KIRIMLI DR. AZIZ BEY COLLECTED COURSES ON INTERNATIONAL HUMANITARIAN LAW – VOL. II

EDITORS
Onur Dur
Mustafa Can Sati
M. Emre Hayyar

KIZILAY
KÜLTÜR SANAT

Kırımlı Dr. Aziz Bey Collected Courses on International Humanitarian Law - Vol. II

Kızılay Culture and Arts Publications: 37

Academy Series: 4

Editors

Onur Dur

Mustafa Can Sati

M. Emre Hayyar

Publication Coordinator

Hafize Zehra Kavak

Production Coordinator

Fatma Sena Yasan

Graphic Design

Nevzat Onaran

ISBN 978-605-73204-7-6

September 2026 Ankara, first edition.

© Kızılay Culture and Arts Publications, 2026

The publication of the work, in accordance with the provisions of the Law on Intellectual and Artistic Works No. 5846, exclusively belongs to Kızılay Culture and Arts Publications, in agreement with the rights holders for their material and moral rights, both domestically and internationally, in Turkish and all other languages.

The digital version of the work can be freely accessed and read on the Turkish Red Crescent Academy website (https://kizilayakademi.org.tr/en/books/) without any additional permission required. It can also be freely downloaded to any digital platform without and shared on all digital platforms without any modification.

Kızılay Culture and Arts Publications publishes its works while remaining faithful to the author, conveying their views to readers when deemed necessary through prefaces, footnotes. It should not be assumed that the Publisher or the Turkish Red Crescent endorses matters in this book.

This publication is not for sale and may not be purchased. This book presents the lectures delivered during the 2023 edition of the Kırımlı Dr. Aziz Bey International Humanitarian Law Competition.

Kızılay Culture and Art Publications
is a registered trademark of the Turkish Red Crescent Association.

Publisher Certificate No.: 47652

Küçükbakkalköy Mah. Rüstemağa Sok.
INMAK Plaza No.2A Ataşehir-İstanbul

Telephone: (+90 212) 263 1868

Printing

Azim Matbaacılık Kağ San. Tic. Ltd. Şti.

Printing House Certificate No.: 47897

Büyük San. 1. Cad. Alibey İşh. 99/33 İskitler, 06030, Altındağ, Ankara, Türkiye

Telephone: (+90 312) 342 03 72

Library Cataloging-in-Publication Data

Kırımlı Dr. Aziz Bey Collected Courses on International Humanitarian Law - Vol.II / editors Onur Dur, Mustafa Can Sati, M. Emre Hayyar.

Istanbul : Kızılay Culture and Arts Publications, 2026.

120 pages ; 16,5 x 23,5 cm.

Kızılay Culture and Arts Publications ; 37. Academy series ; 4.

ISBN 978-605-73204-7-6

1. Law of nations – Enforced settlement of international disputes – Law of war and neutrality. Jus belli – Humanitarian law. 2. Law of nations – Enforced settlement of international disputes – Law of war and neutrality. Jus belli – cyber warfare. 3. Law of nations – Enforced settlement of international disputes – Law of war and neutrality. Jus belli – Protection of environment. 4. Law of nations – Enforced settlement of international disputes – Law of war and neutrality. Jus belli – Prohibition of terrorism.

I. Dur, Onur, 1993-. II. Sati, Mustafa Can, 1992-. III. Hayyar, M. Emre, 1995-.

KZ6440-6530 2023.

KIRIMLI DR. AZIZ BEY COLLECTED COURSES ON INTERNATIONAL HUMANITARIAN LAW – VOL. II

Onur Dur, Mustafa Can Sati, M. Emre Hayyar

KIZILAY
KÜLTÜR SANAT

Editors

Dr. Onur Dur

Onur Dur is an assistant professor of International Law at the Social Sciences University of Ankara. He completed his PhD degree at the University of Basel, with his thesis on "The Prohibition of Terrorism in International Humanitarian Law". He serves as the General Coordinator of the Istanbul Center for International Law (ICIL). Also, Dr. Dur is a co-founder of the Kırımlı Dr. Aziz Bey International Humanitarian Law Competition and Summer School. Onur holds a Master's degree in International Law from the Geneva Graduate Institute, where he was awarded the Wilsdorf Scholarship. He received his LLB degree from the University of Galatasaray. During his bachelor's studies, Onur participated in the Jean Pictet International Humanitarian Law Competition (Francophone edition-2016) and the René Cassin Human Rights Moot Court (2015).

Dr. Mustafa Can Sati

Dr. Mustafa Can Sati earned his PhD in International Law at Maastricht University, where he completed his doctoral thesis on "Military AI Technologies under International Humanitarian Law: Re-evaluation of Fundamental Principles". He serves as the Administrative Director and a member of the Executive Board of the Istanbul Center for International Law (ICIL) and is a co-founder of the Kırımlı Dr. Aziz Bey International Humanitarian Law Competition & Advanced Summer School. He holds an LL.M. in International and European Law from Ghent University. Previously, he worked as a research assistant in the Public International Law Department at Istanbul Kültür University from 2017 to 2019. He was also selected to participate in the 54th session of the International Law Seminar organised by the United Nations Office at Geneva and the International Law Commission.

M. Emre Hayyar

M. Emre Hayyar is a PhD Candidate in public international law at the University of the West of England, Bristol, United Kingdom. He has been a board member at the Istanbul Center for International Law since August 2017. Mr. Hayyar is a co-founder of the Kırımlı Dr. Aziz Bey International Humanitarian Law Competition and Summer School. Emre holds an LL.M. in Public Law from Istanbul Medipol University (Summa Cum Laude, 2022), an LL.M. in International and European Law from Ghent University (Cum Laude, 2021), and an LL.B. from Istanbul University (2018). He worked as a research assistant in public international law at Istanbul Medipol University between February 2019 and January 2023.

Contents

About The Kırımlı Dr. Aziz Bey IHL Competition 6

Chapter I: 'Testing' the Legality of Autonomous Weapons Systems and AI-based Decision Support Systems under International Humanitarian Law/ Daniele Amoroso 11

1. Introduction 11
2. The First Prong of the Test: Distinction 15
3. The Second Prong of the Test: Proportionality 27

Bibliography 48

Chapter II: International Humanitarian Law and the Regulation of Warfare in the Cyber Domain/ Eitan Diamond 53

1. Introduction 53
2. Adapting Old Law to New Cyber Technologies 56
3. Applying IHL to Technologies and Operations Veiled in Secrecy 59
4. Assessing whether Cyber Operations Occurred in the Context of Armed Conflict 61
5. Environmental Instruments 66
6. Conclusion 76

Bibliography 77

Chapter III: Terrorism and International Humanitarian Law/ Onur Dur 79

1. Historic Evolution of the Prohibition of Terrorism in Armed Conflict until the Geneva Conventions of 1949 79
2. IHL Rules Prohibiting Terrorism 85
3. Relationship between Counter-Terrorism Law and International Humanitarian Law . . . 92
4. Conclusion 94

Bibliography 96

Chapter IV: An Overview of the International Law Commission's Principles on the Protection of the Environment in Relation to Armed Conflict/ Nilüfer Oral 99

1. Introduction 99
2. Protection of Environment in Armed Conflict 100
3. Armed Conflict and the Environment at the UN 102
4. International Legal Framework 102
5. Environmental Instruments 106
6. The International Law Commission 110
7. Conclusion 116

Bibliography 118

About The Kırımlı Dr. Aziz Bey IHL Competition

Kırımlı (Crimean) Dr. Aziz Bey

The co-organizers of the Kırımlı Dr. Aziz Bey IHL Competition named the project in honor of Kırımlı Dr. Aziz Bey, acknowledging his influence on the establishment of the humanitarian tradition in 19th century Türkiye.

Kırımlı (Crimean) Dr. Aziz Bey, a renowned medical doctor born in Istanbul in 1840, holds a significant place in the history of Turkish medicine and the advancement of humanitarian efforts in the Ottoman Empire, despite his untimely demise. Collaborating with his colleague Abdullah Bey, Dr. Aziz Bey dedicated his efforts to championing humanitarian ideals, including the moral responsibility of every physician to safeguard human well-being and attend to injured soldiers. Notably, he played a pivotal role in establishing the Association to Help and Rescue the Sick and Wounded Soldiers, which later evolved into the "Hilal-i Ahmer Cemiyeti" (The Red Crescent Society; known today as the Turkish Red Crescent).

Moreover, Aziz Bey took a leading role in founding the Hilal-i Ahmer Cemiyeti within the Ottoman Empire. By designing the emblem of the red crescent and facilitating the transition from the red cross emblem, he paved the way for the establishment of the country's first national red crescent society. Throughout his life, he remained actively engaged in the activities of Hilal-i Ahmer Cemiyeti, serving as both president and delegate until his passing in 1878.

Aziz Bey's contributions extended beyond humanitarian work. He gained recognition as the founder of the first modern medical school that offered education in Turkish. Additionally, he authored the first medical book written in Turkish and acted as the translator for the first medical dictionary in the Ottoman Empire. The enduring legacy of Kırımlı Dr. Aziz Bey lies in his role as one of the foremost pioneers of humanitarian principles and activities in Türkiye.

The IHL Competition

The Kırımlı Dr. Aziz Bey IHL Competition combines advanced IHL lectures with role-playing exercises based on the preceding IHL lectures. The co-organizers carefully select the main topics, with each edition revolving around an overarching theme such as naval warfare, aerial warfare, law of occupation, and IHL principles.

The Kırımlı Dr. Aziz Bey IHL Competition has achieved several noteworthy milestones. It stands as one of the pioneering IHL Competitions ever organized online. Additionally, it holds the distinction of being the first IHL competition to take place in Türkiye. Notably, Aziz Bey sets itself apart as a unique law competition where the delivered lectures align with the scope of the competition. Consequently, the pedagogic approach of the Aziz Bey Competition offers an unparalleled learning opportunity to Turkish and foreign law students.

The Kırımlı Dr. Aziz Bey IHL Competition represents a significant initiative aimed at promoting IHL in Türkiye. The co-organizers actively encourage the participation of Turkish universities and foster dialogue between Turkish and international IHL scholars.

About The Book

The third edition of the Kırımlı Dr. Aziz Bey International Humanitarian Law (IHL) advanced summer school mainly focused on the challenges posed by cyber warfare in armed conflicts. The lectures given during the advanced summer school were transformed into book chapters featured in this volume. Currently, widespread cyber attacks against civilian infrastructures under the veil of anonymity are one of the greatest challenges for International Humanitarian Law.

In the first chapter, Dr. Daniele Amoroso analyses the legality of autonomous weapons systems and AI-based decision support systems under International Humanitarian Law. Dr. Amoroso explains that this modern technology, encompassing artificial intelligence, poses substantial risks for the fundamental principles of IHL such as distinction, proportionality, and precaution. In his comprehensive and critical assessment, Dr. Amoroso unpacks the necessity of a more nuanced approach vis-à-vis the military applications of AI.

In the second chapter, Dr. Eitan Diamond tackles the challenges of cyber-warfare for the rules of IHL. Blurred lines between states and non-state actors further complicate such challenges for the fundamental principles of IHL. Dr. Diamond highlights that the secrecy surrounding cyber operations presents substantial risk for civilians and civilian infrastructure, and further discussion is much needed for the interpretation and adaptation of the established IHL norms applicable in cyberwarfare.

In the third chapter, Dr. Onur Dur explains that terrorization of civilians is a direct attack against the core IHL principles, especially the principle of distinction. Although such a strategy has been condemned by states for a long time, the implications are still present in current armed conflicts. Dr. Dur warns that states deliberately conflate the prohibition of terrorism under IHL with the prohibition of terrorism under Counter-terrorism Law in order to divert attention from the massive civilian casualties into grey zones.

In the last chapter, Dr. Nilüfer Oral enunciates the environmental challenges of armed conflicts. As military technology advances, the concomitant risk for the protection of the environment during armed conflicts also grows. The UN and its specialised bodies and institutions supplemented the legal base established by the Geneva Conventions of 1949 and its additional protocols of 1977 to counter such environmental concerns during armed conflicts. Finally, the International Law Commission of the UN brought a widely appreciated contribution to the development of IHL rules on the protection of the environment with its report entitled "Draft Principles on Protection of the Environment in Relation to Armed Conflicts".

Chapter I: 'Testing' the Legality of Autonomous Weapons Systems and AI-based Decision Support Systems under International Humanitarian Law

Daniele Amoroso[1]

Abstract

Autonomous weapons systems (AWS) and AI-based decision support systems (DSS) have been the subject of intense debates within the realms of international law and normative ethics. The increasing deployment of these technologies in the conflicts in Ukraine and Gaza underscores the immediacy and relevance of this discussion. Against this backdrop, the present Chapter aims to take a fresh look at the question of the legality of the use of such systems under international humanitarian law (IHL). This analysis will be carried out through the lens of Art 36 of the First Additional Protocol to the Geneva Conventions, mandating the legal review of new means and methods of warfare. Central to this analysis will be whether AWS and DSS, in their intended uses, align with the principles of distinction, proportionality, and precaution under IHL.

1. Introduction

Over the past years, the debate on the legality of autonomous weapons systems and, more generally, of the use of AI for targeting purposes has grown relentlessly, turning out to be a veritable goldmine for scholars of international law and normative ethics, including –to be fair– the present author. Until recently, such doctrinal hype might have been perceived as somewhat excessive or premature, given that these technologies were either very rudimentary or not yet ready for actual battlefield use. The (alleged) increasing use of AI-based decision support systems and

1 Associate Professor of International and European Law at the University of Cagliari.

autonomous weapons systems in the conflicts in Ukraine[2] and Gaza[3] has reaffirmed the topicality of the issue, to the point that one world-renowned expert in the field has warned of the 'Perilous Coming Age of AI Warfare'.[4]

Against this backdrop, the time seems ripe for a fresh look at whether, and under what conditions, resort to these technologies in armed conflicts is consistent with international humanitarian law (IHL). Before delving into this analysis, a few preliminary remarks are in order.

First, it is important to clarify what is meant by autonomous weapons systems (AWS) and AI-based decision support systems (DSS). Without claiming to take a definitive stance on this point, I will limit myself to providing the working definitions of both types of systems. On the one hand, I will follow the definition of AWS set out by the International Committee of the Red Cross (ICRC), whereby AWS are weapons systems 'that can select (i.e. search for or detect, identify, track, select) and attack (i.e. use force against, neutralize, damage or destroy) targets without human intervention'. [5] DSS, on the other hand, are here understood as systems that rely on AI technologies to support the targeting process by recommending potential targets and courses of action to human operators.[6] The crucial difference between the two, therefore, lies in the fact that, in the case of DSS, the final decision rests in the hands of human operators, while in the case of AWS the decision to engage is autonomously taken by the machine. This distinction,

2 David Hambling, 'Ukrainian AI Attack Drones may be Killing without Human Oversight' (*New-Scientist,* 31 October 2023) <https://www.newscientist.com/article/2397389-ukrainian-ai-attack-drones-may-be-killing-without-human-oversight/> accessed 23 April 2024.

3 Yuval Abraham, "Lavender': The AI Machine Directing Israel's Bombing Spree in Gaza' (+972 Magazine, 3 April 2024) <https://www.972mag.com/lavender-ai-israeli-army-gaza/> accessed 23 April 2024.

4 Paul Scharre, 'The Perilous Coming Age of AI Warfare. How to Limit the Threat of Autonomous Weapons' (*Foreign Affairs*, 29 February 2024) <https://www.foreignaffairs.com/ukraine/perilous-coming-age-ai-warfare> accessed 23 April 2024.

5 International Committee of the Red Cross, 'Views of the International Committee of the Red Cross (ICRC) on Autonomous Weapon System' (Convention on Certain Conventional Weapons (CCW) Informal Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS), Geneva, 11–15 April 2016) <https://www.icrc.org/en/document/views-icrc-autonomous-weapon-system> accessed 23 April 2024.

6 Ruben Stewart and Georgia Hinds, 'Algorithms of war: The Use of Artificial Intelligence in Decision Making in Armed Conflict' (*Humanitarian Law & Policy,* 24 October 2023) <https://blogs.icrc.org/law-and-policy/2023/10/24/algorithms-of-war-use-of-artificial-intelligence-decision-making-armed-conflict/> accessed 23 April 2024.

however, may become less clear-cut in practice in all cases where the human operator is not in a position (e.g. because of time constraints) to question the machine's judgement.

Second, the ensuing analysis will be conducted through the lens of the obligation to review the legality of new weapons, means and methods of warfare, as laid down by Article 36 of the First Additional Protocol to the Geneva Conventions (hereinafter First Additional Protocol or AP I),[7] whereby.

> In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.

While it is undisputed that AWS should be subject to such a legality test prior to use, this is not necessarily the case for DSS, which are not weapons per se. One might argue, however, that the integration of AI technologies into the targeting process via DSS could be characterized as a new method of combat, thus subject to legal review as well.[8]

Third, and finally, the assessment of the legality of these new technologies of warfare should take into account the 'conceptual challenge' posed by the performance of the critical function of target identification by an artificial agent.[9] In particular, legal reviews cannot be limited to verifying whether the use of AWS or AI-based DSS is prohibited by IHL or whether their technical characteristics allow humans to behave in compliance with IHL, but should rather aim at establishing whether the system itself is capable of acting lawfully when making 'determinations in the targeting cycle which traditionally are being taken care of by a human operator'.[10] In other words, what is at stake

7 *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts* (AP I) 1977.

8 On this issue, see International Committee of the Red Cross, 'Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach' (2020) 102 (913) *International Review of the Red Cross* 463; Klaudia Klonowska, 'Article 36: Review of AI decision-support systems and other emerging technologies of warfare' [2022] 23 (2020) *Yearbook of International Humanitarian Law* 123.

9 Switzerland, 'Towards a "Compliance-Based" Approach to LAWS' (CCW Informal Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS), Geneva, 30 March 2016) para 23.

10 *Ibid.*

is the system's ability to operate in accordance with the norms of IHL governing the targeting process (the so-called 'law of targeting').[11]

On these assumptions, the Chapter will be structured around the basic tenets of the law of targeting: distinction, proportionality, and precaution. Notably, it will subject AWS and DSS to a threefold legality test:

- Are AWS and DSS, in their normal or intended circumstances of use, capable of complying with the applicable distinction obligations?
- Are AWS and DSS, in their normal or intended circumstances of use, capable of making the proportionality assessments required by IHL?
- Do AWS and DSS, in their normal or intended circumstances of use, hinder compliance with the obligation to take every feasible precaution to avoid (or minimize) civilian harm?

Needless to say, the test will not be carried out in relation to a specific system, as it should be, but in an abstract manner, by making a legal assessment of the current state of the art and research trends in the field.

As it will be seen, each question poses a specific challenge. In particular, section 2 will show that fulfilling the distinction obligations involves a number of complex tasks that, in most scenarios, cannot be performed autonomously by AWS and DSS, unless they are provided with the capability to acquire situation awareness. Section 3 will investigate whether and how the thrust of the principle of proportionality, i.e. the obligation to strike a reasonable balance between heterogeneous values (collateral damage and military advantage), can actually be translated into a machine algorithm. Section 4 will show that the positive obligation to take precautionary measures under IHL imposes important constraints on how States should conceive of the distribution of control privileges between humans and machines. Section 5 will wrap up the discussion and make some concluding observations as to whether, to what extent, and under what conditions AWS and DSS can pass the (theoretical) legality test set out in this Chapter.

11 This requirement could be somehow based on Art 51(4)(b) and (c) AP I, which respectively prohibit the use of methods or means of combat which "cannot be directed at a specific military objective" and "cannot be limited as required by th[e] Protocol". On such a conflation between targeting law and weapons law (rectius: means and methods of warfare law). See also Natalia Jevglevskaja, *International Law and Weapons Review. Emerging Military Technology under the Law of Armed Conflict* (CUP 2021) 207–238.

2. The First Prong of the Test: Distinction

A key acquisition of modern international law is that, during armed conflicts, certain persons and objects must be protected from direct attacks. Accordingly, weapons that 'are incapable of distinguishing' between legitimate targets and protected persons/objects should be viewed as 'indiscriminate' and thus forbidden.[12] As far as conventional weapons are concerned, this requirement is understood as prohibiting the use of weapons that do not allow the human user to make such distinctions, on the assumption that a weapon, 'being an inanimate object', cannot perform an activity that implies 'thought'.[13] This could no longer be valid for AWS and DSS, whose defining feature is precisely that of carrying out the critical function identifying targets on their own.[14] Regardless of whether this activity actually requires 'thought', as it has been suggested, the fact remains that the legality of AWS and DSS passes, in the first place, through an assessment of their ability to direct themselves against legitimate targets.

Although its 'seeds' might be traced back to the 1868 Saint Petersburg Declaration,[15] the principle of distinction was expressly formulated only in 1977 with the adoption of the First Additional Protocol to the Geneva Conventions, whose Article 48 (Basic Rule) posits:

> In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.[16]

---

12 *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion [1996] ICJ Reports 226, para 78. See also Art 51(4) AP I.

13 Louise Doswald-Beck, 'International Humanitarian Law and the Advisory Opinion of the International Court of Justice on the Legality of the Threat or Use of Nuclear Weapons' [1997] 316 *International Review of the Red Cross* 35, 39.

14 Kjølv Egeland, 'Lethal Autonomous Weapon Systems under International Humanitarian Law' [2016] 85 *Nordic Journal of International Law* 89, 97.

15 Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight. Saint Petersburg, 29 November/11 December 1868. See, in particular, the statement whereby the "only legitimate object which States should endeavor to accomplish during war is to weaken the military forces of the enemy" and that for this "purpose it is sufficient to disable the greatest possible number of men".

16 *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts* (AP I) 1977.

The same rule is reiterated by Articles 51(2) and 52(1) AP I, which dealing with, respectively, the 'protection of civilian population' and the 'general protection of civilian objects'. The picture is further enriched by a number of protective rules which, while not aimed at immunizing the civilian population from direct attacks, raise analogous issues of distinction. The most important of these is the norm prohibiting attacks on persons hors de combat, namely –according to the definition of Art 41(2) AP I– those enemies who clearly expresses an intention to surrender; or are defenceless because of unconsciousness, shipwreck, wounds or sickness; provided that they abstain from any hostile act and do not attempt to escape.

2.1. Unresolved Issues: Direct Participation in Hostilities and 'Dual-Use' Objects

At a first sight, the prescriptive content of the principle of distinction seems crystal-clear: do not attack civilians and civilian objects or, to put it the other way around, do attack only combatants and military objectives.

Contemporary IHL, however, features the persistence of a number of grey areas, especially in relation to asymmetric warfare, where hostilities are generally conducted in urban settings and armed actors are closely intermingled with civilians, who do not always abstain from participating in hostilities. The latter problem is addressed in very general terms by Article 51(3) AP I, which suspends civilians' immunity from attacks 'for such time as they take a direct part in hostilities', but fails to offer proper directions as to what counts as 'direct participation in hostilities'.

In an attempt to shed light on this question, in 2009 the ICRC issued an *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law,* authored by the then ICRC's Legal Adviser Nils Melzer.[17] The ICRC identified three cumulative criteria to establish whether an act is one of 'direct participation in hostilities':

- The act must reach a 'threshold of harm', namely it must be likely to adversely affect the military operations or capacity of

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

a belligerent party or, alternatively, to harm persons or objects protected against direct attack, and

- There must be a direct causal link between the act and the harm likely to result either from that act, or from a coordinated military operation of which that act constitutes an integral part, and
- The act must be specifically designed to directly cause the required threshold of harm in support of a party to the conflict and to the detriment of another (belligerent nexus)[18]

The same criteria are employed by the ICRC also to identify members of irregular armed forces, who are those carrying out acts of direct participation in a continuous manner (so-called 'continuous combat function' criterion).[19]

To be clear, these criteria have not yet been universally accepted.[20] In the ensuing analysis, however, the authoritative view of the ICRC will be taken as a reference, with the caveat that, even if one adopted the more liberal approaches proposed by the critics of the Interpretive Guidance, this would not significantly diminish the perceptual and evaluative challenges posed to AWS and DSS by the notion of direct participation in hostilities.

Another tricky issue in IHL is posed by objects sometimes labelled as 'dual-use', namely those civilian objects that, similarly to civilians taking part to hostilities, lose their immunity from attacks because, by their use or purpose (i.e. by their actual or intended use), they make an effective contribution to the military action of the enemy.[21] The construction of the 'purpose' and 'use' criteria is indeed featured by a number of grey areas as well. This is illustrated by an oft-cited example: television and radio broadcasting stations, like the Radio Television of Serbia, whose

18 *Ibid.*

19 Nils Melzer, 'Keeping the Balance between Military Necessity and Humanity: A Response to Four Critiques of The ICRC's Interpretive Guidance on the Notion of Direct Participation in Hostilities' [2010] 42 *New York Journal of International Law & Policy* 831, 854.

20 See, for instance, the critical remarks by Kenneth Watkin, 'Opportunity Lost: Organized Armed Groups and the ICRC "Direct Participation in Hostilities" Interpretive Guidance' [2010] 42 *New York Journal of International Law & Policy* 641; Michael Schmitt, 'Deconstructing direct participation in hostilities: The constitutive elements' [2010] 42 *New York Journal of International Law & Policy* 697; William H Boothby, "'And for Such Time As": the Time Dimension to Direct Participation in Hostilities' [2010] 42 *New York Journal of International Law & Policy* 741.

