verbal state practice. At the time of writing, 81 states have already joined and made the call.[102] Among the most recent are the United States of America as well as the European Union.[103] By all accounts, both state praxis and the international framework in place, suggest that international humanitarian law is applicable to cyber operations or state use of ICTs in armed conflicts.

2.5 Military operation and attacks in cyberspace

Military action conducted through cyberspace usually falls within the definition of either a military operation or an attack. However, since the laws of armed conflict were developed in the 1800s and the 1900s, they do not always adequate kinetic military action and cyber military action, as suggested earlier. In treaty law, Additional Protocol I provides for the protection of civilians and civilian objects from attack,[104] the prohibition is also considered to be customary international humanitarian law.[105] As opposed to military operations in general, attack means "acts of violence against the adversary, whether in offence or in defence."[106] The distinction between military operations and military attacks is therefore based on the fact that the use of violence during military action makes it an attack as opposed to non-violent military action. Non-violent military

[99] Tallinn Manual 2.0 (n 4) p. 375 para 1.
[100] For the requirements of an armed conflict, see inter alia: Tallinn Manual 2.0 (n 4) p. 375-396.
[101] Paris call 'The Call' (2018) <https://pariscall.international/en/call> accessed 19 January 2022.
[102] Paris call 'The Supporters' (2018) <https://pariscall.international/en/supporters> accessed 19 January 2022.
[103] France, 'International Law Applied to Operations in Cyberspace' (n 89) p. 4; Paris call 'The Call' (2018) <https://pariscall.international/en/call> accessed 19 January 2022.
[104] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Protocol I) art. 51(2).
[105] ICRC Customary International Humanitarian Law Rules (n 11) p. 3, 25.
[106] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Protocol I) art. 49(1).

action, on the other hand encompasses any non-violent military operation.[107] This interpretation is supported by the commentary of Bothe, Partsch and Solf which states that: "[t]he term 'acts of violence' denotes physical force. Thus, the concept of 'attacks' does not include dissemination of propaganda, embargoes, or other non-physical means of psychological or economic warfare."[108]

In addition, the 1987 ICRC commentary on Additional Protocol I states that "the term 'attack' means 'combat action.'"[109] Non-violent military operations as those described by Bothe, Partsch and Solf, are generally considered to be lawful as long as they do not cause physical harm or human suffering.[110]

It is however important to consider that attacks are not only limited to such combat action that uses physical or kinetic force.[111] Both the text and commentary of the Additional Protocol I, suggest that physical violence is required, since most attacks during the time of drafting employed some kind of kinetic weapon, which caused physical damage when used.[112] However, considering the primary purpose of the Additional Protocol I is to allow for military necessity while affording effective protection to civilians[113] and if interpreting the treaty "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"[114], it is argued the drafters of Additional Protocol I must have intended the Protocol to protect the civilian population from the violent consequences of an attack, rather than from the act of an attack.[115] This approach

---

[107] Tallinn Manual 2.0 (n 4) p. 415; Schmitt MN 'Cyber Operations and the Jus in Bello: Key Issues' (2011) 87 International Law Studies 89 p. 93.
[108] Michael Bothe, Karl Josef Partsch and Waldemar A. Solf, *New Rules for Victims of Armed Conflicts: Commentary to the Two 1977 Protocols Additional to the Geneva Conventions of 1949* (Martinus Nijhoff Publishers 1982) p. 289.
[109] Commentary on the additional protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 (n 39) para. 1880.
[110] Schmitt (n 107) p. 92.
[111] Schmitt (n 107) p. 93; Droege (n 46) p. 557; Tallinn Manual 2.0 (n 4) p. 415-416; Solis GD, *The Law of Armed Conflict: International Humanitarian Law in War* (3rd ed Cambridge University Press 2021) 537.
[112] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Protocol I) art. 48, 51; Commentary on the additional protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 (n 39) para 1875, 1940.
[113] Gisel, Rodenhäuser and Dörmann (n 3) p. 298.
[114] Vienna Convention on the Law of Treaties (n 28) art. 31(1).
[115] Schmitt (n 107) p. 93: Tallinn Manual 2.0 (n 4) p. 415-416.

is suggested to be more in line with the general theme of the protections of the Additional Protocol I.[116]

There exists some means and methods of warfare that rely on biological, chemical or radiological components in causing damage rather than relying on kinetic components, as traditional weapons of warfare. For these non-kinetic weapons, the act of using such means and method of warfare would not be a violent act as such, because the act of deploying such a weapon does not use physical violence. However, the consequences of using means and methods relying on biological, chemical or radiological components could lead to consequences that in turn are harmful or lethal.[117] It is therefore more appropriate for these non-kinetic weapons to use the doctrine that suggested above which relies on violent consequences to qualify as an attack.[118] The shift in focus to the violent consequences of an act has seemed to gain ground considering that the ICTY stated in the *Tadic case*, that a general consensus has emerged where the use of chemical weapons against the civilian population is prohibited.[119]

The doctrine is also supported by the conclusion of the ICRC commentary on Additional Protocol I, which considers an attack to encompass any combat action.[120] Additionally, Article 51(1) states that the "'civilian population and individual civilians shall enjoy general protection against *dangers arising from military operations*."[121] Likewise, Article 57(2)(a)(iii) respectively 57(2)(b) mentions that attacks which could result in the "*loss* of civilian *life*, *injury* to civilians, *damage* to civilian objects, or a combination thereof"[122]

---

[116] Schmitt (n 107) p. 93: Tallinn Manual 2.0 (n 4) p. 415-416.
[117] Haslam E, 'Information Warfare: Technological Changes and International Law' (2000) 5 Journal of Conflict & Security Law 157 p. 170.
[118] Schmitt (n 107) p. 93: Tallinn Manual 2.0 (n 4) p. 415-416.
[119] The statement of the court was made with regards to a non-international armed conflict: Prosecutor v. Dusko Tadic aka "Dule" (Decision on the defence motion for interlocutory appeal on jurisdiction), No. IT-94-AR72 International Criminal Tribunal for the former Yugoslavia (2 October 1995) para 120-124.
[120] Commentary on the additional protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 (n 39) para. 1880.
[121] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Protocol I) art. 51(1) emphasis added.
[122] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Protocol I) art. 57(2)(a)(iii), 57(2)(b) emphasis added.

should be avoided or suspended.[123] Article 57 of Additional Protocol I, containing precautions in attack, is also considered to be customary international law in both international and non-international armed conflicts, although Additional Protocol II does not contain a similar provision.[124]

The realm of cyber warfare is similar to some extent to means and methods of warfare that rely on biological, chemical or radiological components. Similarly, cyber warfare can be conducted as to, for instance alter "the running of a SCADA system controlling an electrical grid and results in a fire"[125] or, a cyber operation could be conducted to manipulate an enemy's air traffic control tower resulting in the crash of an airplane.[126] Because the consequence of such a cyber operation is destructive, entailing an act of violence, the operation would qualify as a cyber attack rather than a cyber operation.[127]

When it comes to cyber operations that have violent consequences, this thesis adopts the definition of a cyber attack suggested in the Tallinn Manual 2.0. According to the definition: "[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."[128] In addition, it would be reasonable to consider that cyber operations, which are conducted with the primary purpose of spreading terror would be prohibited, pursuant to Article 51(2) of Additional Protocol I as well as Article 13(2) of Additional Protocol II, since they prohibit "acts or threats of violence the primary purpose of which is to

[123] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Protocol I) art. 57(2)(a)(iii), 57(2)(b).
[124] ICRC Customary International Humanitarian Law Rules (n 11) rule 15, p. 51.
[125] SCADA meaning Supervisory Control And Data Acquisition is a "Computer systems and instrumentation that provide for monitoring and controlling industrial, infrastructure, and facility-based processes, such as the operation of power plants, water treatment facilities, electrical distribution systems, oil and gas pipelines, airports, and factories." Tallinn Manual 2.0 (n 4) p. 416, 567.
[126] Droege (n 46) p. 553; Dörmann K, 'Applicability of the Additional Protocols to Computer Network Attacks' (2004) (Paper delivered at the International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Stockholm, Nov. 17–19, 2004) p. 2.
[127] Tallinn Manual 2.0 (n 4) p. 416.
[128] Tallinn Manual 2.0 (n 4) p. 415 rule 92; for a similar definition se: Solis GD (n 111) p. 537.

spread *terror* among the civilian population."[129] Additionally, the prohibition is considered customary international humanitarian law.[130]

A military cyber operation that does not rise to the level of an attack is primarily a non-violent military operation. Cyber espionage, operations of psychological warfare (not arising to the level of causing terror) or operations denying access to a certain kind of service that would be regarded to be akin to jamming, would be considered lawful cyber operations against the civilian population.[131] In international humanitarian law there is neither any prohibition against economic sanctions that target the civilian population.[132] Therefore, cyber operations that are tantamount to the effects of economic sanctions are lawful, as long as the cyber operation does not fall under the prohibition of destroying, removing, or rendering useless objects indispensable to the survival of the civilian population of Article 54 of Additional Protocol I.[133] As a general rule of thumb, some scholars have considered that operations targeting civilians that cause only mere inconvenience to the civilian population are considered to be military operations rather than military attacks although this has to be evaluated case by case.[134]

The present chapter has only touched upon the most essential concepts and legal aspects of cyberspace. In the following two chapters the issue of protection of civilian computer data will be tackled. Therefore, chapter 3 begins with considering whether civilian computer data can be considered an object of international humanitarian law.

---

[129] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Protocol I) art. 51(2) emphasis added; Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 609 (Protocol II) art. 13(2) emphasis added.
[130] ICRC Customary International Humanitarian Law Rules (n 11) rule 2, p. 8.
[131] "the jamming of radio communications or television broadcasts has not traditionally been considered an attack in the sense of IHL" International Committee of the Red Cross, 'International humanitarian law and the challenges of contemporary armed conflicts' (2015) 32IC/15/11 p. 42; Schmitt (n 107) p. 96: Tallinn Manual 2.0 (n 4) p. 419.
[132] Droege (n 46) p. 560.
[133] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Protocol I) art. 54.
[134] Schmitt (n 13) p. 377; Droege (46) p. 560.

3. Data as an object of international humanitarian law

3.1 Civilian objects and military objectives

The fundamental principle of international humanitarian law and a cornerstone of civilian protection is the principle of distinction. The ICJ described it as one of the "cardinal principles" of international humanitarian law and it was laid out as early as 1868 in the preamble of the Declaration of St. Petersburg. [135] The Declaration of St. Petersburg states that: "the only legitimate object which States should endeavour to accomplish during war is to weaken the military forces of the enemy".[136] This is the first codification of the principle of distinction, which can now be found across numerous treaties and military manuals.[137]

Additional Protocol I to the Geneva Conventions reiterates the principle of distinction in Articles 48, 51(2) and 52(2).[138] The basic rule of the Protocol (Article 48) ensures the protection of both civilians (persons) as well as civilian objects and requires parties to a conflict to distinguish between military and civilian and only direct their operations against the former.[139] With regard to objects, Article 52(1) prohibits attacks against civilian objects by the means of reprisal.[140] To ensure the protection of civilian objects, both civilians and civilian objects are negatively defined in the Protocol as those objects which are not military objectives per the definition of military objectives of Article 52(2).[141]

---

[135] *Legality of the Threat or Use of Nuclear Weapons* Advisory Opinion (n 7) para 78.
[136] Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight. Saint Petersburg, (adopted 11 December 1868, entered into force 11 December 1868).
[137] ICRC Customary International Humanitarian Law Rules (n 11) p. 25-26.
[138] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Protocol I) art. 48, 51(2), 52(2).
[139] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Protocol I) art. 48.
[140] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Protocol I) art. 52(1).
[141] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Protocol I) art. 52.

