Protection of Data during International Armed Conflicts

Cyber Operations, Data Protection, and Non-State Actors

Filippa Nielsen Norelind

Word Count: 13 716

Master's Thesis, 15 ECTS

Supervisor: Marika Ericson

3 May 2024

International Operational Law

Swedish Defence University

Table of Contents

1. Introduction

In an era where the click of a mouse has the potential to wield the same devastation as was once reserved by bullets and bombs, the landscape of warfare has undergone significant development. Our societies, deeply reliant on computers, networks, and digital systems, have intertwined modern life with data - the core of these technologies.[1] Attacks targeting civilian data may result in the loss of critical information, such as life-saving data from hospitals or humanitarian organizations data collected for humanitarian purposes.[2] The International Committee of the Red Cross has stated that cyber operations that target civilian data "could cause more harm to civilians than the destruction of physical objects".[3] Look no further than the ongoing conflict between Russia and Ukraine, where cyber operations, including those where civilian data is targeted, are being utilized as a part of warfare.[4]

Still, even though actors are warning about the consequences of data being targeted, and the military is starting to consider it as military assets, digital human rights are mainly considered to be a legal issue of peacetime.[5] Moreover, most assume that if an armed conflict breaks out, international humanitarian law would have norms one can rely on for all instances. The core instruments of IHL were created before warfare was fought in both the physical and digital realms. Thus, the framework is, in large, silent on the issue.

---

[1] Marco Roscini, 'World Wide Warfare - Jus ad Bellum and the Use of Cyber Force' (2010) 14 The Max Planck Yearbook of United Nations Law 86, 87; Robin Geiß and Henning Lahmann, 'Protection of Data in Armed Conflict' (2021) 97 INT'L L. STUD. 556, 557

[2] International Committee of the Red Cross, 'Statement by the International Committee of the Red Cross (ICRC)' (Open-Ended Working Group on Information and Communication Technology, New York, 13 December 2023) https://www.icrc.org/en/statement-cyber-oewg-sixth-session accessed 28 April 2024

[3] ICRC, 'International Humanitarian Law and Cyber Operations During Armed Conflicts' (2020) 102(913) International Review of the Red Cross 481, 490

[4] Frederica Cristani, 'Can Anonymous be Prosectued? A Reflection under International Law in the Framework of the Current Armed Conflict in Ukraine' (Centre for International Law, 2022) https://www.iir.cz/can-anonymous-be-prosecuted-a-reflection-under-international-law-in-the-framework-of-the-current-armed-conflict-in-ukraine accessed 29 April 2024

[5] Russel Buchan and Asaf Lubin, 'Introduction' in Russel Buchan and Asaf Lubin (eds), *The Rights to Privacy and Data Protection in Times of Armed Conflict* (NATO CCDCOE 2022) v

Adding to the complexity, there has been a significant surge in civilian involvement in cyber operations within armed conflicts, a trend that is particularly evident in the ongoing conflict between Russia and Ukraine.[6] This development brings forth new concerns, particularly for the ordinary individuals caught in the middle of the conflicts. Numerous sources have expressed their worries, stating that "civilians, civilian digital infrastructures, and services" are at higher risk of "erroneous, unnecessary, or unlawful attacks".[7] This not only affects those being directly targeted but also other civilians who rely on digital tools and services in their day-to-day lives. The participation of civilians in these operations within armed conflicts escalates the potential harm to civilians and civilian infrastructure.[8]

As warfare extends its reach into cyberspace and civilian involvement in cyber operations increases, it is imperative to address the protection of civilian data. Are existing international legal frameworks sufficiently safeguarding civilian data in these instances? To examine the question, the starting point is the intersection of international armed conflicts, the involvement of non-state actors in cyber operations, and the right to privacy and protection of data.

1.1 Purpose of the Thesis

This thesis sets out to investigate the legal complexities surrounding the right to privacy and data protection in cyber warfare within ongoing international armed conflicts. It will explore the

[6] Geneva Academy, 'Rising Civilian Involvement in Cyber Warfare: Legal Implications and Solutions Explored During Expert Meeting' (*Geneva Academy*, 20 October 2023) https://www.geneva-academy.ch/news/detail/650-rising-civilian-involvement-in-cyber-warfare-legal-implications-and-solutions-explored-during-expert-meeting accessed 1 May 2024; Stéphane Duguin and Pavlina Pavlova, 'The Role of Cyber in the Russian War against Ukraine: Its Impact and the Consequences for the Future of Armed Conflict' (*European Parliament*, September 2023) https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf accessed 1 May 2024

[7] Geneva Academy (n 6)

[8] ICRC (n 2)

involvement of non-state actors in cyber operations in international armed conflicts and the protection of data. The research aims to shed light on the frameworks, particularly international humanitarian law and international human rights law, that regulate these operations and their effectiveness in safeguarding civilian data during conflicts.

Moreover, the thesis seeks to identify potential challenges and gaps in the protection of civilian data in armed conflicts, especially in scenarios where non-state actors perpetrate cyber operations. By investigating these complexities, the thesis hopes to contribute insights that will benefit the continued scholarly discourse regarding this pressing issue in contemporary warfare.

1.2 Research Question

The overarching research question of the thesis is: To what extent does international humanitarian law protect civilian data, in particular from non-state actors, during international armed conflicts, and does international human rights law contribute protection in this context?

1.2.1 Subsidiary Questions

Several subsidiary questions need to be considered to answer the research question. These are as follows;

(i) Is international humanitarian law applicable to cyber operations? If so, to what extent?

(ii) How is data protected under international human rights law?

(iii) Does international human rights law still apply during armed conflicts? If so, how does it intersect with international humanitarian law?

1.3 Scope of the Thesis

This thesis's sole focus will be examining jus in Bello, with jus ad Bellum deliberately excluded. This decision stems from acknowledging the extensive scope surrounding the application of jus ad Bellum principles within the context of cyber operations. Exploring this intersection would considerably broaden the thesis's scope. Therefore, to maintain clarity and depth, the choice has been made to narrow the focus to instances where an armed conflict is already established and a cyber operation is conducted within said conflict. This will allow for a more detailed analysis of the specific dynamics and implications of using cyber operations amid armed conflicts.

Furthermore, this thesis will explore international armed conflicts, IACs, while excluding non-international armed conflicts, NIACs. This limitation is justified for several reasons. Firstly, the thresholds in the norms regulating NIACs are different from IACs and often less clear, leading to more extensive discussions that could detract from the primary focus of the thesis. Secondly, NIACs typically involve a significant interplay between national law and international humanitarian law, adding complexity and variability to the legal analysis. By narrowing the scope to IACs, the thesis can provide a more in-depth analysis of the frameworks governing cyber operations targeting civilian data without issues inherent to NIACs interfering. The limitation allows for a more precise and focused examination of the issues most relevant to the protection of civilian data in the context of armed conflicts.

Additionally, while acknowledging the existence of data protection frameworks such as the General Data Protection Regulation (GDPR) and other frameworks, the primary focus will be on international law. These regional and national frameworks will be mentioned to provide context. However, they will not be delved into as the emphasis is on exploring the international dimension of protecting civilian data during international armed conflicts.

1.4 Structural Outline

In the first section, the background and context for the thesis are established by introducing the research question and subsequent inquiries while also outlining its limitations.

The second section will focus on the technological aspect of cyber operations. It will examine terms associated with cyber warfare, investigate possible definitions, and briefly explain technological aspects.

The third section of the thesis will explore the potential application of international humanitarian law to cyber operations. Initially, it will assess the applicability of IHL to cyber activities. Subsequently, it will analyze whether cyber operations can amount to an armed attack in international armed conflicts. Lastly, it will examine if data can be classified as an object under the IHL framework.

In the fourth section, the relationship between international human rights law and IHL will be delved into. It will first examine the right to privacy and data protection under IHRL during peacetime. Following this, it will explore the applicability of IHRL during armed conflicts and to what extent data protection provisions could potentially apply in such scenarios.

Section five will focus on certain non-state actors conducting cyber operations within international armed conflicts, using the conflict between Russia and Ukraine as an example. It will provide an overview of the conflict, including the involvement of non-state actors in cyberspace. Then, an overview of whether IHL offers any protection from these individuals who are not part of armed non-state groups and whose actions cannot be attributed to a State when they are targeting data. Lastly, it will examine the potential responsibility of these individuals and groups of civilians under IHRL and explore the protection of civilians' right to data privacy in these circumstances.

The conclusion in section six will bring together the findings from the preceding sections, emphasizing their potential implications for international law, cyber operations, and human rights. There will also be suggestions on further research, as well as steps States and the international community should take in order to safeguard civilian data from non-state actors in armed conflicts.

2. Cyber Warfare

While cyber tactics are increasingly used in armed conflicts, warfare fought exclusively in cyberspace has yet to occur.[9] However, there have been instances where cyber operations were used alongside traditional kinetic forces during armed conflicts. One of the earliest instances of this is likely the cyber operations during the conflict between Russia and Georgia in 2008.[10] Since then, cyber warfare has become increasingly widespread and more commonly used. In the ongoing conflict between Russia and Ukraine, both Parties have engaged in cyber warfare as well as encouraged non-state actors to conduct cyber operations in support of their respective States.[11]

The use of cyberspace in armed conflicts sparks fundamental questions: What exactly is cyber warfare? Moreover, what sets a cyber attack apart from a cyber operation? This section seeks to clarify these questions, beginning with exploring possible definitions of some essential terms. Subsequently, the second section will briefly explain the technological aspects of cyber operations.

2.1 Cyber Operations and Cyber Warfare: Possible Definitions

Cyberwarfare does not have a universal definition that is used and agreed on. The ICRC has defined it as the "means and methods of warfare that consists of cyber operations amounting to, or conducted in the context of, an armed conflict, within the meaning of IHL".[12] In principle, cyber warfare refers to the use of cyber technologies in armed conflicts.[13]

---

[9] Robin Geiss and Henning Lahmann, 'Protecting Societies: Anchoring a New Protection Dimension in International Law in Times of Increased Cyber Threats' (*Geneva Academy*, 2021) https://www.geneva-academy.ch/joomlatools-files/docman-files/working-papers/Protecting%20Societies%20-%20Anchori.pdf accessed 1 May 2024, 7

[10] Ibid.

[11] Duguin and Pavlova (n 6) 10

[12] International Committee of the Red Cross, 'What Limits Does the Law of War Impose on Cyber Attacks?' (*ICRC*, 28 June 2013) https://www.icrc.org/en/doc/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm accessed 30 April 2024

[13] Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford University Press 2014) 11

Cyber operations are not limited to a particular form; hence, they can look very different. To analyze cyber warfare and cyber attacks further, exploring what cyber operations look like in real life is essential. In order to understand how paralyzing cyber attacks can be for a population, some examples of consequences could be disabling "power generators, cut off the military command, control and communication systems, cause trains to derail and airplanes to crash, nuclear reactors to melt down, pipelines to explode, weapons to malfunction".[14]

Cyberattacks fall within the scope of information operations, encompassing a narrower subset within this broader category.[15] The United States has defined information operations as "the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt or usurp the decision making of adversaries and potential adversaries while protecting our own".[16] IRCs in this instance means 'information related-capabilities'. When it comes to cyber operations, it is instead described as "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace".[17] The Tallinn Manual 2.0, defines cyber operations as "the employment of cyber capabilities to achieve objectives in or through cyberspace".[18] In turn, cyberspace has been described as "the environment formed by physical and non-physical components to store, modify, and exchange data using computer networks".[19] Therefore, the critical distinction between cyber operations and information operations seems to lie in the fact that they intend to cause disruption or harm to adversaries.[20]

---

[14] Roscini (n 1) 88
[15] Roscini (n 1) 91
[16] United States, 'DoD Dictionary of Military and Associated Terms' (March 2017) https://www.tradoc.army.mil/wp-content/uploads/2020/10/AD1029823-DOD-Dictionary-of-Military-and-Associated-Terms-2017.pdf accessed 1 May 2024, 113
[17] Ibid. 60
[18] Michael N. Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge, 2nd ed, Cambridge University Press 2017) 564, hereinafter Tallinn Manual 2.0
[19] Ibid.
[20] Roscini (n 7) 11

From now on, this thesis will distinguish between cyber attacks and cyber operations. Within the IHL framework, the word 'attack' has special thresholds that need to be fulfilled.[21] To avoid confusion, 'cyber attack' will only be used for cyber operations that fulfill the requisites of an attack put forth by IHL.

The thesis will revolve around the protection of data; it is, therefore, essential to understand what data is. A brief overview will be provided here, as Chapter 3 will delve into more perspectives on different categorizations and interpretations of data. In general, computer data can be described as information processed or located within a computer system.[22] It can be saved in a wide array of forms, including text, images, audio files, software programs, and videos. This data may be processed by the computer's central processing unit and stored in files and folders on the hard drive.[23] At its core, data is binary, consisting of ones and zeros. Its binary nature means that data can be transmitted between computers via network connections. Furthermore, data does not deteriorate or lose quality regardless of transfers or time.

2.2 Technological Aspects of Cyber Warfare

Most cyber operations involve either compromising hardware or software or making a system malfunction or collapse by overloading it with data.[24] Denial of Service, DoS, attacks target the computer's hardware or software to corrupt and incapacitate it.[25] It floods the network of the

[21] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of International Armed Conflicts (Protocol I) (8 June 1977) 1125 UNTS 3 Art.49, hereinafter AP I; Michael N. Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge, 1st ed, Cambridge University Press 2013), Art. 30, hereinafter Tallinn Manual

[22] TechTerms, 'Data Definition' (*TechTerms*, 13 December 2022) https://techterms.com/definition/data accessed 1 May 2024

[23] TechTerms, 'Data Definition' (*TechTerms*, 13 December 2022) https://techterms.com/definition/data accessed 1 May 2024

[24] Roscini (n 7) 18

[25] Roscini (n 1) 93

computer with requests to "overload and incapacitate it", causing it to crash.[26] DDoS, distributed denial of service, attacks act in the same way, only that a larger number of computers carry them out. Consequently, the damage that DDoS attacks are capable of is more significant. The attack consists of "multiple compromised systems" that target "a single system causing a denial of service attack".[27] The victim of the attack is not only the computer system experiencing the DoS attack but also the systems used to distribute the attack. An example of a DDoS attack is that against Georgia during the conflict with Russia in 2008.[28] In short, before the actual invasion, the government sites of Georgia fell victim to a DDoS attack, which continued even after the ceasefire was established.[29]

Other typical cyber operations are ransomware and malware wipers. Ransomware often entails encrypting files and demanding a ransom to restore the user's data.[30] Malware wipers, on the other hand, have the sole purpose of damaging or disrupting data.[31] These are a bit unique in the sense that data targeting was traditionally conducted in order to make money.[32] The reasons to use wipers are often to sabotage vital data or software or to destroy evidence. Malware wipers have been frequently used within the conflict between Ukraine and Russia, including on the eve of the invasion of Ukraine in 2022.[33] Some examples of how malware destroys data are by overwriting files with different data, encrypting the files and destroying the key, or attacking the system itself.[34]

---

[26] Ibid. 94; Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (Cambridge, Cambridge University Press 2012) 293

[27] Ibid.