21 Christine Byron, 'International Humanitarian Law and Bombing Campaigns: Legitimate Military Objectives and Excessive Collateral Damage' [2011] 13 (2010) *Yearbook of International Humanitarian Law* 175, 183–188.

headquarters in Belgrade were bombed in 1999 by NATO forces. While it is unlawful to target them only to halt the enemy's propaganda machine (because that would constitute a too remote military advantage), television and broadcasting stations constitute legitimate targets when they are part of the Command, Control and Communications network of the enemy's army, as it was arguably the case of the Radio Television of Serbia.[22]

2.2. The Problem of Situation Awareness

The foregoing provides us with an adequately representative sample of identification tasks that AWS and DSS should be legally required to perform with a view to complying with distinction obligations under IHL. To describe in a synthetic fashion what it takes to properly perform these tasks in a warfare scenario, it is sometimes used a notion borrowed from ergonomics (but more and more resorted to in military studies): that of situation awareness (SA), i.e. the knowledge of 'the state of a dynamic environment'.[23] The performance of these activities, in other terms, requires not only that the pertinent rules of international law are properly coded into algorithms, but also –and even more importantly– that these systems are endowed with the capability to autonomously 'assess' the surrounding environment.[24]

A helpful model to approach this problem was set out by Mica Endsley, former Chief Scientist of the US Air Force, who dissected it into three interrelated and hierarchically structured components: 'Perception of the elements in the environment' (Level 1), 'Comprehension of the current situation' (Level 2), 'Projection of future status' (Level 3).[25] The usefulness of this model will be apparent if we consider the case of the identification of a surrendering combatant. In order to comply with the

22 This point was clearly made by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia, *Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign against the Federal Republic of Yugoslavia* (2000) paras 47, 55 and 77 (OTP Report).

23 MR Endsley, 'Toward a Theory of Situation Awareness in Dynamic Systems' (1995) 37(1) *Human Factors* 32, 36.

24 Lucy Suchman, 'Situational Awareness and Adherence to the Principle of Distinction as a Necessary Condition for Lawful Autonomy.' (Briefing paper, (CCW Informal Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS), Geneva, 12 April 2016).

25 Endsley (n 22) 36.

prohibition of attacking persons hors de combat, an AWS (or a DSS) should be able to perform the following sub-tasks (*a*) to recognize a certain object as a human combatant and to discern his/her gestures (perception of the elements of the environment, both in their static and dynamic dimensions); (*b*) to infer from his/her appearance and gesture, as well as from the context, that (s)he is conveying a message of surrender (comprehension of the current situation); (*c*) to predict, on the basis of the combatant's behavior, whether (s)he does or does not intend to re-engage in hostile acts or attempt to escape (projection of a future status).

2.2.1. Perception of Elements in the Environment (Level 1 SA)

A *sine qua non* condition for situation awareness is the perception 'of the status, attributes, and dynamics of relevant elements in the environment'.[26] Battlefield scenarios may consist of a myriad of elements, but of course not all of them need to be perceived by the decision-maker, be it a human or a machine. For our purposes, therefore, it is sufficient that the system is able to recognize the elements whose perception, misperception, or non-perception could affect the lawfulness of a targeting decisions. How demanding this will be for a system depends on several variables. In this respect, one may distinguish between tractable recognition tasks and perceptual challenges that are still unmatched by current AI research.

A distinction task that is typically tractable by existing technologies is the recognition of so-called 'cooperative' objects. Cooperative objects 'are those that are actively emitting a signal, which makes them easier to detect'.[27] A classic example is the radar that allows enemy forces to find its position by emitting electromagnetic pulses, which are discernible by passive sensors (i.e. sensors that only receive information from the surrounding environment). The autonomy of the Israeli Harpy NG anti-radiation munitions is based on this relatively simple technology that, however, does not allow the weapon to establish whether the source of radio emission is located in the proximity of a protected object (e.g. a school).[28] Quite interestingly, there are some norms of IHL

26 *Ibid.*

27 Paul Scharre, *Army of None. Autonomous Weapons and the Future of War* (WW Norton & Company 2018) 84.

28 NE Sharkey, 'The Evitability of Autonomous Robot Warfare' (2012) 94 (886) *International Review of the Red Cross* 787, 788.

that promote 'cooperation' from protected objects in order to prevent them from being targeted. Annex I to AP I, in particular, contains very detailed provisions regulating the emission of specific light, radio, and electronic signals by medical aircrafts, vessels, and vehicles with a view to making them easily detectable by the Parties to the conflict.[29]

Yet, theatres of war are often populated by 'non-cooperative' objects, be them targetable (e.g. a tank) or protected from attacks (e.g. a school bus), which do not send out signals that may be detected by passive sensors. In this case, the system should be able to 'sense' the operational area; to 'discern' the objects of interest from the surrounding environment; and to 'recognize' the objects, by associating each of them to a certain class (e.g. tanks, non-military vehicles, combatants). Some norms of IHL are in fact aimed at assisting this activity, insofar as they require the display of easily discernible distinctive signs in order to flag that a certain object is not a lawful target. One could think, in this respect, to the provisions governing the use of the emblem of the red cross (and the like) for medical service,[30] the blue shield for cultural property,[31] and the three bright orange circles signaling 'works and installations containing dangerous forces'.[32] The same goes for the combatants' obligation 'to distinguish themselves from the civilian population [e.g. by wearing uniforms] while they are engaged in an attack or in a military operation preparatory to an attack'.[33] In these cases, object perception would boil down to the relatively affordable task of identifying the distinctive signs.

The identification of fast-approaching incoming threats, such as missiles, rockets or aircrafts, is not particularly demanding as well, as it is generally carried out in the light of two simple criteria: speed and trajectory. These are detected with an acceptable degree of reliability by air defense systems.[34] More complex, but still achievable, is the autonomous

29 Annex I to AP I: Regulations concerning identification [1977], Arts 6–8, 10–11.

30 ICRC, 'Emblem: Relevant Articles of the 1949 Geneva Conventions and their Additional Protocols' (1 November 2008) <www.icrc.org/eng/resources/documents/misc/emblem-ihl-011108.htm> accessed 23 April 2024.

31 *Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict* 1954, Arts 16 and 17.

32 Art 56(7) AP I.

33 Art 44(3) AP I.

34 Vincent Boulanin and Maaike Verbruggen, *Mapping the Development of Autonomy in Weapon Systems* (SIPRI 2017) 37–39.

qualification of objects as military objectives *by their nature,* such as tanks, navy ships, helicopters.[35] The UK Brimstone fire-and-forget munition, for instance, is reportedly able to sense and discern the objects in a given operational environment through a high-millimetric band seeker, which provides a high-resolution radar return image of them. These images are evaluated by the system's target recognition algorithms, through a comparison with the templates stored in the target identification library, in order to recognize armored vehicles and distinguish them from other fixed or moving objects, such as houses or cars.[36]

Let us now consider the hard cases. The evaluation as to whether a civilian is directly taking part in hostilities presupposes, at the very least, not only that an object is recognized as a human being, but also the discernment of all the tools (s)he is interacting with (e.g. a rifle), the kind, features and addressees of the actions (s)he is performing (e.g. shooting against friendly forces), as well as the contextual elements that could offer an alternative explanation to his/her behavior (e.g. the need to react to unlawful acts of violence). Likewise, an assessment aimed at qualifying an object as a military objective by its use or purpose entails the ability to perceive a plurality of objects and dynamics thereof (e.g. in the case of a school used as a deposit of ammunitions: a building, a group of enemy combatants transporting munitions into it, trucks parked outside the school, and so on). More in general, counterinsurgency operations in urban settings, where the close intermingling between legitimate targets and protected persons/objects exponentially raises the range of elements to be 'perceived' (i.e. civilians, combatants, military and non-military vehicles, weapons, protected objects, and all the dynamics thereof), make it particularly demanding for an artificial agent to autonomously acquire even the lowest level of situation awareness.

That notwithstanding, recent progresses in the field of deep learning are such that one cannot rule out that a system provided with a sophisticated learning architecture could be trained to discern and recognize all the objects in the surrounding environment, by feeding it with hundreds of thousands of footages showing the operational environments and the

35 Alan Backstrom and Ian Henderson, 'New Capabilities in Warfare: An Overview of Contemporary Technological Developments and the Associated Legal and Engineering Issues in Article 36 Weapons Reviews' (2012) 94(886) *International Review of the Red Cross* 483, 496.

36 Boulanin and Verbruggen (n 33), 49–50.

objects it can find within it (insurgents, military vehicles, civilian cars, kids, and so for).[37] This would be, however, only the bottom rung of the 'situation awareness' ladder. Things become even trickier for AWS when we pass to consider the upper levels.

2.2.2. Comprehension of the Current Situation (Level 2 SA) and Projection of Future Status (Level 3 SA)

Visual recognition would only provide the system with a disjointed knowledge of the objects present in the battlefield, which could prove a very poor basis for taking a lawful target decision. Let us consider the following scenario:

Insurgents (without uniforms) are firing against friendly forces a battery of mortars, located in the middle of an urban street. Mortars' munitions are stored in a nearby school and are transported to the fire position by a civilian truck at regular intervals. In the meanwhile, a bus has approached the area in order to evacuate civilian buildings on the street where armed confrontation is taking place.

Even if endowed with technology granting a high level of accuracy in object recognition, a system would simply identify a disaggregated picture composed of friendly forces, a battery of mortars, a moving truck, a number of buildings (including the school), a bus, and people without uniforms scattered around the area of operations. That could be enough to qualify the mortars as military objectives by nature and friendly forces as protected from attack, but it would say nothing as to the legal status of the other objects, thus preventing the system from conducting a proper distinction analysis. To have a more complete picture as to what is a lawful target and what is not, indeed, analytical perception of the environment should be complemented by an activity of synthesis, aimed at comprehending the dynamics of the elements and predicting future statuses thereof. Only this activity would allow the system to characterize the school and the truck as military objectives objects which, by their use, 'make an effective contribution to military action'; the driver of the truck as taking direct part to the hostilities; and the bus and the other buildings as objects protected from direct attacks.

37 This seems to be the main goal pursued by the US DoD Project Maven. See Julia Press, 'Inside Project Maven, the US Military's Mysterious AI Project' (*Bloomberg*, 29 February 2024) < https://www.bloomberg.com/news/articles/2024-02-28/inside-project-maven-the-us-military-s-flagship-ai-project-big-take-podcast?embedded-checkout=true> accessed 23 April 2024.

Enabling AWS to acquire these levels of situation awareness appears to be a challenge far more demanding than that posed by object perception.[38] In this connection, one may observe that human warfighters generally follow two ways to reach full situation awareness: feature-matching and story-generation. Feature-matching consists in comparing the available data with mental models built on the basis of training and past experience. When no match with existing models is found, the decision-maker generates a causal story in order to give meaning to the cues coming from the environment and to forecast future events.[39]

No doubt, feature-matching could be technically implemented into AWS to enhance their situation assessment capabilities. Notably, a number of templates, or 'signatures', could indeed be loaded into the system's long-term memory with a view to guiding the assessment as to whether a civilian is directly participating in hostilities, an object is a legitimate military objective by reason of its use or purpose, or a pattern of behavior conveys an intention of surrender.[40] It is of the utmost importance, however, that these templates accurately reflect IHL and do not allow leeway for dangerous generalizations. The US practice on signature strikes is a stark reminder of the risk that the adoption of loose targeting criteria (e.g. all males of military-age located in the area of enemy's activities) sets in fact the conditions for indiscriminate attacks against the civilian population.[41] This risk has been confirmed in the recent conflict in Gaza, where Israel Defense Forces reportedly relied on an AI-based DSS ('Lavender') to identify low and medium rank members of the military wings of Hamas. According to some sources, Lavender was trained to establish the likelihood that a Gaza resident was a militant based on a number of pretty controversial signatures, 'such as being in a Whatsapp group with a known militant, changing cell phone every few months, and changing addresses frequently'.[42]

38 David Akerson, 'The Illegality of Offensive Lethal Autonomy', in Dan Saxon (ed.), *International Humanitarian Law and the Changing Technology of War* (Martinus Nijhoff Publishers, 2013) 65, 76–82.

39 George L Kaempf, Steve Wolf and Thomas E Miller, 'Decision Making in the AEGIS Combat Information Center' [1993] 37 *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 1107, 1109.

40 The South Korean sentry robot SGR-A1, now retired, was reported to be able to recognize surrender motions (ie arms held high). See Boulanin and Verbruggen (n 33) 45.

41 Kevin Jon Heller, "One Hell of a Killing Machine': Signature Strikes and International Law' [2013] 11(1) *Journal of International Criminal Justice* 89.

42 Abraham (n 2).

In any case, one cannot take it for granted that the entire range of possible dynamics of unstructured warfare environments can be successfully pre-set into templates to be installed into AWS. In cases not covered by the templates, full situation awareness should therefore be achieved through story-generation (or 'abductive reasoning'), namely by piecing together incomplete information and make 'best guess' decisions. Yet, approaching human-like performances in this field is, unlike object recognition, an enduring problem that machine learning techniques has so far failed to address in an adequate manner.[43]

The foregoing suggests that it cannot be expected, at least in the near future, that AWS and DSS will be endowed with the ability to acquire the levels of situation awareness needed to comply with the principle of distinction in complex battlefield scenarios. This is not to mean, however, that this technological development can never be achieved, as it is sometimes suggested. For all we know, lack of situation awareness is a contingent situation that may no longer hold at some future time.

2.3. Is Situation Awareness Really Needed?

In the debate on the legal implications of autonomy in weapons systems, the need to enable AWS to achieve an adequate level of situation awareness has sometimes been downplayed (if not denied altogether). In general, two arguments have been generally put forward. First, it is submitted that issues of distinction are dealt with by human commanders at the planning stage of the targeting process. Second, it is argued that problems of distinction do not necessarily arise in every battlespace.[44]

The *first objection* is specific to AWS, as DSS are designed to always leave the final decision to engage the recommended target to a human operator.[45]

43 Hossein Chegini, 'Unraveling Abductive Reasoning: Chatgpt's Struggles and Limitations Exposed' (Medium, May 2023) <https://medium.com/coding-intelligence-ai-development-and-analysis/unraveling-abductive-reasoning-chatgpts-struggles-and-limitations-exposed-27fd4da6c60b> accessed 23 April 2024.

44 Michael N Schmitt and Jeffrey S Thurnher, "'Out of the Loop": Autonomous Weapon Systems and the Law of Armed Conflict' [2013] 4(2) *Harvard National Security Journal* 231.

45 Another issue is whether the human operator is put in a position to *meaningfully* intervene in the decision-making process, or merely rubber-stamps the recommendation of the DSS (Daniele Amoroso and Guglielmo Tamburrini, 'Toward a Normative Model of Meaningful Human Control over Weapons Systems' [2021] 35(2) *Ethics & International Affairs* 245). The latter scenario is exemplified by the use of the Lavender system by the Israel Defense Forces. It has indeed been reported that human operators limited themselves to checking whether the proposed target was a man or a woman, since women cannot be part of the Hamas military wing. See Abraham (n 2).

It is based on the assumption that it is at the planning stage that the legal assessment is made as to whether a particular object (e.g. a bridge) constitutes a military objective under IHL. From this perspective, AWS will therefore limit themselves to merely executing targeting decisions assumed by humans in the so-called 'wider loop'.[46]

Indeed, the fact that human decision-makers will always (or at least for a very long time) have a prominent role in planning an attack may be relevant in relation to *deliberate* targeting, which prosecutes targets that are 'known to exist in an area of operations and can be mapped to decisive points on line(s) of operation',[47] but it is largely unhelpful with regard to *dynamic* targeting, which prosecutes targets of opportunity such as unplanned targets (i.e. military objectives which were known to exist, but whose location and/or importance is grasped only after the attack was initiated) and unanticipated targets (i.e. military objectives which were unknown to exist at the planning stage).[48]

Moreover, exclusive reliance on the planning phase seems to overlook that the obligation to 'distinguish between the civilian population and combatants and between civilian objects and military objectives' should be complied with 'at all times',[49] not only at the time when an attack is planned. This aspect is reiterated and expounded on by Article 57 AP I, which obliges the warring parties to take 'constant care […] to spare the civilian population, civilians and civilian objects' and, more in detail, to cancel or suspend an attack 'if it becomes apparent that the objective is not a military one or is subject to special protection'. The latter obligation is imposed upon anyone who has effective control over the attack, who may well be the person in charge of executing the targeting decision, especially if communication with the chain of command are severed.[50]

46 See Jeffrey S Thurnher, 'Examining Autonomous Weapon Systems From a Law of Armed Conflict Perspective', in Hitoshi Nasu and Robert McLaughlin (eds.), *New Technologies and the Law of Armed Conflict* (Springer, 2014) 213, 223–225; Mark Roorda, 'NATO's Targeting Process: Ensuring Human Control over and Lawful Use of 'Autonomous' Weapons', in Andrew Williams and Paul Scharre (eds.), *Autonomous systems: Issues for defence policymakers* (NATO, 2015) 152; Merel A C Ekelhof, 'Lifting the Fog of Targeting: "Autonomous Weapons" and Human Control Through the Lens of Military Targeting' [2018] 71(3) *Naval War College Review* 61.

47 Angus G Houston, 'Australian Defence Doctrine Publication 3.14 – Targeting' (2 February 2009) para 1.11.

48 *Ibid*, para 1.12.

49 AP I, Art 48(1).

50 Ian Henderson, *The Contemporary Law of Targeting* (Brill, 2009) 235.

In case of deliberate targeting carried out through AWS, the person executing the targeting decision (and thus the one legally obliged to ascertain whether the locked-on target actually constitutes a military objective) will be replaced by the weapons systems, which raise again the problem of endowing the latter with SA capabilities. This issue is all the more pressing in case of AWS enabled to loiter on the target area for extended periods of time, as the temporal distance between the planning of the attack and its actual execution makes it highly probable that some change may occur on the battlefield that should be factored in distinction analysis.

The *second objection* may also be of some relevance to DSS, since it could be contended that, in scenarios where there are no issues of distinction, the system would be able to recommend *lawful* targeting decisions even without acquiring SA. While it is true that the need to distinguish civilians and civilian objects does not arise on any battlefield, the rule prohibiting attacks against enemies *hors de combat* which as we have seen poses non-trivial perceptual and evaluative challenges, also applies in a warfare scenario where civilians are not present.[51] The only case in which the use of an AWS or a DSS that is incapable of acquiring high levels of SA would not be problematic under IHL would be if the system were programmed to 'hunt' uninhabited enemy objects, such as armed drones, in uncluttered environments. In this case, all that would be required is for the system to reliably discriminate between the assigned targets and any other object.

2.4. Summary of the Discussion

To be used in accordance with IHL distinction obligation, AWS and DSS should be equipped with the capability to acquire and maintain situation awareness. Currently fielded systems are able to reach Level 1 SA (Perception) in terms of recognizing targets that are discernible on the basis of shape, heat and motion patterns in uncluttered environments. Making lawful targeting decisions in more complex scenarios generally requires the capability to autonomously achieve Level 2 and Level 3 SA (Comprehension and Prediction), which remains a major challenge for AI research.

51 Rob Sparrow, 'Twenty Seconds to Comply: Autonomous Weapon Systems and the Recognition of Surrender' [2015] 91 *International Law Studies* 699, 712.

The obligation to provide AWS and DSS with situation assessment capabilities has not necessarily the same breadth for each and every system and use thereof. Notably, higher levels of situation awareness are required if the system is (*a*) deployed in a cluttered environment, i.e. characterized by the intermingling of protected objects and military objectives; or (*b*) tasked to prosecute targets of opportunity (dynamic targeting); or (*c*) allowed to select and/or engage human targets and/or human-inhabited objects. Conversely, low levels of SA may be sufficient for systems that (*a*) are deployed in uncluttered scenarios; (*b*) are programmed to attack anticipated or known targets within the assigned operational environment; and (*c*) are assigned to attack only uninhabited military objects.

3. The Second Prong of the Test: Proportionality

While an early manifestation of the proportionality principle in IHL may be found in Article 24(4) of the (never adopted) 1923 Hague Rules of Air Warfare, its codification as a legally binding norm is due to Article 51(5)(b) AP I, which labels as 'indiscriminate', and thus prohibited, those attacks that are

> 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.[52]

A provision to the same effect is contained in Article 57(2)(a)(iii) AP I, and both are reinforced by Article 57(2)(b), which obliges warring parties to cancel or suspend an attack 'if it becomes apparent' that it may be expected to cause disproportionate collateral damage. Although the Second Additional Protocol to the Geneva Conventions does not envisage a similar provision in relation to non-international armed conflicts, the ICRC provided convincing evidence that customary law demands respect for the principle regardless of the nature of the conflict.[53]

From a plain reading of the norms embodying the principle, it emerges that proportionality is not concerned with actual outcomes but with

52 AP I, Art 51(5)(b).

53 J-M Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law* (CUP, 2005) 48–49.

ex ante assessments, i.e. the expectations and anticipations of those in charge of the attacks;[54] it also shows that proportionality analysis is made of three steps: (*a*) collateral damage estimation; (*b*) military advantage assessment; (*c*) determination of excessiveness. Conversely, norms on proportionality offer only little guidance as to the way this analysis should be carried out in concrete cases, having particular regard to how collateral damage and military advantage should be values, and mostly how excessiveness is to be measured.

The identification of what constitutes collateral damage is dependent on the scope of the principle of distinction: harm to civilians and civilian objects, whose intentional causation is prohibited under the principle of distinction, qualifies as collateral damage when it ensues from an attack directed against a legitimate target.[55] Proportionality analysis, however, additionally requires the (metaphorical) attribution of a 'weight' to the expected collateral damage in order to compare it with the anticipated military advantage. It should be noted, in this regard, that, while it is true that provisions on proportionality do not explicitly graduate collateral damages, some distinctions can be drawn as a matter of course. It is all too clear, for instance, that damages to property weigh less than human casualties; that recoverable injuries should be valued less than permanent ones; that losses of life are more serious collateral damage than injuries. Also, it can be maintained that harm to certain categories of persons and objects is to be accorded greater weight in proportionality calculations. This could be the case of vulnerable persons (e.g. children),[56] as well as of objects enjoying special protection from attack (e.g. cultural property).[57]

The definition of the other term of the proportionality equation also has a clear connection with the principle of distinction: the notion of 'military advantage' is indeed crucial to establish whether an object

54 Yoram Dinstein, *The Conduct of Hostilities Under the Law of International Armed Conflict* (4th edn, CUP, 2022) 181–182.

55 Kenneth Watkin, 'Assessing Proportionality: Moral Complexity and Legal Rules' [2005] 8 *Yearbook of International Humanitarian Law* 3, 8–9.

56 Dinstein (n 53) 184. Such a differential treatment seems to be warranted by the fact that vulnerable persons benefit from enhanced protection under international law.

57 Henderson (n 49) 192–193. A category of object that is expressly recognized greater weight in proportionality analysis is that envisaged by Art 56 AP I ('Protection of works and installations containing dangerous forces').

may be legitimately targeted. Yet, the application of this notion differs in the two contexts, as 'military advantage" constitutes 'a threshold determination for military objective' in relation to distinction, 'and a balancing for proportionality'.[58] Unlike distinction, in other words, the principle of proportionality does not content itself with the ascertainment of the existence of a military advantage, but requires that this advantage be assigned a value, to be weighed against the expected incidental harm to civilians and civilian objects. This complicates the (already complex) assessment of the military advantage, in that it brings into play factors that are not relevant (or are relatively relevant) when the principle of distinction is at stake. In this respect, mention should be made of the actual likelihood of success of the planned attack. Indeed, the uncertainty of obtaining the anticipated military advantage 'diminishes' its value for the purposes of proportionality (while it remains immaterial in relation to issues of distinction).[59] Furthermore, the value of a military objective may vary as the conflict goes on and even during the same attack, especially if it is of large scale. This means that 'a target folder cannot assign a certain value to the military advantage of a target once and for all',[60] as the assessment of the value of attacking a certain target must be constantly updated.

Once expected collateral damage and anticipated military advantage are assessed and attributed a value, the attacking force has to establish whether the former is 'excessive' in relation to the latter. Here lies the core of the principle of proportionality, as well as the source of the most intractable problems that it poses. The problem is that what proportionality ultimately requires is a comparison 'between unlike quantities and values'[61] (e.g. between the destruction of a bridge used by enemy tanks and a certain number of civilian casualties) –an 'apples vs. oranges' dilemma, as it is often said,[62] which makes it particularly

58 Joseph Holland, 'Military Objective and Collateral Damage: Their Relationship and Dynamics' [2004] 7 *Yearbook of International Humanitarian Law* 35, 54.

59 Laurent Gisel, *The Principle of Proportionality in the Rules Governing the Conduct of Hostilities under International Humanitarian Law*, International Expert Meeting 22–23 June 2016 – Quebec (ICRC, 2018) 18.

60 Henderson (n 49) 202.

61 William J Fenrick, 'The Rule of Proportionality and Protocol I in Conventional Warfare' [1982] 98 *Military Law Review* 91, 94. See also OTP Report (n 21) para 48.