The principle of distinction can also be found in the Additional Protocol II, amended protocol II and protocol III to the Convention on Certain Conventional Weapons.[142] In addition, international courts have also reaffirmed the protection of civilians and civilian objects from military action, with the ICJ stating, in its advisory opinion on the Legality of the Threat or Use of Nuclear Weapons, that: "[s]tates must never make civilians the object of attack"[143] and the Rome Statute of the ICC considering that attacks which are intentionally directed at civilians or civilian objects constitute war crimes.[144] The ICJ has further stated that the principle of distinction is to be considered one of the "intransgressible principles of international customary law", therefore binding on all states.[145] The principle of distinction has been codified by the ICRC study of customary international humanitarian law separately for persons and objects. The principle of distinction pertaining to objects reads as follows: "[t]he parties to the conflict must at all times distinguish between civilian objects and military objectives. Attacks may only be directed against military objectives. Attacks must not be directed against civilian objects."[146]

As noted Additional Protocol I defines civilian objects as "all objects which are not military objective".[147] Therefore, the definition of military objectives enshrined in Article 52(2) of the Protocol and international customary law becomes vital.[148] The first codification of a definition of military objectives was made in the 1923 Hague draft rules of air warfare as "an objective whereof the total or partial destruction would constitute an

---

[142] Protocol On Prohibitions Or Restrictions On The Use Of Mines, Booby-traps And Other Devices (As Amended On 3 May 1996) (adopted 03 May 1996, entered into force 03 December 1998) art. 3(7); Protocol On Prohibitions Or Restrictions On The Use Of Incendiary Weapons (adopted 10 October 1980, entered into force 02 December 1983) art. 2(1).
[143] *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, ICJ GL No 95, [1996] ICJ Rep 22 para 78.
[144] Rome Statute of the International Criminal Court (adopted 17 July 1998, entered into force 1 July 2002) Art. 8(2)(b)(ii).
[145] *Legality of the Threat or Use of Nuclear Weapons* Advisory Opinion (n 7) para 79; for in depth analyses se also: ICRC Customary International Humanitarian Law Rules (n 11) p. 25-26.
[146] ICRC Customary International Humanitarian Law Rules (n 11) p. 25.
[147] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Protocol I) art. 52(1).
[148] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Protocol I) art. 52(2).

obvious military advantage for the belligerent".[149] However, this attempt of the Hague draft rules of air warfare to codify a distinction between civilian objects and military objectives did not make it to the Geneva Conventions of 1949, relating to the wounded and sick and to prisoners of war, even though the rules of the Conventions were largely based on a fundamental distinction between civilian objects and military objectives.[150] Later however, Additional Protocol I took a similar approach, as the Hague draft rules of Air Warfare, defining military objectives as follows:

"In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage."[151]

According to the ICRC study on customary humanitarian law, this codification of military objectives reflects customary humanitarian law applicable in both international armed conflict and non-international armed conflict and therefore binding on all states.[152] Similar codification of the rule is contained within several military manuals of states[153] and supported by several official statements of states. Additionally, it is stated that states who are not party to Additional Protocol I have shown that they support this practice.[154] The International Criminal Tribunal for the former Yugoslavia's Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia also found and stated that both the protection of civilian objects as well as the definition of military objectives is to be considered customary international humanitarian law.[155]

---

[149] 'Rules concerning the Control of Wireless Telegraphy in Time of War and Air Warfare. Drafted by a Commission of Jurists at the Hague, December 1922 - February 1923' (adopted 19.02.1923) art. 24.
[150] Commentary on the additional protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 (n 39) para 1998.
[151] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Protocol I) art. 52(2).
[152] ICRC Customary International Humanitarian Law Rules (n 11) p. 25.
[153] To name a few: The Federal Ministry of Defence Of The Federal Republic Of Germany 'Joint Service Regulation on Law of Armed Conflict Manual' (ZDv 15/2) (2013) para. 407; Us Department of Defence Office of The General Counsel, 'Law of War Manual' (June 2016) Para. 5.6.3; Uk Ministry of Defence, The Joint Service Manual of The Law Of Armed Conflict, Jsp 383 (2004) Para. 5.4.1.
[154] ICRC Customary International Humanitarian Law Rules (n 11) p. 30.
[155] International Criminal Tribunal for the former Yugoslavia 'Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia' (2000) para 42; se also Tallinn Manual 2.0 (n 4) p. 436.

Essentially the requirements of a military objective of Article 52(2) of Additional Protocol I establishes a two-pronged test.[156] For the first prong, it has to be determined whether the object makes an effective contribution based on either its nature, location, purpose or use. The second prong requires that the destruction, capture or neutralization of said object offers a definitive military advantage in the circumstances ruling at the time of the attack. A military objective is present when the requirements of the two-pronged test are fulfilled.[157] Because the drafters of Additional Protocol I could not possibly foresee the future developments of means and methods of warfare, the following subchapter will explore both the qualifications of military objectives and military cyber objectives.

3.2 The qualifications of military objectives

The qualifications of military objectives made in reference to Additional Protocol I are largely based on the 1987 commentary of the protocol by the ICRC. The same qualifications, however, are also present in customary international law.[158] For a military objective to be present the two subsequent requirements of Article 52 paragraph 2 must thus be fulfilled. The object must make an effective contribution to military action either due to its nature, location, purpose or use and the total or partial destruction, capture or neutralization of the same object must at the time of the attack result in a definite military advantage to the attacking party of the conflict.[159]

The first requirement is dependent on an objective's effective contribution to military action. An objective can make an effective contribution to military action in four different ways. Firstly objectives, which by their nature make an effective contribution to military

[156] International Law Association Study Group on the Conduct of Hostilities in the 21st Century 'The Conduct of Hostilities and International Humanitarian Law: Challenges of 21st Century Warfare' (2017) 78 International Law Studies 322 p. 327.
[157] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Protocol I) art. 51(2).
[158] Se for instance: ICRC Customary International Humanitarian Law Rules (n 11) rule 8.
[159] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Protocol I) art. 51(2).

action comprises of those objectives which would directly be used by the armed forces of a state and are inherently used for military action. In traditional warfare, these objects would include objects such as "weapons, equipment, transports, fortifications, depots, buildings occupied by armed forces, staff headquarters, communications centres etc."[160] However, with regards to the cyber objectives, objects which by their nature effectively contribute to military action could include "all weapons, weapons systems and *matériel*, sensor arrays, battlefield devices, military networks and databases, military command and control systems, communications systems and any other digital device purposely built to military specifications."[161]

Equally, data that constitutes a cyber weapon is considered to be a military objective. This conclusion is in part made of the Tallinn Manual 2.0 Rule 103. According to which "cyber means of warfare that are used, designed, or intended to be used to cause injury to, or death of, persons or damage to, or destruction of, objects, that is, that result in the consequences required for qualification of a cyber operation as an attack".[162] The operation of executing such a weapon would amount to an attack for the purposes of international humanitarian law because the consequences of the operation would be violent in nature.[163] Therefore the same cyber weapon could be considered to be a military objective due to its nature. Similarly, data that contains the information on troop movement orders or timetables for military action, also represents data that would fulfill the requirement of making an effective contribution to military action due to its nature.[164]

Objects which make an effective contribution to military action due to their location are traditionally recognized as specific geographical areas such as a mountain pass or a canal.[165] These objects do not need to have a military function by their nature or be military objectives as such but can become military objectives due to their location when

---

[160] Commentary on the additional protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 (n 39) para 2020.
[161] Dinniss (n 73) p. 47; also, se Heather Harrison Dinniss, *Cyber Warfare and the Laws of War*, (Cambridge University Press 2012) p. 185.
[162] Tallinn Manual 2.0 (n 4) rule. 103 para 2.
[163] Commentary on the additional protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 (n 39) para 1875; Schmitt (n 107) p. 93.
[164] Herbert Lin 'Cyber Conflict and International Humanitarian Law' (2012) 886 International review of the Red Cross 515 p. 519.
[165] Dinniss (n 73) p. 48.

they become of importance for furthering military action. The location can in addition be a site that is of special importance for military operations or that it must be controlled to deny its use by the adversary.[166] Physical examples of the objects fulfilling the locational requirement are easy to come by but with regards to cyber objects the task is not as easy. This problem arises mainly because of the distributed characteristics of networks. Although, a cyber objective which might qualify is a civilian wireless network that is located in a certain geographical area. If the wireless network would be located in an area of hostilities the network might be an objective which the adversary military forces could use to intercept the first states communications. The civilian wireless network could qualify as a military objective, by the definition of the first prong of Article 52(2) of Additional Protocol I, since it offers an effective contribution to military action due to its location and if the territorial state would neutralize or destroy it they would gain a definitive military advantage from the objective's destruction. Followingly, the data that controls the network could also be targeted since it similarly amounts to a military objective by making an effective contribution to military action by the location of said wireless network.[167]

The final notion is of objects which effectively contribute to military action through their use or purpose. The criterion of use is made in relation to the current use of the object's function, while purpose on the other hand is related to the future use of an object. Both of these criteria are present since most civilian objects can become valuable military objectives, and either be used as such or converted into military headquarters, fortifications or other establishments used by the armed forces.[168] The most common uses of civilian objects that render the object a military objective is the use of civilian transports, airfields and buildings by military personnel or objectives. In the same sense, any cyber infrastructure connected to the object will simultaneously become a military objective as traditional objects become military through their use.[169] Similarly, any data that is part of the software or which otherwise makes an effective contribution to military

[166] Commentary on the additional protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 (n 39) para 2021.
[167] Dinniss (n 73) p. 48.
[168] Commentary on the additional protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 (n 39) para 2021-2022.
[169] Dinniss (n 73) p. 47-48.

action could qualify as a military objective due to either its actual or intended use or purpose. Some practical examples might be the data that operates civilian railroad networks or the data that controls civilian radio or tv towers to broadcast military information,[170] other examples are for instance the data of a civilian software that controls a satellite capable of taking imagery of the planet's surface which could be used for military action thereby qualifying as a military object through its use or purpose depended on if such purpose was planned beforehand.[171]

With regard to objects qualifying as military objectives, through their purpose, the intended use of an object is vital. Evaluating the potential use of an object does not suffice as a characteristic for determining the object's contribution to military action due to the reference to paragraph 3 of Article 52 in the commentary of Additional Protocol I when regarding objects that are normally used by civilians.[172] The criteria of purpose must be evaluated after the original nature of the object but before the actual use, otherwise it would be redundant in relation to the other criteria's of the paragraph.[173]

The second part of the first pong of the two-pronged test requires that the objective makes an "[e]ffective contribution to military action."[174] The effective contribution an objective entail does not require a direct connection to the hostilities.[175] It is however regarded that the military action employed needs to have a certain nexus to the conflict. Otherwise nearly anything could be labeled a military objective with the argument that it is contributing to a state's economy, thereby supplying its armed forces.[176] Similarly the 1907 Hague Regulations prohibits states from destroying or seizing the enemy states

[170] Tallinn Manual 2.0 (n 4) rule 100 para. 10.
[171] Tallinn Manual 2.0 (n 4) rule 101 para. 8.
[172] Commentary on the additional protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 (n 39) para 2022.
[173] Yoram Dinstein, 'Legitimate Military Objectives under the Current Jus in Bello' (2002) 78 International Law Studies 140, 142–43.
[174] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Protocol I) art. 52(2).
[175] Michael Bothe, Karl Josef Partsch and Waldemar A. Solf, *New Rules for Victims of Armed Conflicts: Commentary to the Two 1977 Protocols Additional to the Geneva Conventions of 1949* (Martinus Nijhoff Publishers 1982) p. 324.
[176] For a more detailed analysis on the American position of the subject regarding war sustaining and war fighting objects: Dinstein Y, *The Conduct of Hostilities under the Law of International Armed Conflict* (3rd edn Cambridge University Press 2016) p. 109-110.

property ”[u]nless such destruction or seizure be imperatively demanded by the necessities of war.”[177] The Tallinn Manual 2.0 confirms the same principle, considering the objective needs to be contributing to the military capabilities of one of the parties to the conflict and referencing the prohibition set forth in the Hague Regulations.[178]

The second requirement of the two-pronged test requires that the total or partial destruction, capture or neutralization of the objective must at the time of the attack result in a definite military advantage to the attacking party of the conflict.[179] According to Bothe *et al.* the use of a *definitive* military advantage, is made to limit the scope of the military advantage gained from an attack to a concrete and perceptible advantage, rather than a speculative or hypothetical one.[180] The limiting factor of the second prong can be seen in the following example. Targeting a church would be an illegitimate targe since that would gain no military advantage, however the church becomes a military object by the use criteria if enemy troops were positioned there altering the equation of the military advantage gained. Before the deployment of the troops, one could argue the church could serve as a military objective due to its potential future use, however destroying it beforehand would not offer a definitive military advantage in the circumstances ruling at the time since the advantage gained cannot be a potential advantage.[181]

According to the ICRC customary international humanitarian law study; military advantage refers to the anticipated advantage of the military attack as a whole and not only as the advantage gained from isolated events or specific parts of the attack.[182] However the military advantage gained cannot be calculated from the war effort as a whole, rather the definite advantage must be calculated on the basis of a specific military

---

[177] Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land The Hague 18 October 1907 (adopted 18 October 1907, entered into force 26 January 1910) art. 23g.
[178] Tallinn Manual 2.0 (n 4) p. 440.
[179] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Protocol I) art. 52(2).
[180] Michael Bothe, Karl Josef Partsch and Waldemar A. Solf, *New Rules for Victims of Armed Conflicts: Commentary to the Two 1977 Protocols Additional to the Geneva Conventions of 1949* (Martinus Nijhoff Publishers 1982) p 325-326.
[181] Dinstein Y, *The Conduct of Hostilities under the Law of International Armed Conflict* (3rd edn Cambridge University Press 2016) p. 107.
[182] ICRC Customary International Humanitarian Law Rules (n 11) p. 31, 50

operation[183] because every military objective that is attacked has to offer a definitive advantage.[184]

The requirement of the advantage being military in nature generally consists of ground gained or of either annihilation of weakening the enemy armed forces.[185] Targets which are directly involved in supporting the logistics of armed forces or enabling military communications and manufacturing weapons for the military can also be included.[186] On the other hand, a target which offers a political, psychological, or economic advantage does not fall within the requirement of military advantage. Similarly, forcing a change in the negotiation approach of the adversary, even if welcomed, through political or economic targets that change in the negotiation approach cannot be deemed as gaining a military advantage.[187]

According to several states, it is the responsibility of those planning and executing the military operations to determine whether or not an actual military advantage can be gained from the action employed on the basis of the information known at the time.[188]

3.3. Data in light of the definition of military objectives and civilian objects

3.3.1. Data as an object

In international humanitarian law, objects only appear in two categories: as civilian objects and as military objectives. The 1949 Geneva Conventions and their additional protocols are in large based on this fundamental distinction between the two and therefore the definition of an object as such, becomes a vital question for the interpretation of the

[183] International Law Association Study Group on the Conduct of Hostilities in the 21st Century 'The Conduct of Hostilities and International Humanitarian Law: Challenges of 21st Century Warfare' (2017) 78 International Law Studies 322 p. 342-343.
[184] Commentary on the additional protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 (n 39) para 2028.
[185] Commentary on the additional protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 (n 39) para 2218.
[186] International Law Association Study Group on the Conduct of Hostilities in the 21st Century 'The Conduct of Hostilities and International Humanitarian Law: Challenges of 21st Century Warfare' (2017) 78 International Law Studies 322 p. 343.
[187] M.N. Schmitt 'Targeting in Operational Law' in T.D. Gill and D. Fleck (eds), *The Handbook of the International Law of Military Operations* (2nd ed, OUP 2015) p. 278-279.
[188] ICRC Customary International Humanitarian Law Rules (n 11) p. 50.

rules of Additional Protocol I as well as customary international law. However, can all things and thereby computer data constitute an object or are objects confined by certain requirements?