[28] Ibid. 290

[29] To read more see; Eneken Tikk, Kadri Kaska and Liis Vihul, *International Cyber Incidents: Legal Considerations* (Tallinn, CCDCOE 2010), 67-90

[30] Byron Denham and Dale R. Thompson, 'Ransomware and Malware Sandboxing' (IEEE 13th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference, IEEE, 2022) 73

[31] Harrison Dinniss (n 25) 293

[32] Check Point, 'What is Wiper Malware?' (*CheckPoint*) https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/what-is-wiper-malware/ accessed 27 April 2024

[33] Duguin and Pavlova (n 6) 6

[34] Check Point (n 31)

3. Cyber Operations and International Humanitarian Law

International humanitarian law, also known as the law of armed conflict, applies in situations of armed conflict, regardless of whether war has been formally declared.[35] Moreover, it is applicable even if the Parties involved do not acknowledge the existence of the armed conflict. When assessing if a conflict is taking place, it is the factual circumstances on the ground that determine its existence rather than being a legal interpretation.[36] The framework is based upon principles such as the principle of humanity, the principle of distinction, the principle of proportionality, and the principle of military necessity.[37] The core instruments of IHL are the four Geneva Conventions of 1949 and their two Additional Protocols.[38] However, none of these instruments explicitly address cyber operations or the cyber domain, which raises the question of whether IHL applies to cyberspace during armed conflicts.[39]

Furthermore, if this is the case, the question of to what extent it applies becomes relevant. Does its application depend on whether the cyber operation is being conducted alongside traditional weaponry, or can it be extended to scenarios where the only target is data? In the following sections, these inquiries will be delved into to determine the applicability of IHL and its scope in cyberspace.

---

[35] International Committee of the Red Cross (ICRC), Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (First Geneva Convention), 12 August 1949, 75 UNTS 31 Art. 2(1) hereinafter GC I

[36] Harrison Dinniss (n 25) 117

[37] International Committee of the Red Cross (ICRC), 'Fundamental Principles of IHL' (*How Does Law Protect in War?*) https://casebook.icrc.org/a_to_z/glossary/fundamental-principles-ihl accessed 1 May 2024

[38] GC I (n 34); Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (Second Geneva Convention) (adopted 12 August 1949) 75 UNTS 85, hereinafter GC II; Geneva Convention Relative to the Treatment of Prisoners of War (Third Geneva Convention) (adopted 12 August 1949) 75 UNTS 135, hereinafter GC III; Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention) (12 August 1949) 75 UNTS 287, hereinafter GC IV; AP I; Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II) (adopted 8 June 1977) 1124 UNTS 609, hereinafter AP II

[39] Tallinn Manual (n 21) 5

3.1 Is International Humanitarian Law Applicable to Cyber Operations?

There is a universal consensus that international law applies to cyber operations.[40] In both Tallinn Manuals, the experts that gathered to draft the Articles unanimously agreed that "general principles of international law applied to cyber space".[41] Therefore, they also concluded that the framework regulating the cyber domain does not need to be reinvented entirely. Instead it can already be found in international law. Consequently, the applicable rules found in treaties, such as the four Geneva Conventions, should be examined in the context of cyber operations, as well as rules of a customary nature, in order to determine their applicability.[42]

When it comes to cyber operations, States have been able to agree upon some multilateral instruments that regulate cyber operations.[43] Nevertheless, there is still an intense debate regarding whether and how IHL applies to cyber operations conducted within armed conflicts.[44] There seems to be a majority consensus among experts on cyber operations, as during the drafting of Tallinn Manual 2.0, the experts unanimously agreed that IHL is applicable in cyberspace.[45] According to these experts, the "basic rules and principles" of IHL "must be applied when conducting cyber operations during armed conflicts".[46] Notably, there were still some differing views within the group of experts gathered for the Tallinn Manual 2.0.[47] Some thought that IHL only regulates those cyber operations that are carried out by a Party to the conflict against an opponent.[48] Others argued that there had to be a link between the cyber activity conducted and the hostilities at play. In summary,

[40] Kubo Mačák, 'Unblurring the Lines: Military Cyber Operations and International Law' (2021) 6(3) Journal of Cyber Policy 411, 413
[41] Tallinn Manual (n 21) 13
[42] Tallinn Manual (n 21) 5
[43] Laurent Gisel, Tilman Rodenhäuser and Knut Dörmann, 'Twenty Years On: International Humanitarian Law and the Protection of Civilians Against the Effects of Cyber Operations During Armed Conflicts' (2020) 102(913) International Review of the Red Cross 287, 289
[44] Ibid. 289
[45] Tallinn Manual 2.0 (n 18) Rule 80 Para. 1
[46] Ibid.; Gisel, Rodenhäuser and Dörmann (n 43) 292
[47] Tallinn Manual 2.0 (n 18) Rule 80
[48] Ibid. Rule 80 Para. 6

even though the Tallinn Manuals reached a consensus that IHL applies to cyberspace, there remains disagreement regarding its specific application.

3.1.1 'Information Security' within the United Nations and International Humanitarian Law

The United Nations has been actively addressing information security since 1998.[49] The Russian Federation initially brought it forward through a draft resolution in the First Committee of the UN General Assembly.[50] Since 2004, there have been six Groups of Governmental Experts, GGEs, who have discussed questions regarding threats to the security of information and communication technologies.[51]

In 2017, the GGE had difficulties reaching a consensus on applying international law to these technologies. A division emerged between States, with two opposing camps, as evidenced by statements from the US and Cuba. The US, represented by Markoff, emphasized the need for "clear and direct statements on how certain international law applies to States' use of ICTs", including IHL, "the right to self-defence, and the law of State responsibility, including countermeasures".[52] They criticized States who were reluctant to affirm such statements, accusing them of wanting to use cyberspace to "achieve their political ends with no limits or constraints on their actions".[53] On the contrary, Cuba expressed concerns that referencing IHL in the context of ICTs "would

[49] UNGA First Committee (53rd Session) 'Agenda Item 63: Role of Science and Technology in the Context of International Security, disarmament and other Related Fields' (30 September 1998) UN Doc. A/C.1/53/3; UNGA Res 53/70 (4 January 1999) UN Doc. A/RES/53/70
[50] Ibid.
[51] Gisel, Rodenhäuser and Dörmann (n 43) 292; UN Office for Disarmament Affairs, 'Developments in the Field of Information and Telecommunications in the context of international security' https://disarmament.unoda.org/ict-security/ accessed 2 May 2024
[52] U.S Department of State, 'Explenation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security' (U.S Department of State, 23 June 2017) https://2017-2021.state.gov/explanation-of-position-at-the-conclusion-of-the-2016-2017-un-group-of-governmental-experts-gge-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-sec/ accessed 1 May 2024
[53] Ibid.

legitimize a scenario of war and military actions" in cyberspace.[54] They feared this could lead to "unilateral punitive force actions, including the application of sanctions and even military action by States claiming to be victims of illicit uses of ICTs", and advocated for prioritizing peaceful settlements instead.[55]

In the last meeting, the GGE managed to agree upon the report in consensus, meaning that the framework regarding Responsible State Behaviour in Cyberspace in the Context of International Security has become more apparent.[56] Moreover, in 2018, the United Nations General Assembly established an open-ended working group in which all member states can participate in discussing issues within information and communications technology.[57]

The UN GGE reports of 2013 and 2015 concluded that "international law, and in particular the Charter of the United Nations, is applicable".[58] It was also noted that established international legal principles apply to the use of information and communication technology, "including, where applicable, the principles of humanity, necessity, proportionality and distinction".[59] Although they do not explicitly mention IHL, many have pointed out that these are IHL's core principles.[60] In 2021, the GGE group expressly mentioned IHL in the context of the cyber domain, saying that IHL "applies only in situations of armed conflict".[61]

---

[54] Cuba, 'Declaration by Miguel Rodriquez, Representative of Cuba' (Speech at the final session of group of governmental experts on developments in the field of information and telecommunications in the context of international security, New York, 23 June 2017)
[55] Ibid.
[56] UNGA Group of Governmental Experts (76th Session) '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, hereinafter UNGA GGE 2021
[57] UNGA Res 73/27 (5 December 2018) UN Doc. A/RES/73/27
[58] UNGA Group of Governmental Experts (68th Session) '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/68/96 Para. 19; UNGA Group of Governmental Experts (70th Session) '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 24, Hereinafter UNGA GGE 2015
[59] UNGA GGE 2015 (n 19) Para.28
[60] Michael N. Schmitt, 'France Speaks Out on IHL and Cyber Operations Part I' (*EJIL:Talk!*, 30 September 2019) https://www.ejiltalk.org/france-speaks-out-on-ihl-and-cyber-operations-part-i/ accessed 1 May 2024
[61] UNGA GGE 2021 (n 56) Para 71(f)

In summary, many efforts within the UN, such as the OEWG and GGE, have been made to discuss questions regarding information security. However, these efforts have not resulted in much progress regarding an agreement on IHL's applicability to cyber operations.[62]

3.1.2 Potential Application of International Humanitarian Law within the Cyber Domain

As mentioned, IHL was created long before the emergence of cyber warfare and, therefore, lacks definitions or explicit provisions that address cyberspace as a domain for war. Thus, whether IHL applies depends on the "nature, effects and circumstances of such operations".[63]

According to the ICRC, it is evident that IHL regulates cyber operations and cyber warfare that take place during armed conflicts.[64] It is even clarified that their stance is not affected by arguments such as whether one considers cyberspace a domain in the same category as land, sea, air, and outer space or its category as a man-made domain. Additionally, the UN General Assembly has affirmed that international law and the core principles of IHL apply to cyber operations. Other international organizations, such as the EU and NATO, have also publicly asserted this view.[65]

The view that IHL is applicable during cyber operations in armed conflicts is also supported by the fact that the purpose of the framework is to be able to regulate future conflicts.[66] States adopted norms within IHL with the intention of anticipating the emergence of new weapons, means, and methods of warfare in the future, ensuring that the framework would still apply to them. In Article 36 of AP I, it is stated that when a Party to the Protocol is "in the study, development, acquisition or

---

[62] Gisel, Rodenhäuser and Dörmann (n 43) 292
[63] Ibid. 297
[64] ICRC, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts' (*ICRC*, 2015) https://www.icrc.org/en/download/file/15061/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf accessed 2 May 2024, 40
[65] See, for example; Council of the European Union, 'General Affairs Council Meeting' (Brussels, Council of the European Union, 25 June 2013) Doc. No. 11357/13; NATO, 'Wales Summit Declaration issued by the heads of State and government participating in the meeting of NATO in Wales' (Wales, NATO, 5 September 2014) Para 72
[66] Gisel, Rodenhäuser and Dörmann (n 43) 298

adoption of a new weapon, means or method of warfare", it is under the obligation to ensure that the employment of such is not "in some or all circumstances /…/ prohibited by this Protocol or by any other rule of international law applicable".[67]

Furthermore, in ICJ's Advisory Opinion on the legality of the threat or use of nuclear weapons, the Court made clear that IHL's rules and principles apply "to all forms of warfare and to all kinds of weapons /…/ those of the present and those of the future".[68] The general principles of IHL were established and incorporated into customary law before nuclear weapons were created, but the Court still held that the framework restricts the use of such weapons. The Court argued that reasoning the opposite would be incompatible with the "intrinsically humanitarian character of the legal principles in question".[69] Therefore, according to the ICJ, IHL is applicable to all weapons and forms of warfare, including cyber technologies.[70]

The question arises of whether cyber technologies can be classified as weapons, means, or methods of warfare under the framework of IHL. Means of warfare include "all weapons, weapons platforms and associated equipment used directly to deliver force during hostility".[71] Methods of warfare are the way weapons are used within the conflict. Finally, weapons are "means to commit acts of violence against human or material enemy forces".[72]

The Tallinn Manual asserts that 'means' of cyber warfare include both cyber weapons and weapon systems, asserting that the general rules determining the legality of weapons "also determine the lawfulness of cyber methods and means of warfare".[73] However, Schmitt and Biller hold that cyber

[67] AP I (n 21) Art. 36
[68] *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) 1996 ICJ Para. 86
[69] Ibid.
[70] Christopher Greenwood, 'The International Court of Justice and the Development of International Humanitarian Law' (2022), *International Review of the Red Cross* 104 (920-921) 1840, 1845
[71] William H. Boothby, 'Methods and Means of Cyber Warfare' (2013) 89 INT'L L. STUD. 387, 387
[72] International Committee of the Red Cross Database, 'Rule 6. Civilians' Loss of Protection from Attack' (*ICRC*) https://ihl-databases.icrc.org/en/customary-ihl/v1/rule6 accessed 2 May 2024
[73] Tallinn Manual 2.0 (n 18) Section 5 Para 1; Tallinn Manual (n 21) Rule 41 Para 2

capabilities do not qualify as either weapons or means of warfare; instead, they are methods of warfare.[74] They argue that cyber technologies themselves do not cause harm to people or property. Instead, it is the code deployed that indirectly causes harm. According to them, "the litmus test for qualifications as a means of warfare" is "the ability to directly inflict the damaging or terminal effect".[75] Since the harm does not stem from the code itself but rather from the infected targeted system, they conclude that cyber capabilities cannot be a means of warfare.

