UNIVERSITÉ DE GENÈVE

GLOBAL STUDIES INSTITUTE

GSI Working Paper **BA LAW 2023/04**

"Applicability of the *Jus in Bello* to Cyber Operations Against Civilian Data: A Legal Grey Zone in the Protection of Data"

Daniela Wildi

Global Studies Institute
10 rue des Vieux-Grenadiers
1205 Geneva
https://www.unige.ch/gsi/fr/

ISSN 2624-8360

Abstract:

Starting from the premise that cyber operations affecting civilian data 'could cause more harm to civilians than the destruction of physical objects', the research sets out to identify the legal grey zone arising from the applicability of the jus in bello and its susceptibility (or potential) to exploitation when conducting cyber operations against civilian data.
Two central concepts have proven to be challenging to apply. First, determining the meaning of the term 'attack' under IHL remains unsettled when applied to cyber operations. In particular, regarding the key threshold of 'attack', consideration should be given as to how below-threshold cyber operations are to be addressed. Second, a related debate centers around the question of whether data can be considered an 'object' under IHL. It follows that various rules of IHL which provide protections to 'objects' – particularly those relating to distinction, proportionality, and precautions in attack – do not protect data if it does not fall within the definition of 'object'. While targeting law provides minimal protection of civilian data beyond those limited operations that would produce physical effects, certain categories of targets enjoy special protections that do not rely on qualifications such as 'attacks or 'objects'.
By emphasizing the relevance of the protection of civilian data in armed conflict, the research illustrates that the law remains unsettled in a way that either places civilians at risk or fails to address currently lawful cyber operations against civilian data that could nevertheless prove highly detrimental to the civilian population. Consequently, a significant coverage gap exists within IHL for the protection of civilian data in modern society. The research proposes expanding perspectives beyond the limited scope of existing IHL, encouraging future research to reflect and engage in detail with the intersection of existing principles of data protection, data security, and other relevant legal frameworks and attempt to apply them to modern armed conflict.

Partant de l'hypothèse que les opérations cybernétiques affectant les données civiles « pourraient causer plus de dommages aux civils que la destruction d'objets physiques », la recherche vise à identifier la zone grise juridique résultant de l'applicabilité du jus in bello et de sa susceptibilité (ou potentiel) à l'exploitation lors de la conduite de cyberopérations contre des données civiles.
Deux concepts centraux se sont révélés difficiles à appliquer. Premièrement, déterminer la signification du terme « attaque » en DIH demeure non résolu lorsqu'il est appliqué aux opérations cybernétiques. En particulier, en ce qui concerne le seuil clé de « l'attaque », il convient de se pencher sur la manière de traiter les opérations cybernétiques en deçà du seuil. Deuxièmement, un débat connexe porte sur la question de savoir si les données peuvent être considérées comme un « objet » en vertu du DIH. Il s'ensuit que diverses règles du DIH qui protègent les « objets » – en particulier celles relatives à la distinction, à la proportionnalité et

à la prise de précautions dans l'attaque – ne protègent pas les données si elles ne rentrent pas dans la définition d'un « objet ». Alors que le droit de ciblage offre une protection minimale des données civiles au-delà de ces opérations limitées qui produiraient des effets physiques, certaines catégories de cibles bénéficient de protections spéciales qui ne reposent pas sur des qualifications telles que « attaques » ou « objets ».
En soulignant l'importance de la protection des données civiles en temps de conflit armé, la recherche montre que le droit demeure non résolu d'une manière qui place soit les civils en danger, soit ne parvient pas à aborder les opérations cybernétiques actuellement légales contre les données civiles qui pourraient néanmoins s'avérer très préjudiciables pour la population civile. Par conséquent, le DIH présente une lacune importante en ce qui concerne la protection des données civiles dans la société moderne. La recherche propose d'élargir les perspectives au-delà de la portée limitée du DIH existant, en encourageant la recherche future à réfléchir et à s'engager en détail avec l'intersection des principes existants de protection des données, de sécurité des données et d'autres cadres juridiques pertinents, et à tenter de les appliquer aux conflits armés modernes.

Keywords: International humanitarian law; Military cyber operations; Civilian data protection; Cyberspace ; Cyber attacks

Author: Daniela Wildi

UNIVERSITÉ DE GENÈVE

GLOBAL STUDIES INSTITUTE

APPLICABILITY OF THE *JUS IN BELLO* TO CYBER OPERATIONS AGAINST CIVILIAN DATA:

A LEGAL GREY ZONE IN THE PROTECTION OF DATA

by

Daniela Wildi

Bachelor Thesis Submitted to Professor Robert Kolb

In Partial Fulfillment of the Requirements for the
Degree of Bachelor in International Relations

At the Global Studies Institute of the University of Geneva

Geneva

August 20, 2023

LIST OF ABBREVIATIONS

AP I	Protocol Additional (I) to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts
art.	article
CAN	Computer Network Attack
CIL	Customary International Law
CND	Computer Network Defence
CNO	Computer Network Operation
CPU	Central Processing Unit
ECtHR	European Court of Human Rights
EU	European Union
GC I	Geneva Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (12 August 1949)
IACtHR	Inter-American Court of Human Rights
ICRC	International Committee of the Red Cross
ICJ	International Court of Justice
ICTY	International Criminal Tribunal for the Former Yugoslavia
IHL	International Humanitarian Law
no.	number
OED	Oxford English Dictionary
SCADA	Supervisory Control and Data Acquisition
UN	United Nations
UNGA	United Nations General Assembly
UNGGE	United Nations Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
UNHRC	UN Human Rights Committee
U.S. DoD	United States Department of Defense
VCLT	Vienna Convention on the Law of Treaties (1969)

TABLE OF CONTENTS

INTRODUCTION

Cyber operations have emerged as an integral component of military strategies employed by both state and non-state actors to achieve military and strategic goals.[1] At the same time, there are growing sensitivities to the crucial role of civilian data and its protection, and the outrage provoked by the ever-increasing sophistication of cyber operations directed against it. Consequently, the rapid development of information technology presents new and unparalleled challenges in understanding and applying international law, and more specifically, international humanitarian law (IHL).[2]

There is a widely accepted consensus that, in general, international law is applicable to military operations in cyberspace.[3] Despite several important advances, disagreements and significant gaps remain regarding the applicability of specific IHL rules to operations in the cyber context.[4] The question is therefore not *whether* IHL applies to cyber operations conducted during armed conflict, but *how* the provisions of IHL apply to, and may limit, cyber operations.[5] Two central concepts have proven to be challenging to apply. First, determining the meaning of the term 'attack' under IHL remains unsettled when applied to cyber operations. Of particular significance is the prohibition on directing attacks against civilian objects, as stipulated in Article 52(1) of the Protocol Additional (I) to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (AP I),[6] and relevant customary law,[7] for unless a cyber operation qualifies as an 'attack' (or the targeted cyber infrastructure enjoys special protection), it may arguably be directed against civilian cyber infrastructure.[8] Second, a related debate centers around the question of whether data can be considered an 'object' under IHL, such that a cyber operation altering or deleting data is unlawful and harm to civilian data in an otherwise lawful attack against a military objective would have to factor in proportionality and precautions in attack assessments.[9]

---

[1] See among 'Significant Cyber Incidents since 2006', Center for Strategic & International Studies, accessed 6 August 2023, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

[2] International humanitarian law (IHL) is commonly referred to as '*jus in bello*' and the 'law of armed conflict', and in the present thesis, these terms are used interchangeably to denote the body of law governing the conduct of hostilities during armed conflicts.

[3] It is worth noting that this was recognized in the consensual reports of the United Nations Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE) in 2013 and 2015. See UNGA, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (24 June 2013), UN Doc A/68/98, para. 19; UNGA, 'Report of the 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. Moreover, several states confirmed this position in their comments to the UN Secretary-General and their national cyberdefense and cybersecurity strategies. See UNGA, 'Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security (Addendum)' (9 September 2013), UN Doc A/68/156/Add.1; UNGA, 'Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security' (30 June 2014), UN Doc A/69/112; UNGA, 'Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security (Addendum)' (18 September 2014), UN Doc A/69/ 112/Add1.

[4] See François Delerue, *Cyber Operations and International Law*, Cambridge Studies in International and Comparative Law (Cambridge: Cambridge University Press, 2020), 16–19, https://doi.org/10.1017/9781108780605.

[5] ICRC, 'International Humanitarian Law and Cyber Operations during Armed Conflicts: ICRC Position Paper (Submitted to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security)' (hereinafter 'ICRC Position Paper'), *International Review of the Red Cross*, Digital Technologies and War, 102, no. 913 (November 2019): 482, https://doi.org/10.1017/S1816383120000478 (emphasis added).

[6] 'Protocol Additional (I) to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts' (hereinafter AP I) (Geneva, 8 June 1977), 1125 UNTS 3, art. 52(1).

[7] Jean-Marie Henckaerts, Louise Doswald-Beck, and Carolin Alvermann, *Customary International Humanitarian Law - Volume 1: Rules*, ed. ICRC (hereinafter *Customary IHL*) (Cambridge: Cambridge University Press, 2005), r. 7, https://doi.org/10.1017/CBO9780511804700 25-29.

[8] See the discussion in Michael N. Schmitt, 'Rewired Warfare: Rethinking the Law of Cyber Attack' (hereinafter 'Rewired Warfare'), *International Review of the Red Cross*, Scope of the Law in Armed Conflict, 96, no. 893 (March 2014): 189–206, https://doi.org/10.1017/S1816383114000381; Michael N. Schmitt, 'Wired Warfare 3.0: Protecting the Civilian Population during Cyber Operations' (hereinafter 'Wired Warfare 3.0'), *International Review of the Red Cross*, Memory and War, 101, no. 1 (April 2019): 333–55, https://doi.org/10.1017/S1816383119000018.

[9] See, e.g., Harrison Dinniss, 'The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives' (hereinafter 'The Nature of Objects'), *Israel Law Review* 48, no. 1 (March 2015): 39–54, https://doi.org/10.1017/S0021223714000272; Kubo Mačák, 'Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law' (hereinafter 'Military Objectives 2.0'), *Israel Law Review* 48, no. 1 (March

Starting from the premise that cyber operations affecting civilian data 'could cause more harm to civilians than the destruction of physical objects',[10] the present thesis sets out to identify the legal grey zone arising from the applicability of the *jus in bello* and its susceptibility (or potential) to exploitation when conducting cyber operations against civilian data. Hence, for the purposes of the present analysis it is assumed that an armed conflict is already established under IHL. The following questions will be discussed:

(I) Under what conditions or circumstances should cyber operations aimed at the destruction of data be considered as 'attacks' under IHL, especially regarding cyber operations without resulting in physical damage?

(II) In particular, does the targeted data qualify as an 'object' under IHL such that the protections afforded to civilian objects extend to it?

(III) If data is not recognized and thus protected as an 'object' under IHL, should certain types of data enjoy protection from cyber operations in armed conflict, irrespective of whether they qualify as an 'object' or not?

The answers to these questions have significant consequences for the conduct of cyber operations in general and the protection of civilian data in particular in times of armed conflict. In order to answer the aforementioned questions, the structure of this thesis unfolds as follows: Chapter I explores the technical and legal aspects related to cyberspace and data and elucidates the complexities and terminology of the conduct of armed conflict in cyberspace, along with a comprehensive discussion of the notion of 'data'. Chapter II analyzes the potential areas for the protection of civilian data under IHL. Particular attention is given to the laws governing the targeting of objects and special categories of protection. The legal issues of defining 'attacks' and 'objects' are central. Contemporary debates of interest to this thesis will be addressed. Chapter III examines the preliminary approach to the current legal threshold of whether cyber operations constitute an 'attack' under AP I. If a cyber operation, in the context of an ongoing armed conflict, qualifies as an 'attack', the law of targeting applies. Chapter IV proceeds to determine the level of protection for civilian data in armed conflicts by considering the meaning of the term 'object' as found in AP I and international customary law. By highlighting the inadequacy of civilian data protection, Chapter V aims to go beyond the current limited scope of existing IHL and advance awareness of insufficiency in civilian protection *vis à vis* cyber operations against civilian data as a starting point for further discussion. Final remarks offer a review of the current status, encouraging future research that could reflect and engage in detail with the intersection of privacy and data protection, emerging technologies, and the laws of IHL.

Overall, the spectrum of different views presented will show that the debate has suffered from ambiguities and inaccuracies concerning the subject matter, and that, consequently, the answers to the questions posed might not be satisfactory at present. The disagreements demarcate much of the grey zones' landscapes. By emphasizing the relevance of the protection of civilian data in armed conflict, the present thesis illustrates that the law remains unsettled in a way that either places civilians at risk or fails to address currently lawful cyber operations against civilian data that could nevertheless prove highly detrimental to the civilian population. Consequently, there exists a significant protection gap. Furthermore, given that international powers active in the cyber domain are unlikely to extend traditional legal protections of objects to civilian data, rapid development in international law to cover this gap seems unlikely. It may be that new approaches need to be developed to adequately protect the various functions of civilian data in modern societies.[11]

2015): 55–80, https://doi.org/10.1017/S0021223714000260; Michael N. Schmitt, 'The Notion of "Objects" during Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision' (hereinafter 'The Notion of "Objects" during Cyber Operations'), *Israel Law Review* 48, no. 1 (March 2015): 81–109, https://doi.org/10.1017/S0021223714000314; Schmitt, 'Wired Warfare 3.0'.

[10] ICRC, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts', Power of Humanity: 32nd International Conference of the Red Cross and Red Crescent (Geneva: ICRC, 31 October 2015), 43.

[11] See, e.g., Schmitt, 'Wired Warfare 3.0', 345–53; Robin Geiss and Henning Lahmann, 'Protection of Data in Armed Conflict', *International Law Studies* 97 (2021): 18.

I. TECHNICAL AND LEGAL ASPECTS RELATED TO CYBERSPACE AND DATA

To understand the applicability of the *jus in bello* to cyber operations against civilian data, it is necessary to pay explicit attention to the terminology as it plays a vital part in understanding the legal challenges presented in this thesis, and in cyberspace in general, for that matter. Following the basic technical and legal understanding of cyberspace and its associated terms, this Chapter seeks to clarify the meaning of 'data' to a degree necessary to this thesis' legal analysis, given its central role in understanding the questions posed and conclusions reached.

A. Cyberspace as a Domain of Operations

The nature of warfare is undergoing a transformative shift. Cyberspace is considered by many to be a new warfighting domain, the conventional domains so far being the land, air, sea, and outerspace.[12]

The prefix 'cyber' derives from the Greek word *kyberno* which translates into the English verb 'to steer' or 'to govern'.[13] The prefix 'cyber' in conjunction with nouns like 'operation', or 'attack' induces in the reader's imagination the transportation of such concepts represented by those nouns to a virtual arena, specifically referred to as cyberspace.[14] Although the legal issues surrounding cyberspace are relatively recent, the actual word 'cyberspace' first emerged in science fiction literature, notably in William Gibson's 1984 novel *Neuromancer*. He characterizes cyberspace as 'a consensual hallucination experienced daily by billions of legitimate operators'. [15] Gibson's conception of cyberspace was accompanied by a number of new meanings, including his search for '[a] graphical representation of data abstracted from banks of every computer in the human system'.[16] He emphasizes the 'unthinkable complexity'[17] inherent to cyberspace. Gibson's imagery of 'lines of light ranged in the non-space of the mind, clusters and constellations of data'[18] captures the ethereal and intangible nature of the virtual domain.