According to the view expressed in the Tallinn Manual 2.0 it is vital to determine how the term object is understood.[189] The Manual references the ICRC Commentary of 1987 on Additional Protocol I which states that the word object "means something that is visible and tangible."[190] Based on this understanding of the ICRC commentary the Tallinn Manual 2.0 has concluded that data does not constitute an object in international humanitarian law and is therefore not protected by the provisions protecting civilian objects.[191] However, the matter is controversial and requires further examination to determine whether computer data constitutes an object of customary international humanitarian law in the present day context. Therefore, the following chapters are aimed at answering that question.

3.3.2. The 'object' requirement

According to the ICRC Commentary of 1987, it is apparent that the use of the word 'object' in English is traditionally conceived as something that is both visible and tangible.[192] The ICRC does this conclusion on the basis of the dictionary definition of the Oxford English Dictionary (OED) of 1970, which states that an object is "something placed before the eyes, or presented to the sight or other sense, an individual thing seen, or perceived, or that may be seen or perceived; a material thing".[193] More generally, an object is nowadays perceived as "a material thing that can be seen and touched."[194] In the equally applicable French version of the protocol the word 'biens' is used. Similarly, to the English version, 'biens' means something that is both visible and tangible. According

[189] Tallinn Manual 2.0 (n 4) p. 437.
[190] Commentary on the additional protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 (n 39) para 2007-2008; also se Tallinn Manual 2.0 (n 4) p. 437.
[191] Tallinn Manual 2.0 (n 4) p. 437.
[192] Commentary on the additional protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 (n 39) para 2008.
[193] 'object, n' *The Oxford English Dictionary*, (1970) Vol. VII, p. 14.
[194] 'object, n' (OED Online, OUP June 2021) <https://www.oed.com/view/Entry/129613?> accessed 7 June 2021.

to the commentary both the English and French versions refer to something that is both visible and tangible.[195]

When it comes to military objectives, the 1967 ICRC Commentary on Additional Protocol I states that the use of the word objective is an abbreviation of the expression: objective point.[196] Again quoting the dictionary definition of the Oxford English Dictionary of 1970, the Commentary considers that an objective point is "the point towards which the advance of troops is directed; hence, [...] the point aimed at".[197] The same goes for the French versions 'objectif' which in large is similar to the word used in the English version and both versions intended both tangible and visible things in their own language. One clear difference is however pointed out by the ICRC Commentary. The French dictionary definition's extended meaning of the word 'objectif', includes that an objective could also be a general objective of an operation or rather the aim and purpose of said operation. Therefore, the extended definition has been excluded by the Commentary. This statement also follows the requirement of tangibility and visibility of an object that the ICRC stated in the Commentary as discussed above. [198]

Some scholars have criticized the view adopted by the Tallinn Manual 2.0 especially with regards to data. For instance, Dinniss has argued that the ICRC 1987 Additional Protocols Commentary on Article 52 of Additional Protocol I, does not require an object to be material per se.[199] Since the definition of the term 'object' referred to is a dictionary definition and not a definition agreed upon at either the working committees or the Diplomatic Conference[200] Dinniss argues that the tangibility requirement set out by the ICRC is therefore rather made as a distinction between different kinds of 'objects'. The fact that the dictionary definitions require something to be material to be an object does not mean that the Additional Protocol I does. In other words, this distinction is made to

[195] Commentary on the additional protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 (n 39) paras 2007-2008.
[196] Commentary on the additional protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 (n 39) para 2009.
[197] 'object, n' *The Oxford English Dictionary*, (1970) Vol. VII, p. 17.
[198] Commentary on the additional protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 (n 39) paras 2008–2010.
[199] Dinniss (n 73) p. 43.
[200] Commentary on the additional protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, (1987) para 2010.

separate between objects as things rather than as an exclusion of an intangible object from the definition of an object.[201] Considering that the Geneva Conventions and their additional protocols are based on the distinction between civilian and military as well as an equally important distinction between people and things, especially with regards to the treatment of both in different situations. Dinniss argues that setting aside any materiality requirement of an object, made by the dictionary definitions, data would qualify as a thing and not as a person. While data lacks a material component it is perceivable by the senses in particular sight, and therefore 'visible'.[202]

3.3.3. Interpretation and International Customary Law

Although the Vienna Convention on the Law of Treaties does not apply to the interpretation of international customary law, the customary rule in question is identical to that of Additional Protocol I Article 52(2).[203] However, it is not uncommon that a customary norm exists both in treaty law as well as in customary law, as stated in Article 38 of the Vienna Convention on the Law of Treaties.[204] As observed by Merkouris, the case law of various international courts suggest that there indeed are rules guiding the identification of customary law.[205] For instance, in the *Nicaragua* case, the ICJ held that "rules which are identical in treaty law and in customary international law are also distinguishable by reference to the methods of interpretation and application."[206] Further, in a similar notion, Judge Tanaka stated in the *North Sea Continental Shelf* case that "[t]he method of logical and teleological interpretation can be applied in the case of customary law as in the case of written law."[207]

Therefore, recognized rules of treaty interpretation can be employed to understand the meaning of the word object. This was the approach used by the experts of the Tallinn

[201] Dinniss (n 73) p. 43.
[202] Dinniss (n 73) p. 43–44.
[203] Vienna Convention on the Law of Treaties (n 28) art. 1(1).
[204] Vienna Convention on the Law of Treaties (n 28) art. 38.
[205] Panos Merkouris 'Interpreting the Customary Rules on Interpretation' (2017) 19 International Community Law Review 126 p. 140-142.
[206] Military and Paramilitary Activities in and against Nicaragua (Merits) (Nicaragua v. United States of America), Judgment, ICJ Reports 1986, para. 178.
[207] North Sea Continental Shelf cases (Federal Republic of Germany v Netherlands and Denmark) Judgment 'Dissenting Opinion of Judge Tanaka' [1969] ICJ Rep 3 p. 182.

Manual 2.0 while interpreting this customary rule defining military objectives, as seen by the references to Article 31(1) of the Vienna Convention on the Law of Treaties when interpreting the ordinary meaning of this customary rule.[208] According to the general rule of treaty interpretation of the Vienna Convention on the Law of Treaties, Article 31(1) 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."[209]

In other words, a treaty, and in this case its formation in customary international law, should be interpreted textually, contextually and teleologically.[210] With regards to the use of the word "object" scholars have argued that the drafters of Additional Protocol I could not have been able to perceive the development of technology and how vital computers would be in the present-day context. Therfore, Dinnis argues that the distinction between objects and non-objects should not be based on materiality but between things and people. And if data is not considered as an object, the conclusion would be contrary to the object and purpose of Additional Protocol I,[211] which is to allow for military necessity while affording effective protection to civilians.[212]

Similarly, Mačák argues that pursuant to Judge Tanaka's statement in the *North Sea Continental Shelf* case, the term object should be interpreted in light of its present day meaning.[213] In the *Dispute Regarding Navigational and Related Rights* case the ICJ held that:

"Where the parties have used generic terms in a treaty, the parties necessarily having been aware that the meaning of the terms was likely to evolve over time, and where the treaty has been entered into for a very long period or is "of continuing duration", the parties

[208] Kubo Mačák, 'Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law' (2015) 48 Isr L Rev 55, p. 66; For the conclusion of the Tallinn Manual se Tallinn Manual 2.0 (n 4) p. 437.
[209] Vienna Convention on the Law of Treaties (n 28) art. 31(1).
[210] Jean-Marc Sorel and Valerie Bore-Eveno 'Article 31' in Olivier Cortenand Pierre Klein (eds), *The Vienna Conventions on the Law of Treaties: A Commentary* (Oxford University Press 2011) p. 804, 808.
[211] Dinniss (n 73) p. 44.
[212] Gisel, Rodenhäuser and Dörmann (n 3) p. 298.
[213] Mačák (n 208) p. 70-71.

must be presumed, as a general rule, to have intended those terms to have an evolving meaning"[214]

Since Additional Protocol I fulfills the requirements set out by the ICJ, the evolved meaning must be considered.[215] According to the OED, the word object in technical use is defined as "the thing or body observed with an optical instrument; (also) the thing of which an image is produced by drawing or draughtsmanship."[216] And with regards to computing "[a] distinct (or discrete) entity, as (a) a package of information (as a data structure definition) together with a description of its manipulation; (b) a single graphic image, or the data that produces such an image."[217] Some courts have taken an evolutionary approach to interpretation. For instance, the Israeli Supreme Court held in 2006 that "new reality at times requires new interpretation. Rules developed against the background of a reality which has changed must take on a dynamic interpretation which adapts them, in the framework of accepted interpretation-al rules, to the new reality."[218]

Vienna Convention on the Law of Treaties Article 32 addresses Supplementary means of interpretation. According to the Article the preparatory work of the treaty and the circumstances of its conclusion can be used in order to confirm the meaning of a provision remains "ambiguous or obscure."[219] The provision is significant for interpreting the use of the word object, since, according to Schmitt, the ICRC 1987 Commentary on the Additional Protocol I reference to "visible and tangible"[220] is precisely a clarification of how the word object should be understood.[221] Against this backdrop and that of state practice, the Tallinn Manual 2.0 adopted a view which considered that data did not suffice as an object of international humanitarian law. However, since international customary

---

[214] Dispute regarding Navigational and Related Rights (Costa Rica v Nicaragua) (Judgment) [2009] ICJ Rep 213 para 66.
[215] Mačák (n 208) p. 70-71.
[216] 'object, n' (OED Online, OUP June 2021) <https://www.oed.com/view/Entry/129613?> accessed 7 June 2021.
[217] 'object, n' (OED Online, OUP June 2021) <https://www.oed.com/view/Entry/129613?> accessed 7 June 2021.
[218] HCJ 769/02, *Public Committee Against Torture in Israel and Palestinian Society for the Protection of Human Rights and the Environment v Israel and Others* ILDC 597 (IL 2006) [2006], para 28.
[219] Vienna Convention on the Law of Treaties (n 28) art. 32.
[220] Commentary on the additional protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 (n 39) para 2008.
[221] Michael N Schmitt 'The Notion of 'Objects' During Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision' (2015) 48 Israel Law Review 81 p. 88-89.

law can change, the following section will deal with current state practice to determine if data can be considered an object *lex lata*.

3.3.4. State practice

3.3.4.1 Usus

Recalling the fact that the definition of military objectives, pursuant to Article 52(2) is considered international customary law, whether during an international armed conflict or a non-international armed conflict,[222] one of the requirements of customary law is *usus* or state practice. As stated by the ICJ in the *Continental Shelf* case of 1985: "It is of course axiomatic that the material of customary international law is to be looked for primarily in the actual practice and opinio juris of States."[223] This section will in turn look at the practice of States, since if practice has changed so can the rules of customary law also.

3.3.4.2 State positions submitted to the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security

Pursuant to Resolution A/76/135 of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, several states participated in the call to contribute their views on how international humanitarian law applies to the use of state cyber capabilities or ICTs.[224] In addition, several states have issued state position papers on how they view international law in the cyber context.

Of the fifteen states answering the call of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, three States expressed a position with regards to data as an object of

[222] ICRC Customary International Humanitarian Law Rules (n 11) p. 25.
[223] International Court of Justice, *Continental Shelf case* (Libyan Arab Jamahiriya v. Malta) (Judgment) [1985], ICJ Reports 1985 para 27.
[224] UNGA 'Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266' (13 July 2021) UN Doc A/76/136* para 2.

international humanitarian law. The first of the three countries, the government of Brazil, did not take a distinct position on the issue, merely raising that whether civilian data should be regarded as an object, is one of many issues with regard to the cyber context.[225]

Similarly, the second country Switzerland, does not exactly tackle the issue either, whether data is an object or not and therefore afforded protection. On the other hand, the government of Switzerland raises the challenging question of how data should be protected in absence of physical damage which would engage the prohibition of attack.[226] A question which would only be relevant if data would be considered as an object and protected by the first paragraph of Article 52 of Additional Protocol I.[227] Additionally, the State of Switzerland proceeds by considering the fact that "the obligation to take all precautionary measures practically possible to spare civilians and civilian objects plays a particularly important role in the use of cyber means and methods of warfare."[228]

In a similar manner as Brazil, the third of the countries, Romania touches upon the ongoing discussion of data as a civilian object. Surprisingly however, the Government of Romania takes an interesting approach, stating that since the discussion is ongoing Romani adopts "the preliminary view that cyber operations against data do trigger the application of international humanitarian law. Therefore, cyber-attacks can only be directed against those data that represent military objectives according to international

[225] UNGA 'Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266' (13 July 2021) UN Doc A/76/136* p. 23.
[226] UNGA 'Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266' (13 July 2021) UN Doc A/76/136* p. 94.
[227] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Protocol I) art. 52(1).
[228] UNGA 'Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266' (13 July 2021) UN Doc A/76/136* p. 94.

humanitarian law and cannot be directed against those data that represent a civilian object which must be protected under the principle of distinction."[229]

3.3.4.3. The French Government

The French Government was one of the first States to state in a publicly released position paper a view on whether data should qualify as an object. The position paper, entitled "International Law Applied to Operations in Cyberspace, contains a similar reasoning as the Romanian Government held in 2021, as discussed above. France takes a position which is contrary to the conclusion reached by the majority of experts of the Tallinn Manual 2.0,[230] stating that: "Although intangible, France considers that civilian content data may be deemed protected objects".[231] The argument is furthered by concluding that data cannot be excluded from being an object, especially considering the digital dependence of society since "such an interpretation would be contrary to the aim and purpose of IHL."[232]

Even though there is no direct reference to operation-level data as such, the French government addresses this issue with regards to special protection, stating that "special protection afforded to certain objects extends to systems and the data that enable them to operate."[233] Therefore, the position paper of the French government takes a rather inclusive approach, including both content-level data as well as when qualifying for special protection including also operation level data.[234] The issue of special protection of data will be further discussed in the following chapter, chapter four.