62 See, among many others, Henderson (n 49) 228–229.

challenging to identify in advance clear-cut, general rules to help the decision-maker to act lawfully. It is noteworthy, in this respect, that the examples usually provided to illustrate breaches of proportionality are pretty obvious (e.g. the bombing of an isolated fuel tanker in the middle of a densely populated city),[63] while the 'hard cases', a label which covers the vast majority of proportionality scenarios, are considered to be resolved on the basis of a contextual, case-by-case analysis.[64]

This is not to mean, however, that the combatants' discretion in this regard is left 'unfettered'.[65] Following an early intuition by William J. Fenrick,[66] courts, academics, NGOs, and military experts have been progressively converging upon the standard against which the proportionality of an attack must be assessed, that of the 'reasonable military commander'.[67] This standard is aimed at fixing the outer limits of the discretion enjoyed by military decision-makers[68] or, to put it differently, to create a zone of reasonable discretion within which all decisions about proportionality are lawful.[69] Even if objective in character, the standard of the 'reasonable military commander' remains quite elusive. The most one can say about it is that 'there will be many cases where reasonable military commanders will agree that the injury to noncombatants or the damage to civilian objects was clearly disproportionate to the military advantage gained'.[70]

3.1. Can AWS and DSS Autonomously Make Proportionality Assessments?

The principle of proportionality introduces a further layer of tasks that AWS and DSS should be able to perform, which come on top of those exacted by the principle of distinction. In the first place, these systems

63 See Gisel (n 58) 53–54.

64 *Public Committee Against Torture in Israel v Government of Israel*, HCJ 769/02 [2006] (Israeli Supreme Court) para 46.

65 Dinstein (n 53) 183.

66 Fenrick (n 50) 127.

67 See, also for references, Ian Henderson and Kate Reece, 'Proportionality under International Humanitarian Law: The "Reasonable Military Commander" Standard and Reverberating Effects' [2018] 51(3) *Vanderbilt Journal of Transnational Law* 835, 845.

68 Gisel (n 58) 64.

69 *Beit Sourik Village Council v. The Government of Israel*, HCJ 2056/04 [2004] (Israeli Supreme Court) paras 42, 46.

70 OTP Report (n 21) para 50.

should be able to make reliable predictions as to the collateral damage casualties expected from a given course of action. In fact, this does not come across as an insurmountable challenge: for more than a decade, the US Army has been using software programs to make collateral damage estimations with a view to identifying the least harmful targeting option.[71]

Far more daunting is the challenge posed by the appraisal of excessiveness. To ensure compliance with this principle, indeed, law-abiding AWS and DSS should be able to assign a value to the expected collateral damage and the military advantage anticipated and to choose a targeting option that strikes a balance between them, in a way that a reasonable military commander would find acceptable. Still, if there is one point on which most (if not all) IHL experts agree it is that, despite what the terms 'proportionality', 'calculus', and 'equation' would suggest, this balancing exercise does not lend itself to be straightforwardly captured by a 'mathematical formula'.[72] It is no surprise, therefore, that these authorities are often cited in support of the conclusion that the proportionality principle is unsuitable to be coded into a computer algorithm.[73] Indeed, the very terms generally employed in legal scholarship to describe the kind of judgements involved in proportionality analysis – 'reasonableness', 'common sense', 'good faith'– are simply a 'non-starter' for programmers.[74]

The reasons for this 'translatability' problem have been well explained by Andreas Matthias.[75] Matthias observed that the idea of a software programmed to inhibit unethical courses of action by weapons systems moves from the assumption that it is possible (*a*) to assign to every

71 Thurnher (n 45) 221; Sharkey (n 27) 788–789.

72 Michael Wells-Greco, 'Operation 'Cast Lead': *Jus in Bello* Proportionality' [2010] 57(3) *Netherlands International Law Review* 397, 416.

73 See, for instance, Jeroen van den Boogaard, 'Proportionality and Autonomous Weapons Systems' [2015] 6(2) *Journal of International Humanitarian Legal Studies* 247, 283; Tanya Krupyi, 'Of Souls, Spirits and Ghosts: Transposing the Application of the Rules of Targeting to Lethal Autonomous Robots' [2015] 16(1) *Melbourne Journal of International Law* 1, 28.

74 Maziar Homayounnejad, '*Ensuring Lethal Autonomous Weapon Systems Comply with International Humanitarian Law*' (TLI Think! Paper 85/2017) 25. See also Suresh Venkatasubramanian, 'Structural Disconnects between Algorithmic Decision-Making and the Law' (*Humanitarian Law & Policy*, 25 April 2019) < https://blogs.icrc.org/law-and-policy/2019/04/25/structural-disconnects-algorithmic-decision-making-law> accessed 23 April 2024.

75 *Ibid* 9.

possible action 'a scalar 'morality' value'; (*b*) to measure this value 'with precision at any point in time'; (*c*) to compare this 'morality value' to that 'of other, alternative actions'; (*d*) to identify, for every moral problem, 'a single optimal target value', viz. the 'one and only one optimal solution', with the consequence that 'all alternative paths of action [would be] deviations from [it]'.[76] Still, moral 'problems', including those involving the use of lethal force on the battlefield, are so labelled for a reason, namely that none of them 'comes with a 'reference answer' which can be considered to solve the moral dilemma in a generally satisfactory way'.[77] If this is true, then the idea of programming an algorithmic inhibitor of immoral actions loses its very *raison d'être*, for '[w]here there is no target value, we cannot speak of a regulation process'.[78]

While originating from the realm of philosophy, Matthias' objection holds true in relation to the IHL principle of proportionality. Proportionality, indeed, does not provide 'reference answers': multiple courses of action are available and none of them may be said to be completely satisfactory, in that each involves a certain amount of harm to civilians and/or civilian objects, whose acceptance is an ultimately moral decision.[79]

Some scholars attempted to dodge this problem by arguing that it is always possible to ensure that the proportionality of the attack is in fact appraised by human beings, by 'pre-determin[ing] the upper limit for civilian casualties and various types of property damage prior to authorising the AWS mission'.[80] A similar argument could be made in relation to DSS to affirm that it is enough, legally speaking, they are designed to correctly identify the targets and estimate collateral damage, since proportionality calculations will still be made by human commanders or operators.

---

76 International Committee of the Red Cross, *Ethics and Autonomous Weapon Systems: An Ethical Basis for Human Control?* (CCW Group of Governmental Experts on Lethal Autonomous Weapons Systems, 28 March 2018, UN Doc. CCW/GGE.1/2018/WP.5) para 21.

77 *Ibid.*

78 *Ibid.*

79 David Kennedy, *Dark Side of Virtue: Reassessing International Humanitarianism* (Princeton University Press, 2004), 290–291; Dale Stephens and MW Lewis, 'The Law of Armed Conflict – A Contemporary Critique' [2005] 6 *Melbourne Journal of International Law* 55.

80 Ian Henderson, Patrick Keane and Josh Liddy, 'Remote and Autonomous Warfare Systems: Precautions in Attack and Individual Accountability', in JD Ohlin (ed.), *Research Handbook on Remote Warfare* (Edward Elgar Publishing, 2017) 335, 352.

At first sight, this line of reasoning may come across as reassuring, in that it seems that the gist of proportionality assessments is kept firmly in human hands. Yet, one should beware that the pre-determination of acceptable collateral damage should not be conducive to a trivialization of proportionality assessments, by turning it into a merely quantitative analysis.[81] This means that human operators cannot limit themselves to putting a 'price tag', in terms of civilian harm, on each generic set of targets (e.g., by 'valuing' the destruction of an enemy tank according to the number of permissible civilian deaths).[82] The authorization of an AWS sortie, or of an attack recommended by a DSS, should instead be made conditional upon a careful ponderation of the expected collateral damage, which takes into account the relative weight of the categories of civilians and civilian objects that may be incidentally affected. Only on the basis of such a comprehensive assessment would the human commander/operator be in a position to appraise whether the military advantage sought by the AWS mission (or the DSS' recommendation) is sufficiently important to justify the expected collateral damage.

The humanitarian catastrophe of the ongoing conflict in Gaza provides a dramatic illustration of the problematic implications of using AI for target identification, couples with a blanket 'price tag' approach to proportionality calculations. According to some sources, in the early weeks of the conflict the number of civilian casualties permitted for the killing of each junior Hamas operative, including those identified by the abovementioned Lavender system, was set at 20. It is no coincidence, on the other hand, that a concept closely related to 'price tagging', the 'non-combatant casualty cut-off value' (NCV), is no longer included in the official US military doctrine.[83]

81 Markus Wagner, 'The Dehumanization of International Humanitarian Law: Legal, Ethical, and Political Implications of Autonomous Weapon Systems' [2014] 47 *Vanderbilt Journal of Transnational Law* 1371, 1397–1398.

82 Louise Doswald-Beck, 'The Value of the 1977 Geneva Protocols for the Protection of Civilians', in MA Meyer (ed.), *Armed Conflict and the New Law: Aspects of the 1977 Geneva Protocols and the 1981 Weapons Convention* (BIICL, 1989) 153, 156 ('it is impossible to state that a factory is worth x civilians'). Regrettably, this view has seemingly been put forward by influential commentators like Schmitt and Thurnher (n 43) 256. For a more nuanced approach, although still based on a 'price-tagging' approach, see Maciek Zając, 'AWS compliance with the ethical principle of proportionality: three possible solutions' [2023] 25(1) *Ethics and Information Technology* 1, 13–14.

83 US Department of Defense, *Civilian Harm Mitigation and Response Action Plan* (25 August 2022).

But what about the possibility to let AWS and DSS make proportionality calculations on their own? If it is true that the principle at hand could not be 'translated' in 'a set of decision rules', researchers are exploring the possibility that AWS and DSS develop a 'practice', built on experience and training, on whose basis to perform legally acceptable proportionality calculations.[84] To put it in the simplest terms, since the principle cannot be directly coded, military research could focus on conceiving of a learning artificial architecture allowing AWS and DSS to approximate legally acceptable proportionality decisions, on the basis of both pre-deployment training and battlefield experience. At the training stage, in particular, the system would be fed with a dataset containing (historical or fictional) warfare scenarios where proportionality issues were resolved in line with the standard of the 'reasonable military commander', *at least in the opinion of the instructors*. This would allow the system, confronted with a new proportionality scenario, to 'retrieve' from its database the solution of the case that is most similar or to develop its own way to make reasonable proportionality decisions.[85]Instructors will continue to correct the systems' mistaken decisions and withhold deployment on the battlefield, until they are satisfied with the level of IHL-compliance of the system's proportionality assessments.[86]

It is worth reiterating that we are not talking about imminent technological innovations, but about long-term goals, whose achievement may be plausibly located in a distant future. However, as some military research projects have taken up this challenge, it is worth pushing our investigation a bit further and testing the claim, often made by AWS proponents, whereby autonomous performance of proportionality assessments would be beneficial to the respect of IHL. In particular, reference is made to the expectation that AWS (and DSS) will one day outperform humans in complying with IHL principles, including that of proportionality. This may be possible with respect to distinction and certain aspects of proportionality (such as the estimation of collateral damage), but it is doubtful that it will ever happen in relation to the core of proportionality,

84 Ronald C Arkin, *Governing Lethal Behavior in Autonomous Robots* (CRC Press, 2009) 47.

85 The latter would be the case if a reinforcement learning technique is opted for (International Committee of the Red Cross, *Autonomy, Artificial Intelligence and Robotics: Technical Aspects of Human Control* (ICRC, August 2019) 16); the former if a Case-Based Reasoning method is adopted (Arkin (n 83) 47–48).

86 Backstrom and Henderson (n 34) 494.

i.e. balancing. To the extent that the principle of proportionality does not set out an objectively identifiable goal to be achieved (such as 'zero civilian casualties'), AWS' and DSS' training will be heavily influenced by the instructors' personal beliefs about what a reasonable military commander would do. The best that can be wished for, thus, is for these systems to carry out proportionality analysis as well as their instructors, who, it can be hoped, but not guaranteed, will be conscientious and competent experts.

3.2. Summary of the Discussion

Unlike distinction, the principle of proportionality cannot be captured by a formula prescribing, in general and abstract terms, the course of action required by the norm. This unique feature of the principle makes it particularly unsuitable to be 'translated' into a computer program.

To overcome this problem, some authors suggest to pre-determine proportionality calculations at the planning stage, so as to ensure that they are made by human commanders. This may provide an adequate legal solution in certain scenarios, but one should carefully avoid turning predetermination into an oversimplification of proportionality assessment.

Autonomous proportionality assessment is in principle possible, although not in the immediate future, thanks to the developments in machine learning techniques. However, expectations about the humanitarian benefits of this should be significantly lowered.

4. The Third Prong of the Test: Precaution

The principles of distinction and proportionality may be described as envisaging obligations that are negative in character: do not target protected persons and objects, do not launch disproportionate attacks. IHL, however, goes beyond that by requiring States to comply with certain positive obligations, which are instrumental to the fullest adherence to the prohibitions set forth by the principles of distinction and proportionality. Here lies the core of the principle of precaution, which brings added normative value to the principles of distinction and proportionality, by introducing the duty take affirmative action, to 'do everything feasible' (or 'take all feasible precautions') to ensure that these principles are fully complied with.[87]

87 Art 57 AP I.

Precautions cover a wide range of measures of very different character (e.g. the issuance of advance warning). For the purposes of our discussion, it will suffice to focus on two of them. On the one hand, there is the obligation to undertake all practicable efforts 'to obtain reliable information' as to whether the target is a legitimate military objective.[88] On the other hand, everything feasible should be done to ensure that combatants have an adequate control over the effects of the weapons they use, with a view to avoiding or at least minimizing damages to civilians and civilian objects.[89] States must therefore mobilize all assets at their disposal, where reasonably available, to facilitate correct target identification. This requirement has to be understood as including human resources too, wherever they are conducive to more accuracy.[90] Also, if practicable, combatants must be in a position to control and limit the effects of the weapons they employ.

4.1. The Normative Implications of the Principle of Precaution for Human-Machine Interaction on the Battlefield

Relying on the research goal of designing AI-based systems outperforming humans on the battlefield, some scholars have argued that autonomy in weapons systems would make 'additional precautions possible', with the consequence that a commander having this kind of weapon in his/her arsenal would be legally required to use it instead of a human-controlled one, wherever feasible.[91]

This argument cannot be accepted on its own terms. This is not so much because, as we have tried to show above, expectations about the performance of AI-based systems on the battlefield should be significantly lowered. Rather, it is because the removal of the human element from the targeting process would preclude a feasible precautionary measure capable of preventing violations of the principles of distinction and proportionality.

88 Program on Humanitarian Policy and Conflict Research at Harvard University, *Manual on International Law Applicable to Air and Missile Warfare* (CUP, 2013) 144 (HPCR Manual).

89 Henckaerts and Doswald-Beck (n 52) rules 17-19.

90 Marina Mancini, 'Air Operations against the Federal Republic of Yugoslavia (1999)', in Natalino Ronzitti and Gabriella Venturini (eds.), *The Law of Air Warfare: Contemporary Issues* (Eleven 2006) 273, 278.

91 See, for instance, Peter Margulies, 'The Other Side of Autonomous Weapons: Using Artificial Intelligence to Enhance IHL Compliance', in RTP Alcala and Eric Talbot Jensen (eds.), *The Impact of Emerging Technologies on the Law of Armed Conflict* (OUP, 2019) 147.

In this regard, one should preliminarily note that, even the most enthusiastic proponents of AI-based systems are ready to admit that they will never be error-free.[92] Yet, this admission is usually accompanied by the observation that human combatants are far from perfect either;[93] that international law would not exact from AI more than it does from human war fighters; and that in any case autonomous targeting will ensure higher standards of compliance.[94] Still, regardless of whether one accepts these arguments, they are ultimately immaterial to our discussion. Indeed, they all proceed from the idea that the legal performances of human and autonomous targeting should be compared along a linear scale to determine which one is the best in terms of IHL-compliance. However, such an approach would only be warranted if human combatants and machines were in principle prone to the same flaws, biases and vulnerabilities, since this would entail that, once humans are outperformed by autonomous weapons, they cannot add any value to the legality of the targeting process.

But this is not the case. A growing body of studies in AI shows that, even when machines prove better than humans in a given task, they still incur mistakes that a human would never have made and for reasons that are sometimes obscure to their programmers themselves.[95] Moreover, machines can be fooled into badly wrong assessments with tricks (e.g. a minor adjustment of an image) that would not even be noticed by humans (so-called 'adversarial attacks')[96] and, conversely, they can 'cheat' human evaluators, by learning how to get their approval during the training phase, regardless of whether they are pursuing the assigned task correctly.[97] In other words, human and autonomous

92 See, for instance, Arkin (n 83) 30–31.

93 *Ibid* 31 – 36; Marco Sassóli, 'Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to be Clarified' [2014] 90 *International Law Studies* 308, 310.

94 Arkin (n 83) 29-30.

95 For an updated survey of – sometimes genuinely weird – AI failures, see Aaron Drapkin, 'AI Gone Wrong: An Updated List of AI Errors, Mistakes and Failures' (*tech.co*, 18 April 2024) <https://tech.co/news/list-ai-failures-mistakes-errors> accessed 23 April 2024.

96 Makaela Nartker, Zhenglong Zhou, and Chaz Firestone, 'When will AI misclassify? Intuiting failures on natural images' [2023] 23(4):4 J*ournal of Vision* 1.

97 Mark Farragher, 'This clever AI Hid Data from its Creator to Cheat at its Appointed Task' (*Medium*, 14 March 2019) <https://mdfarragher.medium.com/this-clever-ai-hid-data-from-its-creator-to-cheat-at-its-appointed-task-8b91ed9872f5> accessed 23 April 2024.

decision-making processes remain qualitatively different and are likely to err in qualitatively different ways.

As explained in a 2019 ICRC report, the source of such qualitative difference lies in what AI experts call the 'semantic gap'. This term indicates the fact that machines do not 'see' the world in the same way as humans, as only the latter have a proper understanding of the meaning or concept of the objects they classify and recognize, and of the context in which they are placed.[98] Accordingly, while it is reasonable to expect that the overall performances of AI-based systems will one day surpass those of humans (at least in some respects), this will not necessarily be the case *in each and every situation* where they are deployed. Indeed, even the most sophisticated system could commit (or be induced to commit) mistakes that could have been avoided had a human operator been involved in the decision-making loop. If we consider that, in the context of targeting, 'mistakes' generally amount to unlawful harm to civilians or civilian objects – that is, precisely what precautionary measures are meant to prevent – it becomes clear that it makes little sense to maintain in the abstract that autonomous targeting would be normatively preferable under the principle of precaution.

As we have said, the principle of precaution requires States to do everything feasible to facilitate correct target identification and to avoid (or minimize) collateral damage. The wide breadth of the obligations imposed by this principle (expressed by the use of words such as 'everything' or 'all') does not substantiate an all-or-nothing approach, whereby the critical functions of target selection and engagement should be entrusted either entirely to machines or entirely to humans. Rather, to ensure respect for the dictate that '*everything feasible*' is done, States must focus on developing human-machine relationships that bring out the best in both, or –which is the same thing– compensate for their mutual weaknesses.[99] Only in this way will they be able to exploit the full potential of the assets at their disposal in order to prevent or minimize unlawful harm.

98 ICRC (n 84) 20.

99 Noel E Sharkey, 'Staying the Loop: Human Supervisory Control of Weapons', in Nehal Bhuta et al., *Autonomous Weapons Systems: Law, Ethics, Policy* (CUP, 2016) 23. This idea is also embodied in the concept of 'centaur warfighting' advocated by Paul Scharre (Paul Scharre, 'Centaur Warfighting: The False Choice of Humans vs. Automation' [2016] 30(1) *Temple International and Comparative Law Journal* 151.

Awareness of the above has led to a number of doctrinal attempts to craft an ideal human-machine interaction, sometimes explicitly characterizing it as a precautionary measure.[100] These debates fall outside of the scope of the present Chapter, as they relate to the overarching concept of Meaningful Human Control, which is the object of several in-depth treatises.[101] For the purposes of the present discussion, we may observe that, in order to be properly qualified as a precautionary measure, this interaction must be designed in such a way as to comply with two guidelines.

On the one hand, the involvement of a human operator must add value to the targeting process.[102] In the debate on AWS, the risk has often been emphasized that the human contribution could be nullified by the so-called 'automation bias', i.e. the propensity to prefer solutions elaborated by the machine, even when contradicted by information coming from other sources.[103]

A tragic example in this sense is represented by Patriot missiles' fratricide incidents, which occurred in Iraq in 2003. The MIM-104 Patriot is an air defense system designed to intercept and destroy tactical ballistic missiles, cruise missiles and advanced aircrafts, which is manufactured by the US defense contractor Rayhteon.[104] The system autonomously identifies possible ballistic missile targets based on an assessment of the speed, altitude, and behavior of the objects detected by its radar, but leaves the actual decision to engage the targets to human operators. It was deployed during *Operation Iraqi Freedom* in 2003, resulting in a

100 This is the case, for instance, of Robin Geiss and Henning Lahmann, 'Autonomous Weapons Systems: A Paradigm Shift for the Law of Armed Conflict?', in Ohlin (n 76) 371, 397. See also International Panel on the Regulation of Autonomous Weapons (iPRAW), *Focus on Human Control*, Report No 5 (Berlin, August 2019) 11 (adhering to the view whereby 'the principle of precaution inherently requires some sort of human control during the attack because the abstract target selection criteria do not allow for sufficient legal assessments prior to the attack'); Jeffrey S Thurnher, *Means and Methods of the Future: Autonomous Systems*, in PAL Ducheine, MN Schmitt and FPB Osinga (eds.), *Targeting: The Challenges of Modern Warfare* (Springer, 2016) 177, 190 (arguing that '[i]n many circumstances, a manned or remotely controlled system may prove to be the necessary choice' to comply with the principle of precaution under IHL

101 See, most recently, Giulio Mecacci et al (eds.), *Research Handbook on Meaningful Human Control of Artificial Intelligence Systems* (Edward Elgar Publishing 2024).

102 Backstrom and Henderson (n 34) 496.

103 LJ Skitka, KL Mosier and Mark Burdick, 'Does Automation Bias Decision-making?' [1999] 51(5) *International Journal of Human-Computer Studies* 991.

104 See 'Patriot Missile Long-Range Air-Defence System, USA' (Army Technology)<https://www.army-technology.com/projects/patriot> accessed 23 April 2024.

very high success rate against Iraqi missiles. On two occasions, however, Patriot misidentified friendly aircrafts as enemy missiles, with the consequence that a British Tornado and a Navy F-18 fighter jet were shot down and their crews killed.[105] Crucially enough, for our purposes, subsequent Army investigations found that the ultimate cause of the fratricide incidents was a widespread culture, among Patriot operators, of 'unwarranted and uncritical trust in automation'.[106] The same 'uncritical trust' seems to characterize the use of Lavender in the Gaza conflict. In this regard, it has been reported that 'if Lavender decided an individual was a militant in Hamas, they were essentially asked to treat that as an order, with no requirement to independently check why the machine made that choice or to examine the raw intelligence data on which it is based'.[107]

Leaving aside the blatant absurdity of a practice that *de facto* equates a recommendation by a DSS with a superior's order, one should note that, contrary to what is sometimes argued,[108] the human propensity to trust machines is not in itself a valid reason to exclude the legal relevance of keeping human operators in the decision-making loop altogether. Rather, it urges the adoption of additional measures to guarantee that the human-machine interaction is effective.

In the first place, human operators should be provided with full knowledge of the system's capabilities and limits, with a view to educating them to trust the technology without completely relinquishing giving up their judgement and critical sense.[109] Moreover, the human-machine distribution of control privileges should be conceived of in such a way as to counter the risk of automation bias. It should be noted, in this respect, that a relationship in which the human chooses a course of action from a list of alternatives provided by the system is less conducive to such a

105 JK Hawley, *Patriot Wars: Automation and the Patriot Air and Missile Defense System* (Center for a New American Security, January 2017) 7-8.

106 Excerpts from the report are in JK Hawley, 'Not by Widgets Alone: The Human Challenge of Technology-intensive Military Systems' (*Armed Forces Journal*, 1 February 2011) <http://armed-forcesjournal.com/not-by-widgets-alone/> accessed 23 April 2024.

107 Abraham (n 2).

108 Sassóli (n 92) 337.

109 This point is well underscored by Paul Scharre who, on the basis of an insightful comparison of the approaches followed by the users of the Patriot and Aegis systems, indicated the latter as a virtuous model in that the machine effectuates warfighters' decision-making, instead of merely replacing it. Scharre (n 26) 161–173.

bias than one in which the weapon recommends a targeting decision, and the human authorizes the attack.[110] And both undoubtedly preserve human awareness better than a distribution of control privileges where autonomous targeting is subject only to human override.[111]

On the other hand, a proper human-machine relationship should address the weaknesses of the human element as well. Especially when put under stressful conditions, humans can be induced to misinterpret the data available to them 'in an unconscious attempt to make available evidence fit a preconceived scenario'.[112] This bias –commonly known as 'scenario fulfillment'– was studied extensively in relation to the 1988 USS Vincennes incident, which involved the shooting down of an Iranian airliner by a US warship in the Persian Gulf during the Iran-Iraq war. The most salient feature of this incident is that, although the available data clearly indicated that the aircraft posed no threat, the crew nevertheless mistakenly believed it to be an Iranian F-14 fighter and attacked it, causing the death of all 290 people on board.

This episode is sometimes relied on to deny that human control is an effective precautionary measure.[113] With all due respect, this pushes the argument too far. While it is true that scenario fulfillment is a typically human bias, this does not automatically rule out that, in other contexts, human control may actually help to avoid harmful events. If there is a lesson to be learned from the USS Vincennes incident, it is that human judgement should not be blindly trusted as well, and that the human-machine relationship should take this into account. One might envisage a 'two-key' mechanism whereby coded authorization by two separate individuals would be required to override the system's assessment that a targeting decision would be unlawful.[114] In this way, human decision-makers would be forced to pause and reconsider their judgement in light of the system's explanations –a measure that would probably have

110 Sharkey (n 98) 34-35; Backstrom and Henderson (n 34) 496.

111 In this perspective, the US Law of War Manual's suggestion that additional precautions should be taken in relation to AWS, which include 'monitoring the operation of the weapon' (US Department of Defense, *Law of War Manual* (updated 31 July 2023), 363) is certainly a welcome step, but does not come across as the best available solution.