In view of the indiscriminate use of expressions derived from the cyber domain, it is important to first clarify the term 'cyberspace' itself, although there is no consistent terminology or widely accepted definition, eluding a uniform approach. The different interpretations of cyberspace range from technically oriented definitions focused on the electromagnetic spectrum, wherein the dynamics of information flow and the interconnections within cyberspace are developed,[19] to more conceptual definitions that consider the interposition of physical and technical layers working in synergy to facilitate cyberspace's functioning.[20] Among these interpretations lies the perspective that regards cyberspace as a new domain for power dynamics.[21] For the purpose of the present thesis, cyberspace is defined as

> '[a] global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies'.[22]

---

[12] Wolff Heintschel von Heinegg, 'Territorial Sovereignty and Neutrality in Cyberspace', *International Law Studies* 89 (2013): 123; David Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power* (London: The International Institute for Strategic Studies (IISS), 2011), 35. Conversely, see Delerue, *Cyber Operations and International Law*, 10.

[13] Andrew N. Liaropoulos, 'Power and Security in Cyberspace: Implications for the Westphalian State System', *Panorama of Global Security Environment*, 2011, 541.

[14] Breno P. Medeiros and Luiz R. F. Goldini, 'The Fundamental Conceptual Trinity of Cyberspace', *Contexto Internacional* 41, no. 1 (2020): 33, http://dx.doi.org/10.1590/s0102-8529.2019420100002.

[15] William Gibson, *Neuromancien* (New York: Ace Books, 1948), 64.

[16] Gibson, 64.

[17] Gibson, 64.

[18] Gibson, 64.

[19] Julie E. Cohen, 'Cyberspace As/And Space', *Columbia Law Review* 107 (2007); Gregory J. Rattray, 'An Environmental Approach to Understanding Cyberpower', in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington D.C.: Potomac Books, 2009).

[20] Daniel Ventre, *Cyber Conflict: Competing National Perspectives* (Hoboken: John Wiley & Sons, 2013); Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND, 2009).

[21] Daniel T. Kuehl, 'From Cyberspace to Cyberpower: Defining the Problem', in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, 1st ed. (Washington, D.C.: Potomac Books, 2009); John B. Sheldon, 'Deciphering Cyberpower: Strategic Purpose in Peace and War', *Strategic Studies Quarterly* 5, no. 2 (2011).

[22] Kuehl, 'From Cyberspace to Cyberpower: Defining the Problem', 24–42.

The U.S. DoD Dictionary of Military and Associated Terms specifies what is meant by information-communication technologies by including 'Internet, telecommunications networks, computer systems, and embedded processors and controllers'.[23]

For the subsequent legal analysis, it is necessary to conceptualize several discrete notions, specifically 'cyber operation' and 'cyber attack', as forms of actions taking place in the realm of cyberspace. The term 'cyber operation', or synonymously 'computer network operation' (CNO) refers to the 'reduction of information to electronic format and the actual movement of that information between physical elements of cyber infrastructure'.[24] Harmful cyber operations can be described as operations seeking to accomplish a wide range of effects, including '[d]estroy data in a network or a system connected to the network';[25] '[b]e an active member of a network and generate bogus traffic;[26] '[c]landestinely alter data in a database stored on the network';[27] and '[d]egrade or deny service on a network.'[28] Furthermore, it is possible to differentiate cyber operations by distinguishing potential targets or intentions. Cyber operations can be categorized as 'computer network attack' (CNA), 'computer network exploitation' (CNE), and 'computer network defence' (CND).[29] While CNAs specifically seek to disrupt, damage, or destroy computer systems and/or the information contained therein, or alternatively manipulate their use,[30] CNE focuses on the gathering of data via intelligent systems. CND protects computer systems and/or the information contained therein, ultimately preventing CNAs and CNE through intelligence, counterintelligence, law enforcement, and military efforts.[31] All the definitions above suggest that cyberspace can at the same time be the target and medium through which an operation that may qualify as an 'attack' under IHL is delivered.[32]

This terminology, which is specific to operations conducted in cyberspace, must be carefully distinguished from existing technical terms of IHL, such as 'attack'.[33] Academic scholarship and popular literature tend to describe all known offensive cyber operations as 'attacks'.[34] Accordingly, legal scholars such as Noam Lubell express dissatisfaction with the widespread misapplication of the term 'attack' to encompass all forms of offensive cyber operations because of the legal uncertainty that the misuse of the term creates.[35] Consequently, he argues, '[f]or sake of legal clarity, it would therefore be advisable to utilize a more legally neutral (at least under the *jus in bello*) description and – unless intending to define an event as an attack under IHL – to speak of cyber operations rather than cyber attacks'.[36] The author agrees with Lubell's viewpoint and will consistently employ the term 'cyber operations' throughout the legal analysis, unless citing a scholar or explicitly referring to an 'attack' regulated by IHL.

Having established the conceptual framework for cyberspace and its associated terms, the thesis will now proceed to define the notion of 'data'.

---

[23] Office of the Chairman of the Joint Chiefs of Staff, 'Cyberspace', in *DOD Dictionary of Military and Associated Terms* (Washington, D.C.: The Joint Staff, 2021), 56.
[24] Nils Melzer, 'Cyberwarfare and International Law', *UNIDIR Ressources*, 2011, 5.
[25] Herbert S. Lin, 'Offensive Cyber Operations and the Use of Force', *Journal of National Security Law and Policy* 4 (2010): 69–70.
[26] Lin, 69–70.
[27] Lin, 69–70.
[28] Lin, 69–70.
[29] Melzer, 'Cyberwarfare and International Law', 4.
[30] Melzer, 4–5.
[31] Melzer, 5.
[32] For instance, in a hypothetical scenario of conflict between Country A and Country B, Country A launches a cyber operation targeting Country B's critical infrastructure (cyberspace as a medium). By infiltrating and gaining control over computer systems that control power plants, communication networks, and transportation, Country A disrupts services and causes blackouts, communication breakdowns, and transportation disruptions (cyberspace as a target).
[33] See AP I, art. 49(1).
[34] An example of this tendency involved journalists covering on the September 2018 cyber security breach at Facebook, during which the personal access tokens of around 50 million users were compromised. See, e.g., Mike Isaac and Sheera Frenkel, 'Facebook Security Breach Exposes Accounts of 50 Million Users', *New York Times*, 28 September 2018, accessed 15 August 2023, https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html.
[35] Noam Lubell, 'Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?' (hereinafter 'Lawful Targets in Cyber Operations'), in *Israel Yearbook on Human Rights*, by Fania Domb, ed. Yoram Dinstein, 43 (Brill | Nijhoff, 2013), 258, https://doi.org/10.1163/9789004242081_003.
[36] Lubell, 258.

B. Data Defined

The term 'data', or more accurately, 'datum' in its singular form, is defined by the Oxford English Dictionary (OED) as 'an item of (chiefly numerical) information considered collectively, typically obtained by scientific work and used for reference, analysis, or calculation.'[37] Specifically, in the context of computing, it is characterized as '[q]uantities, characters, or symbols on which operations are performed by a computer, considered collectively'.[38]

The data stored within a computer serves various purposes. In its most general sense, computer data refers to information that undergoes processing or is held within a computer system. This information can take the shape of textual documents, images, audio, video, software applications, or other classifications of data. The computer's central processing unit (CPU) is tasked with the processing of computer data, which is subsequently archived on the computer's hard drive.[39] At its most basic level, computer data is represented by a succession of binary signals, symbolized by the digits '0' and '1'.[40] The basic binary format enables the creation, processing, preservation, and digital storage of all data. This facilitates the transmission of data across computer systems through network connections or diverse media devices.[41] Fundamentally, all 'raw elements' essential for the operation of a computer system can be categorized as data. Legal scholars and policymakers frequently place emphasis on data representing information that is human-readable or sensory in nature, such as text, visuals, and audio, while neglecting data designed solely for processing computers. This factual distinction holds significance in the context of 'data protection' during armed conflicts.[42]

While scholars generally treat data as a single entity, Heather Harrison Dinniss contends that data should be classified into different types depending on its function.[43] She introduces two distinct categories of data relevant to the subsequent legal analysis: content-level and operational-level data. Content-level data 'such as the text of this article, or the contents of medical databases, library catalogues and the like',[44] represents information that, post-processing, remains intelligible to humans, such as when displayed on a computer screen.[45] Operational-level data 'also known as logical-level data, or more commonly, program data […] gives hardware its functionality and ability to perform the tasks we require'.[46] Comprising machine-readable instructions, this classification of data is also referred to as 'code'.[47] Examples of operational-level data are operating systems, software applications, and supervisory control and data acquisition (SCADA)[48] systems.[49] Her analysis predominantly revolves around the latter classification. This stands in contrast to the prevalent discourse where most scholars address the question of whether and how IHL protects content-level data when explicitly discussing 'data protection' within the context of IHL.[50]

A further distinction is that between content data and metadata, the latter being 'data that describes other data'[51] such as author, date created, or file size. Importantly, metadata is intelligible to humas, and thus

[37] Oxford English Dictionary, 'Datum, n.', in *Oxford English Dictionary* (Oxford University Press, July 2023), Oxford English Dictionary, https://doi.org/10.1093/OED/7571592234.
[38] Oxford English Dictionary.
[39] Geiss and Lahmann, 'Protection of Data in Armed Conflict', 559–60.
[40] Andrzej Yatsko, *Insight into Theoretical and Applied Informatics: Introduction to Information Technologies and Computer Science*, Introduction to Information Technologies and Computer Science (Berlin: De Gruyter Open, 2015), 43.
[41] Geiss and Lahmann, 'Protection of Data in Armed Conflict', 560.
[42] Geiss and Lahmann, 560.
[43] Dinniss, 'The Nature of Objects', 41.
[44] Dinniss, 41.
[45] Geiss and Lahmann, 'Protection of Data in Armed Conflict', 561.
[46] Dinniss, 'The Nature of Objects', 41.
[47] Dinniss, 41.
[48] The term SCADA refers to '[c]omputer systems and instrumentation that provide for monitoring and controlling industrial, infrastructure, and facility-based processes, such as the operation of power plants, water treatment facilities, electrical distribution systems, oil and gas pipelines, airports, and factories'. Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations: Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre for Excellence* (hereinafter *Tallinn Manual 2.0*), 2nd ed. (Cambridge: Cambridge University Press, 2017), 416, 567, https://doi.org/10.1017/9781316822524.
[49] Dinniss, 'The Nature of Objects', 41.
[50] Geiss and Lahmann, 'Protection of Data in Armed Conflict', 561.
[51] Garry Kranz, 'Metadata', in *TechTarget*, accessed 15 August 2023, https://www.techtarget.com/whatis/definition/metadata.

not ‘code’. Dinniss categorizes both content data (such as email content) and metadata as content-level data.

The distinction between data based on factual and definitional aspects is complemented by a normative facet, in particular, the distinction between personal and non-personal data. The differentiation forms the cornerstone of modern data protection frameworks like the European General Data Protection Regulation (GDPR). Personal data refers to ‘any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data’.[52] While ‘operational-level data’, as interpreted by Dinniss, generally falls outside the scope of personal data, ‘content-level data’ often does, albeit not invariably.[53]

It is important to realize that the protection of data in armed conflict is not primarily focused on ‘data protection’ as typically understood in legal terms. The term ‘data protection’ describes the body of law that regulates how personal data may be processed by individuals and entities who control such information.[54] Instead, in the case of armed conflict, the emphasis lies on ‘data security’, a constituent of data protection regulations,[55] yet inherently aligned with the domain of information and IT security. The fundamental principles underlying information and IT security are confidentiality, integrity, and availability within the IT systems responsible for processing data.[56] When assessing cyber operations in the context of armed conflicts, invoking the three basic concepts of information security adds analytical clarity. This is because distinct rules may apply and different legal consequences might ensue, contingent upon the specific protective goal that is concerned.[57] While there are established provisions for the general protection of civilian objects under IHL, it also sets forth certain specific rules to reinforce the protection of some of these objects.

As will be seen in the next Chapter, numerous protections under IHL are limited to civilian ‘objects’ and civilian persons, with the latter clearly not encompassing computer data. Therefore, establishing under what circumstances and whether data qualifies as an ‘object’ under IHL holds considerable significance in determining the legality of activities carried out during an armed conflict.[58]

II. LAWS GOVERNING MILITARY CYBER OPERATIONS

When states engage in military operations against adversaries during armed conflicts, a body of law known as IHL becomes applicable. In situations of armed conflict IHL is considered a *lex specialis*, a term indicating that a body of law takes precedence over more general or conflicting rules in a given situation.[59] Therefore, this Chapter examines potential protections for civilian data the existing IHL may provide within the context of an armed conflict. In particular, the law of targeting, which identifies what and who can be attacked, and how,[60] and special categories of protection are considered. Substantial gaps or disagreements persist concerning the applicability of specific IHL rules to cyber operations, including the protection of civilian data. A comprehensive overview of the overreaching IHL structure will help reveal where these gaps emerge. However, several issues, which will be addressed later, complicate the application of the following rules to civilian data.

---

[52] ‘What Is Personal Data?’, European Commission, accessed 8 August 2023, https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en.

[53] For instance, the details within a medical record disclosing a patient’s specific diagnosis would be classified as personal data. On the other hand, information within a record describing general medical procedures (usually) does not fall into this category.

[54] See, e.g., EU, ‘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 (General Data Protection Regulation)’ (hereinafter ‘GDPR’) (27 April 2016), O.J. L.119/1, art.1(1).

[55] See, e.g., GDPR, art. 32.

[56] For an explanation of the distinction, see Geiss and Lahmann, ‘Protection of Data in Armed Conflict’, 562.

[57] Geiss and Lahmann, 562.

[58] Ori Pomson, ‘“Objects”? The Legal Status of Computer Data under International Humanitarian Law’ (hereinafter 'Objects'), *Journal of Conflict and Security Law*, 30 January 2023, 5.

[59] Dieter Fleck, ed., *The Handbook of International Humanitarian Law*, 4th ed. (Oxford: Oxford University Press, 2021), 37.

[60] The US Joint Doctrine defines ‘targeting’ as ‘the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities’. Joint Chiefs of Staff, ‘Joint Targeting’, *Joint Publication* (31 January 2013), I–1. The rules on targeting also apply to cyber operations by which a party takes control of enemy weapons or weapon systems. Schmitt, *Tallinn Manual 2.0*, 2017, r. 80.