---

[229] UNGA 'Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266' (13 July 2021) UN Doc A/76/136* p. 78.
[230] "The majority of the International Group of Experts agreed that the law of armed conflict notion of 'object' is not to be interpreted as including data, at least in the current state of the law. In the view of these Experts, data is intangible and therefore neither falls within the 'ordinary meaning' of the term object, nor comports with the explanation of it offered in the ICRC Additional Protocols 1987 Commentary." Tallinn Manual 2.0 (n 4) p 437.
[231] France, 'International Law Applied to Operations in Cyberspace' (n 89) p. 15.
[232] France, 'International Law Applied to Operations in Cyberspace' (n 89) p. 15.
[233] France, 'International Law Applied to Operations in Cyberspace' (n 89) p. 15.
[234] France, 'International Law Applied to Operations in Cyberspace' (n 89) p. 15.

3.3.4.4. The Israeli Government

The Israeli Government stated their position on the application of international law in cyberspace in a speech, which was given by Dr. Roy Schöndorf, Israel's Deputy Attorney-General at the Stockton Center for International Law on December 8 of 2020. According to the transcript, the Israeli State considers that: "Objects for the purposes of LOAC have always been understood to be tangible things and this understanding is not domain-specific."[235] They therefore concluded, as the majority of the Tallinn Manual 2.0, that data does not in the current context of the law of war constitute an object.[236]

3.3.4.5. The Finnish Government

The Finnish Government issued a public position paper in 2020 which dealt with international law and cyberspace. The Finnish position does not raise the ongoing debate of whether data constitutes an object. Rather Finland has adopted the position that when planning how cyber means and methods of warfare are used, both their direct and indirect effects shall be accounted for.[237] As other States have held this does not encompass civilian data because it does not fall within the protection of civilian objects. However, the Finnish State position goes on to state that: "Constant care shall be taken to ensure the protection of civilians and civilian objects, including essential civilian infrastructure, civilian services and civilian data."[238]

3.3.4.6. The Federal Government of Germany

The Federal Government of Germany issued their public position paper in early 2021. Generally, it accepts the applicability of international humanitarian law to cyberspace and defines when a cyber operation amounts to a cyber attack. The German paper does not

[235] Roy Schöndorf 'Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations' (2021) 97 International Law Studies 395 p. 401; LOAC = Law of Armed Conflict).
[236] Roy Schöndorf 'Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations' (2021) 97 International Law Studies 395 p. 401.
[237] Ministry for Foreign Affairs 'International law and cyberspace Finland's national positions' (n 90) p. 7.
[238] Ministry for Foreign Affairs 'International law and cyberspace Finland's national positions' (n 90) p. 7.

directly deal with the issue of data as a civilian object of international humanitarian law.[239] However, in defining an attack the paper states that:

"Germany defines a cyber attack in the context of IHL as an act or action initiated in or through cyberspace to cause harmful effects on communication, information or other electronic systems, on the *information that is stored, processed or transmitted* on these systems or on physical objects or persons."[240]

Additionally, the position paper goes on to state that the Federal Government of Germany does require a cyber attack to be violent as regarded in Additional Protocol I Article 49(1). Considering these notions, the position paper seems to adopt the same view as that of the French government, something that becomes even more obvious as the paper takes the view that 'data stocks' can be considered a potential civilian object.[241]

3.3.4.7. Organization of American States

The Inter-American Juridical Committee of the Organization of American States (OAS) has published a report which states the practice and conviction of how international law should be applied to cyberspace according to the following states: Bolivia, Brazil, Chile, Costa Rica, Ecuador, Guatemala, Guyana, Peru, and the United States.[242] According to the report, which was published in November 2020, none of the states was of the view that "civilian data is directly subject to the principle of distinction in armed conflict."[243] Regardless, Chile considered that the principle of distinction should be considered when

[239] Federal Foreign Office 'On the Application of International Law in Cyberspace: Position Paper (2021) <https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf> accessed 14 March 2022, p. 8.
[240] Federal Foreign Office 'On the Application of International Law in Cyberspace: Position Paper (2021) <https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf> accessed 14 March 2022, p. 8 emphasis added.
[241] Federal Foreign Office 'On the Application of International Law in Cyberspace: Position Paper (2021) <https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf> accessed 14 March 2022, p. 8.
[242] Organization of American States the Inter-American Juridical Committee 'International Law and State Cyber Operations' (2020) p. 12 para 12.
[243] Organization of American States the Inter-American Juridical Committee 'International Law and State Cyber Operations' (2020) p. 48.

cyber operations are targeting data if it could affect the civilian population.[244] Guyana adopted a similar view where states employing cyber operations should refrain from attacking data. The view adopted by Chile and Guyana therefore falls within the inclusive approach to civilian data as an object of international humanitarian law.[245]

3.3.4.8. The summarized position of states

State practice is *de facto* scarce, when it comes to public state positions on the application of international law to cyber operations. Of the reviewed state position papers, a very limited part is made with regards to data and even fewer with regards to the notion of civilian data. The positions presented in this subchapter are reflective of only a small portion of the international community. When including the states that participated in the OAS report on "International Law and State Cyber Operations", ten states have publicly stated that they do not consider data to be an object of international humanitarian law.[246] However, out of these ten, two states Chile and Guyana were of the view that the principle of distinction should be considered when attacking civilian data if it could result in negative effects on the civilian population.[247]

The position papers of Switzerland and Brazil have opened up for discussions surrounding the issues of applying international law to the notion of data as a civilian object. However, they have not divulged their official positions on the matter.[248] Of the state positions papers only the governments of Germany, Finland, France and Romania

[244] Organization of American States the Inter-American Juridical Committee 'International Law and State Cyber Operations' (2020) p. 48.
[245] Organization of American States the Inter-American Juridical Committee 'International Law and State Cyber Operations' (2020) p. 49.
[246] Organization of American States the Inter-American Juridical Committee 'International Law and State Cyber Operations' (2020) p. 48; Roy Schöndorf 'Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations' (2021) 97 International Law Studies 395 p 401; LOAC = Law of Armed Conflict).
[247] Organization of American States the Inter-American Juridical Committee 'International Law and State Cyber Operations' (2020) p. 48-49.
[248] UNGA 'Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266' (13 July 2021) UN Doc A/76/136* p. 23, 94.

have adopted a position in which the principle of distinction would require them to treat civilian computer data as a civilian object coupled with the required protection regimes.[249]

3.3.5. Conclusions: Data an object?

The object of chapter 3 has been to determine whether civilian data can be seen as an object of international humanitarian law *lex lata*. As stated by Schmitt "the line between *lex lata* and *lex ferenda* is horribly indistinct."[250] Because the issue at hand is in relation to international customary law, rather than to explicitly treaty law, the importance of official state positions has been considered, because as stated by the ICTY, when considering whether a crystallization of a customary rule of international humanitarian law has emerged "reliance must primarily be placed on such elements as official pronouncements of States, military manuals and judicial decisions."[251] For a new norm of customary international law to crystalize both sufficient state practice and *opinio juris* would be required.[252] On this matter the ICJ stated in the *North Sea Continental Shelf cases* that:

"State practice, including that of States whose interests are specially affected, should have been both extensive and virtually uniform in the sense of the provision invoked; -and should moreover have occurred in such a way as to show a general recognition that a rule of law or legal obligation is involved."[253]

---

[249] Federal Foreign Office 'On the Application of International Law in Cyberspace: Position Paper (2021) <https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf> accessed 14 March 2022, p. 8; Ministry for Foreign Affairs 'International law and cyberspace Finland's national positions' (n 90) p. 7; France, 'International Law Applied to Operations in Cyberspace' (n 89) p. 15; UNGA 'Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266' (13 July 2021) UN Doc A/76/136* p. 78.

[250] Schmitt (n 221) p. 89-90.

[251] Prosecutor v. Dusko Tadic aka "Dule" (Decision on the defence motion for interlocutory appeal on jurisdiction), No. IT-94-AR72 International Criminal Tribunal for the former Yugoslavia (2 October 1995) para 99.

[252] ICRC Customary International Humanitarian Law Rules (n 11) p. xli-xlii.

[253] North Sea Continental Shelf cases (Federal Republic of Germany v Netherlands and Denmark) Judgment [1969] ICJ Rep 3 para 74.

To date, only a handful of states have explicitly stated their positions regarding their understanding of how the rules of international humanitarian law pertain to data in relation to the term object. In the practice of only a few states data does constitute an object of international humanitarian law, however most states have not openly divulged their view on the matter.[254] Considering that it is essentially up to states to determine how the rules of customary international law develop, the ICRC has called on states to take clear positions on how international humanitarian law protects civilian data.[255] However as stated by Schmitt "there is **some** state practice and/*opinio juris*, but not enough to definitively conclude that a new norm has emerged."[256]

Does this mean civilian computer data can be attacked and exploited in any way? As discussed above, the principle of distinction affords protection from military operations amounting to an attack. By the doctrine adopted in chapter 2.5. that considers the violent consequences of an attack rather than the violence of an act, any military operation that has violent consequences qualifies as an attack. Therefore, if a military operation against civilian data is bound to have a violent consequence against a civilian person or civilian object then that operation constitutes an attack and is therefore prohibited.[257]

Even if the data is the intended target, whether or not it is an object of international humanitarian law is irrelevant. Since any "cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects"[258] constitutes a cyber attack. Therefore, attacking civilian data can in some cases be prohibited, because of the consequences that attacking said data would have on civilians and/or civilian objects that are protected.[259] Considering the notion that attacking some data can be prohibited, the next chapter will focus on determining whether

[254] Pomson Ori " 'Objects'? The Legal Status of Computer Data under International Humanitarian Law" (2021) p. 25-26.
[255] International Committee of the Red Cross 'International Humanitarian Law and Cyber Operations during Armed Conflicts: ICRC position paper' (2015) p. 8.
[256] Schmitt (n 221) p. 92 (emphasis added).
[257] Solis GD (n 111) p. 538; Schmitt (n 107) p. 93.
89 p. 93: Tallinn Manual 2.0 (n 4) p. 415-416.
[258] Tallinn Manual 2.0 (n 4) p. 415 rule 92.
[259] Solis GD (n 111) p. 538.

special protection of international humanitarian law can afford civilian data protection from attack in armed conflict.

4. Civilian data protected from attack through possible special protection

4.1. Special protection of international humanitarian law

The ICRC stated in its 2015 position paper on International Humanitarian Law and Cyber Operations during Armed Conflicts, that civilian data should be protected since "medical data, biometric data, social security data, tax records, bank accounts, companies' client files or election lists and records – are an essential component of digitalized societies."[260] However, as shown in chapter 3, data do not *lex lata,* constitute an object of international humanitarian law at the current state of the law.[261]

Although all civilian data might not be universally protected from attacks, the law of armed conflict does, however, offer special protection to certain objects and persons.[262] In such a case when the attribution of special protection becomes relevant, the understanding of the term object is not the issue, because the activities themselves enjoy protection thereby, the data upon which such activities are dependent are protected as well.[263] Although originally stemming from treaty law, especially the 1949 Geneva Conventions and their additional protocols, many of these rules are nowadays considered customary in nature.[264] Whether such rules can offer protection to civilian data *lex lata* will be explored throughout this chapter.