112 Molly Moore, 'Vincennes Report Admits Errors but Urges No Disciplinary Action' (*The Washington Post*, 20 August 1988).

113 Schmitt and Thurnher (n 43) 248.

114 Arkin (n 83) 152–153.

prevented many tragic incidents, including that of the USS Vincennes.

The foregoing may appear quite bold statements as to what States would be obliged to do under the principle of precaution. In fact, it should always be borne in mind that the scope of the obligations deriving from the principle of precaution is subject to the limit of feasibility. As a consequence, while it is normatively desirable that States adopt all the above measures, they are excused for not taking them if they are wholly or partly impracticable. Some of the above requirements come across as relatively unproblematic. This is certainly the case of the obligation to provide adequate training that, as a matter of principle, should always be considered feasible. Likewise, measures aimed at ensuring the double-checking of human decisions could be more or less challenging for AI research but, once the necessary technology is developed, their implementation should not be hindered by military considerations.

Things stand quite differently as to the human-machine distribution of control privileges: there could be indeed scenarios where the enactment of higher levels of human control would be unfeasible because of competing military considerations, insofar as it would pose serious security risks (for defensive systems) or it would hinder mission accomplishment (for offensive systems). A relatively straightforward example of the former case may be that of an air defense system, such as the US Aegis Ballistic Missile Defense System or the Israeli Iron Dome, which has to cope with a saturation attack where multiple threats are incoming at a very fast pace. In this hypothesis, ensuring that human operators have full control over every single targeting decision would be prohibitive, and even the exercise of veto powers would be to a large extent an unavailable option. Accordingly, the decision to lower the level of human control (or even to exclude it, in the most extreme circumstances) would not be incompatible with the requirement of precaution.

More controversial is the case where human involvement in the decision loop –although technically practicable– could hinder mission accomplishment. Unlike the defensive scenario above, in this case the commander has a choice: (s)he can decide not to carry out the mission. In hypotheses of this kind, a crucial role will be played by humanitarian considerations, which also have to be factored into feasibility analysis.

If, given the features of the operational environment, the risks for protected persons and objects are virtually absent, the required level of human control may be lowered. Should such risks be instead present – because, for instance, the mission has to be accomplished in a cluttered urban warfare scenario– the principle of precaution will require the commander to maintain a higher level of human control and, if this makes mission accomplishment too hard, to cancel the attack and opt for a different course of action.[115]

4.2. Summary of the Discussion

Contrary to what is sometimes argued, exclusive reliance on AI systems in warfare –however sophisticated these technologies may be– is not in itself a mandatory precautionary measure under IHL. The obligation to do 'everything feasible' to prevent unlawful harm, indeed, requires States to develop human-machine relationships that bring out the best in both machines and humans, by compensating their reciprocal weaknesses, and not to give absolute preference to one over the other.

To be an effective precautionary measure, the human-machine interaction should be shaped so as to counter the risk of automation bias and scenario fulfillment. The former should be addressed by providing adequate training to human operators, and by choosing a level of human control that preserve human awareness and critical sense; the latter, by allowing the weapon to suspend human targeting decisions that it deems unlawful and request a double-check.

The obligation to adopt the above measures is conditional upon their feasibility. This is particularly true of human control, because in certain scenarios it could hinder mission accomplishment or pose serious security risks, making it impracticable –at least from a purely military perspective. Whether this justifies reducing or even excluding human control cannot be assessed solely on the basis of military evaluations, though. Humanitarian considerations (e.g. the risk of civilian casualties) also play a role in the feasibility equation, balancing the need to achieve the mission's goal.

115 WH Boothby, 'Some Legal Challenges Posed by Remote Attack' [2012] 94 (886) *International Review of the Red Cross* 579, 584.

5. Conclusions

It is now time to wrap up the long discussion carried out so far and to formulate a tentative answer to the questions raised in the introductory section:

- Are AWS and DSS, in their normal or intended circumstances of use, capable of complying with the applicable distinction obligations?
- Are AWS and DSS, in their normal or intended circumstances of use, capable of making the proportionality assessments required by IHL?
- Do AWS and DSS, in their normal or intended circumstances of use, hinder compliance with the obligation to take every feasible precaution to avoid (or minimize) civilian harm?

The first prong of the test presents an eminently technological challenge. Distinction obligations under IHL require that AWS and DSS are able to properly recognize and assess the elements and the dynamics that, in a given operational environment, are relevant for the lawfulness of a targeting decision (what we have referred to as SA capabilities). The scale of the technological challenge posed by this requirement is not the same for every possible use of AWS and DSS, but is determined –individually or in combination– by the following variables: (*a*) the features of the operational environment (cluttered vs. uncluttered); (*b*) the targeting mode (dynamic vs. deliberate); (*c*) the nature of the target (combatants and inhabited military objects vs. uninhabited military objects).

Current technology is up to the task only in a limited number of circumstances, where the values of the above variables converge towards lowering the required level of situation awareness. These may include air defense systems, which are entrusted with a relatively simple distinction task (detecting incoming threats), generally operate in uncluttered environments, and do not have to recognize messages of surrender from potential targets; fire-and-forget munitions that are launched in uncluttered scenarios; loitering munitions that are activated in uncluttered scenarios and are programmed to attack uninhabited military objects (e.g. enemy drones). Similar considerations apply to DSS' capability of proposing lawful targeting decisions. *In relation to these hypotheses, thus, the first prong of the test may be considered to have been passed even at the current state of technological development.*

In the vast majority of cases, however, the lawful use of AWS, as well as the ability of DSS to recommend legitimate targeting decisions, will depend on whether the system will be capable of autonomously acquiring higher levels of situation awareness. There is still a long way to go in AI research in this regard, and it is not possible to make reliable predictions about whether and when this goal will be achieved. *In relation to these hypotheses, the first prong of the test can therefore be considered to have failed, but this failure depends on the state of technological development.*

The second prong of the test raises instead a translational challenge. The principle of proportionality –and notably of the balancing exercise lying at its cor – seems ill-suited to being translated ('coded') into a computer program. As we have seen, two options have been put forth to address this problem. On the one hand, proportionality calculations could be anticipated at the planning stage, so as to ensure that they are still carried out by human decision-makers. This may be an appropriate legal solution in the case of deliberate targeting, but care should be taken not to turn pre-determination into an oversimplification of proportionality assessment. *Subject to these conditions, and provided that the required level of situation awareness is met, the second prong of the test may hence be considered to have been passed when proportionality calculations are made by a human being at the planning stage.*

On the other hand, AWS and DSS might one day be programmed –thanks to reinforcement machine learning techniques– to perform proportionality calculations on their own, not on the basis of some sort of algorithmic formula (which would be impossible to determine in advance), but by directly emulating human reasoning. Yet, such a technological development, although sometimes discussed in the literature, does not appear to be achievable in the near future. *Accordingly, if proportionality calculations are not made by humans, the second prong of the test can be considered to have failed, at least on the basis of the current state of technological development.*

The third and final prong of the test contains a *design* challenge. The positive obligation to take precautionary measures implies that States must develop human-machine relationships that bring out the best in both machines and humans by compensating for their reciprocal weaknesses. On this assumption, a number of specific features of such

a human-machine relationship have been distilled, the most important of which is –for the present discussion– *the need to preserve the operators' awareness and critical sense by ensuring appropriate levels of human control.* The duty to adopt this measure is subject to two qualifications. On the one hand, the obligation to take precautionary measures is instrumental to the fulfillment of the requirements deriving from the principles of distinction and proportionality. Accordingly, it arises only when and to the extent that issues of distinction and proportionality are at stake. On the other hand, precautionary measures need to be adopted only if they are militarily feasible. This implies that, in principle, human control could legitimately be limited or excluded when it could pose serious security risks (e.g. because it hinders a timely reaction against a saturation attack).

Notwithstanding these qualifications, this prong of the test undoubtedly remains the most demanding. Unlike the other two prongs, it does raise a challenge to full autonomy that holds true even with regard to futuristic systems capable of carrying out reliable distinction and proportionality analysis in any warfare scenario. This is an important point, as it partially disproves the conventional wisdom that IHL-based objections to complete reliance on AI technologies in warfare are technologically contingent.[116]

In this perspective, the removal of the human element from the critical functions of target selection and engagement would be legally acceptable only if (*a*) the system is used in a context where issues of protection of civilians under the principles of distinction and proportionality do not arise; or (*b*) human control would be impracticable because it would pose serious security risks. *Subject to these conditions, the third and final prong of the test may be considered satisfied.*

The foregoing calls for a serious reconsideration of the appropriateness of a legal regulation of these systems aimed at identifying a one-size-fits-all solution. The vast taxonomy of AWS and DSS and their diverse applications dictates the adoption of a more nuanced approach. More specifically, a number of variables have been detected that warrant

116 International Committee of the Red Cross, *Ethics and Autonomous Weapon Systems: An Ethical Basis for Human Control?* (CCW Group of Governmental Experts on Lethal Autonomous Weapons Systems, 28 March 2018, UN Doc. CCW/GGE.1/2018/WP.5) para 21.

differential legal treatment depending on the characteristics and intended uses of the system. This highlights the need for a more tailored and context-sensitive approach to regulating the use and deployment of these technologies, particularly with regard to the crucial issue of human-machine interaction.[117] But this, of course, goes well beyond the scope of the present inquiry.

117 The importance of this issue has been acknowledged by the Group of Governmental Experts on Lethal Autonomous Weapons Systems. See Guiding Principles affirmed by the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons System, UN Doc. CCW/MSP/2019/9, Principle (c).

Bibliography

Abraham Y, "Lavender': The AI Machine Directing Israel's Bombing Spree in Gaza' (+972 Magazine, 3 April 2024) https://www.972mag.com/lavender-ai-israeli-army-gaza/ accessed 23 April 2024.

Additional Protocol to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) 1977.

Additional Protocol to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (Protocol I), Annex I: *Regulations Concerning Identification* (1977).

Akerson D, 'The Illegality of Offensive Lethal Autonomy' in D Saxon (ed), *International Humanitarian Law and the Changing Technology of War* (Martinus Nijhoff 2013).

Amoroso D and Guglielmo T, 'Toward a Normative Model of Meaningful Human Control over Weapons Systems' (2021) 35(2) *Ethics & International Affair*s 245.

Arkin RC, *Governing Lethal Behavior in Autonomous Robots* (CRC Press 2009).

Backstrom A and Henderson I, 'New Capabilities in Warfare: An Overview of Contemporary Technological Developments and the Associated Legal and Engineering Issues in Article 36 Weapons Reviews' (2012) 94 *International Review of the Red Cross* 483.

Beit Sourik Village Council v Government of Israel HCJ 2056/04 (Israeli Supreme Court 2004).

Boothby WH, "'And for Such Time As": The Time Dimension to Direct Participation in Hostilities' (2010) 42 *New York University Journal of International Law and Politic*s 741.

Boothby WH, 'Some Legal Challenges Posed by Remote Attack' (2012) 94 *International Review of the Red Cross* 579.

Boulanin V and Verbruggen M, *Mapping the Development of Autonomy in Weapon Systems* (SIPRI 2017).

Byron C, 'International Humanitarian Law and Bombing Campaigns: Legitimate Military Objectives and Excessive Collateral Damage' (2011) 13 *Yearbook of International Humanitarian Law* 175.

Chegini H, 'Unraveling Abductive Reasoning: Chatgpt's Struggles and Limitations Exposed' (Medium, 31 May 2023) https://medium.com/coding-intelligence-ai-development-and-analysis/unraveling-abductive-reasoning-chatgpts-struggles-and-limitations-exposed-27fd4da6c60b accessed 23 April 2024.

Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia, *Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign against the Federal Republic of Yugoslavia* (2000).

Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight (Saint Petersburg Declaration) 1868.

Dinstein Y, *The Conduct of Hostilities Under the Law of International Armed Conflict* (4th edn, Cambridge University Press 2022).

Doswald-Beck L, 'International Humanitarian Law and the Advisory Opinion of the International Court of Justice on the Legality of the Threat or Use of Nuclear Weapons' (1997) 316 *International Review of the Red Cross* 35.

Doswald-Beck L, 'The Value of the 1977 Geneva Protocols for the Protection of Civilians' in MA Meyer (ed), *Armed Conflict and the New Law* (British Institute of International and Comparative Law 1989).

Drapkin A, 'AI Gone Wrong: An Updated List of AI Errors, Mistakes and Failures' (tech.co, 18 April 2024) https://tech.co/news/list-ai-failures-mistakes-errors accessed 23 April 2024.

Egeland K, 'Lethal Autonomous Weapon Systems under International Humanitarian Law' (2016) 85 *Nordic Journal of International Law* 89.

Ekelhof M AC, 'Lifting the Fog of Targeting: "Autonomous Weapons" and Human Control Through the Lens of Military Targeting' (2018) 71(3) *Naval War College Review* 61.

Endsley MR, 'Toward a Theory of Situation Awareness in Dynamic Systems' (1995) 37 *Human Factors* 32.

Farragher M, 'This Clever AI Hid Data from its Creator to Cheat at its Appointed Task' (Medium, 14 March 2019) https://mdfarragher.medium.com/this-clever-ai-hid-data-from-its-creator-to-cheat-at-its-appointed-task-8b91ed9872f5 accessed 23 April 2024.

Fenrick WJ, 'The Rule of Proportionality and Protocol I in Conventional Warfare' (1982) 98 *Military Law Review* 91.

Geiss R and Lahmann H, 'Autonomous Weapons Systems: A Paradigm Shift for the Law of Armed Conflict?' in JD Ohlin (ed), *Research Handbook on Remote Warfare* (Edward Elgar 2017).

Gisel L, *The Principle of Proportionality in the Rules Governing the Conduct of Hostilities under International Humanitarian Law, International Expert Meeting 22–23 June 2016 – Quebec* (International Committee of the Red Cross 2018).

Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict 1954.

Hambling D, 'Ukrainian AI Attack Drones may be Killing without Human Oversight' (New Scientist, 31 October 2023) https://www.newscientist.com/article/2397389-ukrainian-ai-attack-drones-may-be-killing-without-human-oversight/ accessed 23 April 2024.

Hawley JK, 'Not by Widgets Alone: The Human Challenge of Technology-Intensive Military Systems' (*Armed Forces Journal*, 1 February 2011) http://armedforcesjournal.com/not-by-widgets-alone/.

Hawley JK, Patriot Wars: *Automation and the Patriot Air and Missile Defense System* (Center for a New American Security 2017).

Heller KJ, "One Hell of a Killing Machine': Signature Strikes and International Law' (2013) 11 *Journal of International Criminal Justice* 89.

Henckaerts JM and Doswald-Beck L, *Customary International Humanitarian Law* (Cambridge University Press 2005).

Henderson I and Kate R, 'Proportionality under International Humanitarian Law: The "Reasonable Military Commander" Standard and Reverberating Effects' (2018) 51(3) *Vanderbilt Journal of Transnational Law* 835.

Henderson I, Keane P and Liddy J, 'Remote and Autonomous Warfare Systems: Precautions in Attack and Individual Accountability' in JD Ohlin (ed), *Research Handbook on Remote Warfare* (Edward Elgar 2017).

Henderson I, *The Contemporary Law of Targeting* (Brill 2009).

Holland J, 'Military Objective and Collateral Damage: Their Relationship and Dynamics' (2004) 7 *Yearbook of International Humanitarian Law* 35.

Homayounnejad M, 'Ensuring Lethal Autonomous Weapon Systems Comply with International Humanitarian Law' (TLI Think Paper 85/2017).

Houston AG, *Australian Defence Doctrine Publication* 3.14 – Targeting (2 February 2009).

International Committee of the Red Cross, 'Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach' (2020) 102 (913) *International Review of the Red Cross* 463.

International Committee of the Red Cross, 'Emblem: Relevant Articles of the 1949 Geneva Conventions and their Additional Protocols' (1 November 2008) https://www.icrc.org/eng/resources/documents/misc/emblem-ihl-011108.htm accessed 23 April 2024.

International Committee of the Red Cross, 'Views of the International Committee of the Red Cross on Autonomous Weapon Systems' (CCW Meeting of Experts on Lethal

Autonomous Weapons Systems, Geneva, 11–15 April 2016) https://www.icrc.org/en/document/views-icrc-autonomous-weapon-system accessed 23 April 2024.

International Committee of the Red Cross, *Autonomy, Artificial Intelligence and Robotics: Technical Aspects of Human Control* (2019).

International Committee of the Red Cross, *Ethics and Autonomous Weapon Systems: An Ethical Basis for Human Control?* (2018).

International Panel on the Regulation of Autonomous Weapons, *Focus on Human Control* (Report No 5, 2019).

Jevglevskaja N, *International Law and Weapons Review: Emerging Military Technology under the Law of Armed Conflict* (CUP 2021).

Kaempf GL, Wolf S and Miller TE, 'Decision Making in the AEGIS Combat Information Center' (1993) 37 *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 1107.

Kennedy D, *Dark Side of Virtue: Reassessing International Humanitarianism* (Princeton University Press 2004).

Klonowska K, 'Article 36: Review of AI Decision-Support Systems and Other Emerging Technologies of Warfare' (2022) 23 *Yearbook of International Humanitarian Law* 123.

Krupyi T, 'Of Souls, Spirits and Ghosts: Transposing the Application of the Rules of Targeting to Lethal Autonomous Robots' (2015) 16 *Melbourne Journal of International Law* 1.

Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion) [1996] ICJ Rep 226.

Maciek Z, 'AWS Compliance with the Ethical Principle of Proportionality: Three Possible Solutions' (2023) 25(1) *Ethics and Information Technology* 1, 13–14.

Mancini M, 'Air Operations against the Federal Republic of Yugoslavia (1999)' in N Ronzitti and G Venturini (eds), *The Law of Air Warfare* (Eleven 2006).

Margulies P, 'The Other Side of Autonomous Weapons: Using Artificial Intelligence to Enhance International Humanitarian Law Compliance' in RTP Alcala and ET Jensen (eds), *The Impact of Emerging Technologies on the Law of Armed Conflict* (Oxford University Press 2019).

Matthias A, 'Is the Concept of an Ethical Governor Philosophically Sound?' in *TILTing Perspectives 2011: Technologies on the Stand: Legal and Ethical Questions in Neuroscience and Robotics* (Tilburg University 2011).

Mecacci G and others (eds), *Research Handbook on Meaningful Human Control of Artificial Intelligence Systems* (Edward Elgar Publishing 2024).

Melzer N, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (International Committee of the Red Cross 2009).

Moore M, 'Vincennes Report Admits Errors But Urges No Disciplinary Action' (*The Washington Post*, 20 August 1988).

Nartker M, Zhou Z and Firestone C, 'When Will AI Misclassify? Intuiting Failures on Natural Images' (2023) 23 *Journal of Vision* 1.

Patriot Missile System (Army Technology) <https://www.army-technology.com/projects/patriot> accessed 23 April 2024.

Press J, 'Inside Project Maven, the US Military's Mysterious AI Project' (Bloomberg, 29 February 2024) https://www.bloomberg.com/news/articles/2024-02-28/inside-project-maven-the-us-military-s-flagship-ai-project-big-take-podcast?embedded-checkout=true accessed 23 April 2024.

Program on Humanitarian Policy and Conflict Research at Harvard University, *Manual on International Law Applicable to Air and Missile Warfare* (Cambridge University Press 2013).

Public Committee Against Torture in Israel v Government of Israel HCJ 769/02 (Israeli Supreme Court 2006).

Roorda M, 'NATO's Targeting Process: Ensuring Human Control over and Lawful

Use of "Autonomous" Weapons' in Andrew Williams and Paul Scharre (eds), *Autonomous Systems: Issues for Defence Policymakers* (NATO 2015).

Sassóli M, 'Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to be Clarified' (2014) 90 *International Law Studies* 308.

Scharre P, 'The Perilous Coming Age of AI Warfare. How to Limit the Threat of Autonomous Weapons' (*Foreign Affairs*, 29 February 2024) https://www.foreignaffairs.com/ukraine/perilous-coming-age-ai-warfare accessed 23 April 2024.

Scharre P, *Army of None: Autonomous Weapons and the Future of War* (WW Norton & Company 2018).

Schmitt MN and Thurnher JS, 'Out of the Loop: Autonomous Weapon Systems and the Law of Armed Conflict' (2013) 4 *Harvard National Security Journal* 231.

Schmitt MN, 'Deconstructing Direct Participation in Hostilities: The Constitutive Elements' (2010) 42 *New York University Journal of International Law and Politics* 697.

Sharkey NE, 'Staying in the Loop: Human Supervisory Control of Weapons' in Nehal Bhuta and others (eds), *Autonomous Weapons Systems: Law, Ethics, Policy* (CUP 2016).

Sharkey NE, 'The Evitability of Autonomous Robot Warfare' (2012) 94 *International Review of the Red Cross*.

Skitka LJ, Mosier KL and Burdick M, 'Does Automation Bias Decision-Making?' (1999) 51 *International Journal of Human-Computer Studies* 991.

Sparrow R, 'Twenty Seconds to Comply: Autonomous Weapon Systems and the Recognition of Surrender' (2015) 91 *International Law Studies* 699.

Stephens D and Michael WL, 'The Law of Armed Conflict – A Contemporary Critique' (2005) 6 *Melbourne Journal of International Law* 55.

Stewart R and Hinds G, 'Algorithms of War: The Use of Artificial Intelligence in Decision Making in Armed Conflict' *(Humanitarian Law & Policy*, 24 October 2023) https://blogs.icrc.org/law-and-policy/2023/10/24/algorithms-of-war-use-of-artificial-intelligence-decision-making-armed-conflict/ accessed 23 April 2024.

Suchman L, 'Situational Awareness and Adherence to the Principle of Distinction as a Necessary Condition for Lawful Autonomy' (Briefing Paper, CCW Meeting of Experts on Lethal Autonomous Weapons Systems, Geneva, 12 April 2016).

Switzerland, 'Towards a Compliance-Based Approach to Lethal Autonomous Weapons Systems' (CCW Meeting of Experts on LAWS, Geneva, 30 March 2016).

Thurnher JS, 'Examining Autonomous Weapon Systems From a Law of Armed Conflict Perspective' in Hitoshi Nasu and Robert McLaughlin (eds), *New Technologies and the Law of Armed Conflict* (Springer 2014).

Thurnher JS, 'Means and Methods of the Future: Autonomous Systems' in Paul A L Ducheine, Michael N Schmitt and Frans P B Osinga (eds), *Targeting: The Challenges of Modern Warfare* (Springer 2016).

United Nations, Guiding *Principles Affirmed by the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems*, UN Doc CCW/MSP/2019/9 (2019).

US Department of Defense, *Civilian Harm Mitigation and Response Action Plan* (25 August 2022).

US Department of Defense, *Law of War Manual* (updated 31 July 2023).

van den Boogaard J, 'Proportionality and Autonomous Weapons Systems' (2015) 6(2) *Journal of International Humanitarian Legal Studies* 247.

Venkatasubramanian S, 'Structural Disconnects between Algorithmic Decision-Making and the Law' (*Humanitarian Law & Policy*, 25 April 2019) https://blogs.icrc.org/law-and-

policy/2019/04/25/structural-disconnects-algorithmic-decision-making-law accessed 23 April 2024.

Wagner M, 'The Dehumanization of International Humanitarian Law: Legal, Ethical, and Political Implications of Autonomous Weapon Systems' (2014) 47 *Vanderbilt Journal of Transnational Law* 1371.

Watkin K, 'Opportunity Lost: Organized Armed Groups and the ICRC "Direct Participation in Hostilities" Interpretive Guidance' (2010) 42 *New York University Journal of International Law and Politics* 641.

Wells-Greco M, 'Operation Cast Lead: Jus in Bello Proportionality' (2010) 57 *Netherlands International Law Review* 397.

Zając M, 'Autonomous Weapon Systems Compliance with the Ethical Principle of Proportionality: Three Possible Solutions' (2023) 25 *Ethics and Information Technology* 1.

Chapter II: International Humanitarian Law and the Regulation of Warfare in the Cyber Domain

Eitan Diamond[1]

1. Introduction

Throughout history technological advances have made it possible to expand human activity into new domains. We extended across the land, took to the seas, and rose to the sky and onto outer space. Unfortunately, every domain into which humanity has extended its reach has also functioned as a combat zone. International humanitarian law (IHL), also known as the law of armed conflict or the laws of war, seeks to limit and restrain the violence employed in these various arenas of conflict. It develops and evolves as the conflict environment changes and as means of warfare advance. This chapter examines the application of IHL to warfare in the latest domain into which humanity has ventured– cyberspace.

For present purposes, and following widely accepted definitions, the term 'cyberspace' is used here to refer to the notional environment in which communication over computer networks occurs.[2] Cyberspace differs then from other domains in that it is a human construct. It exists outside the physical world and consists of information flowing through computer systems and the networks connecting them. While not part of the physical world, human activity in cyberspace does have real and concrete implications, including harmful effects. These can and have

1 Manager and Senior Legal Expert, Diakonia International Humanitarian Law Centre Jerusalem. Manager and Senior Legal Expert, Diakonia International Humanitarian Law Centre Jerusalem. The views expressed in this article are those of the author and do not necessarily reflect those of the Diakonia IHL Centre. This chapter revisits, updates and expands upon issues that the author had previously examined some ten years ago in Eitan Diamond, 'Applying International Humanitarian Law to Cyber Warfare' in Pnina Sharvit Baruch and Anat Kurz (eds), *Law and National Security: Selected Issues* (INSS Memorandum 138, INSS 2014) 67.