A. The Law of Targeting

The primary treaty governing the protection of civilians and civilian objects in armed conflicts is AP I. Even though a number of states, including key states such as the United States and Israel, are not a party to this treaty,[61] these and other non-party states consider most of the treaty's targeting provisions reflective of customary international law (CIL).[62] Consequently, AP I is used to highlight and discuss those protections. It should be emphasized from the outset that targeting laws do not exist to spare civilians from *all* harm or inconveniences, but rather from the most severe effects associated with armed conflicts.[63] For purposes of discussing civilian data, this Chapter focuses on the provisions of AP I covering civilian objects, as opposed to individuals.

The application and scope of targeting rules in relation to non-violent cyber operations are subject to controversy.[64] As cyber operations can affect civilian data through different means, both violent and non-violent, it is vital to examine targeting laws and understand the meaning of the specific terms used in this context.

1. Principle of Distinction

Determining whether something qualifies as an 'object' may have implications for the rules relating to distinction, which is considered one of the 'cardinal principles' of IHL.[65] It finds current and clear expression concerning objects in article 52(1) of AP I, requiring that '[c]ivilian objects shall not be the object of attack'.[66] Similarly, IHL prohibits indiscriminate attacks, as they 'are of a nature to strike military objectives and civilians or civilian objects without distinction'.[67] In order to protect civilian objects, both civilians and civilian objects are negatively defined in AP I as those objects that do not fall under the definition of military objectives.[68]

Before proceeding, attention should be given to the concept of 'military objective'. Article 52(2) of AP I defines 'military objectives' as 'those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage'.[69] This definition finds application in various other IHL treaties,[70] and it may therefore be presumed as the meaning states have in mind when referencing the notion of 'military objectives' in present-day discourse.[71] The *civilian* nature of an object thus depends on whether or not it constitutes a 'military objective'.[72] Simultaneously, 'military objectives', at least when they do not encompass persons who could be considered 'military objectives',[73] are by definition 'objects'. The question of whether data qualifies as an 'object' holds

---

[61] Other states not party to AP I are Andorra, Azerbaijan, Bhutan, Eritrea, India, Indonesia, Iran, Kiribati, Malaysia, the Marshall Islands, Myanmar, Nepal, Pakistan, Papua New Guinea, Singapore, Somalia, South Sudan, Sri Lanka, Thailand, Turkey, and Tuvalu.

[62] See, e.g., Martin P. Dupuis, John Q. Heywood, and Michéle Y.F. Sarko, 'The Sixth Annual American Red Cross-Washington College of Law Conference on International Humanitarian Law: A Workshop on Customary International Law and the 1977 Protocols Additional to the 1949 Geneva Conventions', *American University International Law Review* 2, no. 2 (1987): 419–415.

[63] For example, there is a long tradition of deliberately affecting the civilian population through non-violent means, such as the use of propaganda to erode public support for the conflict. However, the bulk of targeting law would not apply to propaganda operations because they are nonviolent. Schmitt, *Tallinn Manual 2.0*, 2017, r. 92, para. 2.

[64] See Chapter III for more details.

[65] ICJ, 'Legality of the Threat or Use of Nuclear Weapons', Advisory Opinion (1996), ICJ Rep 226, para. 78.

[66] AP I, art. 52(1).

[67] In this regard, see AP I, art. 51(4)-(5)(a). See also Marco Roscini, 'Targeting and Contemporary Aerial Bombardment', *International and Comparative Law Quarterly* 54, no. 2 (April 2005): 413, https://doi.org/10.1093/iclq/lei006; Djamchid Momtaz, 'Les règles relatives à la protection de l'environnement au cours de conflits armés à l'épreuve du conflit entre l'Iraq et le Koweit', *Annuaire français de droit international* 37, no. 1 (1991): 207–8, https://doi.org/10.3406/afdi.1991.3014.

[68] See AP I, art. 52(2).

[69] AP I, art. 52(2).

[70] 'Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices as Amended on 3 May 1996' (3 December 1998), 2048 UNTS 93, art. 2(7).

[71] Henckaerts, Doswald-Beck, and Alvermann, *Customary IHL*, 25.

[72] Christopher Greenwood, 'Current Issues in the Law of Armed Conflict: Weapons, Targets and International Criminal Liability', *Singapore Journal of International & Comparative Law* 1, no. 2 (1997): 461.

[73] To be precise, combatants and persons directly participating in hostilities. See also Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* (hereinafter *Conduct of Hostilities*), Third edition (Cambridge: Cambridge University Press, 2016), 105.

limited direct legal importance for operations impacting such data, as long as they meet the criteria of a 'military objective'. As observed by Michael Schmitt, regardless of whether the data constitutes an 'object', the protections covering 'civilian data' under IHL would not extend to data that might be considered 'military objective'.[74]

A frequently raised concern in the context of cyber is the one of dual-use targets, which are targets that serve both military and civilian purposes. The fundamental difference in the cyber context lies in the 'systemic interconnectivity of civilian and military infrastructure'.[75] Satellites, routers, cables, servers and even computers can all be regarded as dual-use cyber facilities.[76] This targetable status clearly has implications for civilian uses of shared network infrastructure. For instance, an undersea internet cable utilized by military to establish communication with its overseas troops designates it a military objective. Damaging the cable, by any means, could severely impact civilian data transfer as well. Currently, undersea cables carry most ocean-crossing internet data. Military forces are no exception to this reality and rely heavily on undersea cables to communicate overseas.[77] Simply put, the systemic interconnectivity renders the whole cyber domain a potential dual-use target, at least theoretically.[78] Should there be evidence indicating a definite military use, the military objective criterion applies during the duration of military use, and the object would be subject to attack. Consequently, any cyber infrastructure definitively used for military purposes during an armed conflict becomes a military objective. As a result, it can be targeted by the opposing force.[79] Although the intentional targeting of dual-use objects, such as cyber infrastructure, does not violate the rule of distinction because those objects qualify as military objectives, the dual-use nature of the object would have to be assessed under the application of the rules of proportionality and precautions in attack.[80]

2. Rule of Proportionality

Once an object is determined to meet the qualification of a military objective, in accordance with the rule of proportionality,[81] is it prohibited to carry out an attack that 'may be expected to cause incidental loss of civilian life, injury to civilians, *damage to civilian objects*, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated'.[82] If data is considered an 'object', then it follows that incidental 'damage' to civilian data resulting from an attack must be taken within a proportionality analysis. However, this can be challenging in the cyber context, given the complexity of network operations.[83] Furthermore, target values vary widely depending on the conflict and the prevailing context during an attack.[84]

---

[74] Schmitt, 'The Notion of "Objects" during Cyber Operations', 103.
[75] Robin Geiss and Henning Lahmann, 'Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space', *Israel Law Review* 45, no. 3 (November 2012): 381, https://doi.org/10.1017/S0021223712000179.
[76] Geiss and Lahmann, 386.
[77] Jeffrey Biller and Timothy Goines, 'Protecting Civilian Data in Armed Conflicts: The Need for an Ethical Foundation' (hereinafter 'Protecting Civilian Data'), in *Ethical Dilemmas in the Global Defense Industry*, ed. Daniel Schoeni and Tobias Vestner, Ethics, National Security, and the Rule of Law (Oxford: Oxford University Press, 2023), 199–200.
[78] Geiss and Lahmann, 'Cyber Warfare', 390.
[79] Schmitt, *Tallinn Manual 2.0*, 2017, r. 100, para. 10.
[80] Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford: Oxford University Press, 2014), 185, https://doi.org/10.1093/acprof:oso/9780199655014.001.0001.
[81] In addition to being a principle of IHL, proportionality applies as a *rule* relating to the protection of civilians and civilian objects in the conduct of hostilities (emphasis added). See Sassòli and Nagler, *International Humanitarian Law*, 360–64; Marco Sassòli and Anaïs Maroonian, 'La proportionnalité en droit international humanitaire: principe et règle', in *Proportionnalité, droits fondamentaux et juges*, Rahma Bentirou Mathlouthi (ed.) (Paris: l'Harmattan, 2023), 79–113; Jeroen Van Den Boogaard, 'Proportionality in International Humanitarian Law: Principle, Rule and Practice' (University of Amsterdam, 2019); Jeroen Van Den Boogaad, 'Reimagining IHL Principles Part I: The Wrong Principles', Articles of War, Lieber Institute West Point, 2022, accessed 24 October 2023, https://lieber.westpoint.edu/reimagining-ihl-principles-part-i-wrong-principles/; Anaïs Maroonian, 'Proportionality in International Humanitarian Law: A Principle and a Rule', Articles of War, Lieber Institute West Point, 2022, accessed 24 October 2023, https://lieber.westpoint.edu/proportionality-international-humanitarian-law-principle-rule/.
[82] AP I, art. 57(2)(b) (emphasis added). See also AP I, art. 51(5)(b), art. 57(2)(a)(iii); Robert Kolb, *Advanced Introduction to International Humanitarian Law*, Elgar Advanced Introductions (Cheltenham: Edward Elgar, 2014), 152.
[83] Schmitt, *Tallinn Manual 2.0*, 2017, r. 113, para. 6.
[84] Biller and Goines, 'Protecting Civilian Data', 200.

3. Precautions in Attack

In addition to the proportionality analysis, certain rules under IHL, including customary rules, protect civilian objects by the rule of precautions in attack.[85] The rule, as laid down in article 57 of AP I, requires the attacker to 'do everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects and are not subject to special protection'[86] and 'take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing […] damage to civilian objects'.[87] Furthermore, various 'passive precautions' recognized under IHL are applicable to civilian objects.[88] The obligation to take precautions in an attack entails the responsibility of military forces conducting attacks to issue warnings to civilians when civilian objects will be affected.[89] However, this requirement is only applicable when the circumstances permit such actions.[90] Providing advance warning to the civilian population carries the inherent risk that enemy forces will learn of the operation, leading to a potential reduction in mission effectiveness. In the context of cyber operations, this risk may result in rendering an operation ineffective, thereby eliminating the requirement for issuing a warning.[91] Even if a military operation adheres to the rules of distinction and proportionality, the obligations concerning precautions in attack would extend to civilian data as well if the latter is considered to be an 'object'. However, it may give rise to questions, such as whether a party engaged in armed conflict is obligated to take feasible measures for storing military data separately from civilian data.[92]

At this point, it is essential to reiterate that the legal obligation to take precautions is limited to situations where a civilian *object* is subjected to an *attack*.[93] Chapter III and IV will delve into the definitions of these terms and their significance in the context of cyber operations against civilian data.

B. Special Protection Categories

While targeting law provides minimal protection to civilian data beyond those limited operations that would produce physical effects, certain categories of targets enjoy special protections that do not rely on qualifications such as 'attacks' or 'objects'.[94] While an extensive range of special protections exists, this section particularly concentrates on categories that are deemed highly relevant[95] to cyber operations against civilian data: medical units, objects indispensable to the civilian population, and civil defense organizations.

1. Medical Personnel, Objects, and Activities

The protection of medical units, specifically medical personnel, objects, and activities, holds significant relevance in the context of civilian data protection. From a humanitarian standpoint, data related to the provision of medical care for both civilians and combatants is of utmost importance. The First Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (GC I) provides in article 19(1) that '[f]ixed establishments and mobile medical units of the Medical Service may in no circumstances be attacked, but shall at all times be respected and protected by the Parties to the conflict'.[96] The updated International Committee of the Red Cross (ICRC) Commentary on this provision provides clarification on the obligation that connotes *inter alia* a

[85] Henckaerts, Doswald-Beck, and Alvermann, *Customary IHL*, chap. 5.
[86] AP I, art. 57(2)(a)(i).
[87] AP I, art. 57(2)(a)(ii).
[88] See AP I, art. 58. The exact scope, *vel non*, of similar customary obligations to this provision is controversial. Cf. Marco Sassòli and Patrick Nagler, *International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare* (hereinafter *International Humanitarian Law*) (Cheltenham: Edward Elgar Publishing, 2019), 372, https://doi.org/10.4337/9781786438553. See also Yoram Dinstein, 'The Principle of Distinction and Cyber War in International Armed Conflicts' (hereinafter 'Principle of Distinction'), *Journal of Conflict and Security Law* 17, no. 2 (2012): 275.
[89] AP I, art. 57(2)(c). See also Henckaerts, Doswald-Beck, and Alvermann, *Customary IHL*, r. 20.
[90] Henckaerts, Doswald-Beck, and Alvermann, r. 20.
[91] Biller and Goines, 'Protecting Civilian Data', 201–2.
[92] Pomson, 'Objects', 7.
[93] Emphasis added.
[94] See Henckaerts, Doswald-Beck, and Alvermann, *Customary IHL*, 79–160.
[95] Biller and Goines, 'Protecting Civilian Data', 201.
[96] 'Geneva Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field' (hereinafter 'First Geneva Convention') (Geneva, 12 August 1949), 75 UNTS 31, art. 19(1). See also AP I, art. 12(1) and in particular AP I, art. 12(2) that explicitly extends this coverage to 'civilian medical units' during armed conflicts.

prohibition on 'interfering with their work in order to allow them to continue to treat the wounded and sick in their care'.[97] This logically implies that cyber operations targeting computer data serving such medical establishment and units would be constrained. In other words, the special protection extends to civilian medical data, both content- and operational-level data,[98] since deleting such data or rendering it corrupt could interfere with the work of a medical unit. Thus, the provision interpreted extends beyond mere protections for 'objects'.[99] This position has been explicitly articulated by certain states that have issued statements regarding the application of international law to cyber operations, with France being the most recent and notable example.[100]

2. Objects Indispensable to the Survival of the Civilian Population

In addition, operations against civilian data might also implicate the special protection granted to objects indispensable to the survival of the civilian population. Article 54(2) of AP I prohibits operations

> 'to attack, destroy, remove or render useless objects indispensable to the survival of the civilian population, such as foodstuffs, agricultural areas for the production of foodstuffs, crops, livestock, drinking water installations and supplies and irrigation works, for the specific purpose of denying them for their sustenance value to the civilian population or to the adverse Party, whatever the motive, whether in order to starve out civilians, to cause them to move away, or for any other motive'.[101]

Should the availability of civilian data be deemed indispensable to survival, such data would receive additional protections under the law. A pertinent illustration of this scenario would involve data essential for operating the sole facility capable of providing safe drinking water to a large municipality. In the event that this data were corrupted, resulting in the facility becoming non-functional or 'useless', such an action would violate this protection.[102]

3. Civil Defense Organization

The final special protection to be discussed is that of protection of civilian defense organizations. Article 62(1) of AP I states that '[c]ivilian defense organizations and their personnel shall be respected and protected' and that '[t]hey shall be entitled to perform their civil defence tasks except in case of imperative military necessity'.[103] This section has extensive applicability, encompassing a wide range of operations, including warning and evacuation procedures, firefighting activities, and rescue operations.[104] To illustrate, a scenario should be considered where a state's civil defense organization develops a phone application that provides essential civil defense information to the public. In such a case, a cyber operation that prevents the application from functioning as intended would violate this protection, unless justified by 'imperative military necessity'.[105]