Nevertheless, the scholarly discussion reveals that no matter which side one takes on whether cyber capabilities are a weapon, means, or method of warfare, they can still be put into one of the categories, meaning that they would fall under IHL.[76] Consequently, the Nuclear Advisory Opinion arguments also apply to cyber technology.[77]

3.1.3 State's Opinions on IHL's Applicability to Cyber Operations

States have started to issue their national positions on cyber operations and the applicability of international law. In 2024, the African Union stated that they believe that IHL "govern all means and methods of warfare and reiterate that such principles apply to the use of ICTs in cyberspace as a means of warfare and afford protection to civilian ICTs during armed conflict".[78]

In 2021, Israel published their national position, stating that international law should not automatically apply in the cyber domain.[79] Instead, it should only be applicable if "the practice which arose in other domains is closely related to the activity envisaged in the cyber domain".[80]

[74] Jeffrey T. Biller and Michael N. Schmitt, 'Classification of Cyber Capabilities and Operations as Weapons, Means, or Methods of Warfare' (2019) 95 INT'L L. STUD. 179, 211
[75] Ibid. 211-212
[76] See; Ibid. 225; Tallinn Manual (n 21) Rule 41 Para 2
[77] See for example Gisel, Rodenhäuser and Dörmann (n 43) 298
[78] African Union Peace and Security Council, 'Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace' (29 January 2024) 8
[79] Roy Schöndorf, 'Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations' (2021) 97 INT'L L. STUD 395, 397
[80] Ibid. 397

Moreover, the opinio juris on the specific rule must not be meant for a particular domain. Mačák asserts that this is not how international law functions; there is no rule on the application of international law requiring that a specific domain must be examined.[81]

Further on, Mačák questions how one establishes a clear link between a rule and a specific domain. Certain rules are too general to be able to do so. Hence, he uses the principles of distinction under IHL that prohibit attacks against civilians and civilian objects that do not connect the rule to a specific type of weapon or domain in which the attack occurs. Mačák also highlights that regulations meant to only apply to certain "persons, times, locations or subject matters" already have these limitations established, not because they are domain-specific, but rather that they have an established scope of application.[82] The conclusion reached is that the starting point should always be that "international law is applicable, as a matter of principle, to all forms of human activity".[83] However, many argue that the applicability of IHL does not entice or encourage the militarisation of cyberspace, as any use of force always remains governed by the United Nations Charter.[84] This remains true regardless of whether the force is kinetic or in the cyber domain.

Other States, such as Ireland, have also released their national positions on the matter. They argue that IHL regulates cyber operations conducted in the context of, or if they in themselves amount to, an armed conflict.[85] Interestingly, they refer back to the GGE report, where it was affirmed that the principles of humanity, necessity, proportionality, and distinction applied to ICTs as grounds for the applicability of IHL, even though the report never explicitly stated this. Ireland also makes it clear that they disagree with the argument that affirming IHL applicability to cyberspace would encourage or legitimize "the militarisation of cyberspace".[86]

[81] Mačák (n 39) 416
[82] Ibid.
[83] Ibid. 417
[84] Gisel, Rodenhäuser and Dörmann (n 43) 301
[85] Irish Department of Foreign Affairs, 'Position Paper on the Application of International Law in Cyberspace' (8 July 2023) Para. 29
[86] Ibid. Para. 32

Costa Rica agrees with Ireland, stating that they join the "global consensus of States" that IHL applies both in "cyberspace and to cyber operations during armed conflicts".[87] They use the ICJ's Nuclear Advisory Opinion as an argument and hold, just like Ireland, that the affirmation of IHL's applicability does not encourage the militarization of cyberspace. Instead, they argue that the framework is restrictive, meaning it "acts as a constraint, not an enabler of conflict".[88]

3.1.4 Conclusion

To summarize, scholars widely acknowledge that IHL applies to cyber operations during armed conflicts. However, there is still debate regarding the precise application of IHL in cyber warfare, including whether cyber capabilities constitute a weapon, means, or method of warfare. The ICRC, UN, EU, and NATO have all affirmed the applicability of IHL to cyber operations. Furthermore, most States that have expressed their views on the matter have affirmed the applicability of IHL. While some States have expressed caution, fearing that the assertion that IHL applies in cyberspace may lead to its militarization, other States, such as Costa Rica, argue that the opposite is true, as IHL is a restrictive framework that will not promote militarization. Upon this examination, one can conclude that IHL, indeed, applies to cyber operations that are conducted within armed conflicts.

3.2 Can Cyber Operations Amount to an Attack under IHL?

The terms 'attack' and 'armed attack' under jus in Bello and jus ad Bellum can be confused but consist of different thresholds in nature and scope.[89] Since one of the delimitations of this essay is the fact that it only examines cyber operations in armed conflicts, in jus in Bello, whether cyber

[87] Ministry of Foreign Affairs of Costa Rica, 'Costa Rica's Position on the Application of International Law in Cyberspace' (21 July 2023) Para. 38
[88] Ibid. Para. 39
[89] See, for example; Laurie R. Blank, 'Irreconcilable Differences: The Thresholds for Armed Attack and International Armed Conflict' (2020) 96 Notre Dame L. Rev. 249

operations can amount to an 'armed attack' as understood under the UN Charter before an armed conflict has begun will not be relevant to this thesis. Instead, the focus will be on cyber operations where IHL is applicable, particularly those conducted within international armed conflicts.

Understanding the concept of 'attacks' is crucial as it forms the basis of several key features of IHL.[90] While certain societal functions are protected within and of themselves under IHL, such as medical services and objects indispensable to civilian survival, all other aspects of society's protection hinges on the legal classification of the operation against them.[91] When a cyber operation meets the criteria for an attack within the framework, it triggers legal restraints and protections that are based on the fundamental principles of IHL. These principles include the obligation to distinguish between civilians and combatants, the principle of proportionality, and precautions in attacks.[92] Thus, to examine whether civilian data is protected under IHL, one must first delve into whether cyber operations can amount to an attack.

3.2.1 IHL and Attacks in International Armed Conflicts

It was earlier established that IHL applies to cyber operations conducted during existing armed conflicts or has a nexus to one. Therefore, all Parties to the conflict will be regulated by the framework. States have acknowledged that cyber operations that are carried out in connection with, or as a part of, a kinetic operation during an armed conflict can be governed by IHL.[93] However, the question remains: can a cyber operation in and of itself be an attack without kinetic force?

Article 49(1) of Additional Protocol I clarifies that an attack is an act of violence against the adversary, which could be either in offence or in defence.[94] Opinions vary regarding cyber

[90] Michael N. Schmitt, 'France Speaks out on IHL and Cyber Operations Part II' (*EJIL:Talk!*, 1 October 2019) https://www.ejiltalk.org/france-speaks-out-on-ihl-and-cyber-operations-part-ii/ accessed 2 May 2024
[91] ICRC (n 64) 43 ; Geiß and Lahmann (n 1) 19
[92] ICRC (n 3) 482
[93] Gisel, Rodenhäuser and Dörmann (n 43) 302
[94] AP I (n 21) Art. 49(1)

operations' ability to amount to an attack. However, the agreed-upon baseline seems to be that cyber operations are attacks under IHL if they reasonably foreseeably lead to "physical damage or destruction of objects, or injury or death of persons".[95] Within this line of thinking, it is clear that most cyber operations will not meet the threshold for attacks under IHL, as they often do not result in physical violence.[96] This divergence of opinions underscores the complexity of the issue.

Others argue that merely the loss of functionality caused by a cyber operation targeting a computer system or infrastructure is enough to amount to an attack.[97] The majority of the experts who worked on the Tallinn Manual 2.0 took this position, stating that if a system needs to replace physical components after being targeted, it is enough to amount to an attack.[98] Some scholars argued that it should be enough to amount to an attack if the targeted system had to be reinstalled or if a specific type of data had been targeted.[99]

The ICRC advocates for an expansive interpretation of what constitutes an attack under the IHL framework. In their view, any operation conducted by the military that has the intention to disable an object should amount to an attack.[100] They base this interpretation on two arguments. First, Article 52 of AP I references neutralization, which they conclude means that if an object's function is damaged, it is an attack. Second, they argue that IHL was created to protect both civilian lives and civilian objects against the consequences of an armed conflict. If interpretations within IHL, such as the criteria of attacks, are too strict, the purpose of the framework would be overlooked. The ICRC has also stated that if a cyber operation is "designed to disable a computer or a computer

[95] Geiss and Lahmann (n 9) 9
[96] Tilman Rodenhäuser and Mauro Vignati, '8 Rules for "civilian hackers" during war, and 4 obligations for states to restrain them' (*ICRC*, 4 October 2023) https://blogs.icrc.org/law-and-policy/2023/10/04/8-rules-civilian-hackers-war-4-obligations-states-restrain-them/ accessed 2 May 2024
[97] Tallinn Manual 2.0 (n 18) Rule 92 Para. 10
[98] Ibid.
[99] Ibid. Rule 92 Para 11.
[100] ICRC (n 64)

network", it qualifies as an attack.[101] This is a take that some scholars, such as Schmitt, think is the most reasonable.[102]

3.2.2 State's Viewpoint on Cyber Operations as Attacks in Armed Conflicts

States have started to publish their opinions regarding cyber operations and different issues, such as armed conflicts. One example is France, which published a position paper on how IHL applies to cyber operations.[103] One of the points they made was that if Art. 49(1) of AP I is interpreted in a strict view, most operations that occur between States in conflicts will never reach the qualifications needed to be classified as an attack.[104] France also agrees with the majority of experts in the Tallinn Manual that it is enough with functionality loss and that the targeted system needs to be set up anew.[105]

Australia took a much more vague route, concluding that when cyber operations "rises to the same threshold as that of a kinetic 'attack under IHL', the rules governing such attacks during armed conflicts will apply to those kinds of cyber operations".[106] The statement does not clarify much about State's actual position on the matter. Moreover, Israel flat out rejected the argument of loss of functionality of a system to be able to qualify as an attack.[107] Another State that agrees with this restrictive perspective is Peru.[108] The United States is of the opinion that the critical aspect is whether the effects of the cyber operation are reversible or not.[109] This means that cyber operations

[101] ICRC (n 3) 489
[102] Michael N. Schmitt, 'Chapter 5: Big Data: International Law Issues During Armed Conflict) in Laura A. Dickinson and Edward W. Berg (eds), *Big Data and Armed Conflict: Legal Issues Above and Below the Armed Conflict Threshold* (New York, Oxford Academic 2023) 157
[103] Schmitt (n 90)
[104] Schmitt (n 60)
[105] Ibid.
[106] Government of Australia, 'Australia Non Paper: Case Studies on the Application of International Law in Cyberspace' (2020) 8
[107] Schöndorf (n 79) 400
[108] Organization of American States, 'Improving Transparency: International Law and State Cyber Operations: Fourth Report' (5 March 2020) Para. 43, hereinafter OAS Report
[109] U.S. Department of Defense, 'Law of War Manual' (2015) Para. 16.5.1

could potentially qualify as an attack, but only if the damages made cannot be fixed by repairing or reinstalling the targeted system.

Ecuador and Guatemala take a much more expansive view than the other States mentioned.[110] Both States argue that as long as the functionality of a computer system is lost, then a cyber operation is to be considered as meeting the threshold for an attack.[111]

3.2.3 Conclusion

To summarize, there is no consensus on when cyber operations qualify as an attack under IHL, other than when they are used in conjunction with kinetic force. There is no consensus on the issue, neither within expert opinions nor State interpretations.

Furthermore, within the definition of an attack, it is stated that it is either the injury or death of persons or physical damage or destruction of objects that fulfill the notion. The baseline question should then be whether data can be an object as is understood under the IHL framework. As seen in the opinion of the ICRC, which states that any military operation with the intention of disabling an object is an attack, whether data is an object is essential. Therefore, the next section of the thesis will delve into whether data can fall under the term 'object' as understood under the law of armed conflict.

[110] OAS Report (n 108) Para. 44
[111] Ibid.

3.3 Is Data an Object under the IHL Framework?

3.3.1 Data as an Object: Two Sides

As seen above, the definition of military objectives and the prohibition of attacks on civilian objects refer to and are limited to 'objects'.[112] To answer whether data is protected under the IHL framework, one must answer if it can be an 'object' as the IHL framework interprets it. If data falls under this category, it will entail the protection of the principles of distinction, proportionality, and precaution.

The two major sides in this discussion are that data is not an object as understood under IHL, and secondly, that all, or some, data is an object as the IHL framework means. The side that argues that data cannot be understood as falling under the meaning of 'object' under IHL falls back on the argument that an object is "visible and tangible".[113] This is the view of the experts who created the Tallinn Manual.[114] Denmark, Israel, and Chile are examples of states that hold this view. If this view were to have consensus, it would mean that civilian data is not an object under IHL, meaning that military cyber operations would be allowed to be conducted against such data.[115] This would mean that there is a giant gap in the legal protection of civilians.

The other view of the issue is that all or some data should be seen as an object under the IHL framework. Examples of States that have taken this view are Finland, Germany, Romania, and Norway. This view is supported by modern society's understanding of the term object, as well as the purpose behind the relevant rules of IHL.[116] This side argues that the ICRC's commentary that mentioned objects being 'visible and tangible' only did so to differentiate between 'objects' and the

[112] AP I (n 21) Art. 51
[113] Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (ICRC 1987) Para 2008, hereinafter ICRC Commentary; Mačák (n 39) 422
[114] Tallinn Manual 2.0 (n 18) 437
[115] Mačák (n 39) 422
[116] Ibid.

general "goals and aims of the parties to the conflict".[117] The interpretation of 'object' under IHL has historically been broader than the everyday meaning of the word, as it includes both animals and locations.[118]

Another argument is that when looking at Art. 52 of the Additional Protocol in its six authentic languages, two, French and Spanish, use 'un bien'.[119] This can be translated into English as both 'a good' and as 'a property', meaning that it could be both something that is tangible and intangible. However, the ICRC Commentary answers this question, stating that it is "clear that in both English and French the word means something that is visible and tangible".[120]

According to Schmitt, cyber operations within armed conflicts have no greater clarity regarding "planning, approving, executing or commenting on an attack" if data is seen as an object.[121] If data does fall under the term 'object', and it falls under military objective, it can be attacked. However, it can be targeted if it does not belong under the term as long as the functionality is not lost. He also believes that data should not be seen as an object, agreeing with the experts from the Tallinn Manual.