4.2. Special protection afforded to medical personnel, objects and activities

One of the core imperatives of international humanitarian law is "mitigating, as far as possible, the sufferings inseparable from war."[265] Therefore, the law of armed conflict provides for an extensive protection of medical personnel, objects and activities so that

[260] International Committee of the Red Cross 'International Humanitarian Law and Cyber Operations during Armed Conflicts ICRC position paper' (2015) p. 8.
[261] Roy Schöndorf 'Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations' (2021) 97 International Law Studies 395 p 401; Pomson (n 254) p. 23; Mc Cormack (n 1) p. 240; Tallinn Manual 2.0 (n 4) p. 437.
[262] ICRC Customary International Humanitarian Law Rules (n 11) p. 79-160.
[263] Schmitt (n 221) p. 107.
[264] ICRC Customary International Humanitarian Law Rules (n 11) p. 79-160.
[265] *Final Record of the Diplomatic Conference of Geneva of 1949*, (1949) Vol. II-A p. 9.

they can diminish the suffering and misfortune of the civilian population. The rules for protection are found both in written treaty law as well as in customary international law.[266]

For instance, the first Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (First Geneva Convention) provides in Article 19 that medical units, both fixed and mobile, shall be respected and protected from attack at all times.[267] Additionally, the special protection afforded to medical services also encompasses civilian hospitals as provided by Article 18 of the Convention Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention).[268] Subsequently the Geneva Conventions provide further protection in all circumstances for all kinds of medical activities civilian and military alike.[269] The protection of civilian medical personnel was expanded in Additional Protocol I Article 15,[270] which has gained support in state practice also among States not party to the Protocol.[271] With regard to non-international armed conflict, common Article 3 of the 1949 Geneva Conventions requires that the wounded and sick be cared for,[272] therefore protection of medical personnel and activities is a requirement of the rule.[273] In addition, Additional Protocol II

[266] Kubo Mačák, Laurent Gisel and Tilman Rodenhäuser 'Cyber Attacks against Hospitals and the COVID-19 Pandemic: How Strong are International Law Protections?' (Just Security, 21 March 2020) <https://www.justsecurity.org/69407/cyber-attacks-against-hospitals-and-the-covid-19-pandemic-how-strong-are-international-law-protections/> accessed 16 February 2022.
[267] Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (adopted 12 August 1949, entered into force 05 October 1950) 75 UNTS 31 (First Geneva Convention) art. 19.
[268] Geneva Convention Relative to the Protection of Civilian Persons in Time of War (adopted 12 August 1949, entered into force 05 October 1950) 75 UNTS 287 (Fourth Geneva Convention) art. 18.
[269] For more details see: Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (adopted 12 August 1949, entered into force 05 October 1950) 75 UNTS 31 (First Geneva Convention) art. 24-26; Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (adopted 12 August 1949, entered into force 05 October 1950) 75 UNTS 85 (Second Geneva Convention) art. 12, 36; Geneva Convention Relative to the Protection of Civilian Persons in Time of War (adopted 12 August 1949, entered into force 05 October 1950) 75 UNTS 287 (Fourth Geneva Convention) art. 20.
[270] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Protocol I) art. 15.
[271] ICRC Customary International Humanitarian Law Rules (n 11) p. 79.
[272] Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (adopted 12 August 1949, entered into force 05 October 1950) 75 UNTS 31 (First Geneva Convention) art. 3.
[273] ICRC Customary International Humanitarian Law Rules (n 11) p. 80.

sets out the protection of medical personnel in non-international armed conflicts.[274] The special protection of medical personnel, objects and activities is considered customary international law in both international armed conflict and non-international armed conflict.[275]

Since medical activities as such fall under special protection, data used by the same medical activities would also be protected under the same special protection. In other words, all data that is personal medical files, both content- and operational-level data required to operate medical equipment and programs would be protected against attack or any operation that would negatively affect medical activities.[276] The obligation to respect, prohibits manipulation of data since such actions could cause irreparable damage or suffering to persons as well as render the activities of medical units more difficult.[277] The same view is held by the ICRC, considering that the obligations to respect and protect medical facilities, encompassed in the 1949 Geneva Conventions and customary international law, must be understood as extending to medical data whether an object of international humanitarian law or not.[278]

State position papers such as that of the French government have stated that: "Cyberoperations must also take into account the special protection of certain objects, such as medical units…This protection extends to ICT equipment and services and to the data needed to operate them, such as medical data linked to the operation of a hospital."[279] Furthermore, the view of the French government is also that the systems and data needed to operate the systems are protected by the special protection.[280] Scholars have also

[274] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 609 art. 9(1).
[275] ICRC Customary International Humanitarian Law Rules (n 11) rule 25, 28-30.
[276] Tallinn Manual 2.0 (n 4) p. 515.
[277] Dörmann K, 'Applicability of the Additional Protocols to Computer Network Attacks' (2004) (Paper delivered at the International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Stockholm, Nov. 17–19, 2004 p. 7.
[278] International Committee of The Red Cross, 'International humanitarian law and the challenges of contemporary armed conflicts' (2015) 32IC/15/11 p. 43.
[279] France, 'International Law Applied to Operations in Cyberspace' (n 89) p. 14-15.
[280] France, 'International Law Applied to Operations in Cyberspace' (n 89) p. 15.

recognized the fact that attacks and operations against medical data stored in hospital networks are prohibited.[281]

The special protection afforded to medical activities ceases only if they commit actions that fall outside their humanitarian obligations or act harmfully against an adversary of the ongoing conflict according to the rules set forward in the 1949 Geneva Conventions and their additional protocols.[282]

4.3. Objects indispensable to the survival of the civilian population

The protection of objects indispensable to the survival of the civilian population stems from the general prohibition on attacking civilian objects in Article 52(1) of Additional Protocol I, as shown above the prohibition forms customary law as well.[283] Additionally, a more specific prohibition is set out in Additional Protocol I Article 54(2), which states that it is prohibited to attack, destroy or render useless objects which are indispensable for the survival of the civilian population.[284] The objects in question are regarded as "objects for subsistence"[285] including, *inter alia*, "agricultural areas for the production of

[281] International Law Association Study Group on the Conduct of Hostilities in the 21st Century 'The Conduct of Hostilities and International Humanitarian Law: Challenges of 21st Century Warfare' (2017) 78 International Law Studies 322 p. 340.
[282] Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (adopted 12 August 1949, entered into force 05 October 1950) 75 UNTS 31 (First Geneva Convention) art. 21, 22; Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (adopted 12 August 1949, entered into force 05 October 1950) 75 UNTS 85 (Second Geneva Convention) art. 34, 35; Geneva Convention Relative to the Protection of Civilian Persons in Time of War (adopted 12 August 1949, entered into force 05 October 1950) 75 UNTS 287 (Fourth Geneva Convention) art. 19; Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Protocol I) art. 13; Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 609 art. 11(2).
[283] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Protocol I) art. 52(1); ICRC Customary International Humanitarian Law Rules (n 11) rule 9.
[284] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Protocol I) art. 54(2).
[285] Commentary on the additional protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 (n 39) para 2103.

foodstuffs, drinking water installations and supplies, and crops."[286] With regards to foodstuffs, Article 54(1) states that using starvation as a means of warfare is prohibited,[287] thereby extending the protection to virtually encompass anything in the food producing industries.[288] Several military manuals of states provide for this protection of objects indispensable to the survival of the civilian population,[289] and the Rome Statute of the ICC labels the deprivation of these objects a war crime.[290] In the case of a non-international armed conflict, Additional Protocol II Article 14 provides virtually the same protections as Additional Protocol I.[291] Additionally, there exists no state practice to counter this rule.[292] The prohibition to attack, destroy, remove or render useless objects indispensable to the survival of the civilian population constitutes international customary law in both international armed conflicts and non-international armed conflicts.[293]

State positions by Norway and France have shown that any operation, whether cyber or kinetic, denying the use of objects indispensable to the survival of the civilian population is prohibited.[294] Therefore the protection also covers content- and operational-level data needed for the functioning of these objects, whether data constitutes an object or not is irrelevant.[295]

---

[286] Commentary on the additional protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 (n 39) para 2102.
[287] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Protocol I) art. 54(1).
[288] Harrison Dinniss H, *Cyber Warfare and the Laws of War* (Cambridge University Press 2012) p. 243-244.
[289] ICRC Customary International Humanitarian Law Rules (n 11) p. 190.
[290] Rome Statute of the International Criminal Court (adopted 17 July 1998, entered into force 1 July 2002) Art. 8(2)(b)(xxiv).
[291] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 609 (Protocol II) art. 14.
[292] ICRC Customary International Humanitarian Law Rules (n 11) p. 191.
[293] ICRC Customary International Humanitarian Law Rules (n 11) p. 191; Tallinn Manual 2.0 (n 4) p. 532.
[294] UNGA 'Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266' (13 July 2021) UN Doc A/76/136* p. 74; France, 'International Law Applied to Operations in Cyberspace' (n 89) p. 14-15.
[295] Schmitt (n 221) p. 107.

4.4. Works and installations containing dangerous forces

Works and installations containing dangerous forces are subject to special protection in treaty law and international customary law. In treaty law, the special protection is enshrined with regards to international armed conflict in Additional Protocol I Article 56,[296] and for non-international armed conflict in Additional Protocol II Article 15.[297] In treaty law, the works and installations such as dams, dykes and nuclear electrical generating stations shall not be the object of attack whether a military objective or not.[298] In customary law, the rule does not cover the same level of protection. According to Customary law, particular care must be taken when planning and executing attacks, if works or installations containing dangerous forces are the target of attack or in the vicinity of an attack, to avoid the release of dangerous forces. According to the ICRC study on customary law, this customary norm is not only limited to the listed works or installations, other installations such as chemical treatment centers are also included.[299] However, it is not clear that the duty to take particular care is imposed on other works or installations containing dangerous forces. For instance, the ICRC 1987 Commentary on the additional protocols suggests that although the list of objects is only illustrative, consensus could only be found once Article 56 was limited to dams, dykes and nuclear electrical generating stations.[300] The Tallinn Manual 2.0 has taken the view that other works or installations are not covered by customary law.[301] The scope of protection is widely covered in several state's military manuals. In addition, numerous states have incorporated attacks against works or installations containing dangerous forces as an

[296] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Protocol I) art. 56.
[297] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 609 (Protocol II) art. 15.
[298] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Protocol I) art. 56; Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 609 (Protocol II) art. 15.
[299] ICRC Customary International Humanitarian Law Rules (n 11) p. 139-140.
[300] Commentary on the additional protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 (n 39) paras 2147-2150.
[301] Tallinn Manual 2.0 (n 4) p. 530-531.

offense in domestic legislation. This customary rule is applicable in both international armed conflict and non-international armed conflict.[302]

Data of civilian works and installations containing dangerous forces is protected from attack at all times for those states that are party to Additional Protocol I respectively Additional Protocol II. This protection extends to data even when it is considered a military objective.[303] The customary protection of data is not absolute since customary law only requires that special care is taken when attacking works or installations containing dangerous forces.[304] Although data which is required for works or installations containing dangerous forces is considered to enjoy the same special protection that the protection of the objects themselves enjoy, the special protection is dependent on individual state obligations in this case.[305]

4.5. Cultural property

Cultural property enjoys a wide range of protections, from different legal sources. First and foremost, the 1954 Convention for the Protection of Cultural Property in the Event of Armed Conflict affords protection to cultural property pursuant to the following definition "movable or immovable property of great importance to the cultural heritage of every people."[306] The convention requires parties to respect and protect cultural property in order to safeguard cultural property in the event of an armed conflict, a requirement that can only be waived by imperative military necessity.[307] The Convention is applicable both in international armed conflict and non-international armed conflict and

[302] ICRC Customary International Humanitarian Law Rules (n 11) p. 139-140.
[303] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Protocol I) art. 56; Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 609 (Protocol II) art. 15.
[304] ICRC Customary International Humanitarian Law Rules (n 11) p. 139-140.
[305] Schmitt (n 221) p. 107; France, 'International Law Applied to Operations in Cyberspace' (n 89) p. 14-15.
[306] Hague Convention for the protection of Cultural Property in the Event of Armed Conflict with Regulations for the Execution of the Convention (14 May 1954) 249 UNTS 240, art. 1(a).
[307] Hague Convention for the protection of Cultural Property in the Event of Armed Conflict with Regulations for the Execution of the Convention (14 May 1954) 249 UNTS 240, art. 4.

binding upon 133 State parties, at the time of writing.[308] The principles of the convention are considered customary law in international armed conflict[309] and the customary applicability of the rule to non-international armed conflicts was recognized by the ICTY in the *Tadić case*.[310]

Secondly, according to the Rome Statute of the ICC, intentionally attacking buildings dedicated to religion, education, art, science or charitable purposes as well as historic monuments, constitutes war crimes under international customary law.[311] The obligation to refrain from damaging buildings dedicated to religion, art, science, education or charitable purposes and historic monuments is also evident in state practice, which is well established throughout numerous state military manuals as well as official statements of states.[312]

Thirdly the Hague Regulations Article 56 states that "institutions dedicated to religion, charity and education, the arts and sciences, even when State property, shall be treated as private property. All seizure of, destruction or willful damage done to institutions of this character, historic monuments, works of art and science, is forbidden.[313] International courts have also reinforced the protection of cultural property with the ICTY including a similar prohibition in its statute under violations of the laws and customs of war.[314] All of the above listed rules are considered customary international law and applicable in both international armed conflict and non-international armed conflict.[315]

---

[308] Hague Convention for the protection of Cultural Property in the Event of Armed Conflict with Regulations for the Execution of the Convention (14 May 1954) 249 UNTS 240, art. 18-19.
[309] ICRC Customary International Humanitarian Law Rules (n 11) p. 129.
[310] Prosecutor v. Dusko Tadic aka "Dule" (Decision on the defence motion for interlocutory appeal on jurisdiction), No. IT-94-AR72 International Criminal Tribunal for the former Yugoslavia (2 October 1995) para 98, 127.
[311] Rome Statute of the International Criminal Court (adopted 17 July 1998, entered into force 1 July 2002) Art. 8(2)(b)(ix).
[312] ICRC Customary International Humanitarian Law Rules (n 11) p. 127-128.
[313] Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land The Hague 18 October 1907 (adopted 18 October 1907, entered into force 26 January 1910) art. 56.
[314] UN Security Council, Statute of the International Criminal Tribunal for the Former Yugoslavia (as amended on 17 May 2002), 25 May 1993 Art. 3(d).
[315] ICRC Customary International Humanitarian Law Rules (n 11) p. 127-129, 132-135.