As previously mentioned, various other special protections are incorporated in IHL that, in theory, could potentially protect specific categories of data. Although this section is not exhaustive and only presents some of the more probable examples, when juxtaposed with the lack of coverage in targeting law, these limited special protections demonstrate the minimal level of protection afforded to civilian data under IHL. Many scholars seek to redefine the terms 'attack' and 'object', thereby expanding the protections under targeting law.[106] Although opinions widely diverge on what types of data receive protection and

---

[97] Knut Dörmann et al., eds., *Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field* (hereinafter *Commentary on the First Geneva Convention*) (Cambridge, United Kingdom: Cambridge University Press, 2016), para. 1799.
[98] Schmitt, *Tallinn Manual 2.0*, 2017, 515.
[99] Knut Dörmann, 'Applicability of the Additional Protocols to Computer Network Attacks: An ICRC Viewpoint', in *International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law* (Stockholm, Sweden, 2004), 7, https://www.icrc.org/en/doc/assets/files/other/applicabilityofihltocna.pdf.
[100] Ministère des Armées, 'Droit International Appliqué Aux Opérations Dans Le Cyberespace' (France, 2019), 15, https://www.justsecurity.org/wp-content/uploads/2019/09/droit-internat-appliqué-aux-opérations-cyberespace-france.pdf. See also International Law Association Study Group on the Conduct of Hostilities in the 21st Century, 'The Conduct of Hostilities and International Humanitarian Law: Challenges of 21st Century Warfare', *Stockton Center for the Study of International Law* 93, no. 322 (17 August 2017): 340, https://digital-commons.usnwc.edu/ils/vol93/iss1/12.
[101] AP I, art. 54(2).
[102] Biller and Goines, 'Protecting Civilian Data', 205.
[103] AP I, art. 62(1).
[104] Biller and Goines, 'Protecting Civilian Data', 205.
[105] AP I, art. 62(1).
[106] See, e.g., Mačák, 'Military Objectives 2.0', 55.

under what circumstances, the ICRC is understandably concerned about essential civilian data that does not benefit from such specific protection, such as 'social security data, tax records, bank accounts, companies' client files, or election lists and records'.[107] The ICRC is keen to clarify 'the extent to which such data is already protected by the existing general rules on the conduct of hostilities' and rightly highlights the possibility that '[d]eleting or tampering with such data could quickly bring government services and private businesses to a complete standstill, and could cause more harm to civilians than the destruction of physical objects'.[108] The following Chapters will explore the complex legal aspects of defining 'attacks' and 'objects' under IHL.

III. CYBER OPERATIONS AND THE KEY THRESHOLD OF 'ATTACK'

If, and only if a cyber operation, in the context of an armed conflict, qualifies as an 'attack', then the law of targeting applies as discussed in Chapter II.[109] An established armed conflict is the basis of the present thesis. It must now be determined whether and at what threshold cyber operations count as 'attacks' under IHL. While this is a matter of legal dispute among scholars and states, three approaches to legal interpretation are introduced: the traditional approach, the consequence-based or effects-based approach,[110] and the functionality test. Each approach will be first addressed separately. All three approaches recognize attacks as a term of art with distinct meanings and limitations,[111] as well as setting a key threshold under IHL.[112]

A. 'Acts of Violence'

The definition of 'attack' found in article 49(1) of AP I, which reflects customary law, is the necessary starting point in framing that conduct.[113] Accordingly, attacks are 'all acts of violence against the adversary, whether in offence or in defence'.[114] The notion of 'acts of violence' is crucial in determining when civilian data is protected.[115]

1. Traditional Approach

Traditionally, 'acts of violence' has been interpreted to denote physical force.[116] This authoritative interpretation is based on the Commentary of Bothe, Partsch, and Solf, all of whom were part of the Protocol's drafting stage. The term 'attack' involving physical force is reasonably interpreted to exclude psychological operations as well as 'dissemination of propaganda, embargoes, or other non-physical means of psychological, political, or economic warfare'.[117] The Official Commentary of the ICRC has taken a comparable position, interpreting 'acts of violence' as 'combat action'.[118] Therefore, according

[107] ICRC, '32nd International Conference of the Red Cross and Red Crescent, Geneva, 8–10 December 2015', *International Review of the Red Cross* 97 (December 2015): 1478, https://doi.org/10.1017/S1816383116000357.
[108] ICRC, 1478.
[109] The word 'attack' will be emphasized throughout this Chapter since it is a definitional term that establishes a critical threshold under IHL.
[110] Both the terms 'consequence-based approach' and 'effects-based approach' refer to the same concept.
[111] Lubell, 'Lawful Targets in Cyber Operations', 258.
[112] Michael N. Schmitt, '"Attack" as a Term of Art in International Law: The Cyber Operations Context' (hereinafter 'Attack as a Term of Art'), in *2012 4th International Conference on Cyber Conflict (CYCON 2012)* (Tallinn, 2012), 284.
[113] Henckaerts and Doswald-Beck, *Customary IHL*, 29–32.
[114] AP I, art. 49(1).
[115] Schmitt, *Tallinn Manual 2.0*, 2017, r. 92.
[116] The OED defines 'violence' as 'behavior involving physical force'. Oxford English Dictionary, 'Violence, n.', in *Oxford English Dictionary* (Oxford University Press, 2 March 2023), https://doi.org/10.1093/OED/4998467199.
[117] Michael Bothe, Karl Josef Partsch, and Waldemar A. Solf, *New Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949* (The Hague, Boston, London: Martinus Nijhoff Publishers, 1982), 289.
[118] Yves Sandoz, Christophe Swinarski, and Bruno Zimmermann, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (hereinafter *Commentary on the Additional Protocols*), ed. International Committee of the Red Cross (Geneva: Martinus Nijhoff Publishers, 1987), para. 1880.

to the restrictive approach, cyber operations that do not result in 'acts of violence', such as those targeted at intelligence gathering or cyber espionage, are not included in the definition of article 49 of AP I.[119]

In light of the fact that certain cyber operations do not directly or immediately unleash violent physical forces but nevertheless have the potential to do significant harm, it is pertinent to contemplate reinterpreting the term 'attack'.

2. Consequence-Based or Effects-Based Approach

The second approach to the notion of attack interprets 'acts of violence' as those acts involving violent *consequences*.[120] By rejecting the 'instrumentality-based' definition of 'attack', Schmitt advances a consequence-based or effects-based approach in an effort to operationalize the term.[121] This approach is motivated by conformity and compliance with the Protocol's humanitarian concern. [122] In other words, the consequence of an attack, not its means, is what matters.[123] Schmitt contends that the Protocol itself operationalizes the principle of distinction in terms of effects and results.[124] For example, the Protocol prohibits attacks on 'dams and dykes', and other 'works or installations containing dangerous forces' that may result in 'severe losses among the civilian population'[125] or 'widespread, long term and severe damage' to the natural environment.[126] Finally, he argues, the principle of proportionality evaluates the definitive legitimacy of an attack in terms of the outcome by prohibiting 'incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive to the concrete and direct military advantage anticipated'.[127]

Applying the above to cyber operations, the definition adopted by the Tallinn Manual 2.0 states that a cyber attack is any 'cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects'.[128] For example, altering 'the running of SCADA system controlling an electrical grid'[129] resulting in a fire or a computer network attack that contaminates a water pipeline supplying civilians with water leading to death or illness would qualify as an 'attack'.[130] Comparable, opening the floodgates of a dam in a similar manner would result in physical harm to the civilian population.[131] The aforementioned scenarios are widely accepted as 'attacks' as their effects on the civilian population are obvious and undeniable.[132] Thus, it is uncontroversial that cyber operations resulting in physical damage qualify as 'attacks'. However, the question remains if the occurrence of complex cyber operations whose effects do not immediately result in violent consequences under the sense of article 49(1) of AP I but seriously impair the functionality of the targeted object, constitute an 'attack' under IHL.

3. Functionality Test

The Tallinn Manual 2.0 has proposed the element of 'functionality' as the condition under which some disruptive cyber operations may qualify as 'attacks' in the sense of *jus in bello*. Accordingly, a majority of the international group of experts held the view that interfering with an object's functionality would constitute the damage or destruction required to qualify the cyber operation as an 'attack'.[133] The experts'

---

[119] Elizabeth Mavropoulou, 'Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks' (hereinafter 'Targeting in the Cyber Domain'), *Journal of Law & Cyber Warfare* 4, no. 2 (2015): 29.
[120] Emphasis added.
[121] Schmitt, 'Rewired Warfare', 192–96.
[122] Schmitt, 'Attack as a Term of Art', 284.
[123] In this regard, note that that a general consensus has emerged that the use of chemical, biological, or radiological weapons would constitute 'attacks' as a matter of law, even though they do not usually have kinetic effects on their designated target. See ICTY, 'Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction (Prosecutor v. Dusko Tadic a/k/a "Dule")' (2 October 1995), IT94-AR72, para. 120-124; Schmitt, *Tallinn Manual 2.0*, 2017, 415.
[124] Michael N. Schmitt, 'Cyber Operations and the Jus in Bello: Key Issues', *Naval War College International Law Studies*, 2 March 2011, 93; Schmitt, *Tallinn Manual 2.0*, 2017, 289.
[125] AP I, art. 56(1).
[126] AP I, art. 55(1).
[127] AP I, art. 51(5)(b).
[128] Schmitt, *Tallinn Manual 2.0*, 2017, 415.
[129] Schmitt, 416, 567.
[130] Schmitt, 'Attack as a Term of Art', 291.
[131] Mavropoulou, 'Targeting in the Cyber Domain', 31.
[132] Mavropoulou, 31.
[133] Schmitt, *Tallinn Manual 2.0*, 2017, 417.

views, however, differed as to the degree of requisite interference with functionality. Pursuant to the majoritarian view, disruptive cyber operations reach the key threshold of 'attack' if restoration of functionality requires the replacement of physical components.[134] Some of the experts of the majority further viewed sufficient interference of functionality as fulfilled when the targeted cyber infrastructure would need to reinstall an operating system or particular data essential to its functioning.[135] Regardless of the approach *vis à vis* functionality, many questions remain. For instance, is there a time dimension to the loss of functionality, such that a brief denial of service operation does not meet the criteria unless it results in physical damage or injury? Yoran Dinstein, following Schmitt and his effects-based approach, supports the doctrine of kinetic equivalence[136] for cyber operations and excludes, *inter alia*, the 'breaking through a computer's firewall' or the mere 'disruption of communication'.[137]

B. Comparing Approaches

Determining how disruptive a cyber operation must be in order to meet the key threshold of article 49(1) of AP I remains a difficult task using the effects-based approach. While it holds true that the mere disruption of communication during armed conflict does not reach the threshold, using a *stricto sensu* definition of attack in accordance with the consequence-based approach, all disruptive cyber operations that do not completely irreparably damage the target are left unregulated and thus permissible under the law. Indeed, the effects-based approach limits the definition of attack by excluding those operations that result in severe and disruptive non-physical harm. Cyber operations may be able to disable an object's functionality without causing any outright physical harm to the object.[138]

The kinetic equivalence theory, on the other hand, constitutes a specific application of the consequence-based approach. It posits that certain cyber operations can be considered equivalent to traditional kinetic attacks in terms of their effects and consequences. However, it has been criticized for having an under-inclusive definition of attack based on the occurrence of physical effects on targeted objects.[139] This is where Knut Dörmann's perspective on the definition of attack comes into play. In order to respond to below-threshold cyber operations, the legal adviser of the ICRC expands the notion based on the definition of 'military objective' included in article 52(2) of AP I, ultimately leading to the creation of a rather over-inclusive approach on the notion of attack. As Dörmann notes in the same section of the Protocol and in particular in the definition of a military objective, one of the possible results of an attack is the object's 'neutralization'.[140] A denial-of-service attack using a computer worm, virus, or logic bomb that would merely disable the object or disrupt its functionality without destroying it and without needing the replacement of physical components as the Tallinn Manual 2.0 requires, should count as an attack in the sense of the Protocol under Dörmann's approach.[141]

Schmitt notes that this argument's weakness is that the notion of 'military objective' does not come into play until the threshold of attack has been met.[142] Thus, one has to establish the key threshold of attack before the law of targeting applies to cyber operations that meet the requirement of attacks in the first place. Beyond the rationale behind each argumentation, the central issue in question remains the potentially severe disruptive impact of certain specific cyber operations on otherwise protected persons and objects. Other scholars have also advocated for expanding the definition of attack to include cyber operations that might not cause direct physical harm but can still result in the malfunction of critical cyber infrastructures essential to the civilian population.[143]

The most significant issue with the approaches presented is their inability to address the unique threat posed by cyber operations. For those who do not view military operations resulting in physical harm as

---

[134] Schmitt, 417.
[135] Schmitt, 417–18.
[136] The doctrine of kinetic equivalence suggests treating cyber operations with effects similar to traditional kinetic actions (physical force).
[137] Dinstein, 'Principle of Distinction', 264.
[138] Mavropoulou, 'Targeting in the Cyber Domain', 33.
[139] Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford: Oxford University Press, 2014), 180.
[140] AP I, art. 52(2) (defining 'military objective').
[141] Dörmann, 'Applicability of the Additional Protocols to Computer Network Attacks: An ICRC Viewpoint', 4.
[142] Schmitt, 'Key Issues', 95.
[143] Dieter Fleck, 'Searching for International Rules Applicable to Cyber Warfare—A Critical First Assessment of the New Tallinn Manual', *Journal of Conflict & Security Law* 18, no. 2 (2013): 341.

an indispensable element of an 'attack'[144], the question of whether data qualifies as an 'object' for the purposes of IHL carries serious implications for cyber operations that only have effects on the integrity of data itself, causing severe disruptions without any physical manifestation in the real world. Pursuant to this approach, the mere alteration of data that does not meet the criteria for a military objective, and thus a civilian object, may potentially constitute a violation of IHL when carried out in the context of an armed conflict, at least in certain circumstances. Conversely, those who consider the causation of physical damage as a *sine qua non* criterion for considering an act as an 'attack' under IHL would not regard the mere alteration of data as an 'attack'. As a consequence, the data would not fall within the rules governing distinction and other targeting rules,[145] resulting in limited or no protection in situations of armed conflict, even for those who regard data as an 'object' and regardless of whether it is a *civilian* object or not.[146]

This results in a normative gap whereby cyber operations by nature increase the possibilities of civilian objects to be 'targeted' without falling under the connotation of being 'attacked' according to IHL. Admittedly, the conclusions reached in this Chapter regarding the meaning of 'attack' in IHL may seem unsatisfactory. Yet, the meaning of a legal term may shift over time through the adoption of new treaty law, the slow evolution of customary norms through state practice and *opinio juris*,[147] or the emergence of new understandings in the face of the changing context of conflict to which it applies.[148]

With this context in mind, clarifying the importance and main practical implications in determining the level of protection for civilian data in armed conflicts, the present thesis will now turn to the question whether data itself can be considered an 'object' under IHL.