Dinniss has a unique take: some data should be seen as an object while others should not.[122] She divides data into two categories: content-level data and operational-level data. The first one is, for example, medical databases and library catalogs, which she argues should not fall into the category of being an object under IHL. Operational-level data, which is such data "that gives hardware its functionality and ability to perform the tasks we require", on the other hand, she argues, should be

[117] Kubo Mačák, 'Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law' (2015) 48(1) Israel Law Review 55, 68
[118] Mačák (n 39) 422; Gisel, Rodenhäuser and Dörmann (n 43) 319
[119] Mačák (n 117) 72
[120] ICRC Commentary (n 113) Para 2007-8; See also Michael N. Schmitt, 'The Notion of 'Objects' during Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision' (2015) 48(1) Israel Law Review 81, 95
[121] Schmitt (n 120) 101
[122] Heather A. Harrison Dinniss, 'The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives' (2015) 48(1) Israel Law Review 39, 41

such an object.[123] Schmitt rejects this stance and argues that when such data is attacked in a cyber operation, even if not an object under IHL, it would lead to a loss of functionality in the system.[124] Therefore, he argues that the operation that targets this data, which is in a civilian system and results in the loss of its functionality, is prohibited without being classified as an object in and of itself.

It should be noted that the ICRC takes on the position that the protection granted by IHL should not be lessened because documents move from papers to files on a computer.[125] They take the position that data nowadays is "an essential component of the digital domain and a cornerstone of life in many societies" and therefore, if the "deleting or tampering with essential civilian data would not be prohibited by IHL in today's ever more data-reliant world" it would not "reconcile with the object and purpose" of IHL.[126]

3.3.2 Conclusion

As seen within the discourse surrounding the treatment of data under IHL, there is a notable lack of clarity regarding its classification as an 'object'. Rather than taking a definitive stance on this question, this thesis explores an alternative avenue: international human rights law. By shifting the focus toward this framework, the aim is to investigate whether civilian data can find adequate protection during armed conflicts. This approach recognizes the complexity of the ongoing debate while hopefully offering a constructive way forward. Through this exploration, the thesis highlights potential avenues for safeguarding civilian data, thus contributing to the broader discussion on the nexus of technology, conflict, and human rights.

---

[123] Ibid. 41
[124] Schmitt (n 120) 102
[125] ICRC (n 3) 490
[126] International Committee of the Red Cross, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflict' (*ICRC*, 2019) https://www.icrc.org/en/document/icrc-report-ihl-and-challenges-contemporary-armed-conflicts accessed 2 May 2024, 28

4. The Right to Privacy and Data Protection Under International Human Rights Law

The preceding section demonstrated that IHL applies to cyber operations that occur during armed conflicts. However, a fundamental ambiguity remains regarding the classification of data as an object within the framework of IHL. In order to investigate the protection afforded to civilian data during armed conflict, attention will now shift to international human rights law (IHRL) frameworks, with an emphasis on the right to privacy.

This section will delve into the obligations of States regarding data protection, as outlined by both human rights law in treaties and customary law. The first part will examine the protection of data in peacetime within the human rights framework. Following this, it will explore the extent to which these rights and obligations, typically applicable in peacetime, can be extended to periods of armed conflicts and, if so, in what capacity.

4.1 International Human Rights Law During Peace-Time

Some examples of crucial civilian data that could be targeted by adversarial military cyber operations that aim to disrupt societal functions in enemy territories during armed conflicts are: “civil registries, insurance data, medical data and social security data, tax records, and bank accounts”.[127] This type of data is typically protected under data protection frameworks.

In short, data protection consists of the frameworks that are meant to protect individuals' personal data. In modern society, data is consistently collected, for example, when ordering products online,

[127] Geiß and Lahmann (n 1) 568

registering for email lists, and visiting a doctor.[128] Even in circumstances when persons are entirely unaware that their data is being collected, information is most likely still captured. It is essential that data protection laws be implemented in order to make sure that individuals' data is not exploited and collected without a reason for it. The core of the right to privacy is the protection of oneself from the outside.[129] Within this right, an individual's autonomy over their personal information is encompassed, including the right to control the collection, storage, and dissemination of the data.[130]

4.1.1 The Right to Privacy and Data Protection in International Human Rights Law

Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights states that no one shall be subjected to arbitrary or unlawful interference with their privacy.[131] According to General Comment Number 16 of the Human Rights Committee from 1988, the collection and storage of personal information on devices such as data banks and computers fall under the right to privacy.[132] This means that offline or online communication is protected from arbitrary and unlawful interference.

Moreover, the UN Special Rapporteur 2011 on promoting and protecting the right to freedom of opinion and expression stated that "the protection of personal data represents a special form of respect for the right to privacy".[133] In 2016, the UN General Assembly passed a resolution on the

[128] Privacy International, 'The Keys to Data Protection: A Guide for Policy Engagement on Data Protection' (*Privacy International* 2018) https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf accessed 2 May 2024, 9
[129] Kristian P Humble, 'Human Rights, International Law and the Right to Privacy' (2020) 23(12) Journal of Internet Law 14, 3
[130] Asaf Lubin, 'The Rights to Privacy and Data Protection Under International Humanitarian Law and Human Rights Law' in Robert Kolb, Gloria Gaggioli and Pavle Kilibarda (eds), *Research Handbook on Human Rights and Humanitarian Law: Further Reflections and Perspectives* (Edward Elgar 2022), 12
[131] Universal Declaration of Human Rights (adopted 10 December 1948) UNGA Res 217 A(III) Art. 12, hereinafter UDHR; International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 Art. 17, hereinafter ICCPR
[132] UN Human Rights Committee, 'CCPR General Comment No 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation' (8 April 1988) UN Doc. HRI/GEN/1/Rev Para 10, hereinafter General Comment No 16
[133] UN Human Rights Council, 'Report of the Special rapporteur on the promotion and protection of the right to freedom and expression' (16 May 2011) UN Doc. A/HRC/17/27, Para 58

right to privacy in the digital age. In the resolution, it was made clear that "States must respect international human rights obligations regarding the right to privacy /.../ when they require disclosure of personal data from third parties, including private companies".[134] Thus, one can conclude that according to the UN, the right to privacy and data protection are clearly interlinked.

4.1.1.1 Key Principles of the Right to Privacy

In addition to the protection within treaties, today, there is a substantial amount of jurisprudence and commentary regarding the scope of these rights. For example, courts have recognized that almost every step of handling personal data can interfere with the right to privacy, from the gathering of data to the use, retention, and sharing of it.[135] From the extensive jurisprudence of varying courts, treaty law, and soft law, recurring key principles can be identified in relation to the right to privacy in today's society. Five of these fundamental principles will be examined here.

The principle of legality is fundamental to all instruments within international human rights law. It entails that all restrictions on human rights from a State need to be prescribed by law.[136] The UN General Assembly asserted that these regulations must be "publicly accessible, clear, precise, comprehensive and non-discriminatory".[137] In relation to surveillance and the right to privacy, the European Court of Human Rights has stated that there cannot be any secret rules, guidelines, or interpretations of rules, as this does not reach the quality of law.[138] Furthermore, the law must be foreseeable regarding its effects, and it also needs to be specific enough that one is able to regulate one's actions accordingly.[139] The UN High Commissioner for Human Rights on the Right to Privacy

[134] UNGA Res 71/199 (15 January 2017) UN Doc. A/RES/71/199 Para 3
[135] Human Rights Watch, 'Data Privacy is a Human Right' (*Human Rights Watch* 19 April 2018) https://www.hrw.org/news/2018/04/19/data-privacy-human-right accessed 3 May 2024
[136] See; for example ICCPR (n 131) Art. 17
[137] UNGA Res 72/180 (19 December 2019) UN Doc. A/RES/72/180 Para J
[138] *Case of Silver and Others v. the United Kingdom*, App no 5947/71; 6205/73; 7052/75; 7107;75; 7113/75; 7136/75 (ECtHR, 25 March 1983) Para. 85-86; *Malone v. the United Kingdom*, App no 8691/79 (ECtHR 2 August 1984) Para 67
[139] *Ivanschenko v. Russia* App no 61064/10 (ECtHR 13 February 2018) Para 72

in the Digital Age also stated that when it comes to clear laws, they cannot have vague or overly done justifications "such as unspecific reference to "national security"".[140]

Next, the principle of necessity states that any measure taken that intrudes on the right to privacy needs to be necessary in the circumstances of the present case.[141] There also needs to be a legitimate aim, which the actions taken are necessary to achieve. The Human Rights Committee has stated that "it is not sufficient that the restrictions serve the permissible purposes; they must also be necessary to protect them".[142]

Third is the principle of proportionality, according to which one needs to stay within the appropriate actions taken to achieve a legitimate purpose.[143] The balance between intrusion of internet privacy rights and the gain of doing an investigation by public authority in the interest of the public is part of this principle.[144] Proportionality should be measured on a case-by-case basis, in "the light of all circumstances".[145] In the end, the chosen course of action has to be the least intrusive while still being able to achieve the result that is desired.[146]

In an effective justice system that grants rights, there also needs to be remedies to potential infringements, which is why the fourth principle is the access to remedy. It puts an obligation on States to guarantee victims of right infringements "proper access to effective remedies in cases of

[140] UN High Commissioner for Human Rights, 'The Right to Privacy in the digital age' (3 August 2018) A/HRC/39/29, Para 35
[141] *Toonen v. Australia,* No 488/1992 (UN Doc. CCPR/C/50/D/488/1992 31 March 1994) Para 8.3
[142] UN Human Rights Committee, 'CCPR General Comment No. 27: Article 12 (Freedom of Movement)' (2 November 1999) UN Doc. CCPR/C/21/rev.1/Add.9, hereinafter General Comment No. 27; for applicability to Art.17 see; UN Human Rights Council, 'Report of the Office of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age' (30 June 2014) UN Doc. A/HRC/27/37 Para 25, hereinafter Report on Right to Privacy in the Digital Age
[143] Case C - 239/12 and C-594/12 *Digital RIghts Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärtner Landesregierung and Others* (2014) Para 46
[144] UNGA, 'Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism' (23 September 2014) A/69/397 Para. 51
[145] *Klass and Others v. Germany*, App no 5029/71 (ECtHR 6 September 1978) Para 42
[146] General Comment No.27 (n 142); Report on the Right to Privacy in the Digital Age (n 142) Para 25

abuse".[147] Part of effective remedies is the involvement of "prompt, thorough and impartial investigation of alleged violations".[148] These investigations shall be made by an oversight body that is independent and follow and apply due process and judicial oversight.

Lastly, the umbrella principle of adequate safeguards that have the purpose to limit and avoid abuses of power.[149] It contains procedural requirements that are essential to prevent abuse, for example, in investigations of criminal activity. The European Court of Human Rights has set forth minimum safeguards that should be in law when it comes to secret measures of surveillance.[150] When it comes to data, they conclude that these include the procedure that is to be followed when it comes to "examining, using and storing the data obtained", which precautions should "be taken when communicating the data to other parties", and how the erasure and destruction of the recordings may or must be done.

4.1.2 Data Protection as a Standalone Right?

Several instruments have been created that regulate data protection as a standalone right. Examples are the non-binding UN Guidelines for the Regulation of Computerized Personal Data Files from 1990, the OECD guidelines, and the international treaty with most states in this regard, the Council of European Convention 108.[151] However, as stated before, it is mainly suggested that protection of data derive from the right to privacy.[152] In other words, the "standalone right to data protection is not recognized in the contemporary corpus of human rights law".[153]

---

[147] UN Human Rights Committee, 'Concluding Observations: Belarus' (22 November 2018) CCPR/C/BLR/CO/5 Para 44

[148] UN High Commissioner for Human Rights, 'Report of the Office of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age' (30 June 2014) A/HRC/27/37 Para 41

[149] See; for example *Weber and Saravia v. Germany*, App No 54934/00 (ECtHR 29 June 2006) Para 95

[150] Ibid.

[151] UN Special Rapporteur, 'Guidelines for the Regulation of Computerized Personal Data Files' (14 December 1990) UN Doc. E/CN.4/Sub.2/1988/1; Organization for Economic Co-operation and Development, 'OECD guidelines on the protection of privacy and transborder data flows of personal data' (1980); Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) (adopted 15 June 1999)

[152] Ex. *Z v. Finland*, App No 22009/93 (ECtHR 25 February 1997)

[153] Lubin (n 130) 11

Still, there has been a shift in recent times, separating the right to privacy and protection of data in order to make it a standalone right. The most distinct example is the Charter of Fundamental Rights of the European Union, where Article 8 stipulates a right to the protection of personal data that concerns an individual.[154] There are also national laws regulating privacy and data protection. Some countries have even adopted a right to data protection as a constitutional right. However, there are key aspects of these frameworks that differ in both scope and applicability, meaning that the protection varies to a great extent.[155]

The EU's General Data Protection Regulation (GDPR) went into effect in 2018.[156] This instrument has a broad jurisdictional reach, and the vision is that as more and more companies prioritize becoming GDPR-compliant, a normative standard will evolve that can act as a starting point for both national and regional legislation.[157]

Nevertheless, one must also remember that most of these regulations regarding data protection have derogable rights. The ILC stated in its 2006 report that the principle of derogability is based on the balance of privacy concerns and other value-interests.[158] Examples of such interests are; "national security, public order (ordre public), public health or morality or in order to protect the rights and freedoms of others, as well as the need for effective law enforcement and judicial cooperation".[159] These exemptions are common within these data protection regimes.

---

[154] Charter of Fundamental Rights of the European Union (adopted 2 October 2000, entered into force 2009) Art.8
[155] Rolf H. Weber and Dominic N. Staiger, 'Privacy versus Security' in Joanna Kulesza and Roy Balleste (eds), *Cybersecurity and Human Rights in the Age of Cyberveillance* (Rowman & Littlefield 2016), 65
[156] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR) (2016) OJ L 119/1, hereinafter GDPR
[157] Lubin (n 130) 13
[158] ILC, 'Report of the International Law Commission on the Work of its Fifty-Eighth Session' (2006) UN Doc. (A/61/10), 224
[159] Ibid.