The special protections of cultural property in international customary law, listed above, protects civilian data extensively. Military cyber operations are required to refrain from damaging data that in turn would damage buildings dedicated to religion, education, art, science or charitable purposes as well as historic monuments.[316] The protection also extends to the arts which through the development of technology has become digitized and nowadays form a significant part of culture. Considering the definition of the cultural property as something movable or immovable, the data used by software to render such art is also protected by the requirement to protect and respect cultural property. In practical terms, a digital copy of Leonardo da Vinci's Mona Lisa could become protected by the special protection of cultural property although it was a civilian computer object. This does however require that the number of copies that can be made of said object is limited and even, in some cases, that the original work of artr is inaccessible or destroyed.[317] Similarly, the same protection extends to any digital document that is of "great importance to the cultural heritage of every people"[318] a notion that includes for example demographic data collected by the government.[319]

4.6. The natural environment

The natural environment is one of the objects that is afforded special protection through international law. General protection is afforded by the fact that the natural environment constitutes a civilian object. The destruction of the natural environment is prohibited as long as the object of attack does not constitute a military objective.[320] In international case law, the ICJ stated in the 1996 *Nuclear Weapons case* that: "Respect for the environment is one of the elements that go to assessing whether an action is in conformity with the principle of necessit".[321] Similarly the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia, held, with regards to the environmental impact of the NATO bombings, was best evaluated against the

[316] Schmitt (n 221) p. 107; France, 'International Law Applied to Operations in Cyberspace' (n 89) p. 14-15; ICRC Customary International Humanitarian Law Rules (n 11) p. 127-128.
[317] Tallinn Manual 2.0 (n 4) p. 534.
[318] Hague Convention for the protection of Cultural Property in the Event of Armed Conflict with Regulations for the Execution of the Convention (14 May 1954) 249 UNTS 240, art. 1(a)
[319] Dinniss (n 73) p. 41.
[320] ICRC Customary International Humanitarian Law Rules (n 11) p. 143-144.
[321] *Legality of the Threat or Use of Nuclear Weapons* Advisory Opinion (n 7) para 30.

"underlying principles of the law of armed conflicts such as necessity and proportionality".[322] This rule is considered to reflect customary international law in international armed conflict, which is strongly reflected by both state practice as well as official statements of States.[323]

The protection of data on the basis of the special protection afforded to the natural environment cannot be directly afforded to data, because data does not constitute of the natural environment, however special protection can be afforded consequentially. It is therefore considered that "the destruction of the natural environment carried out wantonly is prohibited. 'Wanton' means that the destruction is the consequence of a deliberate action taken maliciously, that is, the action cannot be justified as militarily necessary.[324] Damaging or altering data through military cyber operations that could lead to the destruction of the natural environment is therefore also prohibited in international armed conflict.[325]

Pursuant to treaty law, State Parties to Additional Protocol I are required to afford the natural environment with enhanced protection. According to Article 35, State Parties are prohibited to employ such cyber operations that "intended, or may be expected, to cause widespread, long-term and severe damage to the natural environment."[326] According to the ICRC customary international humanitarian law study, this rule is considered to be a customary norm in international armed conflict. However, as shown by the commentary of the customary international humanitarian law study, the customary status of this rule is not unchallenged.[327] For instance, the Tallinn Manual 2.0 refused to adopt this rule as a customary norm of international law.[328]

---

[322] International Criminal Tribunal for the former Yugoslavia 'Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia' (2000) para 15.
[323] ICRC Customary International Humanitarian Law Rules (n 11) p. 143-144; Tallinn Manual 2.0 (n 4) p. 537-538.
[324] Tallinn Manual 2.0 (n 4) p. 538.
[325] Tallinn Manual 2.0 (n 4) p. 537-538; ICRC Customary International Humanitarian Law Rules (n 11) p. 143-144.
[326] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Protocol I) art. 35(3).
[327] ICRC Customary International Humanitarian Law Rules (n 11) p. 151-153.
[328] Tallinn Manual 2.0 (n 4) p. 537.

Whether the status of this rule falls within the sphere of customary international law is outside the scope of this thesis. However, the additional protection afforded by Additional Protocol I simply enhances the more general protection discussed above. Since it would be prohibited to attack data, although constituting a military objective, if the intended or expected consequence of the attack would cause widespread, long-term and severe damage to the natural environment.[329] State parties to Additional Protocol I will have to consider this protection when planning their military cyber operations.[330]

4.7. Humanitarian relief operations

Apart from the general protection of civilians,[331] humanitarian relief operations are protected by special protection in international humanitarian law. More specifically, the Fourth Geneva Convention requires that States party to the international armed conflict guarantee the protection of humanitarian relief operations.[332] The same obligation is further set forth in Additional Protocol I stating that: "The Parties to the conflict shall protect relief consignments and facilitate their rapid distribution."[333]

In non-international armed conflict, Article 18(2) of Additional Protocol II requires that relief operations shall be organized with consent of the parties to the conflict.[334] Although it is not specifically required that these humanitarian activities are protected and respected it is a prerequisite for humanitarian assistance. According to the Rome Statute of the ICC, applicable in both international armed conflict and non-international armed conflict, it is

[329] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Protocol I) art. 35(3); Tallinn Manual 2.0 (n 4) p. 537.
[330] France, 'International Law Applied to Operations in Cyberspace' (n 89) p. 14-15.
[331] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Protocol I) art. 48, 52(1).
[332] Geneva Convention Relative to the Protection of Civilian Persons in Time of War (adopted 12 August 1949, entered into force 05 October 1950) 75 UNTS 287 (Fourth Geneva Convention) art. 59.
[333] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Protocol I) art. 70(4).
[334] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 609 (Protocol II) art. 18(2).

prohibited and considered a war crime to "intentionally direct attacks against personnel, installations, material, units or vehicles involved in a humanitarian assistance or peacekeeping mission in accordance with the Charter of the United Nation".[335] The same view was adopted in the Statute of the Special Court for Sierra Leone[336] as well as by several resolutions of the UN Security Council with regards to conflicts in Angola, Liberia and Rwanda.[337] The special protection of humanitarian relief operations is considered customary international law in international armed conflict and non-international armed conflict.[338]

Since humanitarian relief operations require the consent of the parties to the conflict, military cyber operations against data of the humanitarian relief operations can be conducted as long as they do not interfere with their activities. This is pursuant to the fact that according to Article 59 of the Fourth Geneva Convention the parties to the conflict have a right to search through consignments of humanitarian relief activities.[339] However, apart from that right to search through consignments, the data of humanitarian relief operations is protected to the same extent as the rest of the operation.[340]

4.8. Journalists

In international humanitarian law, civilian journalists are protected pursuant to Article 79 of Additional Protocol I as civilians. The protocol requires that journalists are protected from attack,[341] which is also considered to be customary humanitarian law in international

---

[335] Rome Statute of the International Criminal Court (adopted 17 July 1998, entered into force 1 July 2002) Art. 8(2)(b)(iii).
[336] UN Security Council, Statute of the Special Court for Sierra Leone (2002) art. 4(b).
[337] UN Security Council, Resolution 918 (17 May 1994) UN Doc. S/RES/918, para. 10; UN Security Council, Resolution 925 (8 June 1994) UN Doc. S/RES/925, para. 11; UN Security Council, Resolution 950 (21 October 1994) UN Doc. S/RES/950, para. 10; UN Security Council, Resolution 1075 (11 October 1996) UN Doc. S/RES/1075, para. 18; UN Security Council, Resolution 1087 (11 December 1996) UN Doc. S/RES/1087, para. 16.
[338] ICRC Customary International Humanitarian Law Rules (n 11) p. 105-111.
[339] Geneva Convention Relative to the Protection of Civilian Persons in Time of War (adopted 12 August 1949, entered into force 05 October 1950) 75 UNTS 287 (Fourth Geneva Convention) art. 59; Tallinn Manual 2.0 (n 4) p. 541-542.
[340] France, 'International Law Applied to Operations in Cyberspace' (n 89) p. 14-15; Schmitt (n 221) p. 107; Tilman Rodenhäuser 'Hacking Humanitarians? IHL and the protection of humanitarian organizations against cyber operations' (EJIL:talk, 16 March 2020) <www.ejiltalk.org/hacking-humanitarians-ihl-and-the-protection-of-humanitarian-organizations-against-cyber-operations/> accessed 25.2.2022.
[341] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Protocol I) art. 79.

armed conflict.[342] For non-international armed conflict, there is no rule in Additional Protocol II containing a similar provision to that of the Additional Protocol I. However, there is a widespread practice that started before the adoption of the First Protocol which suggests that journalists are protected as civilian persons. Therefore, the ICRC customary law study found that journalists are protected as civilians in non-international armed conflict.[343]

In the ICRC customary law study, the study concluded that customary law requires journalists to be respected in addition to the requirements set out by Additional Protocol I.[344] However, the Tallinn Manual 2.0 did not go as far, considering that customary law only obligates parties to a conflict to protect journalists from attack.[345] Journalists should not be confused with war correspondents, who are separately distinguished under international humanitarian law and who accompany armed forces without being members of the armed forces following the requirements set out in Article 4(A)(4) of the Third 1949 Geneva Convention.[346]

The Tallinn Manual 2.0 adopted the view that the equipment of journalists is not entitled to special protection, and therefore a legitimate target for cyber attacks. Civilian objects used by the journalists are protected as required by the general rules of civilian protection. However, with regards to data the same reasoning follows as presented in chapter 3.3. Because the protection of journalists is based on the protection that is generally afforded to the civilian population as well as to civilian objects, the data of journalists face the same dilemma as that of ordinary civilian data, as discussed in depth throughout chapter 3. Therefore, although journalists are considered to have special protection, the protection afforded does not extend to their data since it does not constitute an object as such.[347]

---

[342] ICRC Customary International Humanitarian Law Rules (n 11) p. 115-116; Tallinn Manual 2.0 (n 4) p. 437, 527.
[343] ICRC Customary International Humanitarian Law Rules (n 11) p. 115-116; Se also Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2ed Cambridge University Press 2017) p. 526.
[344] ICRC Customary International Humanitarian Law Rules (n 11) p. 115-116.
[345] Tallinn Manual 2.0 (n 4) p. 527-528.
[346] Geneva Convention Relative to the Treatment of Prisoners of War (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 135 (Third Geneva Convention) art. 4(A)(4).
[347] Tallinn Manual 2.0 (n 4) p. 528.

The so-called special protection of journalists, at least as it is considered by the Tallinn Manual 2.0, is problematic. This is because of the obvious fact that the requirement to protect, does not afford journalists with any additional protection, as opposed to the protections afforded to the civilian population as a whole.[348] This means that special protection does not extend to the activities of journalists and therefore the computer data they may have.[349] Because, the protection of journalists data requires that data would be protected as a civilian object pursuant to the principle of distinction.

4.9. Conclusion: The special protection of data

Although data cannot, at the time of writing, be considered an object in existing law, that does not mean civilian data is without protection. The special protection regimes of international humanitarian law falling within the different categories presented throughout Chapter 4, provide enhanced protection to civilian computer data. The gist of the matter being that since the activities themselves enjoy special protection, the data used by the activities is afforded the same protection. It is therefore irrelevant whether data constitutes an object or not, because it is protected regardless.[350] Additionally, in some cases, as in the special protection of medical personnel, objects and activities, the military action employed need not rise to the level of an attack, military operations against medical activities are also prohibited and should be respected.[351] Similarly, humanitarian relief operations are protected extensively in customary international law. The computer data that is used by these activities is protected from attack and must be respected in the same regard as the operations themselves. Since the humanitarian relief operations operate by requiring consent of the parties to the conflict, it would be possible for the parties to the conflict to scour the data to check what information it holds. However, such activities can not hinder the operations of the humanitarian relief activities.[352]

---

[348] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Protocol I) art. 79(1).
[349] Tallinn Manual 2.0 (n 4) p. 528.
[350] Schmitt (n 221) p. 92.
[351] Tallinn Manual 2.0 (n 4) p. 515; International Committee of the Red Cross, 'International humanitarian law and the challenges of contemporary armed conflicts' (2015) 32IC/15/11 p. 43.
[352] Tilman Rodenhäuser 'Hacking Humanitarians? IHL and the protection of humanitarian organizations against cyber operations' (EJIL:talk, 16 March 2020) <www.ejiltalk.org/hacking-humanitarians-ihl-and-the-protection-of-humanitarian-organizations-against-cyber-operations/> accessed 25.2.2022.