2 The Oxford English Dictionary, for instance, defines 'Cyberspace' as '[t]he space of virtual reality; the notional environment within which electronic communication (esp. via the internet) occurs'. See *Cyberspace, n.,* OED Online (OUP, May 2024) <www.oed.com/dictionary/cyberspace_n?tab=meaning_and_use#12786295> accessed 15 May 2024.

included harm intentionally inflicted during armed conflict, through operations referred to as cyber warfare.[3]

For the purposes of the analysis here, the term 'cyber warfare' will be used to describe cyber operations that engender an armed conflict or which are part of the hostilities occurring in an armed conflict.[4] Such cyber operations, which involve the development and dispatch of computer code from one or more computers to target computers, aim at infiltrating a computer system to either collect, export, destroy, change, or to encrypt data; or to trigger, alter, or otherwise manipulate processes controlled by the infiltrated system. [5] In this vein, operations constituting cyber warfare, referred to as 'cyber operations during armed conflict', have been defined as 'operations against a computer system or network, or another connected device, through a data stream, when used as a means or method of warfare in the context of an armed conflict'.[6]

Even while directed at computers rather than people, cyber operations of this kind could potentially cause a tremendous degree of human suffering. In times of armed conflict, in particular, there are grounds for concern that cyber operations will be used to undermine the functioning of infrastructure needed for the provision of resources and services of crucial importance for the civilian population. Critical installations, such as power plants, nuclear plants, dams, water treatment and distribution systems, oil refineries, gas and oil pipelines, banking systems, hospital systems, railroads, and air traffic control, all rely heavily on computer systems susceptible to infiltration and manipulation via cyber operations.

3 While parties resorting to cyber warfare do not generally disclose this, there have been cases in which States acknowledged doing so, or where there was evidence to suggest that a party to an armed conflict engaged in cyber operations against its adversary. There have been multiple other instances where States involved in an armed conflict have incurred harmful effects from cyber operations whose authors are not known. For examples and elaboration see Laurent Gisel, Tilman Rodenhäuser, and Knut Dörmann, 'Twenty Years On: International Humanitarian Law and the Protection of Civilians against the Effects of Cyber Operations during Armed Conflicts' (2020) 102(913) *International Review of the Red Cross* 287, 289-290.

4 Note that the chapter focuses only on the subset of cyber operations that constitute cyber warfare. It does not address other potentially harmful types of cyber operations such as cybercrime, cyber terrorism, and cyber espionage.

5 For details on this definition see Cordula Droege, 'Get of My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians' (2012) 94(886) *International Review of the Red Cross* 533, 538.

6 International Committee of the Red Cross, *International Humanitarian Law and Cyber Operations during Armed Conflicts* (Position Paper, ICRC 2019) (n 1) <www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts> accessed 12 May 2024.

The risk that civilians and civilian objects will come to harm in an armed conflict involving cyber warfare is increased by the high level of interconnectivity and interdependence that exists between civilian and military computer infrastructure which makes it difficult to distinguish between them.[7] Thus, an attack on a military computer system may well damage civilian computer systems as well. These in turn may be vital for some civilian services such as water or electricity supply, or the transfer of assets. Recognizing such risks, UN member States have seen fit to warn, in a high-level consensus report, of the 'potentially devastating security, economic, social and humanitarian consequences' that may result from the malicious use of digital information and communication technologies in armed conflict.[8]

In view of these potential risks, it is plainly apparent that there is a humanitarian need for the law to regulate and constrain cyber warfare. In recent years there have been some notable efforts to promote such regulation by clarifying how existing legal frameworks, including IHL, might be applied to the nascent phenomenon of cyber operations in armed conflict.[9] These efforts notwithstanding, many questions about the application of IHL to cyber warfare remain open.

7 Due to Internet interconnectivity, most military networks rely on civilian, mainly commercial, computer infrastructure. Conversely, civilian vehicles, shipping, and air traffic controls are equipped with navigation systems relying on global positioning system (GPS) satellites, which are also used by the military. For elaboration on the risk that cyber operations may inadvertently harm civilian infrastructure even when directed at military objectives due to such interconnectivity see eg, Gisel, Rodenhäuser and Dörmann (n 2) 294.

8 *Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc A/75/816 (18 March 2021) paras 16, 18.

9 For a general overview of such efforts see Lauren M. Cherry and Peter P. Pascucci, '*International Law in Cyberspace*' (American Bar Association, 27 January 2023) <https://www.americanbar.org/groups/law_national_security/publications/aba-standing-committee-on-law-and-national-security-60-th-anniversary-an-anthology/international-law-in-cyberspace/> accessed 15 May 2024. Notable among such efforts were the two Tallinn Manuals on the International Law Applicable to Cyber Operations (the Tallinn Manuals), which were drafted by groups of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence. See Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP 2013) (Tallinn Manual 1.0); Michael N. Schmitt and Liis Vihul (eds), *Tallinn Manual 2.0 on International Law Applicable to Cyber Operations* (2nd ed., CUP 2017) (Tallinn Manual 2.0). The application of IHL to cyber operations has also been discussed in expert consultations involving representatives from UN Members as part of Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace (GGE), established pursuant to UNGA Res 73/266 (22 December 2018) UN Doc A/RES/73/266; and the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG), established pursuant to UNGA Res 73/27 (5 December 2018) UN Doc A/RES/73/27. As detailed in Gisel, Rodenhäuser and Dörmann (n 2) nn 18–22, consultations on the subject have also been held within various regional organizations.

This chapter will not provide comprehensive answers to all such questions. For one thing, it will not attempt to address questions relating to all bodies of law that may be applicable to cyber warfare and will instead address only questions relating to the application of IHL. Furthermore, even while the analysis will thus be confined to the challenges that cyber warfare poses for IHL, some significant questions will remain unanswered. Rather than attempting to provide a complete set of answers, which –for reasons that will be explained– is not currently possible, the chapter will endeavour to map out the most pressing questions and to indicate what challenges must be overcome if IHL is to attain its goal of preserving human dignity and preventing unnecessary human suffering even as warfare extends into the cyber domain.

As a backdrop for the analysis, the chapter will first highlight the general difficulty of applying the long-established rules of IHL to hostilities involving new methods and means of warfare, a difficulty which is particularly evident in the case of cyber operations. The lack of transparency and overall dearth of information surrounding cyber operations create further obstacles for the application of IHL. The chapter will then discuss problems that may arise in determining whether cyber operations have occurred within a situation of armed conflict. This is significant, because IHL only applies during armed conflict. Once it has been determined that a situation of armed conflict exists it is necessary to ascertain how the applicable rules of IHL are to be applied to cyber operations. In this regard, the chapter considers in what circumstances cyber operations trigger the IHL rules on the conduct of hostilities, and how the foundational principles of distinction, proportionality, and precautions, are to be implemented in the context of cyber warfare.

2. Adapting Old Law to New Cyber Technologies

Legal norms are by nature general and forward looking. They establish rules of conduct that are to be applied in diverse and presently unknown future situations. To accomplish this task the law must paint with a broad brush. It cannot possibly spell out specific rules for all sets of circumstances that may arise, and so instead, it applies rules across different general categories that it defines and distinguishes from one another. The transition from such general norms to concrete and ever-changing reality is not seamless and requires a regular process of adaptation.

In the realm of domestic law, this task is achieved in large part through acts of interpretation by national courts, which are constantly called upon to apply the law to specific incidents, and through legislative amendments, which can be enacted in response to changing sensibilities and new realities. When it comes to international law, the process of adaptation is far more cumbersome. For one thing, an international norm cannot be enacted by the legislator of a single State, but instead emerges only when multiple States express their consent to be bound by it.[10] Since States are driven by different and often contrasting interests and incentives, such consensus is difficult to achieve. Adapting international law through judicial interpretation is also complicated since relevant jurisprudence occurs haphazardly in instances from diverse jurisdictions, and it is therefore not always possible to extract a coherent and authoritative interpretation.

The process of adapting law to change is particularly challenging when it comes to IHL, as it regulates situations of armed conflict that naturally evoke contrasting positions between States. Indeed, States so rarely reach the necessary consensus on such matters that the key provisions of IHL are still found in treaties that are many decades old and in some cases date back more than a century.[11] But while the law evolves slowly, new means and methods of warfare are constantly being developed and the battlefield is rapidly changing. Bridging the temporal and contextual gap between the moment of the law's formation and the moment of

10 States express their consent to be bound by an international norm either by becoming party to an international treaty containing it, or via international custom which in turn emerges from the consistent practice of States combined with the view that such practice is mandated by law (*opinio juris*). A norm of customary international law is binding on all States apart from those which expressed a consistent objection to the applicability of the norm in question. For a detailed exposition on customary international law see eg, Jean d'Aspremont, *The Discourse on Customary International Law* (OUP 2021).

11 These treaties include, notably, *Hague Convention (IV) Respecting the Laws and Customs of War on Land and its Annex: Regulations Concerning the Laws and Customs of War on Land* (18 October 1907) 205 CTS 277; *Geneva Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field* (12 August 1949) 75 UNTS 31 (GC I); *Geneva Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea* (12 August 1949) 75 UNTS 85 (GC II); *Geneva Convention (III) Relative to the Treatment of Prisoners of War* (12 August 1949) 75 UNTS 135 (GC III); *Geneva Convention (IV) Relative to the Protection of Civilian Persons in Time of War* (12 August 1949) 75 UNTS 287 (GC IV); *Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts* (Protocol I) (adopted 8 June 1977, came into force 7 December 1978) 1125 UNTS 3 (AP I); *Protocol Additional to the Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims of Non-International Armed Conflicts* (Protocol II) (adopted 8 June 1977, came into force 7 December 1978) 1125 UNTS 609 (AP II).

its application is thus becoming an ever more pressing and ever greater challenge.

Fortunately, the IHL rules governing the conduct of hostilities, including such core principles as the principles of distinction and proportionality and the duty to employ precautionary measures, are broadly and flexibly defined and can therefore accommodate even far-reaching developments. These general rules regulate all means and methods of warfare, including the use of all weapons. Indeed, the International Court of Justice has asserted that the rules and principles of IHL apply to 'all forms of warfare and to all kinds of weapons, those of the past, those of the present and *those of the future*'.[12] Moreover, IHL explicitly imposes a duty on States to determine that the employment of any new weapon, means or method of warfare will not violate their obligations under international law.[13] By explicitly stating or implicitly confirming that IHL applies to all new weapons, means and methods of warfare, these sources point to the conclusion that IHL applies to cyber warfare as well. This conclusion, which has been widely affirmed,[14] is

12 *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) [1996] ICJ Rep 226 (8 July 1996) [86] (emphasis added).

13 See AP I art 36.

14 The view that IHL applies to cyber warfare has been expressed, inter alia, by the EU, NATO, the GGE, and by many individual States. It has also held by the ICRC and by the experts who drafted the Tallinn Manuals. See *EU Council Conclusions*, General Affairs Council meeting, Doc. No. 11357/13 (25 June 2013) (stating the EU's position); Wales Summit Declaration issued by the heads of State and government participating in the meeting of NATO in Wales (5 September 2014) para 72, <www.nato.int/cps/en/natohq/official_texts_112964.htm> accessed 15 May 2024 (stating NATO's position); *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security* (14 July 2021) UN Doc A/76/135 para 71(f) (stating the GGE position); UNGA, *Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution* 73/266 (13 July 2021) UN Doc A/76/136 (containing contributions from 15 States); Brian J. Egan, 'International Law and Stability in Cyberspace' (2017) 35 *Berkeley J Intl L* 169, 172 (stating the US position); Jeremy Wright, 'Cyber and International Law in the 21st Century' (Chatham House, London, 23 May 2018) <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century> accessed 15 May 2024 (stating the UK position); French Ministry of the Armies, *International Law Applied to Operations in Cyberspace* (9 September 2019) (stating the French position); Roy Schöndorf, 'Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations' (2021) 97(1) Intl L Stud 395, 399 (stating Israel's position); *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts* (ICRC 2011) 36–39 <www.icrc.org/en/doc/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-en.pdf> accessed 15 May 2024; *Tallinn Manual 2.0* (n 8) r 80.

also merited because it corresponds with the humanitarian purpose of IHL, as it extends the protection afforded by this body of law to cover the risks posed by hostilities involving cyber operations.

That being said, in the case of cyber warfare IHL's capacity to accommodate change is tested to the extreme. The IHL framework governing the conduct of hostilities was designed to apply to methods and means of warfare involving the use of kinetic force in the physical world, and therefore makes an awkward fit for hostilities that consist of the manipulation of data in cyberspace. In fact, as we shall see, even some of the basic assumptions underlying IHL come into question, and categories and distinctions foundational to IHL –such as the notions of 'armed conflict', 'attack', and 'object', as well as the distinction between 'civilian object' and 'military objective'– are not easily retained when applied to cyber warfare.

3. Applying IHL to Technologies and Operations Veiled in Secrecy

The difficulty of adapting IHL to cyber warfare is compounded by the veil of secrecy enveloping cyber security operations. Law, after all, must be applied to facts. When the facts are not well known it is not possible to have a clear legal reading either. More precisely, key information needed in order to make an informed evaluation of cyber operations' compatibility with IHL is often lacking, including details about (*a*) the technology available, (*b*) the attacks conducted, (*c*) the identity of the parties conducting the attacks, as well as (*d*) the policies, guidelines, and rules that States apply in relation to cyber warfare, along with their reading of the applicable rules of IHL.

Information about the technological capabilities that exist or are under development is necessary to evaluate whether the methods and means of warfare facilitated by these technologies meet the requirements of IHL. In practice, however, States are rarely forthcoming about the offensive and defensive capabilities they already have or are developing for cyber warfare, and little is known about the types of cyber operations or cyber weapons available to non-State actors that are party to an armed conflict.

While there have been some instances in which States acknowledged that they had conducted cyber operations in the context of an armed

conflict,[15] States and other parties to armed conflicts are generally unwilling to divulge details about such operations that they have directed against their adversary, or about those which have been directed against them. Consequently, it is not properly known what attacks have been conducted using cyber technology, let alone what such attacks might have entailed. Likewise, since cyber operations are typically anonymous, it will in most cases be difficult, if not impossible, to identify the party responsible for the operation. Thus, it will often not be possible to determine if the operation was conducted by a party to an armed conflict and, consequentially, if IHL even applies.

The ambiguity surrounding belligerents' capabilities and practices in the field of cyber warfare also extends to the rules and regulations that they apply in relation to cyber operations. Indeed, even while some States have gone some way towards clarifying their views about the correct application of IHL to cyber warfare, they have disclosed only general aspects of their positions and have not provided a detailed account of the rules they apply or deem binding.[16]

Given that States are the authors of international law, the paucity of available information regarding their practice when it comes to cyber warfare, and the opaqueness of some of their legal positions on this matter undermine efforts to attain legal clarity. Commentators are left to speculate, based on the partial picture available to them, what such warfare does or could entail, and to propose, without the benefit of much supporting State practice or legal opinion, how it ought to be conducted.

---

15 Egan, *ibid* 172, for instance, refers to acknowledged US Military cyber operations in the context of the US's armed conflict with the Islamic State of Iraq and the Levant (ISIL). Some more recent examples, recorded by the Center for Strategic and International Studies (CSIS), which maintains a record of 'significant cyber incidents', include a February 2024 US operation against an Iranian military spy ship which US officials said was undertaken as part of the US's response to an Iranian drone strike that killed three U.S. soldiers in Jordan; a December 2023 Israeli cyber operation, reportedly disrupting some 70% of gas stations in Iran, that was said to have been undertaken in retaliation for aggressive actions by Iran and its proxies in the region; and a December 2023 Ukrainian cyber operation, which reportedly crippled Russia's largest water utility plant, that was said to be in retaliation for a Russian cyberattack against Ukraine's largest mobile phone provider, Kyivstar. See *Significant Cyber Incidents* (Center for Strategic and International Studies) <www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents> accessed 15 May 2024.

16 See eg, Egan *ibid*; Paul C. Ney, Jr, 'Some Considerations for Conducting Legal Reviews of U.S. Military Cyber Operations' (2020) 62 *Harvard Intl L J* Online 22, 35; Wright (n 13); French Ministry of the Armies (n 13); Schöndorf (n 13). See also Cherry and Pascucci (n 8).

4. Assessing whether Cyber Operations Occurred in the Context of Armed Conflict

IHL applies only in the context of an armed conflict. [17] Accordingly, the first thing to ascertain when considering if a given cyber operation is subject to IHL is whether the operation in question was conducted in the context of and with a nexus to an armed conflict.

Even when cyber operations occur against the backdrop of an existing armed conflict, it will not necessarily be possible to determine that they are in fact related to the armed conflict. Indeed, since the nature of cyber operations is such that the identity of the actor carrying them out may very well be unknown, there may be no grounds to assert that the operations were conducted by or on behalf of a party to an armed conflict. The severity of this attribution problem may have been alleviated to some degree by reported improvements in States' technical capabilities,[18] but where attribution and thus the connection to armed conflict remains in doubt, so too does the applicability of IHL. Of course, attribution is not a problem from the perspective of the actors who are themselves committing or orchestrating cyber operations: They have all the information necessary to determine what international legal framework is applicable to their operations and what rules they are therefore required to follow.[19]

Establishing a link to an armed conflict is still more problematic in cases where cyber warfare does not occur alongside other forms of hostilities. In such situations there arises the additional question of whether cyber operations can themselves constitute an armed conflict. In addressing this question, it is necessary to distinguish between the two types of armed conflict that are regulated by IHL, namely–international armed conflicts, occurring between States, and non-international armed conflicts, in which at least one of the belligerent parties is a non-State actor.

17 Diakonia International Humanitarian Law Centre, *Easy Guide to International Humanitarian Law* (Revised 4th ed, 2021) 5 <https://www.diakonia.se/ihl/news/easy-guide-to-international-humanitarian-law/> accessed 15 May 2024.

18 Schöndorf (n 13) 404, for instance, observed that concerns about reliable attribution are now'becoming more of a theoretical issue', since '[o]ver time, the attribution capabilities of States have improved, and even States with lesser capabilities have been able to rely on solid information provided by other States and by the private sector'.

19 ICRC Position Paper (n 5) 9.

An **international armed conflict** arises whenever there is a resort to armed force between States.[20] Accordingly, cyber warfare would constitute an international armed conflict only if (*a*) the cyber operations involved are attributable to a State, and (*b*) they amounted to a resort to armed force against another State.

Again, attribution can be difficult in the context of cyber warfare. It has been suggested that this difficulty might be mitigated to some extent by adopting appropriate legal presumptions.[21] Thus, for example, a State would be presumed responsible for any cyber operation originating from its governmental infrastructure unless it could prove otherwise. However, there is no basis in existing international law for such a presumption. Moreover, given the ease with which different guises can be assumed in cyberspace and the difficulty of shielding computer infrastructure from manipulation, the presumption could be extremely artificial and might be said to place an unreasonable burden on States.[22]

Besides the factual difficulties in determining the source of a cyber operation, the attribution of a cyber operation to a State may also be complicated by questions concerning the scope of States' legal responsibility for cyber operations that were not conducted directly by them but rather by private persons or groups. The potential attribution of acts of private agents to the State is not unique to cyber warfare. The general rule in this regard is that the actions of a non-State group are attributable to a State for the purpose of classifying an armed conflict involving that group and another State as an international armed

20 This commonly accepted definition of international armed conflict was articulated by the International Tribunal for the former Yugoslavia (ICTY) in *Prosecutor v. Tadic* (Interlocutory Appeal on Jurisdiction) ICTY-94-1-AR72 (2 October 1995) [70]. International treaties do not contain a detailed definition of international armed conflict. That said, GC I-IV common art 2 does establish that the conventions apply to any armed conflict which may arise between two or more States. AP I art 1(4) extends the scope of application to other situations, but this applies only in relation to States party to the Additional Protocol.

21 See Droege (n 4) 543.

22 Tallinn Manual 2.0 (n 8) r 15, para 13, 91 asserts that 'the mere fact that a cyber operation has been launched or otherwise originates from governmental cyber infrastructure, or that malware used against hacked cyber infrastructure is designed to 'report back' to another State's governmental cyber infrastructure, is usually insufficient evidence for attributing the operation to that State'. The Manual goes on to add that 'such usage can serve as an indication that the State in question may be associated with the operation'.

conflict, if the first State has 'overall control' over the group.[23] Adapting the test of 'overall control' to cyber warfare, where the relevant facts may be more difficult to establish, is likely to prove challenging and may be further complicated by the need to interpret the notion of 'control' in relation to actions and actors operating in cyberspace. Moreover, the test of 'overall control' applies only with respect to organized groups, a category that does not include individuals or loosely organized groups implementing cyber operations. The actions of such individuals, or insufficiently organized groups could be attributed to the State for the purpose of determining the existence of an international armed conflict, only if they were shown to be acting on specific instructions form that State.[24]

Assessing whether cyber operations satisfy the second criterion for an international armed conflict, namely that they amount to the resort to armed force against a State, presents another significant hurdle. The traditional conception of armed force is of hostilities involving means and methods of warfare entailing the use of kinetic force. Applying this conception to the act of developing and sending computer code is not a straightforward exercise. When can such acts be considered to amount to 'armed force'? There is broad agreement among commentators that cyber operations that lead to physical destruction parallel to the destruction produced by attacks employing kinetic force would amount to an armed attack.[25] However, cyber operations are capable of effecting other forms of harm. Rather than physically destroying a target system, they could be

23 See *Prosecutor v. Tadic* (Appeals Chamber Judgment) ICTY-94-1 (15 July 1999) [120]; *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)* (Judgment) [2007] ICJ Rep 2 (26 February 2007) [404]; *Prosecutor v. Lubanga* (Trial Chamber Judgment) ICC-01/04-01/06 (14 March 2012) [541]. See also, Tallinn Manual 2.0 (n 8) r 82, para 4, 381. The ICTY further clarified that more extensive and compelling evidence would be required to show that the State is genuinely in control of the organized group in cases where group is not acting from within the territory of the State in question. See *Tadic ibid* [138].

24 *Tadic ibid* [132], [137], [141], [145]; *Tallinn Manual 2.0 ibid* r 82, para 8, 382.

25 See *Commentary on the Third Geneva Convention: Convention (III) Relative to the Treatment of Prisoners of War* (2nd ed, ICRC 2020) (2020 Commentary on GC III), art 2, para 288; T*allinn Manual 2.0 ibid* r 82, para 16, 384 ; Droege (n 4) 546; Michael N. Schmitt, 'Classification of Cyber Conflict' (2012) 17(2) J Conflict & Sec L 251; Knut Dörmann, 'Applicability of the Additional Protocols to Computer Network Attacks' (ICRC, 2004) 3 <http://www.icrc.org/eng/resources/documents/misc/68lg92.htm> accessed 15 May 2024; Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (CUP 2012) 131; Nils Melzer, 'Cyberwarfare and International Law' (UNIDIR Resources Paper, 2011) 24.

used to impair its functioning. The harm thus caused would take direct effect not in the physical world but in cyberspace. Indeed, this type of cyber operation might very well go undetected, while the indirect effects of such an operation -which could, for example, disrupt the supply of vital resources (such as water, electricity or oil) or the provision of essential services- could be most harmful indeed. If IHL is to be interpreted in accordance with its underlying humanitarian purpose, then presumably cyber operations producing such grave humanitarian consequences ought to be considered to be within the ambit of armed force and thus subject to the protective provisions of IHL.

On the other hand, the classification of a situation as an armed conflict brings into play not only the restrictive provisions of IHL, but also its permissive aspects. IHL allows for -or at least does not prohibit- the intentional use of lethal force against certain categories of people (such as enemy combatants[26] and civilians directly participating in hostilities) and the intentional destruction of certain categories of property (military objectives), and also tolerates a degree of incidental harm to other categories of persons and objects ('collateral damage') that would all be prohibited by the law applicable outside of armed conflict.[27] Those seeking to restrict the scope of force legally permissible might therefore have good reason to favour a more restrictive approach in interpreting when cyber warfare amounts to resort to armed force. In any event, in the absence of State practice or clarification of States' legal reading (*opinio juris*) it remains an open question whether, and if so under what conditions, cyber warfare can be said to constitute resort to armed force even when not producing direct physical destruction.[28]

A **non-international armed conflict** exists whenever there is protracted armed violence, meaning armed violence of a certain degree of intensity, between governmental authorities and organized armed groups or

26 The term combatant applies only to fighters on behalf of the rival parties to an international armed conflict who would be entitled to prisoner of war (POW) status if captured by the adverse party. Fighters in a non-international armed conflict are not entitled to POW status but can be made the target of direct attack by the rival belligerent.

27 For elaboration on the distinction between the rules on the use of force applicable in the conduct of hostilities and in situations of law enforcement outside hostilities see eg, Diakonia International Humanitarian Law Centre (n 16) 17-22.

28 Droege (n 4) 545-549.

between such groups within a State.[29] In other words, in order for a situation to be classified as a non-international armed conflict it must entail armed violence involving at least one non-State actor where (*a*) the parties involved satisfy a minimum level of organization and (*b*) the armed violence reaches a minimum level of intensity.[30] Applying these criteria to cyber warfare raises several difficulties.