IV. WHETHER DATA QUALIFIES AS AN 'OBJECT'

When examining potential obstacles to comprehensive protection of civilian data, whether data even qualifies as an 'object' is as important as the question of what qualifies as an 'attack'. If the target of an adversarial military cyber operation – here, civilian data – does not qualify as an 'object', there is no requirement for the principle of distinction and other standard protections under targeting law to apply.[149] As a consequence, civilian data would not or only minimally be protected in situation of armed conflict. This Chapter proceeds to interpretate the meaning of the term 'object' as found in AP I under the customary rules of treaty interpretation and under customary international law.

A. Under the Additional Protocol I

The term 'object', as a subject of protection under AP I, is mentioned in numerous provisions in AP I,[150] beyond the ones discussed in Chapter II. In order to provide meaning to the term 'object' on the basis

---

[144] Ministère des Armées, 'Droit International Appliqué Aux Opérations Dans Le Cyberespace', 13; German Federal Foreign Office, 'On the Application of International Law in Cyberspace', March 2021, 8, accessed 8 August 2023, www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf; Lubell, 'Lawful Targets in Cyber Operations', 266.

[145] Peter Pascucci, 'Distinction and Proportionality in Cyber War: Virtual Problems with a Real Solution', *Minnesota Journal of International Law* 26 (2017): 443. See also Roscini, *Cyber Operations and the Use of Force in International Law*, 2014, 183–84. But see Schmitt, 'Wired Warfare 3.0', 340.

[146] Pomson, 'Objects', 6.

[147] Different states have issued varying perspectives on what constitutes an 'attack'. For instance, France has explicitly declared that the loss of system functionality is to be regarded as an attack. Ministère des Armées, 'Droit International Appliqué Aux Opérations Dans Le Cyberespace', para. 2.2.1. In contrast, Israel has taken the position that physical damage is required, excluding mere loss of functionality. Roy Schöndorf, 'Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations' 97, no. 1 (2021): 400. However, the vast majority of states, have refrained from defining their stance on this matter.

[148] Nonetheless, as long as the leading cyber-active states, including the United States, the United Kingdom, Israel, Russia, and China, do not adopt a broader definition of 'attack', the coverage gap will persist.

[149] Michael N. Schmitt, 'International Cyber Norms: Reflections on the Path Ahead', *Netherlands Military Law Review* 111, no. 22 (2018): 12.

[150] AP I, arts. 20, 48, 49(3)–(4), 51(4)–(5), 52(1)–(3), 53, 52(2)–(4), 56(1),(6)–(7), 57(1)–(5), 58, 61(1), 62(3), 69(1), 72, 85(3). The word 'object' appears elsewhere as well, but clearly with the meaning of 'a person or thing to which a specified action, thought, or feeling is directed' (OED): AP I, arts. 12(1), 41(1), 42(1)–(2), 51(2), 52(1), 53, 54(4), 56(1),(4)–(5), 76(1), 77(1), 85(3)–(4). The verb 'object' – 'to oppose or disapprove' (OED) – also appears in AP I: AP I, arts. 34(2), 98. The term 'objective', which as noted encompasses 'objects', but also persons, features in AP I, arts. 12(4), 28(1), 48, 49(3), 51(4)–(5),(7), 52(1)–(2), 56(1)–(5), 57(2),(3), 58, 85(4). Pomson, 'Objects', 9.

of the formal sources of international law, one must interpret it in accordance with the customary rules of treaty interpretation, as reflected in articles 31-33 of the Vienna Convention on the Law of Treaties (VCLT).[151] Even though the VCLT itself is not applicable to AP I because the latter was concluded before the VCLT's entry into force,[152] the customary rules of interpretation are applicable to treaties preceding its entry into force.[153]According to article 31(1) of the VCLT, '[a] treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose'.[154] The elements of interpretation, namely ordinary meaning, context, and object and purpose should be considered as a whole.[155] In other words, a treaty should be interpreted textually, contextually, and teleologically.[156]

1. Ordinary Meaning in its Context: The 'Object' Requirement

A significant portion on the question of whether data constitutes an 'object' has focused on its meaning in AP I, and in particular on the ICRC 1987 Commentary on AP I, which states that '[i]t is clear that in both English and French the word means something that is visible and tangible'.[157] The debate about the question of whether data has object-quality for the purposes of IHL comes down to two main positions.

Proponents of the first view content that the notion of 'object' as stipulated in article 52(2) of AP I, taking its ordinary meaning, implies that the target of the military operation must be an entity of physical quality.[158] For example, the majority of the authors of the Tallinn Manual 2.0 consider that 'data is intangible and therefore neither falls within the "ordinary meaning" of the term object, nor comports with the explanation of it offered in the […] 1987 Commentary'.[159] This argument mainly rests on a very literal understanding of 'object'. Data, as something invisible and intangible by definition, can therefore not be conceived as an object for the purposes of IHL, except in two cases.[160] According to Schmitt, the first case refers to data capable of direct transfer into tangible objects, illustrated by the example of banking account data transferable into money through ATMs, while the second refers to data that have intrinsic worth such as digital art.[161] This *prima facie* interpretation seems to be outdated considering the present state of cyber warfare. A minority of the experts of the Tallinn Manual 2.0 hold the viewpoint that data *per se* should be considered as objects, particularly for the purposes of targeting.[162] Otherwise, the minority argued, important civilian data might be excluded from the regulatory reach of the law of armed conflict.[163]

This opposing position holds that data can indeed be subsumed under the notion of 'object'. In spite of the 1987 ICRC Commentary's authoritative character and its invaluable contribution to IHL, the terms 'tangible' and 'visible' are not included in the language of AP I.[164] Having been drafted and published before the digital transformation, the notion of data was beyond the foresight of the drafters. Nonetheless,

---

[151] 'Vienna Convention on the Law of Treaties' (hereinafter VCLT), (Vienna, 23 May 1969), 1155 UNTS 331, art. 31–33.
[152] VCLT, art. 4.
[153] The applicability of these rules to treaties has been recognized by the International Court of Justice (ICJ): ICJ, 'Kasikili/Sedudu Island (Botswana/Namibia)' (1999), ICJ Rep 1045, para. 20; ICJ, 'Dispute Regarding Navigational and Related Rights (Costa Rica v. Nicaragua)' (2009), ICJ Rep 213, para. 47. The application of VCLT to AP I is based on the doctrine of intertemporal law, pursuant to which a treaty should be interpreted according to the rules of interpretation prevailing at the time of its application, rather than at the time the treaty was concluded: Ulf Linderfalk, 'The Application of International Legal Norms over Time: The Second Branch of Intertemporal Law', *Netherlands International Law Review* 58, no. 02 (August 2011): 162–65, https://doi.org/10.1017/S0165070X11200019. Whether the VCLT rules were, in any event, customary in 1977 is beyond the scope of this thesis.
[154] VCLT, art. 31(1).
[155] ICJ, 'Maritime Delimitation in the Indian Ocean (Somalia v. Kenya)', Preliminary Objections (2017), ICJ Rep 3, para. 64.
[156] Olivier Corten and Pierre Klein, eds., *The Vienna Conventions on the Law of Treaties: A Commentary*, Oxford Commentaries on International Law (Oxford: Oxford University Press, 2011), 804, 808.
[157] Sandoz, Swinarski, and Zimmermann, *Commentary on the Additional Protocols*, 634, (emphasis added). See also Pomson, 'Objects', 12–17. This conclusion is based on the dictionary definition of the OED of 1970, which states that an object is 'something placed before the eyes, or presented to the sight or other sense, an individual thing seen, or perceived, or that may be seen or perceived; a material thing'. 'Object, n', in *The Oxford English Dictionary: Volume VII*, 1970, 14.
[158] See, e.g., Pomson, 'Objects', 12–16.
[159] Schmitt, *Tallinn Manual 2.0*, 2017, 437. See also Schmitt, 'The Notion of "Objects" during Cyber Operations', 94.
[160] Schmitt, 'Key Issues', 96; Schmitt, *Tallinn Manual 2.0*, 2017, r. 100, para. 6.
[161] Schmitt, 'Key Issues', 96.
[162] Schmitt, *Tallinn Manual 2.0*, 2017, r. 100, para. 7.
[163] Schmitt, r. 100, para. 7.
[164] Sandoz, Swinarski, and Zimmermann, *Commentary on the Additional Protocols*, para. 2010.

the absence of their incorporation within the initial framework does not signify a deliberate omission on their part.[165] It has also been countered that the 1987 Commentary's 'definitional point about the term "object" was being made merely to distinguish the term as a "thing" from its use in the sense of "aim or purpose" […] rather than to specifically exclude intangible objects from the definition'.[166] In other words, it merely sought to clarify that only concrete things are subject to the principle of distinction and other rules, but not purely abstract concept such as, for example, 'civilian morale'.[167] Considering this binary distinction, data would clearly be notionally more akin to concrete things, given that it can be targeted and destroyed in a similar way as a military would attack a building or an enemy's weapon system. Morale, on the other hand, is a purely subjective category that might be affected by an attack but can hardly be targeted as such.[168] Dinniss further argues that while data lacks a material component, it is perceivable by the senses in particular sight, and therefore 'visible'.[169]

The main argument of the majority of scholarship is that the loss of non-tangible objects such as digital data does not entail analog consequences to the real world. Nowadays, it is possible to destroy millions of vital (civilian) data without any physical harm on the computer in which they are stored.[170] In scenarios like these, determining whether the loss of computer data meets the threshold of an attack, one has to prove damage. Therefore, Lubell has put forward the 'potential restoration capability' test.[171] This test disqualifies computer data from the notion of objects for there is no damage occurred as long as the lost data is retrievable. However, it is important to also consider the relevance of 'back up data' criterion.[172]

Another view permits irretrievable data to be classified as 'objects' under the law of targeting.[173] The classification under the principle of distinction of electronic data would then depend on whether the data could be restored.[174] The 'potential restoration capability' test, however, could wind up excluding from the definition of object many physical structures that have traditionally been considered objects because the damage done to them can be repaired. As electronic data could be potentially restored, buildings could potentially be rebuilt. While the analogy is not perfect, in both cases the restoration of damage can bear significant costs, which we may want the law of armed conflict to address. Finally, as for targeting data, the verification of back up data could be included within the duty of the attacker to take precautions reinforcing thus the argument in favor of data as 'objects'.[175]

In any event, regardless of the ICRC 1987 Commentary's intention, it is widely accepted that it constitutes only a 'subsidiary means for the determination of rules of law'[176], and thus cannot replace a complete analysis based on customary rules of treaty interpretation.

In light of the above, a restrictive literal and contextual interpretation of 'data' would have the consequence that 'many targets whose physical equivalents are firmly protected by IHL from enemy combat action would be considered fair game as long as the effects of the attack remain confined to cyberspace',[177] leading to a critical protection gap. Apart from this textual and contextual reading of article 52(2) of AP I, a teleological interpretation should also be considered.

---

[165] Lubell, 'Lawful Targets in Cyber Operations', 252.
[166] Dinniss, 'The Nature of Objects', 43; Lubell, 'Lawful Targets in Cyber Operations', 267–68; Mačák, 'Military Objectives 2.0', 67–68.
[167] Geiss and Lahmann, 'Protection of Data in Armed Conflict', 566.
[168] Mačák, 'Military Objectives 2.0', 73.
[169] Dinniss, 'The Nature of Objects', 43–44.
[170] Lubell, 'Lawful Targets in Cyber Operations', 267.
[171] Lubell, 268.
[172] The availability of back up copies of the lost data might influence the assessment of whether an 'attack' has occurred. Mavropoulou, 'Targeting in the Cyber Domain', 50.
[173] Lubell, 'Lawful Targets in Cyber Operations', 268.
[174] Lubell, 268.
[175] Lubell, 268.
[176] 'Statute of the International Court of Justice' (hereinafter 'ICJ Statute') (26 June 1945), 59. Stat. 1055, 33 UNTS 933, art. 38(1)(d). See also, specifically regarding ICRC commentaries, Jens David Ohlin and Larry May, *Necessity in International Law*, First edition (New York, NY: Oxford University Press, 2016), 22.
[177] Mačák, 'Military Objectives 2.0', 78.

2. Object and Purpose

In exploring the interpretation process of treaties, one fundamental aspect revolves around the elements of 'object and purpose' as outlined in the VCLT. Diverse perspectives exist regarding the interplay between these elements, with some regarding them as distinct considerations, with the former limiting the effects of the latter.[178] Others, conversely, view both elements simply as referring to the aim(s) of the treaty. Nevertheless, leading publicists concur that the 'object and purpose' of a treaty would not alter interpretation if the ordinary meaning of a term in its context leads to a singular meaning.[179] It is evident from the jurisprudence of the ICJ, that interpretations of specific treaty terms may not align with a treaty's intended purpose.[180]

The preamble of a treaty often serves as a convenient reference for discerning the treaty's underlying purpose,[181] complemented by a comprehensive examination of its provisions.[182] AP I's preamble *inter alia* notes that '[t]he High Contracting Parties […] [b]eliev[ed] it necessary nevertheless to reaffirm and develop the provisions protecting the victims of armed conflicts and to supplement measures intended to reinforce their application'.[183] Throughout the provisions of AP I, a persistent endeavour is evident in striking a balance between humanitarian protection and military exigencies,[184] which aligns with the development of IHL rules by states that persistently aimed to strike a balance between these two.[185]

Some scholars argue that interpreting 'object' to include data would enhance humanitarian protection of civilians.[186] In Kubo Mačák's perspective, as AP I generally aims at improving the protection of victims in armed conflict, and within AP I, Part IV specifically addresses civilians as a subcategory of victims of armed conflict in particular, he concludes that 'the object and purpose of Article 52(2) and its normative context is the enhancement of the protection of civilians during armed conflict'.[187] In light of this, a restrictive literal interpretation of 'data' would have as a result that 'many targets whose physical equivalents are firmly protected by IHL from enemy combat action would be considered fair game as long as the effects of the attack remain confined to cyberspace',[188] leading to a critical protection gap.[189]

---

[178] See, particularly, Isabelle Buffard and Karl Zemanek, 'The "Object and Purpose" of a Treaty: An Enigma?', *Austrian Review of International and European Law Online* 3, no. 1 (1998): 331–32, https://doi.org/10.1163/157365198X00177.

[179] Ulf Linderfalk, *On the Interpretation of Treaties: The Modern International Law as Expressed in the 1969 Vienna Convention on the Law of Treaties*, Law and Philosophy Library 83 (Dordrecht: Springer, 2007), 203–4; Oliver Dörr and Kirsten Schmalenbach, 'Article 31. General Rule of Interpretation', in *Vienna Convention on the Law of Treaties*, ed. Oliver Dörr and Kirsten Schmalenbach (Berlin, Heidelberg: Springer, 2012), 584–87, https://doi.org/10.1007/978-3-642-19291-3_34; Mustafa Kamil Yasseen, 'L'interprétation Des Traités d'après La Convention de Vienne Sur Le Droit Des Traités' (hereinafter 'L'interprétation Des Traités'), *Receuil Des Cours* 151, no. 1 (1 March 1976): 58.