The data of objects indispensable to the survival of the civilian population holds its own enhanced protection. The protection covers all content- and operational-level data that is required for the operations of such objects, since international customary law prohibits attacking, destroying, removing or rendering these objects useless.[353] Dams, dykes and nuclear electrical generating stations fall within the category of works and installations containing dangerous forces. The protection of these objects is not as substantive as that of objects indispensable to the survival of the civilian population. However, any cyber attack or operation against such objects is required to take special care in conducting the military conduct regardless of whether data is targeted or not.[354]

Civilian computer data falling within the vast definition of cultural property is extensively protected. Following the broad definition of objects which are protected as cultural property all data that either by itself falls under the requirements of cultural property or consequentially affects cultural property in a negative way is protected from attacks. The protection even covers content-level data such as demographic data and essentially any data that qualifies as being of "great importance to the cultural heritage of every people"[355]

However, the special protection regime of international humanitarian law is not perfect. Journalists that are protected from attack as civilians fall victims of the same problematic definition of objects as the rest of the civilian population. Until either the notion of how an object is perceived in international humanitarian law changes or journalists are afforded more extensive protection, they will fall victim to cyber attacks without consequence.[356] It is, therefore, important to note that the protection afforded through special protection does not provide sufficient protection of civilian computer data. Rather it should be regarded as a shortcut to protecting a small, although important part of civilian

[353] ICRC Customary International Humanitarian Law Rules (n 11) p. 189.
[354] Schmitt (n 221) p. 107; France, 'International Law Applied to Operations in Cyberspace' (n 89) p. 14-15.
[355] Hague Convention for the protection of Cultural Property in the Event of Armed Conflict with Regulations for the Execution of the Convention (14 May 1954) 249 UNTS 240, art. 1(a); Dinniss (n 73) p. 41.
[356] Tallinn Manual 2.0 (n 4) p. 528.

data. It is the view of the author that humanitarian law should develop into considering data as an object so that is would be protected, because it is an "essential component of the digital domain and a cornerstone of life in many societies".[357]

[357] International humanitarian law and the challenges of contemporary armed conflicts - recommitting to protection in armed conflict on the 70th anniversary of the geneva conventions (n 16) p. 28.

5. Conclusion

The Russian invasion and the cyber attacks that followed against the Ukrainian government in early 2022 has once again showed the destructive capabilities of cyber warfare.[358] Today data is an "essential component of the digital domain and a cornerstone of life in many societies."[359] There is however differentiating views on whether data should be considered an object of international humanitarian law and therefore protected by the principles and rules governing the conduct of hostilities.[360] Therefore this thesis has examined whether data constitutes an object of international humanitarian law and how the special protection of international humanitarian law applies to civilian data.

From a standpoint of enhanced civilian protection, it would be beneficial to consider that civilian computer data constitutes an object of international humanitarian law. However, such an inclusive approach reflects that of *de lege ferenda* and not *lex lata,* as has been shown throughout chapter 3.[361] One of the main arguments against civilian computer data constituting an object of international humanitarian law, is based on the 1987 ICRC Commentary of Additional Protocol I characterizing objects as "visible and tangible."[362] It should be noted that the commentary is made pursuant to treaty law rather than to international customary law[363] and that it is up to states to determine whether data constitutes an object of customary international humanitarian law or not, which is why emphasis has been placed on the two elements of customary law.[364] Since the reasoning of the Tallinn Manual 2.0 is based in part on the ICRC 1987 Commentary on Additional

---

[358] Alaz ab Mamoun 'Russia is using an onslaught of cyber attacks to undermine Ukraine's defence capabilities' (theconversation, 24 February 2022) <https://theconversation.com/russia-is-using-an-onslaught-of-cyber-attacks-to-undermine-ukraines-defence-capabilities-177638> accessed 1.3.2022; Tidy Joe 'Ukraine crisis: 'Wiper' discovered in latest cyber-attacks' (BBC, 25 February 2022) <https://www.bbc.com/news/technology-60500618> accessed 1.3.2022.

[359] International humanitarian law and the challenges of contemporary armed conflicts - recommitting to protection in armed conflict on the 70th anniversary of the geneva conventions (n 16) p. 28.

[360] International humanitarian law and the challenges of contemporary armed conflicts - recommitting to protection in armed conflict on the 70th anniversary of the geneva conventions (n 16) p. 28.

[361] Tallinn Manual 2.0 (n 4) p. 437; Pomson (n 254) p. 34.

[362] Commentary on the additional protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 (n 39) para 2007-2008.

[363] Pomson (n 254) p. 34.

[364] Prosecutor v. Dusko Tadic aka "Dule" (Decision on the defence motion for interlocutory appeal on jurisdiction), No. IT-94-AR72 International Criminal Tribunal for the former Yugoslavia (2 October 1995) para 99.

Protocol I, the author is eagerly awaiting for a renewed commentary on the First Protocol. The ICRC has released updated commentaries on the First Geneva Convention in 2016,[365] on the Second Geneva Convention in 2017[366] and on the Third Geneva Convention in 2020.[367] It therefore only stands to reason that after an updated commentary on the Fourth Geneva Convention is released, there will also be one on Additional Protocol I.

With regards to treaty law, it must be considered that the drafters of the 1949 Geneva Conventions as well as their additional protocols could not possibly predict the development of technology or the implications such development would bring about. Considering treaty interpretation, some scholars have argued that the word object should be interpreted in light of its present day meaning, as opposed to the requirement set out by the Vienna Convention on the Law of Treaties.[368] However, such an interpretation would only be legitimate following evidence of a change in how states perceive the notion of an object, and such evidence has not emerged.[369]

Similarly, in customary international humanitarian law, with regards to computer data as a civilian object, there is not enough state practice to consider that a new norm of customary international humanitarian law has emerged or that the present one has changed.[370] In addition, the practice of states that does exist, is far from uniform and cannot be considered as a "general recognition that a rule of law or legal obligation is involved."[371] The lack of state commitment to publicly state how international humanitarian law should apply to cyberspace, probably boils down to strategic reasons. If states remain reluctant to share their views on the matter of how data should be regarded

---

[365] 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* (2016) 2nd edition <https://ihl-databases.icrc.org/ihl/full/GCI-commentary> accessed 6 April 2022.
[366] ICRC, *Commentary on the Second Geneva Convention: Convention (II) for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea* (2017) 2nd edition <https://ihl-databases.icrc.org/ihl/full/GCII-commentary> accessed 6 April 2022.
[367] ICRC, *Commentary on the Third Geneva Convention: Convention (III) relative to the Treatment of Prisoners of War* (2020) 2nd edition <https://ihl-databases.icrc.org/ihl/full/GCIII-commentary> accessed 6 April 2022.
[368] Se for instance: Kubo Mačák, 'Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law' (2015) 48 Isr L Rev 55, p. 70-71.
[369] Schmitt (n 221) p. 94.
[370] Schmitt (n 221) p. 107; Pomson (n 254) p. 34; Mc Cormack (n 1) p. 240.
[371] North Sea Continental Shelf cases (Federal Republic of Germany v Netherlands and Denmark) Judgment [1969] ICJ Rep 3 para 74.

in international humanitarian law, they can operate in somewhat of a gray area. In terms of how this affects cyber operations and attacks, states would not have to apply the principle of distinction when targeting, if the target would not qualify as an object or be subject to special protection. Likewise, states would not have to factor in the effects of cyber attacks in their proportionality calculations to determine whether the attack is proportional in light of the gained military advantage.

Because the use of cyber means and methods of warfare allows for the targeting of even smaller parts of systems connected in cyberspace, it should be noted that the specificity level of which cyber attacks are conducted is always relevant when considering civilian protection. Whenever data is targeted, it should be considered whether the military operation disrupts the functioning of the system connected to said computer data, whether content-level or operational-level. If that is the case, then the system using that data is the intended target not the data itself, and the protection of civilian objects would be applicable considering that the attacked system constitutes a civilian object.[372] Additionally, as previously stated any "cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects"[373] amounts to a cyber attack and engages the protection of civilians and civilian objects, regardless of the target being data, an object or not.[374]

Although, some data is indeed protected through special protection, the author considers that civilian data is not adequately protected from the effects of hostilities in present day context. To exclude data as an object, allows for the targeting of data that can cause indirect harm to the civilian population. For instance, personal information, tax-records, bank account information, or any other data could be acquired during a cyber operation and used later outside the scope of an armed conflict to cause harm to civilians. According to the views of the author, data should somehow be afforded similar protection to that of civilian objects from an attack. Since the civilian population enjoys protection from the effects of attacks, [375] the indirect consequences of an attack should also be considered. At

[372] Dinniss (n 73) p. 50-52; Robin Geiss and Henning Lahmann 'Working Pappers: Protection of Data in Armed Conflict' (2021) Geneva Academy, p. 5.
[373] Tallinn Manual 2.0 (n 4) p. 415.
[374] Schmitt (n 221) p. 86.
[375] ICRC Customary International Humanitarian Law Rules (n 11) p. 68.

the time of writing however, this cannot be done since a cyber operation against data would only in very specific cases classify as an attack. That is if it would amount to a cyber attack which is a cyber operation "offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[376] The views of the author does however at the time of writing reflect that of *de lege ferenda*.

Finally, this thesis has only applied written law and international customary norms of international humanitarian law. Other regimes of international law can also be applicable although, international humanitarian law is usually considered to be *lex specialis.* The legal regime of international human right law might afford further protection to civilian data in situations of armed conflict whether international or non-international. For instance, the ICJ has stated in the Legality of the Threat or Use of Nuclear Weapons advisory opinion that "the protection of the International Covenant on Civil and Political Rights does not cease in times of war, except by operation of Article 4 of the Covenant whereby certain provisions may be derogated from in a time of national emergency"[377] And in the more recent *Legal Consequences of the Construction of a Wall case* the court considered that:

"that the protection offered by human rights conventions does not cease in case of armed conflict… As regards the relationship between international humanitarian law and human rights law, there are thus three possible situations: some rights may be exclusively matters of international humanitarian law; others may be exclusively matters of human rights law; yet others may be matters of both these branches of international law."[378]

However, considering the applicability of civilian data protection arising from international human rights or regional human rights frameworks such as the General Data Protection Regulation of the European Union requires more research and is beyond the scope of this thesis.

---

[376] Tallinn Manual 2.0 (n 4) p. 415 rule 92.
[377] *Legality of the Threat or Use of Nuclear Weapons* Advisory Opinion (n 7) para 25.
[378] Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, ICJ 9 July 2004 para 106.

Bibliography

MONOGRAPHS AND ARTICLES

Bellinger JB III and Haynes WJ II, 'A US government response to the International Committee of the Red Cross study Customary International Humanitarian Law' (2007) 886 International Review of the Red Cross 443

Bothe M, Partsch KJ and Solf WA, *New Rules for Victims of Armed Conflicts: Commentary to the Two 1977 Protocols Additional to the Geneva Conventions of 1949* (Martinus Nijhoff Publishers 1982)

Betz DJ and Stevens T, 'Cyberspace and the State: Toward a Strategy for Cyber-power' (2011) 51 Adelphi Series

Dinniss HH, *Cyber Warfare and the Laws of War*, (Cambridge University Press 2012)

Dinniss HH, 'The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives' (2015) 48 Isr L Rev 39

Dinstein Y, 'Legitimate Military Objectives under the Current Jus in Bello' (2002) 78 International Law Studies

Dinstein Y, *The Conduct of Hostilities under the Law of International Armed Conflict* (3rd ednCambridge University Press 2016)

Droege C, 'Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians' (2012) 94 International Review of the Red Cross 533

Dörmann K, 'Applicability of the Additional Protocols to Computer Network Attacks' (2004) (Paper delivered at the International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Stockholm, Nov. 17–19, 2004

Fellmeth AX and Horwitz M, *Guide to Latin in International Law* (2009) Oxford University Press USA OSO

Haslam E, 'Information Warfare: Technological Changes and International Law' (2000) 5 Journal of Conflict & Security Law 157

Henckaerts JM, Doswald-Beck L, and ICRC, *Customary International Humanitarian Law, Volume 1: rules* (Cambridge University Press, 2005)

Hollis D, 'Cyberwar Case Study: Georgia 2008' (2010) Small War Journal

Geiss R and Lahmann H 'Working Pappers: Protection of Data in Armed Conflict' (2021) Geneva Academy

Gisel L, Rodenhäuser T and Dörmann K, 'Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts' (2020) 913 International Review of the Red Cross 287

Liaropoulos A, 'Power and Security In Cyberspace: Implications for The Westphalian State System' (2011)

Lin H 'Cyber Conflict and International Humanitarian Law' (2012) 886 International review of the Red Cross 515

Inglis C. 'Cyberspace - Making Some Sense of It All' (2016) 15(2) Journal of Information Warfare 17

International Law Association Study Group on the Conduct of Hostilities in the 21st Century, 'The Conduct of Hostilities and International Humanitarian Law: Challenges of 21st Century Warfare' (2017) 78 International Law Studies 322.

Mačák K, ‘Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law’ (2015) 48 Israel Law Review 55

Mc Cormack T, ‘International Humanitarian Law and the Targeting of Data’ (2018) 94 International Law Studies 222

Medeiros BP and Goldoni LRF ‘The Fundamental Conceptual Trinity of Cyberspace’ (2020) 42(1) Contexto Internacional 31

Merkouris P ‘Interpreting the Customary Rules on Interpretation’ (2017) 19 International Community Law Review 126

Pomson O, “ ‘Objects’? The Legal Status of Computer Data under International Humanitarian Law” (2021)

Schmitt MN, ‘Wired warfare 3.0: Protecting the civilian population during cyber operations’ (2019) 101 International Review of the Red Cross 333

Schmitt MN, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2ed Cambridge University Press 2017)

Schmitt MN, ‘Targeting in Operational Law’ in T.D. Gill and D. Fleck (eds), *The Handbook of the International Law of Military Operations* (2nd edn, OUP 2015).

Schmitt MN, ‘The Law of Cyber Targeting’ (2015) 68 Naval War College Review 16

Schmitt MN, 'The Notion of ‘Objects’ During Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision' (2015) 48 Israel Law Review 81.