4.2 Data Protection in Armed Conflicts?: Intersection of International Human Rights Law and International Humanitarian Law

In the ICRC's annual report from 2019 on the challenges IHL faces from modern armed conflicts, they stated that international human rights law might be able to regulate some use of digital technology regarding surveillance and disinformation, whereas IHL cannot. However, they did not expand further on the relationship between the two frameworks. This needs to be clarified, both in regards to whether they are able to apply at the same time and, if they are, to what extent.

Although there has been instances where the intersection of human rights and humanitarian law have been brought up, it is often quite vague when it comes to the right to privacy and data protection. For example, in the Palestinian Wall Advisory Opinion from the ICJ, it was brought up that Article 17 of the ICCPR, the right to privacy, applied to the territories of Palestine that were occupied.[160] However, they did not specify how it applied. Moreover, the ICRC touched on the intersection of the two frameworks regarding hospital ships that communicate personal health data in armed conflicts, stating that "such data must be afforded a reasonable level of security".[161]

In Article 31(3)(c) of the Vienna Convention on the Law of Treaties, it is exclaimed that the interpretation of treaties is allowed to consider "relevant rule of international law applicable in the relations between the parties".[162] The article hints that the treaty considers international law as a cohesive framework that is characterized by interconnectedness among its various legal sources.[163] Additionally, Article 72 of Additional Protocol I to the Geneva Conventions states that

[160] *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory* (Advisory Opinion) 2004 ICJ Para. 128, hereinafter Palestinian Wall Advisory Opinion
[161] International Committee of the Red Cross, 'Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea: Commentary of 2017' (*ICRC*, 2017) https://ihl-databases.icrc.org/en/ihl-treaties/gcii-1949/introduction/commentary/2017 accessed 2 May 2024, Para. 2395
[162] Vienna Convention on the Law of Treaties (adopted 23 May 1969) Art. 31(3)(c)
[163] Daniel Ivo Odon, *Armed Conflict and Human Rights Law: Protecting Civilians and International Humanitarian Law*, (Oxford, 1st ed., Oxford, Routledge 2022), 88

humanitarian law provisions serve as supplementary to existing international law rules concerning the safeguarding of fundamental human rights in times of armed conflict.[164]

The issue is that many see IHL as lex specialis as it only applies in times of armed conflict and, therefore, has a narrower scope.[165] IHRL, on the other hand, may at first glance seem to be of lex generalis character, as it is based on the principle of universality and applies at all times. However, there are many crossovers between the two frameworks, and from a theoretical standpoint both regimes have common legal grounds on which they are able to interact.[166] Furthermore, both IHRL and IHL share human dignity as a common ideal.[167]

Three different theoretical models can be applied to the relationship between IHRL and IHL: the displacement model, the complementarity, and the conflict resolution model.[168]

The displacement model argues that when an armed conflict occurs, IHL is lex specalis and governs exclusively, and therefore, it completely displaces human rights in these situations. However, very few adhere to this method as it is an extreme one. It would also minimize the serious commitments that have been made to human rights law.[169]

Moving on, the model of complementarity assumes that both frameworks are applied simultaneously and are interpreted in conjunction with each other.[170] This approach relies on the fact that both bodies of law are based on the common goal of protecting human life and human dignity.[171] The ICJ asserted in the Palestinian Wall Advisory Opinion that "the Court will have to

[164] AP I (n 21) Art. 72
[165] Odon (n 163) 85
[166] Ibid. p.84
[167] Ibid.
[168] Lubin (n 130) 19
[169] Ibid; Oona A. Hathaway and others, 'Which law Governs during Armed Conflict? The Relationship Between International Humanitarian Law and Human Rights Law' (2012) 96 *Minnesota Law Review* 1883, 1897
[170] Hathaway and others (n 169) 1886
[171] Ibid. 1897

take into consideration both these branches of international law, namely human rights law and, as lex specialis, international humanitarian law".[172] In General Comment Number 31, the UN Human Rights Committee stated that the "more specific rules of international humanitarian law may be specially relevant for the purposes of the interpretation of Covenant rights, both spheres of law are complementary, not mutually exclusive".[173] This model faces two critical challenges.[174] Firstly, it does not offer a straightforward solution for situations where IHRL and IHL are irreconcilable with each other. Secondly, if there is tension between the two frameworks, a compromise may be necessary, potentially diluting their integrity and diminishing their ability to protect rights effectively. In doing so, the very purpose of the model - which is to safeguard both bodies of law by simultaneous application - could be compromised.

Lastly, the conflict resolution model has been suggested by scholars to address the problems that were previously outlined.[175] This model applies the complementary model when there is a harmonious relationship between IHRL and IHL. However, in cases of conflict between the two frameworks, the model gives specific tools that can be used to resolve the tension. Three alternative tools have been suggested for resolving these potential conflicts. The first tool is event-specific displacement, which asserts that humanitarian law displaces human rights law when a dispute arises between them.[176] The second tool, reverse event-specific displacement, favors instead human rights law over humanitarian law in all instances of conflict.[177] Lastly, the specificity rule states that the legal framework most tailored to the specific circumstances of the case at hand should be favored.[178]

[172] Palestinian Wall Advisory Opinion (n 160) 106
[173] UN Human Rights Committee, 'General Comment No. 31: The Nature of the General Legal Obligations Imposed on States Parties to the Covenant' (26 May 2004) U.N. Doc. CCPR/C/21/Rev.1/Add.13, Para. 11, hereinafter General Comment No. 31
[174] Hathaway and others (n 169) 1902; Lubin (n 130) 19
[175] Lubin (n 130) 19
[176] Hathaway p.1906
[177] Ibid. 1909
[178] Ibid. 1910

Lubin contends that while there, in certain instances, will be tension between IHRL and IHL, such conflicts are rare.[179] He specifically points to the area of advanced surveillance and communication technologies, highlighting examples such as military encryption protocols and the handling of biometric data of an occupying power, and argues that IHL, in most of these cases, will remain silent on the issues. IHRL, on the other hand, has evolved at a much higher pace to address the challenges posed by modern technology, while IHL has not been able to keep the same pace. Consequently, Lubin suggests that conflicts between the two bodies of law, particularly when it comes to the protection of data, are minimal. He proposes that in most cases, existing treaties and customary laws on the right to privacy and data protection can be directly applied to situations IHL governs to fill the gaps.[180] This is the stance that the thesis will apply going forward.

4.2.1 Potential Issues Regarding the Application of IHRL in Armed Conflicts

While the thesis now has established that IHRL and IHL are both applicable in times of armed conflict, some issues still need to be addressed when it comes to applying IHRL to armed conflict. Possible derogations, extraterritorial applications, and the customary nature of the right to privacy will be discussed shortly.

4.2.1.1 Derogations

Derogability was touched upon under section 4.1.2. However, the possible derogation of the right to privacy has not been examined. Why apply the human rights regime, including the right to privacy, to armed conflicts if these rights can be derogated, such as when national security is at risk?

Article 4(1) of the ICCPR contains the possibility of derogation from certain rights, including the one in Article 17.[181] The derogation is only possible in "time of public emergency which threatens

[179] Lubin (n 130) 20
[180] Ibid. 20-21
[181] ICCPR (n 131) Art. 4(1) and Art. 4(2)

the life of the nation".[182] The Human Rights Committee has, in their General Comment No. 29, stated that the fact that there is an ongoing armed conflict in and of itself is not enough to fulfill this threshold of a threat.[183] The State needs to, in fact, show that there is a threat to the life of their nation. If it fails to do so, human rights will still apply at the same time as IHL.

Moreover, even if a State manages to show that there is a public emergency that fulfills the threat threshold, it does not mean that it can use any course of action to derogate from the right to privacy.[184] Only necessary and proportionate derogations, where the measure taken is "strictly required by the exigencies of the situation".[185]

4.2.1.2 Extraterritorial Application

This thesis will not delve deeply into the issue of human rights and whether or not one can apply human rights extraterritorial. In the Human Rights Committee General Comment 31, they conclude that States "must respect and ensure the rights" from the covenant "to anyone within the power or effective control" of the State, even if the individual "is not situated within the territory of the State Party".[186] This is the same position as this thesis will take regarding the issue. It is also worth mentioning that the five principles discussed under the right to privacy in relation to data protection are applicable extraterritorial.[187]

[182] Ibid. Art. 4(1)
[183] UN Human Rights Committee, 'CCPR General Comment No 29: Art. 4 (Derogations during a State of Emergency)' (31 August 2001) UN Doc. CCPR/c/21/Rev 1/Add 11 Para 3
[184] Ibid. Para 4: Applies to all rights of the covenant.
[185] Ibid.; Odon (n 163) 94
[186] General Comment No. 31 (n 173) Para 10
[187] Lubin (n 130) 9

4.2.1.3 Is the Right to Privacy Customary?

Another potential issue when applying the right to privacy is if the concerned State Party is not part of any human rights treaties that establish this right. Therefore, one must question whether the right to privacy is one that is customary in nature.

The right to privacy is recognized in some of the most important human rights treaties, both international and regional.[188] Moreover, at least parts of the right of privacy are included in most constitutions of States, different instruments of law, and a large amount of jurisprudence.[189] Today, nearly every country has aspects of the right to privacy as a component of their law systems.[190] According to Rengel, these recognitions of the right are enough, together with scholars highlighting the importance of the right, to establish that the right is part of customary international law.

However, the scope of the right to privacy's customary nature is debated. Nevertheless, Lubin argues forward that even so, there is a minimum portion of the right that is customary.[191] He suggests that States that are not part of treaties regulating human rights cannot use this rejection "as the sole basis for their refusal to recognize their obligations to respect the right to privacy during armed conflict".[192]

4.3 Conclusion

To conclude, individuals data is constantly being collected in today's society. Therefore, it is of the utmost importance to protect them from exploitation. Data protection can be tied to the right to

[188] Alexandra Rengel, 'Privacy as an International Human Right and the Right to Obscurity in Cyberspace' (2014) 2(2) Groningen Journal of International Law 33, 41
[189] George E. Edwards, 'International Human Rights Law Challenges to the New International Criminal Court: The Search and Seizure Right to Privacy" (2001) 26 Yale Journal of International Law 323, 327
[190] Rengel (n 188) 42
[191] Lubin (n 130) 10
[192] Ibid.

privacy, one of the fundamental rights in international human rights law. There is extensive jurisprudence on how this protection works in peacetime, including the principles of legality, neutrality, proportionality, legal remedies, and adequate safeguards. Although there are regional and national instruments giving rise to data protection, these, more often than not, include possibilities of derogation, which means they mostly do not apply in times of conflict.

As IHRL is applicable alongside IHL during armed conflicts, the protection of data also applies in times of conflict. Although there is a possibility of derogation under this framework as well, it does not automatically apply just because an armed conflict exists.

5. Ukraine and Russia: Non-State Actors, Cyber Operations, and Civilians' Right to Privacy

At the seventh session of the Opened-Ended Working Grouop, the OEWG, in March 2024, the involvement of non-state actors in cyber operations during armed conflicts was a topic of discussion. The ICRC echoed concerns expressed by States at the session, highlighting the increasing participation of civilians who are "encouraged and supported, or otherwise deciding to, take part in cyber operations against the civilian infrastructures of countries affected by armed conflict".[193] In 2023, the ICRC emphasized that "individuals, hacker groups and companies" are now more active in cyber operations, a trend that can be seen in the conflict between Russia and Ukraine.[194] With civilians taking on a more significant role in military operations and civilian technologies such as satellite communication and cloud infrastructure being repurposed for military use, the risk of civilian casualties and damage to civilian infrastructure grows.[195] The urgency to address this issue and explore possible safeguards for protecting civilians was emphazised, including protecting civilian data.

The following sections will delve into the involvement of non-state actors in cyber operations within the context of international armed conflicts, using the conflict between Russia and Ukraine as an example. Initially, the conflict itself will be examined to provide context. Subsequently, the attention will shift toward the role of non-state actors participating in international armed conflicts through cyberspace. This will be followed by an investigation into whether IHL can protect civilian data against these actors. Finally, consideration will be given to whether IHRL can offer any protection.

[193] International Committee of the Red Cross, 'Statement on the Existing and Potential Threats in the Sphere of Information Security' (Open-Ended Working Group on Information and Communication Technology, New York, 5 March 2024) https://www.icrc.org/en/un-oewg-cyber-threats-7th-meeting-statement accessed 1 May 2024
[194] ICRC (n 2); See; for example Duguin and Pavlova (n 6)
[195] Ibid.

5.1 The Conflict Between Russia and Ukraine and the Use of Cyber

The outbreak of the war between Ukraine and Russia was in conjunction with a cyber attack. An hour before Russia invaded Ukraine on February 24th, 2022, Viasat satellites were targeted.[196] The Ukrainian military used the Viasat satellites to communicate with the front troops. Thus, the attack was a central element of the invasion.[197] According to the NCSC, it is almost certain that Russia is responsible for this attack. However, even months before the full-scale invasion took place, there was an increase of significant magnitude in hostile cyber operations from Russia.[198] In 2022, Ukraine was the target of 4,200 cyberattacks, according to Illia Vitiuk, the Head of the Department of Cyber and Information Security of the Security Service of Ukraine.[199] Moreover, as of September 12th, 2023, the Cyber Peace Institute has found that 494 cyberattacks were directed against civilian targets.[200]

As of April 2022, the Russian Foreign Ministry published a statement condemning international hackers who were executing waves of cyber operations against Russian websites.[201] In November of 2022, Microsoft claimed that hackers with close ties to the Russian military had conducted the Prestige ransomware operation that targeted both Ukrainian and Polish transportation and logistics organizations.[202]

---

[196] National Cyber Security Centre, 'Russia behind cyber attack with Europe-wide impact an hour before Ukraine invasion' (*NCSC*, 10 May 2022) https://www.ncsc.gov.uk/news/russia-behind-cyber-attack-with-europe-wide-impact-hour-before-ukraine-invasion accessed 1 May 2024

[197] Christopher Miller, Mark Scott and Bryan Bender, 'UkraineX: How How Elon Musk's space satellites changed the war on the ground' (*Politico*, 8 June 2022) https://www.politico.eu/article/elon-musk-ukraine-starlink/ accessed 2 May 2024

[198] Per-Erik Nilsson, 'Unravelling the Myth of Cyberwar - Five Hypothesis on Cyberwarfare in the Russo-Ukranian War (2014-2023)' (*FOI*, 2023) https://www.foi.se/rest-api/report/FOI-R--5513--SE accessed 1 May 2024, 38

[199] Ibid.