[180] See, particularly, ICJ, 'Arbitral Award of 31 July 1989 (Guinea-Bissau v. Senegal)' (1991), ICJ Rep 53, para. 55-56; Kamil Yasseen, 'L'interprétation Des Traités', 58. See also ICJ, 'Land, Island and Maritime Frontier Dispute (El Salvador/Honduras: Nicaragua Intervening)' (1992), ICJ Rep 351, para. 376; ICJ, 'Territorial Dispute (Libya/Chad)' (1994), ICJ Rep 6, para. 41; ICJ, 'Application of the International Convention on the Elimination of All Forms of Racial Discrimination (Qatar v. United Arab Emirates), Preliminary Objections (2021), ICJ Rep 71, para. 81.

[181] See ICJ, 'Sovereignty over Pulau Ligitan and Pulau Sipadan (Indonesia/Malaysia)' (2002), ICJ Rep 625, para 51; ICJ, 'Questions relating to the Obligation to Prosecute or Extradite (Belgium v. Senegal)' (2012), ICJ Rep 422, para. 68; ICJ, 'Certain Iranian Assets (Iran v. United States)', Preliminary Objections (2019), ICJ Rep 7, para. 57. See also Makane Moïse Mbengue, 'Preamble', in Max Planck Encyclopedia of Public International Law, ed. Anne Peters and Rüdiger Wolfrum, September 2008.

[182] See ICJ, 'Oil Platforms (Iran v. United States)', Preliminary Objection (1996), ICJ Rep 803, para. 27-28; ICJ, 'Question of the Delimitation of the Continental Shelf between Nicaragua and Colombia beyond 200 Nautical Miles from the Nicaraguan Coast (Nicaragua v. Colombia)', Preliminary Objections (2016), ICJ Rep 100, para. 33.

[183] AP I, preamble.

[184] For a few explicit examples, see, e.g., AP I, arts. 13(1), 51(5)(b), 65(1), 70(3).

[185] Michael N. Schmitt, 'Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance', *Virginia Journal of International Law* 50, no. 4 (2010): 795, https://doi.org/10.1007/978-90-6704-740-1_3; Dinstein, *Conduct of Hostilities*, 9–10.

[186] See Mačák, 'Military Objectives 2.0', 77–78. See also Tim McCormack, 'International Humanitarian Law and the Targeting of Data', *International Law Studies* 94, no. 1 (4 November 2018): 240.

[187] Mačák, 'Military Objectives 2.0', 73.

[188] Mačák, 73.

[189] ICRC, 'International Humanitarian Law and Cyber Operations during Armed Conflicts: ICRC Position Paper' (International Committee of the Red Cross, November 2019), 8, https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts.

However, this broader interpretation may have significant implications for cyber operations during armed conflict, raising doubts that such expansion will indeed reflect sufficient sensitivity to military exigencies and aim at the appropriate balance between them and humanitarian considerations.[190] Given that manipulating or deleting data might offer a convenient – and arguably less lethal or destructive – approach to weaken the enemy,[191] certain states would likely not accept an expansive interpretation of the notion of 'object' that would include data *per se*.[192]

Certain approaches seek to address the potentially far-reaching implications by proposing, often on the basis of policy considerations,[193] to limit the concept of 'object' to data such as 'civilian data that is "essential" to the well-being of the civilian population',[194] or content data.[195]

Taking Dinniss' fundamental distinction between operational-level data and content-level data as a starting point, the analysis of legal protections under IHL will differ. Cyber operations affecting operational-level data's availability or integrity can 'result in loss of functionality of the system'.[196] Although data itself might not be the direct target, but rather the affected system, classifying all software code as 'data' implies that most cyber operations inherently target data.[197] To assess the applicability of IHL and potential prohibitions arising from violations of the principle of distinction, proportionality, and the duty of precautions in attack, one needs to look at the consequences of the cyber operation, debated in Chapter III. Applying IHL to cyber operations targeting content-level data presents, however, a legal grey zone.[198] According to Dinniss, cyber operations impacting data integrity 'will leave the system intact, albeit with corrupted or missing data',[199] while operations affecting availability hinder accessibility. In the context of cyber operations aimed at data confidentiality, no direct harm to the system or stored data occurs, but a copy is created unless any unforeseen events occur.[200] Current debate's focus on IHL's applicability to cyber operations compromising data integrity as '[d]eleting or tampering with [essential civilian data] could quickly bring government services and private businesses to a complete standstill, and could cause more harm to civilians than the destruction of physical objects'.[201]

Ori Pomson challenges these viewpoints, pointing out their limitations. He contends that differentiating content-level data from other data types is impractical since they all consist of 1s and 0s. This is even more pertinent when considering data deemed 'essential civilian data',[202] although the exact meaning of this term remains unclear. In terms of the principles outlined in AP I, there appears to be no basis to distinguish between various types of data. Furthermore, the method by which such approaches manage to differentiate between diverse data types remains uncertain from a definitional standpoint.[203]

In light of the above, regardless of one's position on the role of the 'object and purpose' of a treaty in interpretation, if data is not considered as an 'object' under IHL, the conclusion could be contrary to the

[190] Cf. Schmitt, 'The Notion of "Objects" during Cyber Operations', 101.
[191] Schmitt, 'Wired Warfare 3.0', 342.
[192] Michael N. Schmitt, 'The Law of Cyber Warfare: Quo Vadis?', *Stanford Law & Policy Review* 25 (2014): 298.
[193] ICRC, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts: Recommitting to Protection in Armed Conflict on the 10th Anniversary of the Geneva Conventions', 28.
[194] Schmitt, *Tallinn Manual 2.0*, 2017, 437.
[195] Ministère des Armées, 'Droit International Appliqué Aux Opérations Dans Le Cyberespace', 16.
[196] Dinniss, 'The Nature of Objects', 42.
[197] Exceptions exist, such as certain side-channel attacks that manipulate code through viruses, worms, trojan horses, rootkits, and related means. Geiss and Lahmann, 'Protection of Data in Armed Conflict', 563.
[198] Geiss and Lahmann, 563.
[199] Dinniss, 'The Nature of Objects', 42.
[200] Nevertheless, it can be argued that encrypting data in a ransomware attack, even with an existing decryption key, is actually directed towards compromising its integrity rather than simply limiting it availability.
[201] ICRC, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts', 43.
[202] The ICRC stated that the category of essential civilian data encompasses crucial information such as 'medical data, biometric data, social security data, tax records, bank accounts, companies' client files or election lists and records'. ICRC, 'International Humanitarian Law and Cyber Operations during Armed Conflicts', 490.
[203] Pomson, 'Objects', 19.

object and purpose of AP I,[204] which is to allow for military necessity while affording effective protection to civilians.[205]

3. Evolutionary Interpretation?

An implicit consensus appears to suggest that, at least in the past, the term 'object' has not been understood to include data.[206] However, some argue for an 'evolutionary' interpretation of the term so that it can also encompass data in the present context.[207] In a candid statement by one scholar, a position that views computer data as not constituting an 'object' is criticized for taking a 'too traditional approach relying on the old interpretation of the rule which had been developed when the possibility of cyber attacks must have appeared as mere science fiction'.[208]

As to law, it must be recognized that so-called 'evolutionary' interpretation, if it is considered part of the existing treaty interpretation law, and not *lex ferenda*, cannot stand as a separate method of interpretation beyond the rules laid out in the VCLT. Any changes in the treaty interpretation over time, must be a result of applying the VCLT's interpretation rules to the treaty.[209] However, considering that several scholars invoked 'evolutionary' interpretation to different extents when interpreting the term 'object', it seems appropriate to touch upon this argument.

The ICJ's stance in the *Navigational Rights case* indicated that if parties use generic terms in a treaty, especially for treaties lasting a long time or of continues duration, it is presumed that they were aware the terms would evolve over time.[210] If AP I fulfills the requirements set out by the ICJ, the evolved meaning might be considered.[211] Moreover, Mačák argues that the 'object and purpose' of the Protocol as a treaty providing for the protection of victims of armed conflicts supports resort to the evolutionary interpretation. [212] Notably, influential human rights tribunals 'have established that human rights treaties are living instruments which must be interpreted in light of present day conditions'[213] and that when in doubt, the evolutive reading should prevail for multilateral treaties crafted for the protection of individuals, a core principle shared by both, human rights treaties and the Protocol.[214] Additionally, the evolutionary interpretation has been applied to other terms in AP I previously. For example, the ICJ's *Nuclear Weapons* advisory opinion highlighted the Martens Clause in article 1 of AP I as means of addressing what the Court called 'the rapid evolution of military technology'.[215]

This dynamic approach and the degree to which ideas of warfare have evolved due to the development of cyber technologies should be further assessed, inviting contemplation on alternative perspectives and approaches that may not have been explored within this thesis.

Regardless of the perspective one ultimately chooses to endorse, analysing the Protocol's provision in the context of cyber reality strengthens the existing body of IHL. Resisting new interpretations could

---

[204] Dinniss, 'The Nature of Objects', 44.

[205] 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', *International Review of the Red Cross* 102, no. 913 (April 2020): 288, https://doi.org/10.1017/S1816383120000387.

[206] Mačák, 'Military Objectives 2.0', 68–71; Lubell, 'Lawful Targets in Cyber Operations', 267–68; Rain Liivoja and Tim McCormack, 'Law in the Virtual Battlespace: The Tallinn Manual and the Jus in Bello', in *Yearbook of International Humanitarian Law Volume 15, 2012*, ed. Terry D. Gill et al. (The Hague: T.M.C. Asser Press, 2014), 53–54, https://doi.org/10.1007/978-90-6704-924-5_3.

[207] Liivoja and McCormack, 'Law in the Virtual Battlespace', 53–54; Mačák, 'Military Objectives 2.0', 68–71; Lubell, 'Lawful Targets in Cyber Operations', 267–268.

[208] Kai Ambos, 'International Criminal Responsibility in Cyberspace', in *Research Handbook on International Law and Cyberspace* (Northampton: Edward Elgar Publishing, 2015), 131.

[209] Pomson, 'Objects', 20.

[210] ICJ, 'Dispute regarding Navigational and Related Rights (Costa Rica v. Nicaragua)', para. 66: '[W]here the parties have used generic terms in a treaty, the parties necessarily having been aware that the meaning of the terms was likely to evolve over time, and where the treaty has been entered into for a very long period or is "of continuing duration", the parties must be presumed, as a general rule, to have intended those terms to have an evolving meaning'.

[211] Mačák, 'Military Objectives 2.0', 70–71.

[212] See Chapter IV(A)(2) below for a detailed analysis of the 'object and purpose' of AP I in respect of the analyzed provision.

[213] ECtHR, 'Tyrer v. United Kingdom' Judgement (1978), 2 EHRR 1, para 31; IACtHR, 'The Right to Information on Consular Assistance in the Framework of the Guarantees of the Due Process of Law' Advisory Opinion, (1999), no. 16, para. 114; UN HRC, 'Roger Judge v. Canada', (2003), UN Doc CCPR/C/78/D/829/1998, para 10.3.

[214] Mačák, 'Military Objectives 2.0', 70.

[215] ICJ, 'Legality of the Threat or Use of Nuclear Weapons', para. 78.

render the existing rules outdated or misapplied.[216] Given the cyber reality, it becomes essential to reassess the concept of objects to ensure data is subject to the principle of distinction and other laws of targeting. Neglecting this consideration would result in digital data falling outside the scope of regulation within the law of armed conflict, creating a normative gap. The interpretation of rules will be influenced by future cyber conflicts and state practices, which will contribute to a clearer understanding of the notion of digital data and their status under the law of targeting. The next Chapter will delve deeper into the matter of international customary law.

B. Under Customary International Law: State Practice and *Opinio Juris*

It appears that a significant portion of the debate regarding whether data is considered an 'object' has focused on its meaning in AP I, rather than its status under customary international law. Consequently, it is appropriate to examine the latter. Prior to delving into this matter, it is important to offer several observations about the methodology to be employed, especially considering the historical controversies surrounding the identification of customary rules over time.

According to a recent statement by the International Law Commission, determining 'the existence and content of a rule of customary international law, it is necessary to ascertain whether there is a general practice that is accepted as law (*opinio juris*)'.[217] The widely accepted two-element approach among states,[218] which demands the existence of state practice and acceptance, will be adhered to here. Acceptance as law should be viewed as a (unilateral) juridical act, 'a manifestation of will intended to produce the legal consequences determined by this will'.[219] It follows that it is necessary to ascertain the specific meaning that states attribute to the term 'object' as a subject of protection within the framework of conducting hostilities.[220] In this context, given that the matter under consideration pertains to international customary law, as opposed to explicit treaty law, 'reliance must primarily be placed on such elements as official pronouncements of States, military manuals and judicial decisions'.[221]

State practice is *de facto* scarce concerning public state positions on the application of international law to cyber operations. In recent years, despite the increasing prominence of cyber warfare, only a limited number of states have explicitly articulated their positions concerning the interpretation of the term 'object' under IHL, both in a general context and particularly with respect to data, and even fever with regards to the notion of civilian data.[222] Notably, only a few states have raised the question of whether data qualifies as an 'object' under IHL while refraining from providing definite responses.[223]

The Norwegian Manual of the Law of Armed Conflict asserts that '[i]n the context of target selection, data shall be regarded as objects and may only be attacked directly if they qualify as a lawful target.'[224] According to an official paper released by the French Ministère des Armées, France holds the view that '[a]lthough intangible, France considers that civilian content data may be deemed protected objects'.[225] Additionally, the German Government's position paper cites examples of 'objects' such as 'computers,

---

[216] Mavropoulou, 'Targeting in the Cyber Domain', 51.

[217] UN International Law Commission, 'Draft Conclusions on Identification of Customary International Law, with Commentaries' (2018), UN Doc A/73/10, 124. See also, e.g., ICJ, 'Asylum (Colombia/Peru)', 1950, ICJ Rep 266, 277; ICJ, 'North Sea Continental Shelf (Federal Republic of Germany/Denmark; Federal Republic of Germany/Netherlands)' (1969), ICJ Rep 3, para. 73-77.

[218] See, e.g., UNGA, 'Report of the International Law Commission on the Work of its 63rd and 65th Sessions: Topical Summary of the Discussion Held in the 6th Committee of the General Assembly during its 68th Session, Prepared by the Secretariat' (2014), UN Doc A/CN.4/666, para. 43.

[219] Roberto Ago, 'Second report on State responsibility', *Yearbook of the International Law Commission*, no. 2 (1970): 186.

[220] Pomson, 'Objects', 27.

[221] ICJ, 'North Sea Continental Shelf (Federal Republic of Germany/ Denmark; Federal Republic of Germany/Netherlands)' (1969), ICJ Rep 3, para. 74.

[222] Pomson, 'Objects', 25–26.

[223] While raising the issue without adopting a definitive position, see Brian J. Egan, 'Remarks on International Law and Stability in Cyberspace', U.S. Department of State, 10 November 2016, https://2009-2017.state.gov/s/l/releases/remarks/264303.htm; 'Switzerland's Position Paper on the Application of International Law in Cyberspace (Annex UN GGE 2019/2021)', Federal Department of Foreign Affairs FDFA, 10, accessed 2 August 2023, www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-20192021_EN.pdf; UNGA, 'Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States' (2021), UN Doc A/76/136, 23.