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

Schmitt MN, ‘Cyber Operations and the Jus in Bello: Key Issues’ (2011) 87 International Law Studies 89

Schöndorf R, ‘Israel’s Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations’ (2021) 97 International Law Studies 395

Sevastik P, Nyman-Metcalf K, Spiliopoulou Åkermark S, Mårsäter O *En bok i folkrätt* (Norstedts Juridik, 2013)

Solis GD, *The Law of Armed Conflict: International Humanitarian Law in War* (3rd ed Cambridge University Press 2021)

Sorel JM and Bore-Eveno V, ‘Article 31’ in Olivier Cortenand Pierre Klein (eds), *The Vienna Conventions on the Law of Treaties: A Commentary* (Oxford University Press 2011).

Smits JM, ‘WHAT IS LEGAL DOCTRINE? ON THE AIMS AND METHODS OF LEGAL-DOGMATIC RESEARCH’ (2015) Maastricht European Private Law Institute Working Paper No. 2015/06

von Heinegg WH, ‘Territorial Sovereignty and Neutrality in Cyberspace’ (2013) 89 International Law Studies 123

Rattray GJ, ‘An environmental approach to understanding cyberpower.’ In Franklin D Kramer, Stuart H Starr and Larry K Wentz (eds), Cyberpower and National Security (Washington, DC: National Defense University Press 2009)

Talbot JE, ‘The Tallinn Manual 2.0: Highlights and Insights’ (2017) 48 Georgetown Journal of International Law 735

Tsagourias N and Russell B, 'Research Handbook on International Law and Cyberspace' (Edward Elgar Publishing 2015)

TREATIES AND STATUTES

Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight. Saint Petersburg, (adopted 11 December 1868, entered into force 11 December 1868)

United Nations, Statute of the International Court of Justice, 24 October 1945, 33 UNTS 993

Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (adopted 12 August 1949, entered into force 05 October 1950) 75 UNTS 31 (First Geneva Convention)

Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (adopted 12 August 1949, entered into force 05 October 1950) 75 UNTS 85 (Second Geneva Convention)

Geneva Convention Relative to the Treatment of Prisoners of War (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 135 (Third Geneva Convention)

Geneva Convention Relative to the Protection of Civilian Persons in Time of War (adopted 12 August 1949, entered into force 05 October 1950) 75 UNTS 287 (Fourth Geneva Convention)

Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Additional Protocol I).

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 609 (Additional Protocol II)

Vienna Convention on the Law of Treaties (adopted 23 May 1969, entered into force 27 January 1980) 1155 UNTS 331

Protocol On Prohibitions Or Restrictions On The Use Of Incendiary Weapons (adopted 10 October 1980, entered into force 02 December 1983)

Statutes of the International Red Cross and Red Crescent Movement adopted by the 25th International Conference of the Red Cross at Geneva in 1986, amended in 1995 and 2006

UN Security Council, Statute of the International Criminal Tribunal for the Former Yugoslavia (as amended on 17 May 2002), 25 May 1993

Protocol On Prohibitions Or Restrictions On The Use Of Mines, Booby-traps And Other Devices (As Amended On 3 May 1996) (adopted 03 May 1996, entered into force 03 December 1998)

UN Security Council, Statute of the Special Court for Sierra Leone (2002)

INTERNATIONAL CASE LAW

International Court of Justice

Nottebohm Case (Lichtenstein v Guatemala) (Judgment) [1955] ICJ Rep 4

North Sea Continental Shelf cases (Federal Republic of Germany v Netherlands and Denmark) Judgment [1969] ICJ Rep

North Sea Continental Shelf cases (Federal Republic of Germany v Netherlands and Denmark) Judgment ‘Dissenting Opinion of Judge Tanaka’ [1969] ICJ Rep

Continental Shelf case (Libyan Arab Jamahiriya v. Malta) (Judgment) [1985], ICJ Reports 1985

Military and Paramilitary Activities in and against Nicaragua (Merits) (Nicaragua v. United States of America), Judgment, ICJ Reports 1986

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, ICJ GL No 95, [1996] ICJ Rep 226

Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, ICJ 9 July 2004

International Crimes Tribunal of the Former Yugoslavia

Prosecutor v. Dusko Tadic aka "Dule" (Decision on the defence motion for interlocutory appeal on jurisdiction), No. IT-94-AR72 International Criminal Tribunal for the former Yugoslavia (2 October 1995)

Supreme Court of Israel

HCJ 769/02 *Public Committee Against Torture in Israel and Palestinian Society for the Protection of HumanRights and the Environment v Israel and Others* ILDC 597 (IL 2006) [2006].

UN DOCUMENTS

UN General Assembly

UNGA ‘Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security’ (24 June 2013) UN Doc A/68/98

UNGA ‘Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security’ (22 July 2015) UN Doc A/70/174

Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security 'Chair's Summary' (10 March 2021) UN doc A/AC.290/2021/CRP.3

UNGA 'Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266' (13 July 2021) UN Doc A/76/136*

UNGA 'Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security' (14 July 2021) UN Doc A/76/135

Un Security Council

UN Security Council, Resolution 918 (17 May 1994) UN Doc. S/RES/918
UN Security Council, Resolution 925 (8 June 1994) UN Doc. S/RES/925
UN Security Council, Resolution 950 (21 October 1994) UN Doc. S/RES/950
UN Security Council, Resolution 1075 (11 October 1996) UN Doc. S/RES/1075
UN Security Council, Resolution 1087 (11 December 1996) UN Doc. S/RES/1087

ICRC DOCUMENTS

Final Record of the Diplomatic Conference of Geneva of 1949, (1949) Vol. II-A

International Committee of the Red Cross, *Commentary on the additional protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, (1987)

International Committee of the Red Cross 'INTERNATIONAL HUMANITARIAN LAW AND THE CHALLENGES OF CONTEMPORARY ARMED CONFLICTS -

International Committee of the Red Cross 'International Humanitarian Law and Cyber Operations during Armed Conflicts ICRC position paper' (2015)

International Committee of the Red Cross, 'International humanitarian law and the challenges of contemporary armed conflicts' (2015) 32IC/15/11

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* (2016) 2nd edition <https://ihl-databases.icrc.org/ihl/full/GCI-commentary> accessed 6 April 2022.

ICRC, *Commentary on the Second Geneva Convention: Convention (II) for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea* (2017) 2nd edition <https://ihl-databases.icrc.org/ihl/full/GCII-commentary> accessed 6 April 2022.

Recommitting To Protection In Armed Conflict On The 70th Anniversary Of The Geneva Conventions' (2019)

ICRC, *Commentary on the Third Geneva Convention: Convention (III) relative to the Treatment of Prisoners of War* (2020) 2nd edition <https://ihl-databases.icrc.org/ihl/full/GCIII-commentary> accessed 6 April 2022.

ICRC, 'International Humanitarian law and cyber operations during armed conflicts ICRC position paper submitted to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, November 2019' (2020) 913 International Review of the Red Cross 481

INTERNET SOURCES

Alaz ab Mamoun ‘Russia is using an onslaught of cyber attacks to undermine Ukraine’s defence capabilities’ (theconversation, 24 February 2022) <https://theconversation.com/russia-is-using-an-onslaught-of-cyber-attacks-to-undermine-ukraines-defence-capabilities-177638> accessed 1.3.2022

Christensson Per ‘Cyberspace Definition’ (TechTerms.com, 2006) <https://techterms.com/definition/cyberspace> accessed 26 November 2021.

Christensson Per ‘Data Definition’ (TechTerms.com, 2006) <https://techterms.com/definition/data> accessed 26 November 2021.

Durham Helen ‘Cyber operations during armed conflict: 7 essential law and policy questions’ (ICRC Humanitarian Law & Policy Blog, 26 March 2020) <https://blogs.icrc.org/law-and-policy/2020/03/26/cyber-armed-conflict-7-law-policy-questions/> accessed 10 February 2022.

International Criminal Court ‘The State Parties to the Rome Statute’ (no date) <https://asp.icc-cpi.int/en_menus/asp/states%20parties/pages/the%20states%20parties%20to%20the%20rome%20statute.aspx> accessed 6 April 2022

Jeremy Fleming, ‘Director’s Speech at CyberUK18’ (GCHQ 12 April 2018) accessed 3 June 2021 at: www.gchq.gov.uk/pdfs/speech/director-cyber-uk-speech-2018.pdf

Kubo Mačák, Laurent Gisel and Tilman Rodenhäuser ‘Cyber Attacks against Hospitals and the COVID-19 Pandemic: How Strong are International Law Protections?’ (Just Security, 21 March 2020) <https://www.justsecurity.org/69407/cyber-attacks-against-hospitals-and-the-covid-19-pandemic-how-strong-are-international-law-protections/> accessed 16 February 2022.

Mike Burgess, 'Offensive Cyber and the People Who DoIt', speech given to the Lowy Institute, Australian Signals Directorate (27 March 2019) accessed 3 June 2021 at: www.asd.gov.au/speeches/20190327-lowy-institute-offensive-cyber-operations.htm

Oxford English Dictionary Online, (OUP June 2021) <https://www.oed.com/view/Entry/129613?> accessed 7 June 2021.

Paris call 'The Call' (2018) <https://pariscall.international/en/call> accessed 19 January 2022

Paris call 'The Supporters' (2018) <https://pariscall.international/en/supporters> accessed 19 January 2022

Paul M. Nakasone, 'Statement of General Paul M. Nakasone, Commander, United States Cyber Command, before the Senate Committee on Armed Services' (14 February 2019) accessed 3 June 2021 at: www.armed-services.senate.gov/imo/media/doc/Nakasone_02-14-19.pdf -***-

Tilman Rodenhäuser 'Hacking Humanitarians? IHL and the protection of humanitarian organizations against cyber operations' (EJIL:talk, 16 March 2020) <www.ejiltalk.org/hacking-humanitarians-ihl-and-the-protection-of-humanitarian-organizations-against-cyber-operations/> accessed 25.2.2022.

Tidy Joe 'Ukraine crisis: 'Wiper' discovered in latest cyber-attacks' (BBC, 25 February 2022) <https://www.bbc.com/news/technology-60500618> accessed 1.3.2022.

OTHER DOCUMENTS

Commonwealth of Australia, Department of Foreign Affairs and Trade 'Australia's International Cyber Engagement Strategy' (2017)

Federal Department of Foreign Affairs ‘Switzerland's position paper on the application of international law in cyberspace’ (2021) <https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf> accessed 19 January 2022.

Federal Foreign Office ‘On the Application of International Law in Cyberspace: Position Paper (2021) <https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf> accessed 14 March 2022.

Foreign, Commonwealth & Development Office ‘Policy paper: Application of international law to states’ conduct in cyberspace: UK statement’ (Gov.uk, 3 June 2021) <https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement> accessed 17.1.2022

Government of the Kingdom of the Netherlands ‘Appendix: International law in cyberspace’ <https://www.government.nl/binaries/government/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace/International+Law+in+the+Cyberdomain+-+Netherlands.pdf> accessed 19 January 2022

International Criminal Tribunal for the former Yugoslavia ‘Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia’ (2000)

Ministère des Armées de France, ‘INTERNATIONAL LAW APPLIED TO OPERATIONS IN CYBERSPACE’ (2019) <https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf> accessed 19 January 2022

Ministry for Foreign Affairs ‘International law and cyberspace Finland’s national positions’ (2020) <https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727> accessed 19 January 2022.

Ministry of Foreign Affairs ‘On the Application of International Law in Cyberspace Position Paper’ (2021) <https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf> accessed 19 January 2022.

Ministry of Foreign Affairs of Japan ‘Basic Position of the Government of Japan on International Law Applicable to Cyber Operations’ (2021) <https://www.mofa.go.jp/files/100200935.pdf> accessed 19 January 2022.

Ministry of Foreign Affairs and International Cooperation ‘ITALIAN POSITION PAPER ON ‘INTERNATIONAL LAW AND CYBERSPACE’ (2021) <https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf> accessed 19 January 2022.

Mission of Israel to the UN in Geneva ‘Application of International Law to Cyberspace’ (https://embassies.gov.il/ 25 October 2021) <https://embassies.gov.il/UnGeneva/priorities-statements/ScienceTechnologyDevelopment/Pages/Israel-approach-on-the-Application-of-International-Law-to-Cyberspace.aspx> accessed 19 January 2022.

Norwegian Government Security and Service Organisation ‘NORWEGIAN POSITIONS ON SELECTED QUESTIONS OF INTERNATIONAL LAW RELATING TO CYBERSPACE’ (2021) <https://www.regjeringen.no/contentassets/a8911fc020c94eb386a1ec7917bf0d03/norwegian_positions.pdf> accessed 19 January 2022

Organization of American States the Inter-American Juridical Committee ‘International Law and State Cyber Operations’ (2020)

Uk Ministry Of Defence, The Joint Service Manual Of The Law Of Armed Conflict, Jsp 383 (2004)

US Department of Defense, ‘Department of Defense Dictionary of Military and Associated Terms’ (2021)

The Federal Ministry Of Defence Of The Federal Republic Of Germany ‘ Joint Service Regulation on Law of Armed Conflict Manual’ (ZDv 15/2) (2013)

Us Department Of Defence Office of The General Counsel, ‘Law Of War Manual’ (June 2016)

DICTIONARIES

‘object, n’ The Oxford English Dictionary, (1970) Vol. VII