[200] Ibid. 40

[201] Tsvetelina J. van Benthem, 'Privatized Frontlines: Private-Sector Contributions in Armed Conflict' in *2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon)* (NATO CCDCOE 2023), 55

[202] Sean Lyngaas, 'Microsoft Blames Russian military-linked hackers for ransomware attacks in Poland and Ukraine' (*CNN* 14 November 2022) https://edition.cnn.com/2022/11/10/politics/microsoft-russian-linked-hackers-poland-ukraine/index.html accessed 1 May 2024

Malware wipers have been used most frequently during the conflict in order to destroy and encrypt data and systems.[203] An illustrative example is the attack on the Viasat satellites, as mentioned above. Another example is an attack that was discovered in March of 2023, where an actor whom the Russian State sponsored targeted EU countries.[204] They sent spear-phishing e-mails that contained malware, which allowed for files to be dropped onto the computer and then be able to access the network to collect data.[205]

5.2 Non-State Actors Engaged in Cyber Operations

A non-state actor can be defined as an individual or a group that is neither a State nor an organ of a State.[206] When it comes to cyberspace as a domain, non-state actors are more prominent than in any of the other classical domains of armed conflicts, namely land, sea, air, and space.[207] Cyberspace is a global domain accessible to nearly anyone with a computer, smartphone, or other device and an internet connection.

In the war between Russia and Ukraine and the use of cyber, non-state actors have played a significant role.[208] Both Parties to the conflict pleaded for non-state actors to join a 'cyber army' to help in the hostilities. On the Ukrainian side, they have an 'IT-army' of volunteers that operate under instructions from the Ukrainian government. They are also provided with a 14-page manual that teaches volunteers how to start.[209] One can, therefore, establish that they are under the instruction of Ukraine, and one can contribute their actions to the State.[210]

---

[203] Duguin and Pavlova (n 6) 6
[204] Brad Smith, 'Defending Ukraine: Early Lessons from the Cyber War' (*Microsoft* 22 June 2022) https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/ accessed 1 May 2024
[205] Ibid.
[206] Philip McReynolds, 'How to Think About Cyber Conflicts Involving Non-State Actors' (2015) 28(3) Philosophy and Technology 427, 428
[207] Jason Andress and Steve Winterfeld *Cyber Warfare* (Syngress 2011) 240
[208] Duguin and Pavlova (n 6) 10
[209] Ibid.
[210] ILC, 'Draft Articles on Responsibility of States for Internationally Wrongful Acts' (2001) UN Doc. A/56/10 Art. 8

However, these non-state actors who are sponsored by States and whose actions can be attributed to them are not the only ones participating.[211] It can be challenging to differentiate between those affiliated with a State and those operating independently in cyberspace. Nevertheless, some groups and individuals engaged in cyber operations claim not to be under the instructions of a State.[212] An example of such a group is Anonymous. They claim to be an online collective where individuals with the same central objective of defending fundamental rights by utilizing cyberspace can gather.[213] Usually, they select a target together and then execute a cyber operation against them in a manner they collectively have deemed appropriate. Such operations could include a DDoS attack, deleting or modifying data, and leaking sensitive information.[214] Anonymous has many times claimed that they are in a cyber war with different States that are Parties to a conflict or that they are committing cyber warfare against them.[215]

Although these types of groups and individuals do not typically carry out targeting where civilians are injured or killed, the hacking of databases and servers is still very likely to "affect civilian data on a largescale basis".[216] Most likely, it is illegal for non-state actors to engage in these types of cyber operations under the national law of their residing State.[217] However, the legislation varies a great deal between States, meaning that there is an inconsistency in addressing these cyber threats. There may also be legal gaps within national law where non-state actors could use loopholes in order to escape convictions. Additionally, cyberspace operates across borders, which sometimes makes it incredibly difficult to determine which States domestic law should apply. These are just some examples of the issues regarding domestic law being the sole legislation controlling these

[211] Duguin and Pavlova (n 6) 9
[212] Mačák (n 39) 419
[213] Russell Buchan, 'Cyber Warfare and the Status of Anonymous under International Humanitarian Law' (2016) 15(4) Chinese Journal of International Law 741, 741
[214] Ibid. 742
[215] Ibid. 743
[216] Stephan Koloßa, 'The Dangers of Hacktivism: How Cyber Operations by Private Individuals May Amount to Warfare' (*Völkerretchsblog* 15 June .2022) https://voelkerrechtsblog.org/the-dangers-of-hacktivism/ accessed 2 May 2024
[217] McReynolds (n 206) 430

individuals. Thus, it would be beneficial if international law could also offer protection for civilian data from private individuals conducting cyber operations.

5.3 Cyber Operations, Non-State Actors, and International Humanitarian Law

As established in Section 3, the law of armed conflict applies in the cyber domain. The Tallinn Manual declares the same and specifies that if non-state actors take part in cyber operations that are carried out in armed conflicts, then "their activities are subject to the law of armed conflict".[218] Furthermore, they state that the cyber operations that the individuals are engaged in need to be "in the context of and associated with the armed conflict".[219] However, it is not specified how to interpret if the targeting has a nexus to an armed conflict, but it can be assumed that this needs to be done on a case-by-case basis. For analytical purposes, the thesis will assume that cyber operations against Ukraine and Russia are conducted within the context of the international armed conflict between the two States. Therefore, these types of operations from individuals can be regulated by IHL.

Since these individuals and groups do not amount to organized armed groups and cannot be attributed to a state, the question asked under IHL is whether the actions of non-state actors can amount to direct participation in hostilities.[220] If it is concluded that they are directly participating, their protection under IHL as civilians is suspended while taking part in the conduct. Most notably, this entails that the individual can be directly attacked as if they have the status of a combatant.

The treaties regulating IHL do not define direct participation in hostilities, and the concept is not clearly interpreted either. Nevertheless, the ICRC has set forth three cumulative criteria in an

[218] Tallinn Manual 2.0 (n 18) Rule 33 Para. 6
[219] Ibid. Rule 84 Para. 3
[220] AP I (n 21) Art. 51 (3)

interpretative guide for the additional protocols.[221] Firstly, the act must meet a certain threshold of harm, where it "must be likely to adversely affect the military operations or military capacity of a party" or "inflict death, injury or destruction on persons or objects protected against direct attack".[222] Secondly, there must be direct causation "between the act and the harm".[223] Lastly, there needs to be a belligerent nexus.[224]

The main issue is whether the threshold can be fulfilled in cyber operations that do not have physical damages, where only civilian data falls victim to non-state actors. Theoretically, these individuals may be directly participating in the hostilities. However, establishing when cyber operations meet the threshold of harm required is complex.[225] Targeting that impedes one of the State Parties' communications with their troops may fulfill these criteria and constitute an armed attack, given its adverse effects on military operations.[226] Even if the harm is established, it is also difficult to confirm the link of causality between the harm and the attack.

Furthermore, if the "harm caused is not military in nature, it must still provide violent consequences, such as death, injury, or destruction, and be directed against civilians or civilians' objects".[227] Suppose individuals exclusively target civilian data, considering that most of these cyber operations do not result in physical harm, they will not meet the threshold for direct participation in hostilities.

---

[221] Nils Melzer, 'Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law' (ICRC, 2009) Part 1 Para V
[222] Ibid. Part 1 Para V(1)
[223] Ibid. Part 1 Para V(2)
[224] Ibid. Part 1 Para V(3)
[225] Russell Buchan and Nicholas Tsagourias, 'Ukranian 'IT Army': A Cyber Levée en Masse or Civilians Directly Participating in Hostilities?' (*EJIL:Talk!* 2022) https://www.ejiltalk.org/ukranian-it-army-a-cyber-levee-en-masse-or-civilians-directly-participating-in-hostilities/ accessed 1 May 2024
[226] Ibid.
[227] Angelo Stirone, 'Hacking and International Humanitarian Law' (2020) 3(1) Humanitäres Völkerrecht: Journal of International Law of Peace and Armed Conflict 123, 132; AP I (n 21) Art. 49

Referring back to the discussion in Section 3.3 about whether data qualifies as an object under IHL, it is interesting to note that even if data is deemed an object, as proposed by some scholars, it would still not necessarily be protected in scenarios where civilians are engaged in cyber operations solely targeting civilian data. This is because, as reiterated before, it does not result in physical harm.

In summary, the majority of cyber operations carried out by civilians fall short of the criteria for direct participation in international armed conflicts. While they may pose challenges for various actors, cause significant harm, and potentially be subject to prosecution under domestic criminal law, this does not make them targetable under IHL. Consequently, there are no repercussions for such individuals, such as Anonymous, who engage in cyber operations that could compromise civilian data. Therefore, civilian data lacks adequate protection from these actors under IHL.

5.4 Cyber Operations, Non-State Actors, and International Human Rights Law

5.4.1 Human Rights and Possible Obligations for Non-State Actors

Human rights law is known for adapting to new issues and modernizing its framework as society evolves.[228] With these changes, it is no surprise that IHRL norms have had to adapt to new situations by going through significant changes in the framework's scope and pre-existing norms. One such change is the application of human rights law to cyberspace, for example, the freedom of expression that is now applied both offline and online.[229] However, sometimes, it is not as easy to transition the application of existing human rights norms into the digital space as the normative gap is too big. In these cases, it might be warranted to develop new human rights.[230] Examples of such

[228] Yuval Shany, 'Digital Rights and the Outer Limits of International Human Rights law' (2023) 24(3) German Law Journal 461, 463
[229] See; UNGA, 'Special Rapporteur on the Promotion and Protection of the right to freedom of opinion and expression' (9 October 2019) UN Doc. A/74/486
[230] Shany (n 227) 463

newly created rights within the digital space are the right to be forgotten and not to be subject to algorithmic decisions.[231]

From a traditional view of international law, one has been primarily concerned with rules regarding the behavior of States. These norms could only be violated by States, and, therefore, private actors fall outside the scope of international law, including human rights law.[232] The human rights framework has expanded beyond merely limiting the authority of States. Today, positive human rights obligations are imposed, requiring governments to prevent and sanction private violations. Some argue, like Rodley, that the human rights framework and its norms only apply to "mediate the relationship between governments and their subjects".[233] This thesis will explore the opposite view, that human rights could acutally be applicable horizontally in the relationship between non-state actors.

The underlying purpose of the IHRL framework is the protection of human dignity.[234] Some scholars argue that the integrity of this fundamental principle falters when only individuals whose rights have been infringed upon by a State are afforded protection.[235] Moreover, international law states that human rights are universally effective.[236] The universality aspect should not only be applied to areas such as space or geography; instead, it should also be applied to those who have had their rights infringed upon and are protected subjects.[237]

The most prominent argument against non-state actors having human rights obligations is that the treaties of the UN regarding human rights are only binding upon States that have ratified the

[231] GDPR (n 156) Art. 17 and 21
[232] Fernando Teson *A philosophy of international law* (Routledge 1998) 163
[233] Nigel S. Rodley, 'Can Armed Opposition Groups Violate Human Rights?' in Kathleen E. Mahoney and Paul Mahoney (eds), *Human Rights in the Twenty-first Century: A Global Challenge* (Netherlands: Kluwer Academic Publishers 1993) 299
[234] Andrew Clapham *Human rights obligations of non-state actors* (Oxford, Oxford University Press 2006) 28
[235] Nicolas Carrillo Santarelli, 'Non-State Actors' Human Rights Obligations and Responsibility under International Law' (2008) 15 Revista Electronica de estudios internacionales, 2
[236] Vienna declaration and programme of action 1993 par. I.1
[237] Carrillo Santarelli (n 234) 2

instruments. Nevertheless, parts of these frameworks could indicate that non-state actors also have a certain responsibility when it comes to the human rights of individuals. In the proclamatory paragraph of the Universal Declaration of Human Rights, it is stated that;

> "every individual and every organ of society, keeping this Declaration constantly in mind, shall strive by teaching and education to promote respect for these rights and freedoms and by progressive measures, national and international, to secure their universal and effective recognition and observance, both among the people of Member States themselves and among the peoples of territories under their jurisdiction"[238]

Furthermore, in Article 29 of the UDHR, it is stated that "everyone has duties to the community in which alone the free and full development of his personality is possible".[239] Another example is Article 30 of the UDHR and Article 5(1) of both the Covenant on Economic, Social, and Cultural Rights and the Covenant on Political and Civil Rights, which states that "nothing in this /…/ may be interpreted as implying for any State, group or person any right to engage in any activity or to perform any act aimed at the destruction of any of the rights and freedoms" that are presented in the respective instrument.[240] These articles and texts are examples of when UN human rights treaties seem to open the potential for non-state actors to bear responsibilities. This was also recognized by the Fifty-fourth Commission on Human Rights, which reported that the UDHR and the two Covenants "in their preambular paragraphs recognise duties on individuals to promote respect for human rights".[241] However, some argue that they only reference an individual's responsibility to promote human rights and not that it implies binding legal obligations.[242]

---

[238] UDHR (n 131) Preamble
[239] Ibid. Art. 29
[240] Ibid. Art. 30; International Covenant on Economic, Social and Cultural Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 (ICESCR) Art. 5(1); ICCPR (n 131) Art. 5(1)
[241] UN Secretary General, 'Minimum Humanitarian Standards: Analytical Report of the Secretary-General submitted pursuant to Commission on Human Rights resolution 1997/21' (5 January 1998) UN Doc. E.CN.4/1998/87, 15
[242] Rodley (n 132) 307

Santarelli rejects the idea that non-state actors cannot have obligations under human rights law.[243] He argues that if such actors can have rights under IHRL, why must then the possibility of having obligations be immediately denied? In fact, his opinion is that if non-state actors do not have obligations under IHRL it undermines the protection it is meant to serve, and denies the standard of universality that underlines the framework.[244]

At their core, those arguing for individuals' capability to have human rights obligations emphasize the importance of effective protection of human rights, rather than focusing on identifying the violators of these obligations.