For one thing, the nature of virtually organized groups of the type active in cyber space –such as groups of hackers cooperating in joint cyber operations– is such that they will rarely, if ever, satisfy the requirement of a minimum level of organization as thus far understood. Under this requirement, the group should have a command structure with a level of hierarchy and discipline sufficient to enable it both to carry out sustained acts of warfare and to implement the basic rules of IHL.[31] It is difficult to see how groups whose members are linked only by virtual communication and who may never have met in person or even know each other's identity, would fit this mould.[32] For this reason it would seem that while the activities of such groups could certainly constitute criminal behaviour, it would be incorrect to say that they also amount to an engagement in armed conflict. However, this conclusion might be met with some unease when it is observed that the cyber operations conducted by virtually organized groups could potentially result in levels of harm and destruction akin to those produced by armed conflict.

When cyber operations indeed bring about levels of physical destruction comparable to those produced by kinetic operations, it would not seem contentious to say that they could meet the threshold of intensity required to bring a non-international armed conflict into play.[33] However, as with the criterion of resort to armed force discussed above in relation to international armed conflict, it is by no means clear when

29 This definition was articulated by the ICTY in *Prosecutor v. Tadic* (Decision on the Defence Motion for Interlocutory Appeal) ICTY-94-1-I (2 October 1995) [70].

30 See, *Commentary on the Third Geneva Convention: Convention (III) relative to the Treatment of Prisoners of War* (2nd ed, ICRC 2020) (2020 Commentary on GC III), art 3, para 455; *Prosecutor v. Tadić* (Trial Chamber Judgment) ICTY-94-1-T (7 May 1997) [562].

31 See, *Prosecutor v. Boskoski* (Trial Chamber Judgement) ICTY-04-82-T (10 July 2008) [199]–[203]; *Prosecutor v. Limaj* (Trial Chamber Judgement) ICTY-03-66-T (30 November 2005) [94]–[134]; *Prosecutor v. Haradinaj* (Trial Chamber Judgement) ICTY-04-84-T (3 April 2008) [60].

32 *Tallinn Manual 2.0* (*n 8*) r 83, paras 11-15, 389-392.

33 See however *ibid* r 83, para 7, 388 observing that 'cyber operations alone can trigger a non-international armed conflict in only rare cases', because they are unlikely to cross the intensity threshhold.

and under what conditions the harm engendered by cyber operations through the manipulation of computer networks (rather than direct physical destruction) might also be deemed of such intensity as to have generated a non-international armed conflict.[34] Here, again, instructive State practice and *opinio juris* are in short supply and humanitarian considerations do not point conclusively in favour of a particular interpretive approach.

5. Environmental Instruments

If occurring in the context of armed conflict, cyber operations would be subject to IHL, including in particular the IHL rules governing the conduct of hostilities. It is clear, however, that the application of these rules to operations involving the deployment of computer code in cyberspace, as opposed to the use of kinetic force in the physical world, is no simple matter.

The first challenge in this regard would be to determine what types of cyber operations would be subject to the rules governing the conduct of hostilities. This question is pertinent because of cyber operations' capacity to disrupt the functioning of key infrastructure without causing physical destruction of the type produced by traditional methods and means of warfare. With respect to the types of cyber operations that do fall within the conduct of hostilities framework it will then be necessary to consider how the relevant rules, and most fundamentally the principles of distinction, proportionality and precautions, are to be adapted and applied to cyber warfare.

5.1. When are Cyber Operations Subject to the Rules on the Conduct of Hostilities?

The rules on the conduct of hostilities codified in AP I are broadly recognized as being reflective of customary international law applicable both in international and non-international armed conflicts. [35] Most

34 *Ibid* r 83, para 10, 289.

35 For authoritative analysis of customary rules of IHL see, International Committee of the Red Cross, *Customary International Humanitarian Law,* Vol 1: Rules (Jean-Marie Henckaerts and Louise Doswald-Beck eds, CUP 2005). For a regularly updated online version of this study see, 'Customary IHL Database' (*ICRC*) <https://ihl-databases.icrc.org/en/customary-ihl> last accessed 15 May 2024 (ICRC Customary IHL Study).

of the specific rules contained in this framework are formulated as restrictions on those military operations that constitute an 'attack'.[36] However, it would be wrong to maintain that the rules on the conduct of hostilities apply only to cyber operations constituting an attack as defined in IHL. For one thing, it would be difficult to reconcile such a position with the fact that the provisions of AP I, reflective of customary international law, which establish the principles of distinction, proportionality and precautions all contain clauses relating to military operations in general.[37] If these clauses are not to be deemed superfluous, the core principles governing the conduct of hostilities should be understood to apply not only to attacks, but also to hostilities more broadly, i.e. to other military operations carried out in the context of an armed conflict with the purpose of harming the adversary.

Moreover, the IHL rules on the conduct of hostilities provide specific protection to certain types of objects, which prohibits not only attacks but also other harmful acts against those objects, including harmful cyber operations.[38] Thus, it is prohibited not only to attack and destroy objects indispensable to the survival of the population, but also to remove or render them useless,[39] including through cyber means and methods of warfare.[40] Simliarly, medical services must be respected and protected by parties carrying out cyber operations during armed conflicts, a protection which applies irrespective of whether the operation is an attack.[41]Accordingly, any cyber operation disrupting data belonging to a medical unit, which is essential for the unit to discharge its medical function, would be prohibited even if it did not cause any

36 Multiple references to 'attack' are found, notably, in AP I arts 51, 52, and 54–58. For elaboration see Michael N Schmitt, 'Cyber Operations and the *Jus in Bello*: Key Issues', (2011) 87 *Naval War College Intl L Stud* 91.

37 The formulation of the principle of distinction in AP I art 48 stipulates that the parties to an armed conflict '…shall direct their *operations* only against military objectives'. The first paragraph of AP I art 51 stipulates that civilians 'shall enjoy general protection against the dangers arising from *military operations*' and AP I art 57, para 1 instructs that 'in the conduct of *military operations*, constant care shall be taken to spare the civilian population, civilians and civilian objects' (emphasis added).

38 ICRC Position Paper (n 5) 7.

39 AP I art 54; AP II art 14; ICRC Customary IHL Study r 54.

40 ICRC Position Paper (n 5) 6.

41 *Ibid*. See also, GC I art 19; GC II art 12; GC IV art 18; AP I art 12; AP II art 11; ICRC Customary IHL Study rr 22–24.

physical damage or destruction.[42] Humanitarian personnel and relief consignments too must be respected and protected and should therefore not be subjected to cyber attacks or to other cyber operations that could adversely affect the delivery of the humanitarian assistance which they provide.[43]

All the same, since most of the rules governing the conduct of hostilities are indeed confined to cases of attacks, it is clearly important to ascertain what cyber operations would in fact amount to an attack. Article 49 of AP I, which reflects customary IHL, defines attacks as 'acts of violence against the adversary, whether in offence or in defence'. It is accepted that the term 'violence' refers here to the consequences of the attack and not to the means used to bring about those consequences: the sending of computer code, though not itself an act of physical violence, could nonetheless constitute an attack if producing a violent outcome. This view is reflected in the Tallinn Manuals which define 'cyber attack' as 'a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects'.[44] The majority of experts involved in drafting the Tallinn Manuals took the view that the notion of an 'object' for the purpose of this definition is limited to tangible things (individuals or physical objects), as opposed to intangibles such as digital data.[45] Even on this view, which others have disputed,[46] cyber attacks do encompass cyber operations against data when these will foreseeably result in the injury or death of individuals or damage or destruction of physical objects. This is the case, even while data are non-physical entities, because the individuals or objects that will foreseeably be harmed by the cyber operation are considered to be the 'object of attack'.[47]

A pressing question that this definition does not resolve, and which remains subject to debate is whether cyber operations that disrupt the functionality of an object (which does not benefit from specific protections such as those afforded, e.g., to medical services) might be

42 ICRC Position Paper (n 5) 8.

43 *Tallinn Manual 2.0* (n 8) r 80, para 4, 376; Gisel, Rodenhäuser and Dörmann (n 2) 329.

44 *Tallinn Manual 1.0* (n 8) r 30; *Tallinn Manual 2.0* (n 8) r 92, 415.

45 *Tallinn Manual 2.0* (*ibid*) r 92, para 6, 416; and r 100, para 6,437.

46 *Tallinn Manual 2.0* (*ibid*) r 100, para 7, 437; ICRC Position Paper (n 5) 8.

47 *Tallinn Manual 2.0* (*ibid*) r 92, para 6, 416.

deemed to constitute an attack even when they do not involve direct physical damage or destruction. Some have answered in the affirmative maintaining that an operation designed to disable a computer or a computer network during an armed conflict constitutes an attack as defined in IHL whether the object is disabled through destruction, by disruption of its functionality, or in any other way. This, they maintain, better accords with IHL's humanitarian purpose as it would extend protection against cyber operations that could disrupt critical infrastructure and services with dire humanitarian consequences.[48] Others have contended that this goes too far and that it would be unreasonable to maintain that any interference with a computer system would amount to an attack that brings all the rules governing the conduct of hostilities into play.[49]

While the exact line of demarcation between cyber operations amounting to an attack and those which do not remains elusive, some considerations can help to distinguish between them. For one thing, in cases where the reasonably foreseeable harm caused by a cyber operation is a disruption of functionality that would require replacement of physical components to restore functionality (effectively causing damage to a physical object), the prevailing view is that it constitutes an attack.[50] Furthermore, since the IHL concept of attack does not apply to non-physical means of psychological or economic warfare, such as the dissemination of propaganda or the establishment of an embargo,[51] cyber operations equivalent to such forms of 'warfare' do not amount to an attack.[52] Unlike attacks, which may never justifiably be directed at civilians, IHL does

48 ICRC, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, 32nd International Conference of the Red Cross and Red Crescent (8–10 December 2015) 41–42; Laurent Gisel, Tilman Rodenhäuser and Knut Dörmann (n 2) 313. The position is based also on an inference from the fact that the definition of 'military objectives' in Article 52(2) of AP I refers not only to destruction or capture but also to 'neutralization' as a possible result of an attack, implying that the notion of 'attack' also encompasses operations that impair the functioning of an object (ie neutralize it).

49 Schmitt (n 35) 95–96.

50 *Tallinn Manual 2.0* (n 8) r 92, para 10, 417. Some experts have further taken the view that disrupting functionality can amount to an attack where reinstallation of the operating system or of particular data is required in order for the targeted cyber infrastructure to perform the function for which it was designed. Ibid, para 11, 417-418.

51 See, Michael Bothe, Karl Josef Partsch and Waldemar A. Solf, N*ew Rules for Victims of Armed Conflicts: Commentary to the Two 1977 Protocols Additional to the Geneva Conventions of 1949* (Martinus Nijhoff 1982) 289.

52 Schmitt (n 36) 91.

not prohibit directing blockades and economic sanctions at the civilian population. Accordingly, cyber operations tantamount to economic sanctions cannot be said to constitute an attack.[53] Espionage too does not constitute an attack, and so the collection of data through cyber operations –as opposed to manipulating or destroying data to subvert functionality or directing a system to cause physical damage or destroy physical objects– is not an attack.[54] Moreover, just as interferences with communications such as the jamming of radio or television broadcasts are not considered an attack under IHL and can therefore be directed at civilian communication systems as well, so too not every disruption of computer-based communication systems would constitute an attack.[55] Of course, some types of interference with computer-based communications could have far reaching impact (e.g. disrupting the operation of financial institutions) and it therefore remains necessary to clarify exactly when, if ever, such interferences would constitute an attack.

Relatedly, and as noted, there is ongoing disagreement as to whether data, or at least some forms of data, should be regarded as objects for the purpose of applying IHL to cyber operations during armed conflict.[56] A cyber operation directed at data *per se* (as opposed to one that manipulates data as a means to target a physical object) could only be regarded as an attack if the concerned data are considered to be an object. As elaborated in the following section, this dispute has significant implications when it comes to assessing whether cyber operations directed at civilian data are in breach of the principal of distinction.

5.2. Applying the Principle of Distinction in Cyberspace

Under the principle of distinction, the parties to an armed conflict are obligated to distinguish at all times between the civilian population and combatants, and between civilian objects and military objectives, and may

53 Droege (n 4) 559.

54 ICRC, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, *32nd International Conference of the Red Cross and Red Crescent* (8–10 December 2015) 41-42; Tallinn Manual 2.0 (n 8) r 92, para 14, 418.

55 ICRC *ibid; Tallinn Manual 2.0 ibid.*

56 Eg, ICRC Position Paper (n 5) 8; *Tallinn Manual 2.0 ibid*, r 100, paras 6-7, 437; Gisel, Rodenhäuser and Dörmann (n 2) 317–320.

direct their operations only against military objectives.[57] Accordingly, cyber operations should only be directed at military objectives, namely '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'.[58] Any object that does not fall within this definition is considered a civilian object and may not be the target of an attack.[59] Moreover, in case of doubt whether an object normally dedicated to civilian purposes is being used to make an effective contribution to military action, it should be presumed not to be so used and, consequently, may not be made the target of an attack.[60]

As noted, there are currently diverging views when it comes to applying the principle of distinction to cyber operations directed at civilian data *per se*. On the view that data, being intangible, are not an object, such operations do not constitute an attack and the principle of distinction consequently does not apply to them.[61] Noting that certain civilian data –such as biometric data, social security data, tax records, bank accounts, companies' client files or election lists and records– are now essential for civilian life to function, others have insisted that such data should be regarded as a civilian object that is protected from attack.[62] Proponants of the latter view have observed that operations deleting or tampering with essential civilian data could cause more harm to civilians than the destruction of physical objects. On these grounds they argue that excluding such data from the protection afforded by IHL to civilian objects would result in a protection gap at odds with the object and purpose of IHL.[63]

57 AP I art 48; ICRC Customary IHL Study rr 1, 7.

58 AP I art 52(1); ICRC Customary IHL Study r 8.

59 AP I art 52(1); ICRC Customary IHL Study r 9.

60 AP I art 52(3); T*allinn Manual 2.0* (n 8) r 95, para 1, 424, and r 102, para 5, 448; Ryan Goodman, 'Clear Error in the Defense Department's Law of War Manual: On Presumptions of Civilian Status' (*Just Security,* 9 February 2022) <https://www.justsecurity.org/80147/clear-error-in-the-defense-departments-law-of-war-manual-on-presumptions-of-civilian-status/> last accessed 15 May 2024.

61 As observed at text to nn 37–42, in the case of data relating to objects indispensable to survival of the population, and to medical services and humanitarian relief operations, IHL extends special protection that applies beyond cases of attack.

62 ICRC Position Paper (n 5) 8, *Tallinn Manual 2.0 ibid*, r 100, para 7, 437.

63 ICRC Position Paper (*ibid*).

Beyond disputes about extending the notion of civilian object to certain non-physical entities, a major difficulty in applying the principles of distinction to cyber warfare lies in the fact that most of the cyber infrastructure utilized for military purposes is dual use, serving also for civilian purposes. The currently prevailing position is that dual use objects are military objectives because of the military purpose they serve.[64] When applied to cyberspace, this position implies that many elements of international cyber infrastructure should be classified as military objectives and (subject to other IHL rules) could be susceptible to attack.[65] To be sure, where the military objective of a cyber attack contains clearly distinguishable civilian components, these components should be treated as civilian objects, rather than as part of the military objective,[66] however it will not always be possible to distinguish the civilian and military components of an objective. Accordingly, the cables, nodes, routers, and satellites on which so many civilian systems depend would all be deemed military objectives because they have the dual function of transmitting military information. With so many objects in the cyber realm thus considered military objectives, the principle of distinction –which is conceived as the foundational rule for shielding civilians from the dangers arising from hostilities– is at risk of becoming largely devoid of protective value. Whatever protection that IHL might provide to civilian cyber infrastructure and to the civilian systems and services dependent on it would have to be derived from the principles of proportionality and precautions.

Even civilian cyber infrastructure that is not dual use and which *would* therefore be protected from direct attack might nevertheless come to harm because of the interconnectedness of cyberspace. In order to avoid this outcome, and in accordance with the prohibition on indiscriminate attacks,[67] belligerent parties are prohibited from employing cyber weapons that are indiscriminate by nature, such as malware computer programmes that replicate without control (viruses, worms) and whose harmful effects could not be limited as required by IHL.[68] Furthermore,

64 *Tallinn Manual 2.0* (n 8) r 100, para 10, 438, and r 101, para 1, 445.

65 *Ibid*, r 101, para, 4, 446.

66 r 101, para 3, 445; Gisel, Rodenhäuser and Dörmann (n 2) 321.

67 AP I 51(4); ICRC Customary IHL Study rr 11–12.

68 *Tallinn Manual 2.0* (n 8) r 105.

a belligerent intending to mount a cyber attack would have to first verify that in the given circumstances, the cyber weapon employed can be and is in fact directed at a military objective and that its effects can be limited as required by IHL.[69]

The wide-ranging list of military objectives in cyber warfare gives rise to questions concerning the geographical limits of the armed conflict. After all, cyber operations can utilize cyber infrastructure located anywhere in the world and could involve thousands or even millions of computers in diverse locations around the globe. If all such infrastructure were to be deemed a military objective, an armed conflict involving cyber warfare could be expanded to cover every corner of the Earth. Every cyber war would be a potential cyber world war. In international armed conflicts the consequences would be checked to some degree by the laws of neutrality, which would limit the belligerent States' right to attack infrastructure located in the territory of a neutral State to those cases where the neutral State itself fails to terminate breaches of neutrality emanating from its territory; where such breaches constitute a serious and immediate threat to the attacked State's security; and when there is no other feasible and timely alternative response available.[70] In non-international armed conflicts, in which the law of neutrality is not applicable, questions about the geographical limitations of the battlefield are the subject of ongoing debate and become all the more vexing when the conflict involves cyber warfare.[71]

5.3. Applying the Principle of Proportionality in Cyberspace

Under the principle of proportionality an attack is prohibited if it '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'.[72] Here again a key question when applying the principle to cyber warfare will be to determine to what extent the term 'damage' encompasses loss of functionality. In view of the severity

69 *Ibid*, r 111.

70 *Ibid*, rr 151–153, 556–561.

71 *Ibid* para 3, 379.

72 AP I 51(5)(b); ICRC Customary IHL Study r 14. For application of the rule to cyberwarfare see *Tallinn Manual 2.0* (n 8) r 113.

of the consequences that may arise when the functionality of civilian infrastructure is disrupted, it seems only reasonable that such harm should figure in the proportionality calculus. On the other hand, and as already noted, it remains to be clarified exactly what types of disruptions to functionality fall within the relevant category of damage.

A further challenge in applying the principle of proportionality would be to determine whether the incidental damage to civilian objects that may be expected is excessive in relation to the military advantage anticipated. To be sure, the exercise of weighing expected harm to civilians or civilian objects against anticipated military advantage is always problematic, but in the case of cyber warfare the problems are exacerbated by the difficulty to assess with any accuracy what scope of incidental damage can be expected. This is so both because cyber operations are a relatively novel phenomenon and so little is known about their impact, and because the interconnected nature of cyberspace makes it particularly difficult to foresee all of the possible effects of such operations.

5.4. Applying the Principle of Precaution in Cyberspace

IHL requires belligerents to take precautions in attack,[73] as well as precautions against the effects of attack.[74]

Precautions in attack are mandated by a general rule, applicable to all military operations, whereby constant care must be taken to spare the civilian population and civilian objects,[75] and by additional rules establishing specific precautionary requirements. Among other things, these rules require those who plan or decide upon an attack to do everything feasible to verify that targets are military objectives[76] and to take all feasible precautions in the choice of means and methods of warfare with a view to avoiding and in any event minimizing incidental harm to civilians.[77] Belligerents are further required to cancel or suspend

73 AP I art 58; ICRC Customary IHL Study r 15.

74 AP I art 58; ICRC Customary IHL Study r 22.

75 AP I art 57(1); ICRC Customary IHL Study r 15. For application of the rule to cyberwarfare see *Tallinn Manual 2.0* (n 8) r 114.

76 AP I art 57(2)(a)(i); ICRC Customary IHL Study rr 16; *Tallinn Manual 2.0* (*ibid*) r 115.

77 AP I art 57(2)(a)(ii); ICRC Customary IHL Study rr 17; *Tallinn Manual 2.0* (*ibid*) r 116.

an attack if it becomes apparent that it will entail a breach of the principle of proportionality.[78]

In light of these rules, a party to an armed conflict planning to implement a cyber attack would have to do everything feasible to gain the information necessary to verify that the projected target is a military objective and to ascertain that the attack will not cause excessive harm. This may require employing technical experts to analyse the target network and the systems with which it is interconnected as best possible. When the expertise necessary to gain and properly to evaluate the required information is missing, the attack would need to be avoided altogether. In any event, attacks would have to be limited to those targets about which sufficient information is available.[79]

In certain circumstances, the duty to choose means and methods of warfare with a view to minimizing incidental harm to civilians could in fact require belligerents to pursue their military objective via cyber attack rather than resorting to more destructive means involving kinetic force.

The duty to take precautions against the effects of attacks requires that, to the maximum extent feasible, the parties to an armed conflict will endeavour to keep military objectives apart from civilians and civilian objects and will take other necessary precautions to protect civilians and civilian objects under their control against the dangers resulting from military operations.

In principle belligerents may thus be required to do everything feasible to separate their military and civilian cyber infrastructure. In practice, however, military and civilian cyber infrastructures are so thoroughly interwoven that the endeavour to separate them is not likely to be deemed feasible. Perhaps more promisingly, belligerents would also need to take all feasible measures to ensure that critical civilian infrastructure will be protected as much as possible from the effects of cyber attacks, e.g. by ensuring that necessary data is safely stored and effectively backed-up and by providing for timely repair of civilian systems that come to harm.

78 AP I art 57(2)(b); ICRC Customary IHL Study rr 18–19; *Tallinn Manual 2.0* (*ibid*) r 117, 119.

79 Droege (n 4) 574.

6. Conclusion

Cyber warfare involves operations that consist not of kinetic force employed in the physical world but of electronic communication occurring in a space of virtual reality. Yet even while unfolding in a notional environment, this form of warfare does not occur in a legal void. Indeed, since cyber operations can have very real and far-reaching implications there is wide recognition that they must be regulated by law, and that when they occur in the context of an armed conflict they are governed by IHL. However, the recognition that IHL applies invites many questions about how it is to be applied to cyber warfare. Despite some notable efforts to address these questions, they remain largely unsettled.

Because of the shroud of secrecy surrounding cyber operations, and because they occur in an environment and involve methods and means of warfare so drastically different from those which IHL has evolved to regulate, it will often be difficult even to ascertain whether they are occurring within and in connection to an armed conflict. Even when this is established and the applicability of IHL rules on the conduct of hostilities is not in doubt, it is not entirely clear which cyber operations would be subject to these rules. Nor is there any clarity as to how IHL's long established rules are to be adapted to this new form of warfare.

From a humanitarian perspective it is of the utmost importance that these questions be answered and that IHL be applied in such manner as to provide civilians and civilian infrastructure with effective protection from the harmful effects of cyber warfare. This will require careful interpretation of existing rules in light of the underlying humanitarian purpose of IHL and may also necessitate the development of some more stringent rules to ensure that humanitarian values will not be compromised.

Bibliography

Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro) (Judgment) [2007] ICJ Rep 2.

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

Cherry LM and Pascucci PP, 'International Law in Cyberspace' (American Bar Association, 27 January 2023) https://www.americanbar.org/groups/law_national_security/publications/aba-standing-committee-on-law-and-national-security-60-th-anniversary-an-anthology/international-law-in-cyberspace/ accessed 15 May 2024.

Commentary on the Third Geneva Convention: Convention (III) relative to the Treatment of Prisoners of War (2nd edn, ICRC 2020).

d'Aspremont J, *The Discourse on Customary International Law* (OUP 2021).

Diamond E, 'Applying International Humanitarian Law to Cyber Warfare' in Pnina Sharvit Baruch and Anat Kurz (eds), *Law and National Security: Selected Issues* (INSS Memorandum 138, INSS 2014).

Dinniss HH, *Cyber Warfare and the Laws of War* (CUP 2012).

Diakonia International Humanitarian Law Centre, *Easy Guide to International Humanitarian Law* (4th rev edn, 2021) https://www.diakonia.se/ihl/news/easy-guide-to-international-humanitarian-law/ accessed 15 May 2024.

Droege C, 'Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians' (2012) 94(886) *International Review of the Red Cross* 533.

Dörmann K, 'Applicability of the Additional Protocols to Computer Network Attacks' (ICRC 2004) http://www.icrc.org/eng/resources/documents/misc/68lg92.htm accessed 15 May 2024.

Egan BJ, 'International Law and Stability in Cyberspace' (2017) 35 *Berkeley Journal of International Law* 169.

European Union Council, *EU Council Conclusions* (General Affairs Council, Doc No 11357/13, 25 June 2013).

French Ministry of the Armies, *International Law Applied to Operations in Cyberspace* (9 September 2019).

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

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

Geneva Convention (III) relative to the Treatment of Prisoners of War (12 August 1949) 75 UNTS 135.

Geneva Convention (IV) relative to the Protection of Civilian Persons in Time of War (12 August 1949) 75 UNTS 287.

Gisel L, Rodenhäuser T and Dörmann K, 'Twenty Years On: International Humanitarian Law and the Protection of Civilians against the Effects of Cyber Operations during Armed Conflicts' (2020) 102(913) *International Review of the Red Cross* 287.

Goodman R, 'Clear Error in the Defense Department's Law of War Manual: On Presumptions of Civilian Status' (*Just Security*, 9 February 2022) https://www.justsecurity.org/80147/clear-error-in-the-defense-departments-law-of-war-manual-on-presumptions-of-civilian-status/ accessed 15 May 2024.

Hague Convention (IV) Respecting the Laws and Customs of War on Land and its Annex (18 October 1907) 205 CTS 277.