[224] The Chief of Defence, *Manual of the Law of Armed Conflict*, (Norway: 2013), 210, quoted in Pomson, 'Objects', 28.

[225] Ministère des Armées, 'Droit International Appliqué Aux Opérations Dans Le Cyberespace', 16.

computer networks, cyber infrastructure, and data stocks.'[226] Romania's preliminary stance is 'that cyber operations against data do trigger the application of IHL', and that '[t]herefore cyber-attacks can only be directed against those data that represent military objectives according to IHL and cannot be directed against those data that represent a civilian object which must be protected under the principle of distinction'.[227] Conversely, the Danish Military Manual maintains that '[g]enerally speaking […] (digital) data do not in general constitute an object'.[228] Similarly, Chile's perspective is that 'under current international humanitarian law […] data would not qualify as objects' in principle, because they are essentially intangible, without prejudice to the physical elements containing the data – hardware, for example'.[229] Moreover, Israel's Deputy Attorney-General of International Law contends that it is his state's position, as it currently stands, under the law of armed conflict, that 'only tangible things can constitute objects',[230] leaving computer data excluded.

Clearly, there is no discernible pattern among states regarding the classification of data as an 'object' under IHL, and the scarcity of official statements, predominantly from Western states, is insufficient to lend it legal significance.[231] As a result, data, as of now, does not qualify as an 'object' under customary international law. While it remains plausible that future development in customary international law may include digital data within the ambit of protection accorded to 'objects', such a shift would necessitate widespread recognition among states to extend such protection to data, together with state practice in accordance with the potential rules. The present state of affairs falls far short of meeting these criteria.

V. LIMITATIONS OF EXISTING APPLICABLE LAW: THE WAY AHEAD

As demonstrated in the preceding Chapters, the discussion on civilian data protection in armed conflict has encountered confusion and uncertainty in defining 'attack' and 'data'. The present thesis has aimed to provide some clarification.

At its most fundamental level, one can claim that all cyber operations inherently involve targeting data. The complexities of incorporating this core aspect of cybersecurity into the current framework of IHL may be (partially) resolved by emphasizing the consequences of cyber operations for the purpose of legal assessment (consequence- or effects-based approach).[232] Yet, such debate is inherently limited since it does not tackle the issue of which rules, if any, pertain to cyber operation targeting data that merely represent information, the targeting of which does not entail any physical effects at all. Hence, the discussion should extend beyond what Dinniss calls 'operational-level data' and focus on 'content-level data'. In this context, the ongoing discourse among experts and policymakers has revealed the limitations of current IHL, which primary addresses the physical effects of armed conflict. As a result, existing protections only cover cyber operations affecting availability or integrity, provided that they result in physical or otherwise tangible harmful consequences. Operations targeting data confidentiality, such as surveillance, espionage, or the exploitation of personal data in order to coerce or otherwise influence the behavior of individuals in situations of armed conflict, remain beyond the purview of existing IHL unless they fall under a specifically protected data category. It appears that ensuring the confidentiality of personal data, a fundamental aspect of existing data protection frameworks, often falls beyond the scope of what has so far been considered to require or deserve protection during armed conflict. Nonetheless, many essential civilian data sets, potentially affected by adversarial military cyber

[226] German Federal Foreign Office, 'On the Application of International Law in Cyberspace', 8 (emphasis omitted).
[227] UNGA, Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States', 78.
[228] Peter Bartram and Jes Rynkeby Knudsen, *Military Manual on International Law Relevant to Danish Armed Forces in International Operations* (Danish Ministry of Defence, 2016), 292.
[229] Quoted in Duncan B. Hollis, 'International Law and State Cyber Operations - Improving Transparency: Fourth Report', CIJ/doc 603/20, March 2020, para. 48.
[230] Schöndorf, 'Israel's Perspective', 401.
[231] Pomson, 'Objects', 29.
[232] Schmitt, 'The Notion of "Objects" during Cyber Operations', 97.

operations, fall within the ambit of personal data as previously defined. Examples include 'civil registries, insurance data, medical data',[233] and 'social security data, tax records, and bank accounts'.[234]

Given these considerations, it is proposed that these inherent limitations necessitate a discussion that goes beyond the current debates that have taken the rules and principles of existing IHL, in particular the notions of 'attack' and 'object' and applied them to 'data'. An alternative approach could involve using existing principles of data protection, data security, and other relevant legal frameworks and attempt to apply them to modern armed conflict, alongside the rules of IHL.[235] Modern data protection frameworks function as legislative substantiations for the human right to privacy. This requires an examination of the relationship between IHL and international human rights law,[236] while also considering the application of human rights treaties to virtual scenarios.[237] Such an approach could potentially be more fitting to acknowledge the true importance of data in the information society and address the resulting protection needs in times of armed conflict.

CONCLUSION

According to the analyses of the present thesis, a significant coverage gap exists within IHL for the protection of civilian data in modern society. The thesis underscores the absence of international jurisprudence on cyber operations in armed conflicts, leaving conclusions on the applicability of the *jus in bello* to cyber operations against civilian data restricted to academic scholarship, speculation, and emerging state practices. The legal grey zones revolving around the definition of 'attack' and 'object' take center stage, encompassing the contemporary debates that lie within the purview of this thesis.

First, there is no agreed definition on what constitutes a cyber attack within IHL. In particular, regarding the key threshold of 'attack' under the *jus in bello*, consideration should be given as to how below-threshold cyber operations are to be addressed. Second, the question of the protection of civilian data in situations of armed conflict has been discussed from the angle of its object-quality, which makes the concept more readily fit the existing body of IHL. It follows that various rules of IHL which provide protections to 'objects' – particularly those relating to distinction, proportionality, and precautions in attack – do not protect data if it does not fall within the definition of 'object'. While targeting law provides minimal protection to civilian data beyond those limited operations that would produce physical effects, certain categories of targets enjoy special protections that do not rely on qualifications such as 'attacks' or 'objects'.[238]

Against this background, the analysis has so far demonstrated the issues to be further considered and reassessed in the context of cyber operations against civilian data in IHL. The present thesis proposes expanding perspectives beyond the established traditional scope and instead exploring what kind of approach will be required to comprehend and adequality protect the various functions of data, which rely on confidentiality, integrity, and availability for both personal and non-personal data. With this in mind, the thesis has attempted to outline preliminary thoughts, serving as a catalyst for initiating discussions.

---

[233] Laurent Gisel and Tilman Rodenhäuser, 'Cyber Operations and International Humanitarian Law: Five Key Points', Humanitarian Law & Policy Blog, 28 November 2019, accessed 10 August 2023, https://blogs.icrc.org/law-and-policy/2019/11/28/cyber-operations-ihl-five-key-points/.

[234] Schmitt, 'Wired Warfare 3.0', 340.

[235] Geiss and Lahmann, 'Protection of Data in Armed Conflict', 570.

[236] See, e.g., Janina Dill, 'Towards a Moral Division of Labour between IHL and IHRL during the Conduct of Hostilities', in *Law Applicable to Armed Conflict*, by Ziv Bohrer, Janina Dill, and Helen Duffy, 1st ed. (Cambridge: Cambridge University Press, 2020), 197, https://doi.org/10.1017/9781108674416.

[237] See, e.g., Helen McDermott, 'Application of the International Human Rights Law Framework in Cyber Space', in *Human Rights and 21st Century Challenges*, by Helen McDermott et al. (Oxford: Oxford University Press, 2020), 190, https://doi.org/10.1093/oso/9780198824770.003.0009.

[238] Henckaerts and Doswald-Beck, *Customary IHL*, 79–160.

STATUTORY DECLARATION

‘I hereby declare that the thesis with the title “Applicability of the Jus in Bello to Cyber Operations against Civilian Data: A Legal Grey Zone in the Protection of Data” has been composed by myself autonomously and that no means other than those declared were used. In every single case, I have marked parts that were taken out of published or unpublished work, either verbatim or in a paraphrased manner, as such through a quotation. This thesis has not been handed in or published before in the same or similar form.’

Geneva, 20.08.2023

(Signature)

BIBLIOGRAPHY

Articles/Books/Reports

Ambos, Kai. ‘International Criminal Responsibility in Cyberspace’. In *Research Handbook on International Law and Cyberspace*. Northampton: Edward Elgar Publishing, 2015.

Ago, Roberto. 'Second Report on State Responsibility'. *Yearbook of the International Law Commission*, no. 2 (1970): 177-97.

Bartram, Peter, and Jes Rynkeby Knudsen. *Military Manual on International Law Relevant to Danish Armed Forces in International Operations*. Danish Ministry of Defence, 2016.

Betz, David, and Tim Stevens. *Cyberspace and the State: Toward a Strategy for Cyber-Power*. London: The International Institute for Strategic Studies (IISS), 2011.

Biller, Jeffrey, and Timothy Goines. ‘Protecting Civilian Data in Armed Conflicts: The Need for an Ethical Foundation’. In *Ethical Dilemmas in the Global Defense Industry*, edited by Daniel Schoeni and Tobias Vestner, 544. Ethics, National Security, and the Rule of Law. Oxford: Oxford University Press, 2023.

Bothe, Michael, Karl Josef Partsch, and Waldemar A. Solf. *New Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949*. The Hague, Boston, London: Martinus Nijhoff Publishers, 1982.

Buffard, Isabelle, and Karl Zemanek. ‘The “Object and Purpose” of a Treaty: An Enigma?’ *Austrian Review of International and European Law Online* 3, no. 1 (1998): 311–43. https://doi.org/10.1163/157365198X00177.

Cohen, Julie E. ‘Cyberspace As/And Space’. *Columbia Law Review* 107 (2007).

Corten, Olivier, and Pierre Klein, eds. *The Vienna Conventions on the Law of Treaties: A Commentary*. Oxford Commentaries on International Law. Oxford: Oxford University Press, 2011.

Delerue, François. *Cyber Operations and International Law*. Cambridge Studies in International and Comparative Law. Cambridge: Cambridge University Press, 2020. https://doi.org/10.1017/9781108780605.

Dill, Janina. ‘Towards a Moral Division of Labour between IHL and IHRL during the Conduct of Hostilities’. In *Law Applicable to Armed Conflict*, by Ziv Bohrer, Janina Dill, and Helen Duffy, 1st ed. Cambridge: Cambridge University Press, 2020. https://doi.org/10.1017/9781108674416.

Dinniss, Harrison. ‘The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives’. *Israel Law Review* 48, no. 1 (March 2015): 39–54. https://doi.org/10.1017/S0021223714000272.

Dinstein, Yoram. *The Conduct of Hostilities under the Law of International Armed Conflict*. Third edition. Cambridge: Cambridge University Press, 2016.

Dinstein, Yoram. ‘The Principle of Distinction and Cyber War in International Armed Conflicts’. *Journal of Conflict and Security Law* 17, no. 2 (2012): 261–77.

Dörmann, Knut, Liesbeth Lijnzaad, Marco Sassòli, Philip Spoerri, Jean-Marie Henckaerts, and ICRC, eds. *Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*. Cambridge, United Kingdom: Cambridge University Press, 2016.

Dörr, Oliver, and Kirsten Schmalenbach. 'Article 31. General Rule of Interpretation'. In *Vienna Convention on the Law of Treaties*, edited by Oliver Dörr and Kirsten Schmalenbach, 521–70. Berlin, Heidelberg: Springer, 2012. https://doi.org/10.1007/978-3-642-19291-3_34.

Dupuis, Martin P., John Q. Heywood, and Michéle Y.F. Sarko. 'The Sixth Annual American Red Cross-Washington College of Law Conference on International Humanitarian Law: A Workshop on Customary International Law and the 1977 Protocols Additional to the 1949 Geneva Conventions'. *American University International Law Review* 2, no. 2 (1987).

Egan, Brian J. 'Remarks on International Law and Stability in Cyberspace'. U.S. Department of State, 10 November 2016. https:// 2009-2017.state.gov/s/l/releases/remarks/264303.htm.

Fleck, Dieter. 'Searching for International Rules Applicable to Cyber Warfare—A Critical First Assessment of the New Tallinn Manual'. *Journal of Conflict & Security Law* 18, no. 2 (2013): 331–51.

Fleck, Dieter, ed. *The Handbook of International Humanitarian Law*. 4th ed. Oxford: Oxford University Press, 2021.

Geiss, Robin, and Henning Lahmann. 'Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space'. *Israel Law Review* 45, no. 3 (November 2012): 381–99. https://doi.org/10.1017/S0021223712000179.

Geiss, Robin, and Henning Lahmann. 'Protection of Data in Armed Conflict'. *International Law Studies* 97 (2021): 18.

Gibson, William. *Neuromancien*. New York: Ace Books, 1948.

Gisel, Laurent, 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'. *International Review of the Red Cross* 102, no. 913 (April 2020): 287–334. https://doi.org/10.1017/S1816383120000387.

Greenwood, Christopher. 'Current Issues in the Law of Armed Conflict: Weapons, Targets and International Criminal Liability'. *Singapore Journal of International & Comparative Law* 1, no. 2 (1997): 441–67.

Heintschel von Heinegg, Wolff. 'Territorial Sovereignty and Neutrality in Cyberspace'. *International Law Studies* 89 (2013).

Henckaerts, Jean-Marie, Louise Doswald-Beck, and Carolin Alvermann. *Customary International Humanitarian Law - Volume 1: Rules*. Edited by ICRC. Cambridge: Cambridge University Press, 2005. https://doi.org/10.1017/CBO9780511804700.

Hollis, Duncan B. 'International Law and State Cyber Operations - Improving Transparency: Fourth Report'. CIJ/doc 603/20, March 2020.

International Law Association Study Group on the Conduct of Hostilities in the 21st Century. 'The Conduct of Hostilities and International Humanitarian Law: Challenges of 21st Century Warfare'. *Stockton Center for the Study of International Law* 93, no. 322 (17 August 2017).

Joint Chiefs of Staff. 'Joint Targeting'. *Joint Publication* (31 January 2013).

Kamil Yasseen, Mustafa. 'L'interprétation Des Traités d'après La Convention de Vienne Sur Le Droit Des Traités'. *Receuil Des Cours* 151, no. 1 (1 March 1976).

Kolb, Robert. *Advanced Introduction to International Humanitarian Law*. Elgar Advanced Introductions. Cheltenham: Edward Elgar, 2014.

Kuehl, Daniel T. 'From Cyberspace to Cyberpower: Defining the Problem'. In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, 1st ed. Washington, D.C.: Potomac Books, 2009.

Liaropoulos, Andrew N. 'Power and Security in Cyberspace: Implications for the Westphalian State System'. *Panorama of Global Security Environment*, 2011.

Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Santa Monica: RAND, 2009.