5.4.2 The Status of Human Right Obligations for Non-State Actors Today

Although the previous section presented several arguments for the potential of individuals having human rights obligations, the reality is that it is highly contested to what extent non-state actors have human rights obligations. There are possibilities for non-state actors to have human rights obligations. For example, there are attachments of rights to international organizations and armed non-state groups.[245]

Moreover, it is interesting to mention that individuals do have human rights responsibilities in some instances, such as parents under the Convention on the Rights of the Child, where they have explicit obligations.[246] There is also a 'general responsibility' of individuals to at least "respect the human

[243] Carrillo Santarelli (n 234) 3
[244] Carrillo Santarelli (n 234) 10
[245] See; Andrew Clapham, 'The Rights and Responsibilities of Armed Non-State Actors: The Legal Landscape & Issues Surrounding Engagement' (2010) Geneva Academy of International Humanitarian Law and Human Rights
[246] UN High Commissioner for Human Rights, 'Frequently asked questions on human rights-based approach to development cooperation' (2006) UN Doc. HR/PUB/06/8, 3

rights of others".[247] Still, one cannot currently say that these non-state actors have actual binding international human rights obligations.[248]

5.4.2.1 Jurisprudence from UN Human Rights Treaties Monitoring Bodies - Non-State Actors

In practice, there are two different approaches that the UN monitoring bodies have taken for different human rights treaties. These are pure indirect horizontal effects and categorical indirect horizontal effects.[249] The first one regulates the conduct of non-state actors by holding the State responsible for their breaches of human rights, meaning that the effect is perhaps more diagonal than horizontal as the focus is on the State's obligation to protect rather than on the non-state actor. This approach is partly based on the obligation of due diligence, meaning that it is more so the steps the States take, such as legal and administrative, that are focused on rather than the actual results and actions taken.[250]

The second approach concerns non-state actors who have replaced the State in certain important public functions. These groups are seen to have effective control over the territory and are thus re-categorized as public actors in order to hold them accountable for the human rights breaches they are committing.[251] So far, this approach has only been applied to non-state armed groups and is limited as most of the UN monitoring bodies, and on an international level in general, there has yet to be a case brought fully against such an actor.[252] However, the CteeAT has applied this to some extent, for example, in Sadiq Shek Elmi v. Australia, where they deemed that groups that could be

[247] Ibid. 4
[248] Lottie Lane, 'The Horizontal Effect of International Human Rights Law in Practice: A Comparative Analysis of the General Comments and Jurisprudence of Selected United Nations Human Rights Treaty Monitoring Bodies' (2018) 5(1) European Journal of Comparative Law and Governance 5, 87
[249] Ibid.
[250] Ibid. 30 and 77
[251] Ibid.
[252] Ibid. 80

seen as public authorities took over territories from Somalia, which had failed as a State.[253] It, therefore, stated that the State of Somalia no longer was relevant in the case.

Jurisprudence also clearly states that individuals do not yet have obligations. However, the monitoring bodies are clearly interacting and exploring the idea of how to hold non-state actors directly responsible for human rights violations.

5.4.3 Conclusion

As stated before, IHRL has shown its capability to evolve with societal changes. As individuals and non-state groups, with the same legal complexities as Anonymous, become more and more involved with human rights breaches, there might be a change in the future where obligations can be forced upon them. As stated before, human rights are at its core based on human dignity, and the rights belong to the individual. These natural rights should be respected not only by states but also by every entity.

The reality is that individuals partaking in cyber operations targeting civilian data in armed conflicts cannot be held directly accountable under IHRL, as IHRL primarily imposes its obligations on States. While individuals may be held accountable under domestic law, this depends on the extent to which the domestic law regulates such conduct. Since national frameworks vary in coverage and enforcement, the accountability of individuals for these actions largely depends on the specific legal provisions and enforcement mechanisms within each jurisdiction.

[253] *Sadiq Shek Elmi v. Australia* (UN Doc *CAT/C/22/D/120/1998*, CteeAT, 25 May 1999) Para 5.5 and 6.5

6. Conclusion

As discussed in Section 3, IHL is relevant and applicable to cyber operations within armed conflicts. The framework was created with the idea of being able to accommodate the evolving weapons, means, and methods of future warfare. However, there is no denying that its norms were created with more traditional forms of warfare in mind, which has led to challenges in interpreting and applying its principles to cyber operations. Two key issues include determining when a cyber operation can qualify as an attack and whether data qualifies as an object under IHL. While there is a general consensus that cyber operations whose effects resemble traditional kinetic warfare fall within the protection of IHL rules, there is still considerable debate regarding the applicability of IHL to cyber operations solely targeting data.

Exploring how data is protected under IHRL revealed its origin from the right to privacy, a fundamental international human right. The principles of legality, necessity, proportionality, access to remedy, and adequate safeguards guide the protection under the right to privacy. Moreover, IHRL remains applicable during armed conflicts, where the model of conflict resolution should guide the intersection of the two frameworks. As Lubin observes, the absence of explicit references to data protection or cyber operations in IHL ensures minimal friction between the frameworks, suggesting that IHRL's protection of data should be directly applied to address the gaps of IHL.

Examining concerns about the involvement of certain non-state actors in cyber operations during international armed conflicts, exemplified by the Russia-Ukraine conflict, unveils a new aspect of warfare that brings with it new challenges. The participation of individuals and groups such as Anonymous signifies a shift that raises even more questions about the protection of civilian data during conflicts. Under IHL, determining whether such individuals are directly participating in

hostilities remains controversial, as does establishing if the conducted cyber operation met the required harm threshold.

Furthermore, under IHRL, the possibility of protection from non-state actors is equally as daunting. There is little consensus on the possible human rights obligations of non-state actors. Consequently, there is not much within the IHRL framework that can protect civilian data from these actors during armed conflicts, except the obligations put on States.

After examination of the subsidiary questions posed in this thesis, it becomes evident that the extent of protection provided by international humanitarian law for civilian data, in particular from non-state actors, in international armed conflicts is nearly nonexistent. Similarly, IHRL fails to offer any protection in this regard. Despite the claimed adaptability of IHL to accommodate modern developments of weapons, means, and methods of warfare, groups like Anonymous have effectively employed cyber operations to partake in major armed conflicts while managing to sidestep the constraints of IHL norms. If this trend continues, allowing actors to use cyberspace to participate in conflicts without being bound by the rules of armed conflict, there is a possible risk of IHL, a legal framework of immense value, becoming obsolete.[254]

One might claim that the lack of protection within international law is not problematic as data protection is adequately addressed by both regional instruments and a majority of States' own legislation. However, as previously mentioned, these regulations, more often than not, include provisions of derogations from the protection, for example, in the interest of the State's security. Thus, the protection of civilian data in armed conflicts, especially when the perpetrators are non-state actors not associated with armed groups or States, is significantly deficient.

[254] See; for example Stirone (227) 140

6.1 Potential Next Steps: Addressing the Legal Gap

Given the significant legal gaps within international law concerning the protection of civilian data during armed conflicts, it's of utmost importance to consider what steps can be taken to enhance the protection of civilians. A crucial initial step would be to further clarify how IHL applies in cyberspace, particularly regarding the criteria for attacks and what qualifies as an object under the framework. This task should be undertaken not only by scholars but also by States. Within these discussions, it is essential to consider the consequences if data is not seen as an object and if cyber operations cannot amount to an attack without physical damage. The thesis has underscored that applying an overly restrictive interpretation of IHL would leave a huge aspect of civilian lives without protection from direct targeting.

Additionally, there needs to be further examination regarding the potential of non-state actors having human rights obligations and whether such responsibilities could develop in the future. This requires thorough consideration regarding the implications of such developments.

In addition to examining the application of IHL, both states and the international community need to take other steps.[255] At the national level, States should enforce national laws against hacking, thereby strengthening protection for civilian victims of cyber operations. Moreover, harmonizing national laws on data protection across borders could potentially ensure equal protection for individuals regardless of location.

Internationally, collaboration is essential to tackle these issues effectively. Information sharing and developing common norms and standards are examples of actions that can help establish a better approach to safeguarding civilian data in armed conflicts.

[255] See; for example Rodenhäuser and Vignati (n 96)

Furthermore, extensive research is necessary to understand the role of cyber operations, data targeting, the involvement of non-state actors, and their impact on civilian data and conflicts. Such research should also be done on current conflicts, such as the one between Russia and Ukraine, as referenced in the thesis. Additionally, further research should also be done on how the rules and protection potentially change if the conflict is a non-international armed conflict.

Hopefully, the efforts from different organizations, such as the ICRC, to finally address the issue of civilian involvement in cyber operations during armed conflicts will lead to efforts to enhance the protection of civilians and their data in these instances. By taking the outlined steps, we can address and mend the legal gaps, moving towards upholding the right to privacy in modern warfare.

Bibliography

Articles

Alexandra Rengel, ‘Privacy as an International Human Right and the Right to Obscurity in Cyberspace’ (2014) 2(2) Groningen Journal of International Law 33

Andrew Clapham, ‘The Rights and Responsibilities of Armed Non-State Actors: The Legal Landscape & Issues Surrounding Engagement’ (2010) Geneva Academy of International Humanitarian Law and Human Rights

Angelo Stirone, ‘Hacking and International Humanitarian Law’ (2020) 3(1) Humanitäres Völkerrecht: Journal of International Law of Peace and Armed Conflict 123

Byron Denham and Dale R. Thompson, ‘Ransomware and Malware Sandboxing’ (IEEE 13th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference, IEEE, 2022)

Christopher Greenwood, ‘The International Court of Justice and the Development of International Humanitarian Law’ (2022), International Review of the Red Cross 104 (920-921) 1840

George E. Edwards, ‘International Human Rights Law Challenges to the New International Criminal Court: The Search and Seizure Right to Privacy” (2001) 26 Yale Journal of International Law 323

Heather A. Harrison Dinniss, ‘The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives’ (2015) 48(1) Israel Law Review 39

Jeffrey T. Biller and Michael N. Schmitt, ‘Classification of Cyber Capabilities and Operations as Weapons, Means, or Methods of Warfare’ (2019) 95 INT’L L. STUD. 179

Kristian P Humble, ‘Human Rights, International Law and the Right to Privacy’ (2020) 23(12) Journal of Internet Law 14

Kubo Mačák, ‘Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law’ (2015) 48(1) Israel Law Review 55

Kubo Mačák, ‘Unblurring the Lines: Military Cyber Operations and International Law’ (2021) 6(3) Journal of Cyber Policy 411

Laurie R. Blank, ‘Irreconcilable Differences: The Thresholds for Armed Attack and International Armed Conflict’ (2020) 96 Notre Dame L. Rev. 249

Laurent Gisel, Tilman Rodenhäuser and Knut Dörmann, ‘Twenty Years On: International Humanitarian Law and the Protection of Civilians Against the Effects of Cyber Operations During Armed Conflicts’ (2020) 102(913) International Review of the Red Cross 287

Lottie Lane, ‘The Horizontal Effect of International Human Rights Law in Practice: A Comparative Analysis of the General Comments and Jurisprudence of Selected United Nations Human Rights Treaty Monitoring Bodies’ (2018) 5(1) European Journal of Comparative Law and Governance 5

Marco Roscini, ‘World Wide Warfare - Jus ad Bellum and the Use of Cyber Force’ (2010) 14 The Max Planck Yearbook of United Nations Law 86

Michael N. Schmitt, ‘The Notion of ‘Objects’ during Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision’ (2015) 48(1) Israel Law Review 81

Nicolas Carrillo Santarelli, ‘Non-State Actors’ Human Rights Obligations and Responsibility under International Law’ (2008) 15 Revista Electronica de estudios internacionales

Oona A. Hathaway and others, ‘Which law Governs during Armed Conflict? The Relationship Between International Humanitarian Law and Human Rights Law’ (2012) 96 *Minnesota Law Review* 1883

Philip McReynolds, ‘How to Think About Cyber Conflicts Involving Non-State Actors’ (2015) 28(3) Philosophy and Technology 427

Robin Geiß and Henning Lahmann, ‘Protection of Data in Armed Conflict’ (2021) 97 INT’L L. STUD. 556

Roy Schöndorf, ‘Israel’s Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations’ (2021) 97 INT’L L. STUD 395

Russell Buchan, ‘Cyber Warfare and the Status of Anonymous under International Humanitarian Law’ (2016) 15(4) Chinese Journal of International Law 741

William H. Boothby, ‘Methods and Means of Cyber Warfare’ (2013) 89 INT’L L. STUD. 387

Yuval Shany, ‘Digital Rights and the Outer Limits of International Human Rights law’ (2023) 24(3) German Law Journal 461

Books

Andrew Clapham *Human rights obligations of non-state actors* (Oxford, Oxford University Press 2006)

Asaf Lubin, ‘The Rights to Privacy and Data Protection Under International Humanitarian Law and Human Rights Law’ in Robert Kolb, Gloria Gaggioli and Pavle Kilibarda (eds), *Research Handbook on Human Rights and Humanitarian Law: Further Reflections and Perspectives* (Edward Elgar 2022)

Daniel Ivo Odon, *Armed Conflict and Human Rights Law: Protecting Civilians and International Humanitarian Law*, (Oxford, 1st ed., Oxford, Routledge 2022)

Eneken Tikk, Kadri Kaska and Liis Vihul, *International Cyber Incidents: Legal Considerations* (Tallinn, CCDCOE 2010)

Fernando Teson *A philosophy of international law* (Routledge 1998)

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

Jason Andress and Steve Winterfeld *Cyber Warfare* (Syngress 2011)

Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford University Press 2014)

Michael N. Schmitt, ‘Chapter 5: Big Data: International Law Issues During Armed Conflict) in Laura A. Dickinson and Edward W. Berg (eds), *Big Data and Armed Conflict: Legal Issues Above and Below the Armed Conflict Threshold* (New York, Oxford Academic 2023)