Henckaerts J-M and Doswald-Beck L (eds), *Customary International Humanitarian Law*, Vol I: Rules (CUP 2005).

International Committee of the Red Cross, *International Humanitarian Law and Cyber*

Operations during Armed Conflicts (Position Paper, ICRC 2019) https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts accessed 12 May 2024.

International Committee of the Red Cross, *International Humanitarian Law and the Challenges of Contemporary Armed Conflict*s (ICRC 2011).

International Committee of the Red Cross, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts* (32nd International Conference of the Red Cross and Red Crescent, 8–10 December 2015).

International Tribunal for the Former Yugoslavia, *Prosecutor v Tadić* (Interlocutory Appeal on Jurisdiction) ICTY-94-1-AR72 (2 October 1995).

Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion) [1996] ICJ Rep 226.

Melzer N, 'Cyberwarfare and International Law' (*UNIDIR Resources Paper*, 2011).

Ney PC Jr, 'Some Considerations for Conducting Legal Reviews of U.S. Military Cyber Operations' (2020) 62 *Harvard International Law Journal Online* 22.

Oxford English Dictionary, 'Cyberspace' (OED Online, May 2024) <www.oed.com> accessed 15 May 2024.

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

Prosecutor v Boskoski and Tarčulovski (Trial Chamber Judgment) ICTY-04-82-T (10 July 2008).

Prosecutor v Haradinaj (Trial Chamber Judgment) ICTY-04-84-T (3 April 2008).

Prosecutor v Limaj (Trial Chamber Judgment) ICTY-03-66-T (30 November 2005).

Prosecutor v Lubanga Dyilo (Trial Chamber Judgment) ICC-01/04-01/06 (14 March 2012).

Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II) 1125 UNTS 609.

Schmitt MN (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP 2013).

Schmitt MN and Vihul L (eds), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, CUP 2017).

Schmitt MN, 'Classification of Cyber Conflict' (2012) 17 *Journal of Conflict and Security Law* 251.

Schmitt MN, 'Cyber Operations and the Jus in Bello: Key Issues' (2011) 87 *Naval War College International Law Studies* 91.

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

United Nations General Assembly, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace* UN Doc A/76/135 (14 July 2021).

United Nations General Assembly, *Official Compendium of Voluntary National Contributions* UN Doc A/76/136 (13 July 2021).

United Nations General Assembly, *Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security* UN Doc A/75/816 (18 March 2021).

NATO, *Wales Summit Declaration* (5 September 2014) <www.nato.int> accessed 15 May 2024.

Wright J, 'Cyber and International Law in the 21st Century' (Chatham House, 23 May 2018) https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century accessed 15 May 2024.

Chapter III: Terrorism and International Humanitarian Law

Onur Dur[1]

Abstract

Terrorization of civilians assumes targeting the morale of the civilian population as a legitimate military goal.[2] Therefore, such a concept exacerbates the civilian casualties by diluting the constraints imposed by cardinal principles of IHL, more particularly, the principle of distinction during the hostilities. As this line of thought erodes the backbone of IHL, namely, the principle of distinction, it is especially dangerous to adopt such a concept, as it imperils the protection of civilians in armed conflict and also further risks the politicization of IHL, the same as counter-terrorism law. This chapter focuses on the prohibition of terrorism under international humanitarian law (IHL) by excluding the counter-terrorism law prohibition of terrorism in peacetime.

1. Historic Evolution of the Prohibition of Terrorism in Armed Conflict until the Geneva Conventions of 1949

One of the first technological innovations that changed the battlefields was the introduction of airplanes to the hostilities. For instance, the first actual use of an airplane in an actual armed conflict was noted in 1911 during the war between Italy and the Ottoman Empire in Libya. The Italian press mentioned that the aerial bombardment 'terrorized the Turks'.[3]

The use of airplanes was significant because such development enlarged the geographic scope of the battlefield, and belligerents had access to

1 Assistant Professor of International Law at the Social Sciences University of Ankara.

2 Agnieszka Jachec-Neale, *The Concept of Military Objectives in International Law and Targeting Practice* (Routledge 2014) 252.

3 James Wilford Garner, *International Law and The World War Volume I* (Longmans 1920) 459.

rear areas far away from the actual conflict lines.[4] Starting with the introduction of airplanes to the war theater, this part traces the early stages of the prohibition of terrorism under IHL.

1.1. World War I

During the World War I, the potential destruction by planes upon enemy cities seemed tempting for the generals of the Royal Air Force of the United Kingdom, while the Prime Minister, W. Churchill, was disagreeing.[5] Such a view defending the terrorization of the enemy through aerial bombardments had its nuances. For example, General Trenchard of the RAF was advocating the terrorization of industrial workers of the enemy.[6] Meanwhile, General Harris was contending the terrorization of enemy civilians would bring early surrender of the enemy.[7] This disagreement influenced the dominant position among RAF commanders until the end of World War II.

In the state practice throughout the World War I, it can be seen that targeting enemy civilians would cause panic among the enemy civilians at first. However, such panic and terror would easily backfire; namely, angered civilians supported their governments more, even pushing for retaliations against the enemy.[8] This was the case when the German Air Force bombed London in 1917, hoping to break the morale of the British public.[9] The impact of aerial bombardment during the war was minimal;[10] however, the psychological effect on the society was significant.[11]

At the end of World War I, the victorious states entertained the project of establishing a war crimes tribunal for the crimes committed by the

4 Robert A Pape, *Bombing to Win: Air Power and Coercion in War* (Cornell University Press 1996) 62.

5 Tami Davis Biddle, *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas about Strategic Bombing, 1914–1945* (Princeton University Press 2004) 79.

6 *Ibid* 96.

7 James Molony Spaight, *Air Power and War Rights* (3rd edn, Longmans 1947) 14.

8 Morton William Royse, *Aerial Bombardment and the International Regulation of Warfare* (Harold Vinal 1928) 214.

9 Tami Davis Biddle, 'Strategic Bombardment: Expectation, Theory and Practice in the Early Twentieth Century' in Matthew Evangelista and Henry Shue (eds), *The American Way of Bombing: Changing Ethical and Legal Norms, from Flying Fortresses to Drones* (Cornell University Press 2014) 31.

10 *Ibid* 33.

11 Spaight 5.

Central Powers. For that purpose, 1919 Commission on Responsibilities was established to work on the legal framework for the said tribunal.[12] As a result, the Committee on Responsibilities identified 32 types of war crimes; one of them was 'murder and massacres; systematic terrorism'.[13] When we take a closer look at the final report of the Committee, the use of 'terrorism' in that work was more descriptive in manner by illustrating the evil character of the enemy than in a normative sense.[14] Such a war crimes tribunal project was not properly implemented. The Leipzig Trials did not produce a judgement on the war crime of terrorism.[15]

1.2. From World War I to World War II

During the interwar period, the idea of air superiority was producing the first concrete results in military aviation technology and military doctrines. The popularization of air forces in the militaries in the aftermath of the World War I forced states to negotiate and set new rules for aerial warfare. One of the first concrete efforts in this sense was the acceptance of the Hague Rules of Aerial Warfare (HRAW) in 1923 by major powers.

Despite the negotiation and acceptance of HRAW by the leading militaries, such states did not ratify HRAW, so it remained a non-binding instrument due to the divergent national positions prioritizing national interests over a shared humanitarian concern to protect civilians.[16] Nevertheless, HRAW remained as an important instrument for the regulation of aerial warfare. About HRAW, Toman observed that 'to a great extent, they correspond to the customary rules and general principles underlying the conventions on the law of war on land and at sea'.[17] After a careful analysis of the individual provisions of HRAW, this view is still supported by experts.[18] In the judicial decisions, one example

12 Mineichirō Adatci, 'Commission on the Responsibility of the Authors of the War and on Enforcement of Penalties' (1920) 14 *American Journal of International Law* 95, 95.

13 *Ibid* 114.

14 *Ibid* 113.

15 M Cherif Bassiouni, 'The United Nations Commission of Experts Established Pursuant to Security Council Resolution 780 (1992)' (1994) 88 *American Journal of International Law* 784, 786.

16 Hays Parks, 'Air War and the Law of War' (1990) 32 *Air Force Law Journal* 1, 31.

17 Dietrich Schindler and Jiří Toman, *The Laws of Armed Conflicts: A Collection of Conventions, Resolutions, and Other Documents* (3rd edn, Martinus Nijhoff 2004) 315.

18 Michael N Schmitt, 'Air Warfare' in Andrew Clapham and Paola Gaeta (eds), *The Oxford Handbook of International Law in Armed Conflict* (Oxford University Press 2014) 122.

on the value of HRAW could be the *Shimoda* case before the Tokyo District Court, which took HRAW into account as an equivalent to an international treaty.[19]

The novel nature of the HRAW was also about the prohibition of terrorism. In article 22 of HRAW, it was stipulated that 'Aerial bombardment for the purpose of terrorizing the civilian population, of destroying or damaging private property not of a military character, or of injuring non-combatants is prohibited'.[20]

Article 22 of HRAW for the first time set a limitation on aerial bombardment without military justification. In the absence of such provision, destroying the morale of enemy civilians could be accepted as a legitimate military objective.[21] Such an assumption resulted in the humanitarian catastrophe during World War II.

The wording of article 22 of HRAW left a substantial mark on the subsequent legal endeavors to prohibit terrorism in armed conflict. For instance, the negotiations at the XIXth International Conference of the Red Cross in New Delhi in 1957, where ICRC's Draft Rules for the Limitation of the Dangers Incurred by the Civilian Population in Time of War were adopted. Later, the wording of Article 51 (2) of Additional Protocol I to the Geneva Conventions, which prohibits 'acts or threats of violence the primary purpose of which is to spread terror among civilian population'[22] is very similar to that of Article 22 of HRAW.[23]

This optimistic reading also reveals the shortcoming of article 22 of HRAW during the interwar years. Royse contended that 'Article 22 as it stands today expresses, perhaps, world opinion, but at best it is only an expression of a general desire rather than a genuine world-wide social sanction. A revised Article 22 will be necessary for sufficient protection to civilian populations against terrorization'.[24] In addition, technological constraints undermined this provision, especially during World War II.

19 Ben Saul, *Defining Terrorism in International Law* (Oxford University Press 2006) 275.

20 Schindler and Toman, *The Laws of Armed Conflicts* 319.

21 Hersch Lauterpacht, 'The Problem of the Revision of the Law of War' (1952) 29 *British Year Book of International Law* 360, 368.

22 AP I, Art 51(2).

23 Remigiusz Bierzanek, '1923 Hague Rules' in Natalino Ronzitti and Gabriella Venturini (eds), *The Law of Air Warfare: Contemporary Issues* (Eleven International Publishing 2006), 403.

24 Royse, *Aerial Bombardment and International Regulation of Warfare* 221.

For example, the air forces preferred night operations in order to avoid air defense systems. However, such preference impaired the ability to strike targets with distinction due to the absence of advanced built-in radar in the fighter planes.[25]

Finally, despite the collapse of the League of Nations system during the interwar period, the International Law Association adopted a Draft Convention for the Protection of Civilian Populations against the New Engines of War. Article 4 of this draft also suggested, 'Aerial bombardment for the purpose of terrorizing the civilian population is expressly prohibited'.[26]

1.3. World War II and Aftermath

Air power doctrine was theorized since the introduction of airplanes to the armies. However, such a theory was truly transformed into practice during the World War II. In this part, the air power doctrine will be briefly explained, and its impact on the military circles resulting in the terror bombing campaigns will be demonstrated.

1.3.1. Air Power Doctrine and its Application during the Second World War

Until the Second World War, the air power doctrine was not materialized in the actual theater of war; rather, it stayed as a promising idea. With the advancement of aviation and weapons technology, the air forces were ready to test such hypotheses famously stipulated by Douhet. Douhet suggests that 'a complete breakdown of the social structure cannot but take place in a country subjected to this kind of merciless pounding from the air. The time would soon come when, to put an end to horror and suffering, the people themselves, driven by the instinct of self-preservation, would rise up and demand an end to the war before their army and navy had time to mobilize at all!'[27]

Through different interpretations of Douhet's air power doctrine, such strategy was embraced to different extents by the belligerents during the

25 Williams P. Whitcomb, 'Legitimate Targets in Aerial Bombardment' (1929) 23 *American Journal of International Law* 3, 581.

26 Schindler and Toman, *The Laws of Armed Conflicts* 332.

27 RGiulio Douhet, *The Command of the Air* (Translated Dino Ferrari, Coward-McCann 1942) 58.

Second World War. For example, at the beginning of the war, Germany considered the Luftwaffe as the secondary force to complement the land forces.[28] Terror bombing was considered as a tool for reprisal rather than main strategy for the German air force.[29] Nevertheless, such reciprocal reprisals were committed at a widespread scale by both sides during the war. Americans shifted their position throughout the war. In the beginning, they consider the terror bombardments as illegal; for instance, in 1941, the manual entitled 'Tentative Instructions for the Navy of the United States Governing Maritime and Aerial Warfare' stipulated that 'Aerial bombardment for the purpose of terrorizing the civilian population, of destroying or damaging private property not of a military character, or of injuring noncombatants is prohibited. In any bombardment every practicable precaution should be taken to avoid injury to civilians'.[30] However, towards the end of the war, Americans were inclined to adopt terror bombings as a preferred strategy.[31] When we look at the British approach, one can observe the readiness to adopt terror bombing to destroy enemy civilians' morale and the disruption of the war-supporting activities of the enemy among the military circles even before World War II.[32] Although at the beginning of the war, British politicians were vehemently opposed to terror bombardments due to the haunting legacy of the Guernica campaign,[33] the Royal Air Force swiftly embraced the air power doctrine at the later stages of the war.[34]

1.4. War Crimes Trials after the World War II

For the war crime prosecutions, the Allies created the Nuremberg and Tokyo trials. The 'Systematic atrocities against or systematic terrorism

28 Jeffrey W Legro, *Cooperation under Fire: Anglo-German Restraint during World War II* (Cornell University Press 2013) 112.

29 *Ibid* 112.

30 Hays Parks, 'Air War and the Law of War' (1990) 32 *Air Force Law Journal* 1, 38.

31 Nathan A Canestaro, 'Legal and Policy Constraints on the Conduct of Aerial Precision Warfare' (2004) 37 *Vanderbilt Journal of Transnational Law* 431, 443.

32 Stephen A Garrett, 'Airpower and Non-Combatant Immunity: The Road to Dresden' in Igor Primoratz (ed), *Civilian Immunity in War* (Oxford University Press 2007) 163.

33 *Ibid* 167–168.

34 Horst Boog, *The Conduct of the Air War in the Second World War: An International Comparison: Proceedings of the International Conference of Historians in Freiburg im Breisgau, Federal Republic of Germany from 29 August to 2 September 1988* (Berg 1992) 21.

or ill-treatment or murder of civilians' was also considered to be listed as a war crime in the Charter of the Nuremberg Tribunal upon the suggestion made by the British delegation.[35] However, such a suggestion did not materialize.

In the judgments rendered by both the Nuremberg and Tokyo Tribunals. None of the accused persons were ever condemned for terrorism in armed conflict. The use of 'terrorism' was only about the description of the Nazi barbarity in these judgments.[36] It was a missed opportunity for the development of the prohibition of terrorism in armed conflict.

2. IHL Rules Prohibiting Terrorism

As the terror bombing policy did not yield the intended result during the World War II, the drafters of the Geneva Conventions of 1949 had a window of opportunity to enact more detailed and comprehensive provisions on the regulation of armed conflict,[37] which also included the prohibition of terrorism. In this part, the IHL provisions prohibiting terrorism will be explained in chronological order.

2.1. Article 33 of GC IV of 1949

Article 33 of the GC IV is indeed a novelty by simply prohibiting terrorism in armed conflict for the first time with a legally binding rule. The subsequent provisions included in the Additional Protocols of 1977 reinforced this modest beginning of the prohibition of terrorism in armed conflict.

Article 33 of the Geneva Convention IV prohibits collective punishment and terrorism as follows:

'No protected person may be punished for an offence he or she has not personally committed. Collective penalties and likewise all measures of intimidation or of terrorism are prohibited.'[38]

35 Saul 284.

36 *Ibid* 285–286.

37 Otfried Nippold, *The Development of International Law After the World War* (Translated Amos S Hershey, The Lawbook Exchange 2004) 144.

38 Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949 75 U.N.T.S. 287 (GC IV), 309.

In the Pictet commentary, this provision was elaborated as follows:

> During past conflicts, the infliction of collective penalties has been intended to forestall breaches of the law rather than to repress them; in resorting to intimidatory measures to terrorise the population, the belligerents hoped to prevent hostile acts. Far from achieving the desired effect, however, such practices, by reason of their excessive severity and cruelty, kept alive and strengthened the spirit of resistance. They strike at guilty and innocent alike. They are opposed to all principles based on humanity and justice and it is for that reason that the prohibition of collective penalties is followed formally by the prohibition of all measures of intimidation or terrorism with regard to protected persons, wherever they may be.[39]

This reasoning for the prohibition of terrorism reminds us of the colonial policing concept in the interwar period that lasted until the popularization of guerrilla warfare. Such colonial policing was carried out by the colonial powers through aerial bombardment in order to terrorize the civilian population in order to break the will of resistance against the colonial rule. It was perceived by colonial rulers as a cost-effective solution instead of operating with the ground forces. Such practice was adopted by the British in Somalia (1920), Iraq (1922-1925), and Palestine (1936-1939),[40] also by the French in Syria (1925).[41] Italians resorted to chemical weapons in Ethiopia to terrorize the local population to cement their colonial rule.[42]

During the World War II, the official Nazi directives suggested employing terrorization of civilians in order to avoid the distraction of troops from the active battle zones: 'The troops available for securing the conquered eastern territories are only sufficient, given the vastness of this area, (…) if the occupying power spreads that terror which alone is capable of eliminating any appetite for defiance on the part of the population. (…) The commanders must find the means for keeping their rear areas in order by applying corresponding draconian measures and not by demanding more security forces'.[43] Such a strategy was condemned in the *Judges* case before the Nuremberg Military Tribunal as '(…) employed the Ministry

39 Jean Pictet, *Commentary on the Geneva Convention IV Relative to the Protection of Civilian Persons in Times of War* (International Committee of the Red Cross 1958) 225-226.

40 Tami Biddle, *Rhetoric and Reality in Air Warfare:* 82.

41 Quincy Wright, 'The Bombardment of Damascus' (1926) 20 T*he American Journal of International Law* 263, 264.

42 Joseph Burns Kelly, 'Gas Warfare in International Law' (1960) 9 *Military Law Review* 1, 13.

43 Alex J Kay, *Empire of Destruction: A History of Nazi Mass Killing* (Yale University Press 2021) 76

of Justice as a means for exterminating the Jewish and Polish populations, terrorizing the inhabitants of occupied countries, and wiping out political opposition at home'.[44] In the decolonization period, the local population residing in the colonized territories adapted against the terrorization of air policing through employing guerilla warfare to reverse the power asymmetry between the resistance and colonizers. Hence, such a policy of air policing was slowly abandoned.[45]

Although the dictionary definitions of terrorism suggest the connotation of the term 'terrorism' under counter-terrorism law, Article 33 of GC IV suggests a more technical and limited meaning constrained with a nexus to an armed conflict.[46] The Special Court of Sierra Leone highlighted that Article 33 of GC IV is only applicable to the civilians at the hand of the enemy,[47] namely, detained civilians other than nationals of the occupying power in the occupied territories. Also, Article 33 of GC IV was considered as applicable to the residents of the non-occupied territories. Hence, this provision does not constrain the operational aspects of the terrorization of civilians as it was stipulated by the Galić judgement of the ICTY.[48] However, such limitation was remedied with the related provisions in the Additional Protocols I and II.[49]

Updated ICRC's Commentary on GC IV enumerates a list of acts that could be considered as terrorism in armed conflict in the sense of this provision, such as 'imposing disproportionate penalties, taking hostages, deliberately exposing dead bodies, making threats of violence, or writing racist or derogatory slogans on property, provided those acts aim to instill terror among the protected persons or intimidate them'.[50]

---

44 Nikolaus Wachsmann, *Hitler's Prisons: Legal Terror in Nazi Germany* (Yale University Press 2004) 343–344.

45 David E Omissi, *Air Power and Colonial Control: The Royal Air Force, 1919-1939* (Manchester University Press 1990) 113.

46 ICRC, *Commentary on the Fourth Geneva Convention Relative to the Protection of Civilian Persons in Time of War* (2025 update, Article 33) https://ihl-databases.icrc.org/en/ihl-treaties/gciv-1949/article-33/commentary/2025 last accessed 14 February 2026.

47 *Prosecutor v Brima (Alex Tamba), Kamara (Brima Bazzy), and Kanu (Santigie Borbor)* (Trial Judgment) SCSL-04-16-T (20 June 2007) para 664.

48 *Prosecutor v Galić* (Trial Judgment) ICTY-98-29-T (5 December 2003) para 119.

49 Updated Commentary on the Geneva Convention IV accessible at https://ihl-databases.icrc.org/en/ihl-treaties/gciv-1949/article-33/commentary/2025?activeTab=#c__Toc211342998 last accessed 14 February 2026.

50 *Ibid*.

2.2. Article 51(2) of AP I of 1977[51]

After long diplomatic efforts to expand the regulation of IHL rules on the conduct of hostilities and updating the old norms contained in the Hague Regulations and Geneva Conventions of 1949, states finally adopted the Additional Protocols I and II in 1977. However, such negotiations were not without hurdles.

2.2.1. Negotiation Process

The decolonization movements resulted in the long discussions over the status of guerrillas. As such, anti-colonial resistance style challenged one of the core obligations of the fighting parties, namely, distinguishing themselves from the civilians; mainly the states with colonial history opposed the recognition of guerrilla fighters as combatants. However, such impasse was partly resolved through the recognition of guerrillas as combatants and imposing on them the obligation to respect IHL applicable in IACs. The side effect of the compromise was the refusal of certain significant actors to ratify AP I such as the United States.[52] In addition, the United States was not ready to leave its legal position on considering the war-sustaining activities of the enemy as legitimate military targets.[53]

The provisions of AP I do not give a free pass to national liberation movements engaging in guerilla warfare as opposed to the critics who suggest that the additional protocol legitimizes terrorism. If the guerillas violate IHL provisions, the perpetrators shall be punished.[54] Also, such fighters should distinguish themselves from the civilian population, should not deliberately attack civilians, and should not commit indiscriminate attacks.[55] In addition, spreading terror among

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

52 Hans-Peter Gasser, 'Acts of Terror, "Terrorism" and International Humanitarian Law' (2002) 84 *International Review of the Red Cross* 547, 564.

53 Canestaro 431, 449.

54 Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (International Committee of the Red Cross 1987) 526.

55 Marco Sassòli, *International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare* (Edward Elgar Publishing 2019) 502.

the civilian population would significantly harm the legitimacy of their cause in the eyes of the international community.[56]

Nevertheless, one can also state that the unconditional prohibition of terrorism in armed conflict is indeed a success considering the never-ending debates about the root causes of terrorism, debates that still cause controversies among states.

2.2.2. Wording of the Provision

Article 51(2) of AP I stipulates that 'The civilian population as such, as well as individual civilians, shall not be the object of attack. Acts or threats of violence the primary purpose of which is to spread terror among the civilian population, are prohibited'.[57]

This provision outright rejects the legal position accepting war-sustaining activities of the enemy as legitimate targets. The literal interpretation prohibits targeting civilians, neither as a group nor as an individual.[58] At the same time, the commentary of AP I withdraws two situations from the scope of the provision. Firstly, the natural fear caused by an armed conflict due to any event of violence could cause fear among the civilian population. Secondly, terrorization of enemy combatants in order to push them to early surrender is not a violation of this provision.[59]

For the application of article 51(2), physical violence is not necessary. The aim of spreading terror among the civilian population could also be achieved through verbal threats, declarations, or even through social media campaigns[60] depending on the credibility of the threat.

Throughout the twentieth century, military technology regarding the targeting capabilities constantly evolved. Such evolution was expensive and required a lot of resources. For that reason, guided munitions were not widely used, especially in prolonged conflicts. However, in today's world, FPV drones and loitering munition technology have become accessible in all parts of the world at very little cost. Therefore,

56 Elizabeth Chadwick, Self-Determination, *Terrorism and International Humanitarian Law of Armed Conflict* (Martinus Nijhoff 1996) 171.

57 Schindler and Toman, *The Laws of Armed Conflicts* 736.

58 Sandoz, Swinarski and Zimmermann 618.

59 *Ibid* 618.

60 Stefan Oeter, 'Means and Methods of Combat' in Dieter Fleck and Michael Bothe (eds.) T*he Handbook of International Humanitarian Law* (3rd edn, Oxford University Press 2013) 237.

deliberately launching indiscriminate attacks against urban centers would be interpreted as spreading terror among civilians in the sense of Article 51(2) of AP I.

2.2.3. Harvard Manual

The military manuals on the specific aspects of warfare drafted by experts are helpful guidance for the interpretation of the provisions of the Geneva Conventions and their additional protocols. One noteworthy instance with regard to article 51(2) of AP I is 'The Humanitarian Policy and Conflict Research at Harvard University Manual on International Law Applicable to Air and Missile Warfare,' also known as the Harvard Manual.