Liivoja, Rain, and Tim McCormack. 'Law in the Virtual Battlespace: The Tallinn Manual and the Jus in Bello'. In *Yearbook of International Humanitarian Law Volume 15, 2012*, edited by Terry D. Gill, Robin Geiß, Robert Heinsch, Tim McCormack, Christophe Paulussen, and Jessica Dorsey, 45–58. The Hague: T.M.C. Asser Press, 2014. https://doi.org/10.1007/978-90-6704-924-5_3.

Lin, Herbert S. 'Offensive Cyber Operations and the Use of Force'. *Journal of National Security Law and Policy* 4 (2010).

Linderfalk, Ulf. *On the Interpretation of Treaties: The Modern International Law as Expressed in the 1969 Vienna Convention on the Law of Treaties*. Law and Philosophy Library 83. Dordrecht: Springer, 2007.

Linderfalk, Ulf. 'The Application of International Legal Norms over Time: The Second Branch of Intertemporal Law'. *Netherlands International Law Review* 58, no. 02 (August 2011): 147–72. https://doi.org/10.1017/S0165070X11200019.

Lubell, Noam. 'Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?' In *Israel Yearbook on Human Rights*, by Fania Domb, 23–43. edited by Yoram Dinstein. 43. Brill | Nijhoff, 2013. https://doi.org/10.1163/9789004242081_003.

Mačák, Kubo. 'Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law'. *Israel Law Review* 48, no. 1 (March 2015): 55–80. https://doi.org/10.1017/S0021223714000260.

Mavropoulou, Elizabeth. 'Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks'. *Journal of Law & Cyber Warfare* 4, no. 2 (2015): 23–93.

McCormack, Tim. 'International Humanitarian Law and the Targeting of Data'. *International Law Studies* 94, no. 1 (4 November 2018).

McDermott, Helen. ‘Application of the International Human Rights Law Framework in Cyber Space’. In *Human Rights and 21st Century Challenges*, by Helen McDermott, Dapo Akande, Jaako Kuosmanen, Helen McDermott, and Dominic Roser, 190–210. Oxford: Oxford University Press, 2020. https://doi.org/10.1093/oso/9780198824770.003.0009.

Melzer, Nils. ‘Cyberwarfare and International Law’. *UNIDIR Ressources*, 2011.

Ministère des Armées. ‘Droit International Appliqué Aux Opérations Dans Le Cyberespace’. France, 2019. https://www.justsecurity.org/wp-content/uploads/2019/09/droit-internat-appliqué-aux-opérations-cyberespace-france.pdf.

Momtaz, Djamchid. ‘Les règles relatives à la protection de l’environnement au cours de conflits armés à l’épreuve du conflit entre l’Iraq et le Koweit’. *Annuaire français de droit international* 37, no. 1 (1991): 203–19. https://doi.org/10.3406/afdi.1991.3014.

Office of the Chairman of the Joint Chiefs of Staff. ‘Cyberspace’. In *DOD Dictionary of Military and Associated Terms*. Washington, D.C.: The Joint Staff, 2021.

Pascucci, Peter. ‘Distinction and Proportionality in Cyber War: Virtual Problems with a Real Solution’. *Minnesota Journal of International Law* 26 (2017).

Pomson, Ori. ‘“Objects”? The Legal Status of Computer Data under International Humanitarian Law’. *Journal of Conflict and Security Law*, 30 January 2023.

Rattray, Gregory J. ‘An Environmental Approach to Understanding Cyberpower’. In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. Washington D.C.: Potomac Books, 2009. https://doi.org/10.2307/j.ctt1djmhj1.

Roscini, Marco. *Cyber Operations and the Use of Force in International Law*. Oxford: Oxford University Press, 2014. https://doi.org/10.1093/acprof:oso/9780199655014.001.0001.

Roscini, Marco. ‘Targeting and Contemporary Aerial Bombardment’. *International and Comparative Law Quarterly* 54, no. 2 (April 2005): 411–44. https://doi.org/10.1093/iclq/lei006.

Sandoz, Yves, Christophe Swinarski, and Bruno Zimmermann. *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*. Edited by International Committee of the Red Cross. Geneva: Martinus Nijhoff Publishers, 1987.

Sassòli, Marco, and Anaïs Maroonian. ‘La proportionnalité en droit international humanitaire: principe et règle’. In *Proportionnalité, droits fondamentaux et juges*, Rahma Bentirou Mathlouthi (ed.). Paris: l’Harmattan, 2023.

Sassòli, Marco, and Patrick Nagler. *International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare*. Cheltenham: Edward Elgar Publishing, 2019. https://doi.org/10.4337/9781786438553.

Schmitt, Michael N. ‘“Attack” as a Term of Art in International Law: The Cyber Operations Context’. In *2012 4th International Conference on Cyber Conflict (CYCON 2012)*, 1–11. Tallinn, 2012.

Schmitt, Michael N. ‘Cyber Operations and the Jus in Bello: Key Issues’. *Naval War College International Law Studies*, 2 March 2011.

Schmitt, Michael N. ‘International Cyber Norms: Reflections on the Path Ahead’. *Netherlands Military Law Review* 111, no. 22 (2018).

Schmitt, Michael N. ‘Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance’. *Virginia Journal of International Law* 50, no. 4 (2010). https://doi.org/10.1007/978-90-6704-740-1_3.

Schmitt, Michael N. ‘Rewired Warfare: Rethinking the Law of Cyber Attack’. *International Review of the Red Cross*, Scope of the Law in Armed Conflict, 96, no. 893 (March 2014): 189–206. https://doi.org/10.1017/S1816383114000381.

Schmitt, Michael N, ed. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations: Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre for Excellence*. 2nd ed. Cambridge: Cambridge University Press, 2017. https://doi.org/10.1017/9781316822524.

Schmitt, Michael N. ‘The Law of Cyber Warfare: Quo Vadis?’ *Stanford Law & Policy Review* 25 (2014): 269–99.

Schmitt, Michael N. ‘The Notion of “Objects” during Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision’. *Israel Law Review* 48, no. 1 (March 2015): 81–109. https://doi.org/10.1017/S0021223714000314.

Schmitt, Michael N. ‘Wired Warfare 3.0: Protecting the Civilian Population during Cyber Operations’. *International Review of the Red Cross*, Memory and War, 101, no. 1 (April 2019): 333–55. https://doi.org/10.1017/S1816383119000018.

Schöndorf, Roy. ‘Israel’s Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations’ 97, no. 1 (2021).

Sheldon, John B. ‘Deciphering Cyberpower: Strategic Purpose in Peace and War’. *Strategic Studies Quarterly* 5, no. 2 (2011).

The Chief of Defence. *Manual of the Law of Armed Conflict*. Norway, 2013.

Van Den Boogaard, Jeroen. ‘Proportionality in International Humanitarian Law: Principle, Rule and Practice’. University of Amsterdam, 2019.

Ventre, Daniel. *Cyber Conflict: Competing National Perspectives*. Hoboken: John Wiley & Sons, 2013.

Yatsko, Andrzej. *Insight into Theoretical and Applied Informatics: Introduction to Information Technologies and Computer Science*. Introduction to Information Technologies and Computer Science. Berlin: De Gruyter Open, 2015.

Treaties and Statutes

‘Geneva Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field’, Geneva, 12 August 1949, 75 UNTS 31.

‘Protocol Additional (I) to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts’, Geneva, 8 June 1977, 1125 UNTS 3.

‘Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices as Amended on 3 May 1996’, 3 December 1998, 2048 UNTS 93.

‘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 (General Data Protection Regulation), 27 April 2016, O.J. L.119/1.

‘Statute of the International Court of Justice’, 26 June 1945, 59. Stat. 1055, 33 UNTS 933.

‘Vienna Convention on the Law of Treaties’, Vienna, 23 May 1969, 1155 UNTS 331.

Internet Sources

Center for Strategic & International Studies. ‘Significant Cyber Incidents since 2006’. Accessed 6 August 2023. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

European Commission. ‘What Is Personal Data?’ Accessed 8 August 2023. https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en.

Federal Department of Foreign Affairs FDFA. ‘Switzerland’s Position Paper on the Application of International Law in Cyberspace (Annex UN GGE 2019/2021)’. Accessed 2 August 2023. www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-20192021_EN.pdf.

German Federal Foreign Office. ‘On the Application of International Law in Cyberspace’. Accessed 8 August 2023. https://www.auswaertigesamt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf

Gisel, Laurent, and Tilman Rodenhäuser. ‘Cyber Operations and International Humanitarian Law: Five Key Points’. Humanitarian Law & Policy Blog. Accessed 10 August 2023. https://blogs.icrc.org/law-and-policy/2019/11/28/cyber-operations-ihl-five-key-points/.

Isaac, Mike, and Sheera Frenkel. ‘Facebook Security Breach Exposes Accounts of 50 Million Users’. *New York Times*, 28 September 2018. Accessed 15 August 2023. https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html.

Kranz, Garry. ‘Metadata’. In *TechTarget*. Accessed 15 August 2023. https://www.techtarget.com/whatis/definition/metadata.

Maroonian, Anaïs. ‘Proportionality in International Humanitarian Law: A Principle and a Rule’. Articles of War. Lieber Institute West Point, 2022. Accessed 24 October 2023. https://lieber.westpoint.edu/proportionality-international-humanitarian-law-principle-rule/.

Van Den Boogaad, Jeroen. ‘Reimagining IHL Principles Part I: The Wrong Principles’. Articles of War. Lieber Institute West Point, 2022. Accessed 24 October 2023. https://lieber.westpoint.edu/reimagining-ihl-principles-part-i-wrong-principles/.

International Case Law

International Court of Justice

ICJ. ‘Application of the International Convention on the Elimination of All Forms of Racial Discrimination (Qatar v. United Arab Emirates), Preliminary Objections, 2021, ICJ Rep 71.

ICJ. ‘Arbitral Award of 31 July 1989 (Guinea-Bissau v. Senegal)’, 1991, ICJ Rep 53.

ICJ. ‘Asylum (Colombia/Peru)’, 1950, ICJ Rep 266.

ICJ. ‘Certain Iranian Assets (Iran v. United States)’, Preliminary Objections, 2019, ICJ Rep 7.

ICJ. ‘Dispute regarding Navigational and Related Rights (Costa Rica v. Nicaragua)’, Judgment, 2009, ICJ Rep 213.

ICJ. ‘Land, Island and Maritime Frontier Dispute (El Salvador/Honduras: Nicaragua Intervening)’, 1992, ICJ Rep 351.

ICJ. ‘Legality of the Threat or Use of Nuclear Weapons’, Advisory Opinion, 1996, ICJ Rep 226.

ICJ. ‘Maritime Delimitation in the Indian Ocean (Somalia v. Kenya)’, Preliminary Objections, 2017, ICJ Rep 3.

ICJ. ‘North Sea Continental Shelf (Federal Republic of Germany/Denmark; Federal Republic of Germany/Netherlands)’, 1969, ICJ Rep 3.

ICJ, ‘Oil Platforms (Iran v. United States)’, Preliminary Objection, 1996, ICJ Rep 803.

ICJ. ‘Question of the Delimitation of the Continental Shelf between Nicaragua and Colombia beyond 200 Nautical Miles from the Nicaraguan Coast (Nicaragua v. Colombia)’, Preliminary Objections, 2016, ICJ Rep 100.

ICJ. ‘Questions relating to the Obligation to Prosecute or Extradite (Belgium v. Senegal)’, 2012, ICJ Rep 422.

ICJ. ‘Sovereignty over Pulau Ligitan and Pulau Sipadan (Indonesia/Malaysia)’, 2002, ICJ Rep 625.

ICJ. ‘Territorial Dispute (Libya/Chad)’, 1994, ICJ Rep 6.

International Criminal Tribunal for the Former Yugoslavia

ICTY. ‘Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction (Prosecutor v. Dusko Tadic a/k/a “Dule”)’, 1995, IT94-AR72.

Others

ECtHR. ‘Tyrer v. United Kingdom’ Judgement, 1978, 2 EHRR 1.

IACtHR. ‘The Right to Information on Consular Assistance in the Framework of the Guarantees of the Due Process of Law’ Advisory Opinion, 1999, no. 16.

UNHRC. ‘Roger Judge v. Canada’, 2003, UN Doc CCPR/C/78/D/829/1998.

UN Documents

UNGA. ‘Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States’, 2021, UN Doc A/76/136.

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

UNGA. ‘Report of the 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. ‘Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security (Addendum)’, 9 September 2013, UN Doc A/68/156/Add.1.

UNGA. ‘Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security’, 30 June 2014, UN Doc A/69/112.

UNGA. ‘Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security (Addendum)’, 18 September 2014, UN Doc A/69/ 112/Add1.

UNGA. ‘Report of the International Law Commission on the Work of its 63rd and 65th Sessions: Topical Summary of the Discussion Held in the 6th Committee of the General Assembly during its 68th Session, Prepared by the Secretariat’, 2014, UN Doc A/CN.4/666.

UN International Law Commission. ‘Draft Conclusions on Identification of Customary International Law, with Commentaries’, 2018, UN Doc A/73/10.

International Committee of the Red Cross

Dörmann, Knut. ‘Applicability of the Additional Protocols to Computer Network Attacks: An ICRC Viewpoint’. In *International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law*. Stockholm, Sweden, 2004. https://www.icrc.org/en/doc/assets/files/other/applicabilityofihltocna.pdf.

ICRC. ‘32nd International Conference of the Red Cross and Red Crescent, Geneva, 8–10 December 2015’. *International Review of the Red Cross* 97 (December 2015): 1379–1502. https://doi.org/10.1017/S1816383116000357.

ICRC. ‘International Humanitarian Law and Cyber Operations during Armed Conflicts: ICRC Position Paper (Submitted to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security)’. *International Review of the Red Cross*, Digital technologies and war, 102, no. 913 (November 2019): 481–92. https://doi.org/10.1017/S1816383120000478.

ICRC. ‘International Humanitarian Law and the Challenges of Contemporary Armed Conflicts’. Power of Humanity: 32nd International Conference of the Red Cross and Red Crescent. Geneva: ICRC, 31 October 2015. https://www.icrc.org/en/document/international-humanitarian-law-and-challenges-contemporary-armed-conflicts.

ICRC. ‘International Humanitarian Law and the Challenges of Contemporary Armed Conflicts: Recommitting to Protection in Armed Conflict on the 10th Anniversary of the Geneva Conventions’. ICRC, 2019. https://www.icrc.org/en/document/icrc-report-ihl-and-challenges-contemporary-armed-conflicts.

Dictionaries

Mbengue, Makane Moïse. 'Preamble'. In *Max Planck Encyclopedia of Public International Law*, edited by Anne Peters and Rüdiger Wolfrum, September 2008.

'Object, n'. In *The Oxford English Dictionary: Volume VII*, 1970.

Oxford English Dictionary. 'Datum, n.' In *Oxford English Dictionary*. Oxford University Press, 26 July 2023. Oxford English Dictionary. https://doi.org/10.1093/OED/7571592234.

Oxford English Dictionary. 'Violence, n.' In *Oxford English Dictionary*. Oxford University Press, 2 March 2023. https://doi.org/10.1093/OED/4998467199.