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

Michael N. Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge, 1st ed, Cambridge University Press 2013)

Rolf H. Weber and Dominic N. Staiger, 'Privacy versus Security' in Joanna Kulesza and Roy Balleste (eds), *Cybersecurity and Human Rights in the Age of Cyberveillance* (Rowman & Littlefield 2016)

Russel Buchan and Asaf Lubin, 'Introduction' in Russel Buchan and Asaf Lubin (eds), *The Rights to Privacy and Data Protection in Times of Armed Conflict* (NATO CCDCOE 2022)

Internet Resources

Brad Smith, 'Defending Ukraine: Early Lessons from the Cyber War' (*Microsoft* 22 June 2022) https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/ accessed 1 May 2024

Check Point, 'What is Wiper Malware?' (*CheckPoint*) https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/what-is-wiper-malware/ accessed 27 April 2024

Christopher Miller, Mark Scott and Bryan Bender, 'UkraineX: How How Elon Musk's space satellites changed the war on the ground' (*Politico*, 8 June 2022) https://www.politico.eu/article/elon-musk-ukraine-starlink/ accessed 2 May 2024

Frederica Cristani, 'Can Anonymous be Prosecuted? A Reflection under International Law in the Framework of the Current Armed Conflict in Ukraine' (*Centre for International Law*, 2022) https://www.iir.cz/can-anonymous-be-prosecuted-a-reflection-under-international-law-in-the-framework-of-the-current-armed-conflict-in-ukraine accessed 29 April 2024

Geneva Academy, 'Rising Civilian Involvement in Cyber Warfare: Legal Implications and Solutions Explored During Expert Meeting' (*Geneva Academy*, 20 October 2023) https://www.geneva-academy.ch/news/detail/650-rising-civilian-involvement-in-cyber-warfare-legal-implications-and-solutions-explored-during-expert-meeting

Human Rights Watch, 'Data Privacy is a Human Right' (*Human Rights Watch* 19 April 2018) https://www.hrw.org/news/2018/04/19/data-privacy-human-right accessed 3 May 2024

Michael N. Schmitt, 'France Speaks Out on IHL and Cyber Operations Part I' (*EJIL:Talk!*, 30 September 2019) https://www.ejiltalk.org/france-speaks-out-on-ihl-and-cyber-operations-part-i/ accessed 1 May 2024

Michael N. Schmitt, 'France Speaks out on IHL and Cyber Operations Part II' (*EJIL:Talk!*, 1 October 2019) https://www.ejiltalk.org/france-speaks-out-on-ihl-and-cyber-operations-part-ii/, accessed 1 May 2024

National Cyber Security Centre, 'Russia behind cyber attack with Europe-wide impact an hour before Ukraine invasion' (*NCSC*, 10 May 2022) https://www.ncsc.gov.uk/news/russia-behind-cyber-attack-with-europe-wide-impact-hour-before-ukraine-invasion accessed 1 May 2024

Per-Erik Nilsson, 'Unravelling the Myth of Cyberwar - Five Hypothesis on Cyberwarfare in the Russo-Ukranian War (2014-2023)' (*FOI*, 2023) https://www.foi.se/rest-api/report/FOI-R--5513--SE accessed 1 May 2024

Privacy International, 'The Keys to Data Protection: A Guide for Policy Engagement on Data Protection' (*Privacy International* 2018) https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf accessed 2 May 2024

Robin Geiss and Henning Lahmann, 'Protecting Societies: Anchoring a New Protection Dimension in International Law in Times of Increased Cyber Threats' (*Geneva Academy*, 2021)

https://www.geneva-academy.ch/joomlatools-files/docman-files/working-papers/Protecting%20Societies%20-%20Anchori.pdf accessed 1 May 2024

Russell Buchan and Nicholas Tsagourias, 'Ukranian 'IT Army': A Cyber Levée en Masse or Civilians Directly Participating in Hostilities?' (*EJIL:Talk!* 2022) https://www.ejiltalk.org/ukranian-it-army-a-cyber-levee-en-masse-or-civilians-directly-participating-in-hostilities/ accessed 1 May 2024

Sean Lyngaas, 'Microsoft Blames Russian military-linked hackers for ransomware attacks in Poland and Ukraine' (*CNN* 14 November 2022) https://edition.cnn.com/2022/11/10/politics/microsoft-russian-linked-hackers-poland-ukraine/index.html accessed 1 May 2024

Stephan Koloßa, 'The Dangers of Hacktivism: How Cyber Operations by Private Individuals May Amount to Warfare' (*Völkerretchsblog* 15 June .2022) https://voelkerrechtsblog.org/the-dangers-of-hacktivism/ accessed 2 May 2024

Stéphane Duguin and Pavlina Pavlova, 'The Role of Cyber in the Russian War against Ukraine: Its Impact and the Consequences for the Future of Armed Conflict' (European Parliament, September 2023) https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf accessed 1 May 2024

TechTerms, 'Data Definition' (*TechTerms*, 13 December 2022) https://techterms.com/definition/data accessed 1 May 2024

Official Materials and Rapports

African Union Peace and Security Council, 'Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace' (29 January 2024)

Council of the European Union, 'General Affairs Council Meeting' (Brussels, Council of the European Union, 25 June 2013) Doc. No. 11357/13

Cuba, 'Declaration by Miguel Rodriquez, Representative of Cuba' (Speech at the final session of group of governmental experts on developments in the field of information and telecommunications in the context of international security, New York, 23 June 2017)

Government of Australia, 'Australia Non Paper: Case Studies on the Application of International Law in Cyberspace' (2020)

Irish Department of Foreign Affairs, 'Position Paper on the Application of International Law in Cyberspace' (8 July 2023)

Ministry of Foreign Affairs of Costa Rica, 'Costa Rica's Position on the Application of International Law in Cyberspace' (21 July 2023)

Organization for Economic Co-operation and Development, 'OECD guidelines on the protection of privacy and transborder data flows of personal data' (1980)

Organization of American States, 'Improving Transparency: International Law and State Cyber Operations: Fourth Report' (5 March 2020)

Tsvetelina J. van Benthem, 'Privatized Frontlines: Private-Sector Contributions in Armed Conflict' in *2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon)* (NATO CCDCOE 2023)

U.S Department of Defense, 'Law of War Manual' (2015)

U.S Department of State, 'Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security' (U.S Department of State, 23 June 2017)

https://2017-2021.state.gov/explanation-of-position-at-the-conclusion-of-the-2016-2017-un-group-of-governmental-experts-gge-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-sec/ accessed 1 May 2024

United States, ‘DoD Dictionary of Military and Associated Terms’ (March 2017) 113

UN Materials

ILC, ‘Draft Articles on Responsibility of States for Internationally Wrongful Acts’ (2001) UN Doc. A/56/10

ILC, ‘Report of the International Law Commission on the Work of its Fifty-Eighth Session’ (2006) UN Doc. (A/61/10)

UNGA, ‘Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism’ (23 September 2014) A/69/397

UNGA, ‘Special Rapporteur on the Promotion and Protection of the right to freedom of opinion and expression’ (9 October 2019) UN Doc. A/74/486

UNGA First Committee (53rd Session) ‘Agenda Item 63: Role of Science and Technology in the Context of International Security, disarmament and other Related Fields’ (30 September 1998) UN Doc. A/C.1/53/3

UNGA Group of Governmental Experts (68th Session) ‘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/68/96

UNGA Group of Governmental Experts (70th Session) ‘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

UNGA Group of Governmental Experts (76th Session) ‘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

UNGA Human Rights Council, ‘Report of the Special rapporteur on the promotion and protection of the right to freedom and expression’ (16 May 2011) UN Doc. A/HRC/17/27

UNGA Res 53/70 (4 January 1999) UN Doc. A/RES/53/70

UNGA Res 71/199 (15 January 2017) UN Doc. A/RES/71/199

UNGA Res 72/180 (19 December 2019) UN Doc. A/RES/72/180

UNGA Res 73/27 (5 December 2018) UN Doc. A/RES/73/27

UN High Commissioner for Human Rights, 'Frequently asked questions on human rights-based approach to development cooperation' (2006) UN Doc. HR/PUB/06/8

UN High Commissioner for Human Rights, 'Report of the Office of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age' (30 June 2014) A/HRC/27/37

UN Human Rights Committee, 'CCPR General Comment No. 27: Article 12 (Freedom of Movement)' (2 November 1999) UN Doc. CCPR/C/21/rev.1/Add.9

UN Human Rights Committee, 'CCPR General Comment No 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation' (8 April 1988) UN Doc. HRI/GEN/1/Rev

UN Human Rights Committee, 'CCPR General Comment No 29: Art. 4 (Derogations during a State of Emergency)' (31 August 2001) UN Doc. CCPR/c/21/Rev 1/Add 11

UN Human Rights Committee, 'Concluding Observations: Belarus' (22 November 2018) CCPR/C/BLR/CO/5

UN Human Rights Committee, 'General Comment No. 31: The Nature of the General Legal Obligations Imposed on States Parties to the Covenant' (26 May 2004) U.N. Doc. CCPR/C/21/Rev.1/Add.13

UN Human Rights Council, 'Report of the Office of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age' (30 June 2014) UN Doc. A/HRC/27/37

UN Office for Disarmament Affairs, 'Developments in the Field of Information and Telecommunications in the context of international security' https://disarmament.unoda.org/ict-security/ accessed 2 May 2024

UN Secretary General, ‘Minimum Humanitarian Standards: Analytical Report of the Secretary-General submitted pursuant to Commission on Human Rights resolution 1997/21’ (5 January 1998) UN Doc. E.CN.4/1998/87

UN Special Rapporteur, ‘Guidelines for the Regulation of Computerized Personal Data Files’ (14 December 1990) UN Doc. E/CN.4/Sub.2/1988/1

Case Law

Case C - 239/12 and C-594/12 *Digital RIghts Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärtner Landesregierung and Others* (2014)

Case of Silver and Others v. the United Kingdom, App no 5947/71; 6205/73; 7052/75; 7107;75; 7113/75; 7136/75 (ECtHR, 25 March 1983)

Ivanschenko v. Russia App no 61064/10 (ECtHR 13 February 2018)

Klass and Others v. Germany, App no 5029/71 (ECtHR 6 September 1978)

Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory (Advisory Opinion) 2004 ICJ

Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion) 1996 ICJ

Malone v. the United Kingdom, App no 8691/79 (ECtHR 2 August 1984)

Sadiq Shek Elmi v. Australia (UN Doc *CAT/C/22/D/120/1998*, CteeAT, 25 May 1999)

Toonen v. Australia, No 488/1992 (UN Doc. CCPR/C/50/D/488/1992 31 March 1994)

Weber and Saravia v. Germany, App No 54934/00 (ECtHR 29 June 2006)

Z v. Finland, App No 22009/93 (ECtHR 25 February 1997)

Treaties and Conventions

Charter of Fundamental Rights of the European Union (adopted 2 October 2000, entered into force 2009)

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) (adopted 15 June 1999)

Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (First Geneva Convention) (adopted 12 August 1949) 75 UNTS 31

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

Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention) (12 August 1949) 75 UNTS 287

Geneva Convention Relative to the Treatment of Prisoners of War (Third Geneva Convention) (adopted 12 August 1949) 75 UNTS 135

International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171

International Covenant on Economic, Social and Cultural Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 (ICESCR)

NATO, 'Wales Summit Declaration issued by the heads of State and government participating in the meeting of NATO in Wales' (Wales, NATO, 5 September 2014)

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of International Armed Conflicts (Protocol I) (adopted 8 June 1977) 1125 UNTS 3

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II) (adopted 8 June 1977) 1124 UNTS 609

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR) (2016) OJ L 119/1

Universal Declaration of Human Rights (adopted 10 December 1948) UNGA Res 217 A(III)

Vienna Convention on the Law of Treaties (adopted 23 May 1969)

ICRC Material

ICRC, 'International Humanitarian Law and Cyber Operations During Armed Conflicts' (2020) 102(913) International Review of the Red Cross 481

ICRC, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts' (*ICRC*, 2015) https://www.icrc.org/en/download/file/15061/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf accessed 2 May 2024

International Committee of the Red Cross, 'Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea: Commentary of 2017' (*ICRC*, 2017) https://ihl-databases.icrc.org/en/ihl-treaties/gcii-1949/introduction/commentary/2017 accessed 2 May 2024

International Committee of the Red Cross, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflict' (*ICRC*, 2019) https://www.icrc.org/en/document/icrc-report-ihl-and-challenges-contemporary-armed-conflicts accessed 2 May 2024

International Committee of the Red Cross, 'Statement by the International Committee of the Red Cross (ICRC)' (Open-Ended Working Group on Information and Communication Technology, New York, 13 December 2023) https://www.icrc.org/en/statement-cyber-oewg-sixth-session accessed 28 April 2024

International Committee of the Red Cross, 'Statement on the Existing and Potential Threats in the Sphere of Information Security' (Open-Ended Working Group on Information and Communication Technology, New York, 5 March 2024) https://www.icrc.org/en/un-oewg-cyber-threats-7th-meeting-statement accessed 1 May 2024

International Committee of the Red Cross, 'What Limits Does the Law of War Impose on Cyber Attacks?' (ICRC, 28 June 2013)

https://www.icrc.org/en/doc/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm accessed 30 April 2024

International Committee of the Red Cross (ICRC), 'Fundamental Principles of IHL' (How Does Law Protect in War?) https://casebook.icrc.org/a_to_z/glossary/fundamental-principles-ihl, accessed 1 May 2024

International Committee of the Red Cross Database, 'Rule 6. Civilians' Loss of Protection from Attack' (*ICRC*) https://ihl-databases.icrc.org/en/customary-ihl/v1/rule6 accessed 2 May 2024

Nils Melzer, 'Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law' (ICRC, 2009)

Tilman Rodenhäuser and Mauro Vignati, '8 Rules for "civilian hackers" during war, and 4 obligations for states to restrain them' (*ICRC*, 4 October 2023) https://blogs.icrc.org/law-and-policy/2023/10/04/8-rules-civilian-hackers-war-4-obligations-states-restrain-them/ accessed 2 May 2024

Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (ICRC 1987)