Rule 18 of the Manual stipulates that 'Acts or threats of violence in the course of air or missile operations cannot be pursued for the sole or primary purpose of spreading terror among the civilian population'.[61] In addition to this clear reiteration of the prohibition of terrorism in article 51(2) of AP I, the commentary also elaborates on hybrid operations or psychological warfare through disinformation campaigns. This aspect was narrowly limited and excluded from the scope of spreading terror among civilians. The commentary suggests that 'It must be distinguished from operations designed to affect civilian morale without spreading terror among the civilian population. Examples of such operations – often labeled psychological operations or information operations– are calls to the civilian population to overthrow its national government or to otherwise diminish support for their leadership. Such operations do not come within the bounds of the definition of an "attack"'.[62]

2.3. Article 4 and Article 13 of AP II of 1977[63]

The substance of two provisions prohibiting terrorism in non-international armed conflicts is almost the same as those prohibiting terrorism in international armed conflicts. Article 13(2) of AP II was modeled after article 51(2) of AP I. Similarly, article 4(2)(d) was

61 *HPCR Manual on International Law Applicable to Air and Missile Warfare* (Cambridge University Press 2013) 110.

62 *Ibid* 111.

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

modelled after article 33 of GC IV. Because the national liberation struggles were accepted as international armed conflict with the Additional Protocol I, article 13(2) of AP II could have more relevance. Regarding the substance, the acts to spread terror among the civilian population can be diverse, from specific types of weapons like chemical or nuclear weapons to specific types of acts such as weaponization of sexual violence.

Article 4 (2) (d) of the Additional Protocol II stipulates that 'without prejudice to the generality of the foregoing, the following acts against the persons referred to in paragraph 1 are and shall remain prohibited at any time and in any place whatsoever: (…) (d) acts of terrorism'.[64]

In this provision, the word 'terrorism' was used in a broad sense, and no definition was given in the protocol. Therefore, the definition provided by the International Criminal Tribunal for Former Yugoslavia (ICTY) could be useful at this juncture. The ICTY provided a definition of terrorism in armed conflict in *the Galić* case:

> 1. Acts of violence directed against the civilian population or individual civilians not taking direct part in hostilities causing death or serious injury to body or health within the civilian population.
>
> 2. The offender willfully made the civilian population or individual civilians not taking direct part in hostilities the object of those acts of violence.
>
> 3. The above offence was committed with the primary purpose of spreading terror among the civilian population". [65]
>
> In the same judgement, the ICTY also elaborated on the specific intent requirement for spreading terror among civilians by contending that 'the nature of the acts or threat of violence directed against the civilian population can vary; the primary concern, as explained below, is that those acts or threats of violence be committed with the specific intent to spread terror among the civilian population. Further, the crime of acts or threats of violence the primary purpose of which is to spread terror among the civilian population is not a case in which an explosive device was planted outside of an ongoing military attack but rather a case of "extensive trauma and psychological damage" being caused by "attacks [which] were designed to keep the inhabitants in a constant state of terror"'.[66]

64 Schindler and Toman, The Laws of Armed Conflicts 778.

65 Prosecutor v Galić (Trial Judgment) para 91.

66 *Ibid* para 102.

2.4. Customary Prohibition of Terrorism in Armed Conflict

The ICRC's customary international humanitarian law study listed the prohibition of terrorism as Rule 2, which stipulates that 'acts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited'.[67] In the Galić case, ICTY confirmed the customary nature of the prohibition of terrorism in armed conflict by highlighting that 'it is satisfied that the prohibition of terror against the civilian population as enshrined in Article 51 (2) of Additional Protocol I and Article 13 (2) of Additional Protocol II was a part of customary international law from the time of its inclusion in those treaties. The Appeals Chamber, by majority, Judge Schomburg dissenting, is further satisfied that a breach of the prohibition of terror against the civilian population gave rise to individual criminal responsibility pursuant to customary international law at the time of the commission of the offences for which Galić was convicted [1992- 1993]'.[68] Such a dictum also underlined the possibility of individual criminal responsibility based on the customary prohibition of terror.

3. Relationship between Counter-Terrorism Law and International Humanitarian Law

In this part, the interaction between international humanitarian law and counter-terrorism law will be briefly analyzed. Such interplay is one of the fundamental reasons of the conflation of terrorism in armed conflict and terrorism in peacetime.

The approach of two legal fields is radically different, as there is equality of belligerents under IHL, but terrorists are always the evil side under counter-terrorism law.[69] Such different approaches create substantial practical differences.

In IHL, the distinction between civilians and combatants as separate categories is the main obstacle to applying the IHL prohibitions of terrorism in peacetime by analogy because such categories do not exist

67 Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law - Volume 1: Rules* (Cambridge University Press 2005) 8.

68 *Prosecutor v Galić (Appeal Judgment)* IT-98-29-A (30 November 2006) para 86.

69 Sassòli, *International Humanitarian Law* 496.

in counter-terrorism law.[70] Also, the states do not appreciate the risk of providing legitimacy to terrorist groups by simply applying IHL to them.[71] However, Common Article 3 expressly rejects any change of status of non-state armed groups through the application of IHL.

By looking at the international treaties touching upon the terrorism connection, there is no formal claim of *lex specialis* from either of the fields.[72] Under the auspices of the UN, there are nineteen sectoral counter-terrorism treaties adopted by the states. However, there is no harmony between these treaties regarding the applicability of such treaties in the event of armed conflict. Some of the sectoral treaties contain partial or full exclusion clauses in favor of IHL, such as the Convention on Offences and Certain Other Acts Committed on Board Aircraft, also known as the Tokyo Convention,[73] having partial exclusion, or the Terrorist Bombing Convention having full exclusion.[74] Some other treaties are silent. For instance, the Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons,[75] including Diplomatic Agents, has no mention of the applicability of the treaty during an armed conflict.

In the context of an armed conflict, IHL could be considered as *lex specialis*, as it offers more in-depth regulation than counter-terrorism law. Counter-terrorism law's sectoral approach often presents contradictory or ambiguous insights to the legal issues. Whereas IHL offers a coherent legal framework. Most of the sectoral counter-terrorism treaties have a 'political offense' exception with regards to extradition; therefore, political considerations play significant role. Also, the number of state parties to the sectoral counter-terrorism treaties significantly diverges.[76] Furthermore, the possibility of making a reservation for each counter-

70 Torsten Stein, 'How Much Humanity Do Terrorists Deserve?' in Astrid J.M. Delissen, Gerard J. Tanja (eds.), *Humanitarian law of armed conflict challenges ahead* (Brill Nijhoff 1991) 573.

71 Richard Barnes, 'Of Vanishing Points and Paradoxes: Terrorism and International Humanitarian Law' in Justin Morris, Nigel D White and Richard Burchill (eds), I*nternational Conflict and Security Law: Essays in Memory of Hilaire McCoubrey* (Cambridge University Press 2005) 152.

72 Ben Saul, 'From Conflict to Complementarity: Reconciling International Counterterrorism Law and International Humanitarian Law' (2021) 103 *International Review of the Red Cross* 157, 158.

73 Omer Yousif Elagab and Jeehan Elagab, I*nternational Law Documents Relating to Terrorism* (Routledge Cavendish 2007) 407

74 *Ibid* 473.

75 *Ibid* 427.

76 Barnes 156.

terrorism treaty varies greatly.[77] But all states are state-party to the four Geneva Conventions of 1949, and reservations are very limited.

Considering the co-application of both fields during an armed conflict, it would provide little added value. Determination of certain acts that could become the violations of international humanitarian law, also known as terrorist acts, would only label them as 'heinous' in parallel with the legality of such behaviors.[78] Hence, the advantage is marginal, such as additional prosecution before the domestic courts, but the risk is disproportional, especially the politicization of IHL.

4. Conclusion

A daunting ghost from the past is the US' war on terror policies. Although an attack carried out by a non-state actor did not reach the intensity criteria,[79] nevertheless the US invoked IHL and applied a rather radical interpretation of IHL provisions under the pretext of counter-terrorism. Conflation of counter-terrorism law and IHL resulted in state practices included, but were not limited to, extraordinary renditions,[80] indefinite detention,[81] denial of habeas corpus for the terrorism suspects,[82] subjecting the detainees to inhumane and degrading treatment amounting to torture,[83] and conducting drone strikes in other countries without any connection with an armed conflict reaching the level of aggression.[84]

A similar pattern was followed by Israel in the aftermath of the October 7 attacks. Relentless Israeli bombardments against densely populated Gaza are reminiscent of the terror bombardments of the World War II. In addition, Israel's justification of its possible war crimes with the

77 Antonio Cassese, 'The International Community's "Legal" Response to Terrorism' (1989) 38 *International & Comparative Law Quarterly* 589, 595.

78 Barnes 145.

79 Robert Kolb, *Advanced Introduction to International Humanitarian Law* (Edward Elgar 2014), 148.

80 David Weissbrodt and Amy Bergquist, 'Extraordinary Rendition and the Humanitarian Law of War and Occupation' (2007) 47 *Virginia Journal of International Law* 295, 297–298.

81 Marco Sassòli, 'Use and Abuse of the Laws of War in the War on Terrorism' (2017) 22 *Minnesota Journal of Law & Inequality* 195, 210.

82 Silvia Borelli, "Casting Light on the Legal Black Hole: International Law and Detentions Abroad in the 'War on Terror'" (2005) 87 *International Review of the Red Cross* 39, 67.

83 Weissbrodt and Bergquist 295, 344.

84 Kolb 148–152.

counter-terror narrative would seem like the replication of the US' war on terror discourse. Indeed, such widescale wanton destruction without military necessity would be considered as the spreading of terror among the civilian population.[85]

In conclusion, despite the distinct conceptualization of 'the terrorization of civilians' under IHL, the state practice demonstrates that deliberate conflation of the term with the broad understanding of the term 'terrorism' under counter-terrorism law serves state interests. Such function is useful for the belligerent states to portray the enemy belligerents in pejorative terms. In addition, such 'conflation' of the understanding of terrorism serves as leeway for dubious state practice in order to diminish the gravity of their exploitation of IHL norms in the name of 'fight against terrorism'. Despite such vulnerability to be exploited by states through deliberate conflation of terrorism under IHL and terrorism under counter-terrorism law, the added value of the application of terrorism under counter-terrorism law during an armed conflict would be very limited as most of the offences under counter-terrorism law were already covered by IHL. Therefore, the precision in the use of the concept of terrorism should be an urgent concern for all the stakeholders aiming to avoid the politicization of IHL to offer better protection to all civilians impacted by armed conflicts all around the world.

85 Luigi Daniele, Nicola Perugini and Francesca Albanese, *Humanitarian Camouflage: Israel Rewrites the Laws of War to Legitimize Genocide in Gaza* (Current Issues in Depth Issue No 12, Institute for Palestine Studies 2024) 15–16.

Bibliography

Adatci M, 'Commission on the Responsibility of the Authors of the War and on Enforcement of Penalties' (1920) 14 *American Journal of International Law* 95.

Barnes R, 'Of Vanishing Points and Paradoxes: Terrorism and International Humanitarian Law' in Justin Morris, Nigel D White and Richard Burchill (eds), *International Conflict and Security Law: Essays in Memory of Hilaire McCoubrey* (Cambridge University Press 2005).

Bassiouni MC, *The United Nations Commission of Experts Established Pursuant to Security Council Resolution 780* (1992) (1994).

Biddle TD, 'Strategic Bombardment: Expectation, Theory and Practice in the Early Twentieth Century' in Matthew Evangelista and Henry Shue (eds), *The American Way of Bombing: Changing Ethical and Legal Norms, from Flying Fortresses to Drones* (Cornell University Press 2014).

Biddle TD, *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas about Strategic Bombing, 1914-1945* (Princeton University Press 2004).

Bierzanek R, '1923 Hague Rules' in Natalino Ronzitti and Gabriella Venturini (eds), *The Law of Air Warfare: Contemporary Issues* (Eleven International Publishing 2006).

Boog H, *The Conduct of the Air War in the Second World War: An International Comparison* (Berg 1992).

Borelli S, 'Casting Light on the Legal Black Hole: International Law and Detentions Abroad in the "War on Terror"' (2005) 87 *International Review of the Red Cross* 39.

Canestaro NA, 'Legal and Policy Constraints on the Conduct of Aerial Precision Warfare' (2004) 37 *Vanderbilt Journal of Transnational Law* 431.

Cassese A, 'The International Community's "Legal" Response to Terrorism' (1989) 38 *International & Comparative Law Quarterly* 589.

Chadwick E, *Self-Determination, Terrorism and International Humanitarian Law of Armed Conflict* (Martinus Nijhoff 1996).

Daniele L, Perugini N and Albanese F, *Humanitarian Camouflage: Israel Rewrites the Laws of War to Legitimize Genocide in Gaza* (Institute for Palestine Studies 2024) https://www.palestine-studies.org/en/node/1656283 accessed 15 February 2026Douhet G, The Command of the Air (Dino Ferrari tr, Coward-McCann 1942).

Elagab OY and Elagab J, *International Law Documents Relating to Terrorism* (Routledge Cavendish 2007).

Garner JW, *International Law and The World War Volume I* (Longmans 1920).

Garrett SA, 'Airpower and Non-Combatant Immunity: The Road to Dresden' in Igor Primoratz (ed), *Civilian Immunity in War* (Oxford University Press 2007).

Gasser H, 'Acts of Terror, "Terrorism" and International Humanitarian Law' (2002) 84 *International Review of the Red Cross* 547.

Henckaerts J and Doswald-Beck L, *Customary International Humanitarian Law - Volume 1: Rules* (Cambridge University Press 2005).

HPCR, *Manual on International Law Applicable to Air and Missile Warfare* (Cambridge University Press 2013).

ICRC, *Commentary on the Fourth Geneva Convention Relative to the Protection of Civilian Persons in Time of War* (2025 update, Article 33) https://ihl-databases.icrc.org/en/ihl-treaties/gciv-1949/article-33/commentary/2025 accessed 14 February 2026.

Jachec-Neale A, *The Concept of Military Objectives in International Law and Targeting Practice* (Routledge 2014).

Kay AJ, *Empire of Destruction: A History of Nazi Mass Killing* (Yale University Press 2021).

Kelly JB, 'Gas Warfare in International Law' (1960) 9 *Military Law Review* 1.

Kolb R, *Advanced Introduction to International Humanitarian Law* (Edward Elgar 2014).

Lauterpacht H, 'The Problem of the Revision of the Law of War' (1952) 29 *British Year Book of International Law* 360.

Legro JW, *Cooperation under Fire: Anglo-German Restraint during World War II* (Cornell University Press 2013).

Nippold O, *The Development of International Law After the World War* (Amos S Hershey tr, The Lawbook Exchange 2004).

Oeter S, 'Means and Methods of Combat' in Dieter Fleck and Michael Bothe (eds), *The Handbook of International Humanitarian Law* (3rd edn, Oxford University Press 2013).

Omissi DE, *Air Power and Colonial Control: The Royal Air Force, 1919-1939* (Manchester University Press 1990).

Pape RA, *Bombing to Win: Air Power and Coercion in War* (Cornell University Press 1996).

Parks H, 'Air War and the Law of War' (1990) 32 *Air Force Law Journal* 1.

Pictet J, *Commentary on the Geneva Convention IV Relative to the Protection of Civilian Persons in Times of War* (International Committee of the Red Cross 1958).

Royse MW, *Aerial Bombardment and the International Regulation of Warfare* (Harold Vinal 1928).

Prosecutor v Brima (Alex Tamba), Kamara (Brima Bazzy), and Kanu (Santigie Borbor) (Trial Judgment) SCSL-04-16-T (20 June 2007).

Prosecutor v Galić (Appeal Judgment) IT-98-29-A (30 November 2006).

Prosecutor v Galić (Trial Judgment) ICTY-98-29-T (5 December 2003).

Geneva Convention Relative to the Protection of Civilian Persons in Time of War (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 287 (GC IV).

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

Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 60.

Sandoz Y, Swinarski C and Zimmermann B (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (International Committee of the Red Cross 1987).

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

Sassòli M, 'Use and Abuse of the Laws of War in the War on Terrorism' (2017) 22 *Minnesota Journal of Law & Inequality* 195.

Saul B, 'From Conflict to Complementarity: Reconciling International Counterterrorism Law and International Humanitarian Law' (2021) 103 I*nternational Review of the Red Cross* 157.

Saul B, *Defining Terrorism in International Law* (Oxford University Press 2006).

Schindler D and Toman J, T*he Laws of Armed Conflicts: A Collection of Conventions, Resolutions, and Other Documents* (3rd edn, Martinus Nijhoff 1988/2004).

Schmitt MN, 'Air Warfare' in Andrew Clapham and Paola Gaeta (eds), T*he Oxford Handbook of International Law in Armed Conflict* (Oxford University Press 2014).

Spaight JM, *Air Power and War Rights* (3rd edn, Longmans 1947).

Stein T, 'How Much Humanity Do Terrorists Deserve?' in Astrid JM Delissen and Gerard J Tanja (eds), *Humanitarian Law of Armed Conflict Challenges Ahead* (Brill Nijhoff 1991).

Wachsmann N, *Hitler's Prisons: Legal Terror in Nazi Germany* (Yale University Press 2004).

Weissbrodt D and Bergquist A, 'Extraordinary Rendition and the Humanitarian Law of War and Occupation' (2007) 47 *Virginia Journal of International Law* 295.

Whitcomb WP, 'Legitimate Targets in Aerial Bombardment' (1929) 23 *American Journal of International Law* 581.

Wright Q, 'The Bombardment of Damascus' (1926) 20 *The American Journal of International Law* 263.

Chapter IV: An Overview of the International Law Commission's Principles on the Protection of the Environment in Relation to Armed Conflict

Nilüfer Oral[1]

1. Introduction

Armed conflict is inherently harmful to humans and communities. But armed conflict is also harmful to the environment. World War I was the first global conflict where the widescale impact of technology and the use of modern military resources, including chemical warfare, produced massive environmental harm in addition to the death of millions of people. It was by far the most destructive war both in loss of life and damage to the environment up until then. Unfortunately, the destructive forces of war over time became even more harmful. However, since World War I armed conflicts not only grew scale, such as in World War II, but also in the scale of fatalities and injuries to humans and the environment. However, international humanitarian law (IHL), once referred to the laws of war, did not make express reference to the natural environment until 1977 with the adoption of Additional Protocol I to the Geneva Conventions that an express reference to the natural environment was made.[2] One year earlier, the General Assembly had approved the Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques (ENMOD) which entered into force in 1978.[3]

---

1 Director of the Centre for International Law, National University of Singapore, Member of the UN International Law Commission.

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

3 *Convention on the Prohibition of Military or any Other Hostile Use of Environmental Modification Techniques* (adopted 18 May 1977) 1108 UNTS 151.

The progress of the development of IHL in relation to protection of the environment and armed conflict has been a slow process. However, in 2022, at the recommendation of UNEP, the International Commission adopted the Principles on Protection of the Environment in Relation to Armed Conflict, that represent a modernized approach to IHL taking into account the development in international environment law. This chapter will examine the background of IHL and the environment, how it has developed, and provide an overview of the work of the International Law Commission on protection of the environment in relation to armed conflict.

2. Protection of Environment in Armed Conflict

2.1. World War I and II and the Environment

During the World War I (WWI), he use of chemicals destroyed and altered the soil of Europe permanently. Today, there still exists an area known as the Red Zone (Zone Rouge), which before WWI was farmland. Because it was contaminated with all the chemical warfare, such as the use of mustard gas, that took place during WWI, over a century later it remains uninhabitable and cannot be used.[4] In addition, during WWI, some 350,000 hectares of forests were destroyed.[5]

During World War II there was a greater massive expansion of technology and destructive capacity of warfare. The bombardment of cities and the destruction of forests, farms, transport systems and irrigation networks during World War II produced devastating environmental consequences, and by the end of the war there were almost 50 million refugees and displaced people.[6] The worst was the US use of nuclear bombs in Hiroshima and Nagasaki.

In addition to the devastation brought by World War II to Europe, there was also much destruction caused in Asia. The environment in

4 Drew Heiderscheidt, 'The Impact of World War One on the Forests and Soils of Europe' (2018) 7 zhttps://digscholarship.unco.edu/cgi/viewcontent.cgi?article=1175&context=urj accessed 9 February 2026; see also National Geographic https://education.nationalgeographic.org/resource/red-zone/ accessed 9 February 2026.

5 *Ibid.*

6 Jennifer Leaning, 'Environment and Health: Impact of War' (2000) 163 *Canadian Medical Association Journal* 1157–1161.

Asia was impacted very much. Toxic chemicals were used and there was massive pollution. But of course, most significant was the nuclear bomb and its unprecedented scale of destruction for humans, communities and the environment.

2.2. The Vietnam and Kuwait Wars

The Vietnam War started in the 1950s when the French were the colonial powers. After the French withdrew from Vietnam, the US entered the Vietnam War and started using Agent Orange to clear the plants and trees for bombing purposes. The US sprayed some 11,000,000 gallons of Agent Orange over 20 million acres of Vietnam. This resulted in the loss of 3.1 million hectares of tropical forests and mangroves.[7] Another important war that had great impact on the environment was in 1991 when Iraq invaded Kuwait and set fire to over 800 oil wells.[8] Obviously, the environmental consequences, both for air and soil pollution were very serious. In the past, the impact of armed conflict and climate change mostly concerned air pollution, soil pollution, harm to forests and biodiversity. But now, the impact of armed conflict on climate change is a new factor. It is estimated that the emissions from the burning oil and gas in Kuwait amounted to some 130–140 million tons of carbon dioxide emissions, which is about two to three per cent of the global annual anthropogenic contribution from human use of fossil fuels.[9] It is known that trees store carbon dioxide and when destroyed, the carbon dioxide is released into the air. Carbon dioxide is one of the main elements of climate change. We can now also add climate change as a new harm to the natural environment caused by armed conflict. Scientists estimate that in the eighteen months of the armed conflict between Russia and Ukraine produced some 77 MtCO2-eq of greenhouse gas emissions.[10]

7 Kiem N Truong and Khuong V Din, 'Agent Orange: Half-Century Effects on the Vietnamese Wildlife Have Been Ignored' (2021) 55(22) Environmental Science & Technology 15007–15009.

8 Olof Linden, Arne Jerneloev and Johanna Egerup, *The Environmental Impacts of the Gulf War 1991*, IIASA Interim Report (IIASA, Laxenburg 2004) https://pure.iiasa.ac.at/id/eprint/7427/1/IR-04-019.pdf accessed 9 June 2026.

9 *Ibid.*

10 *Ibid.*

3. Armed Conflict and the Environment at the UN

These cases of environmental damage caused by armed conflict raised much attention on the relationship between armed conflict and protection of the environment. In response, protection of the environment was placed on the agenda of the United Nations: first under the heading 'Exploitation of the environment as a weapon in times of armed conflict and the taking of practical measures to prevent such exploitation' and subsequently under 'Protection of the environment in times of armed conflict'—originally proposed by Jordan in 1991.[11]

In 1992, the General Assembly included the topic 'Protection of the environment in times of armed conflict' on its agenda and allocated it to the Sixth Committee (see General Assembly decision 46/417 of 9 December 1991). The Secretary-General submitted his first report on the protection of the environment in times of armed conflict in 1992 and a second report in 1993.

The International Committee of the Red Cross (ICRC) was mandated by the General Assembly to work on the issue. As a consequence, expert meetings were held, and the issue was also on the agenda of the International Conferences of the Red Cross and Red Crescent. One result was the Guidelines for military manuals and instructions on the protection of the environment in times of armed conflict, annexed to the report submitted by the ICRC to the forty-eighth session of the United Nations General Assembly.

4. International Legal Framework

4.1. Additional Protocol I to the 1949 Geneva Conventions

I will now discuss the international legal framework for protection of the environment and armed conflict. In the existing IHL instruments, there are basically two specific direct references to the environment, which are found in Article 35 and Article 55 of the Additional Protocol I to the 1949 Geneva Conventions.[12] Under Article 35, under the general heading of methods and means of warfare, there is a prohibition on

11 UNGA Decision 46/417, UN Doc A/46/417 (9 December 1991).

12 Additional Protocol I (n 1).

the employment of methods or means of warfare which are intended, or may be expected, to cause widespread, long-term and severe damage to the natural environment. It entails a 'foreseeability' element and thus not a strict liability standard for any damage to the natural environment. Second and important is the scale of the damage, which must be 'widespread, long term and severe'. This is a very high threshold as all three elements must exist- 'widespread', 'long term' *and* 'severe'. In other words, the trio of elements must all exist.

However, what does widespread mean? A kilometer? 100,000 hectares? What does long term mean exactly — and severe damage? This threshold has been criticized for being so high threshold and difficult to meet. According to the Commentary, the 'long term' standard for the Protocol was understood to mean lasting for a matter of decades. By contrast, the ENMOD Convention prohibition of 'long-lasting' modification of the climate, which could harm another State Party to the Convention, was understood to mean in a matter of months.[13]

In relation to Article 55 of AP I—which concerns protection of the civilian population against the effects of hostilities—it provides that:

> 1. Care shall be taken in warfare to protect the natural environment against widespread, long-term and severe damage. This protection includes a prohibition of the use of methods or means of warfare which are intended or may be expected to cause such damage to the natural environment and thereby to prejudice the health or survival of the population.[14]

It should be noted that the current view is that the environment is considered to be a civilian object and thus protected. Another question concerns the element of the methods or means of warfare that 'may be expected to cause such damage to the natural environment and thereby to prejudice the health or survival of the population' as formulated by the article 55 of AP I. The use of population has a broad scope. It is not just the civilian population but the overall population that is protected.[15]

13 *Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts* (Protocol I) (adopted 8 June 1977), Commentary of 1987, para 1452 https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-35/commentary/1987?activeTab=undefined accessed 9 February 2026.

14 *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts* (Protocol I) (adopted 8 June 1977), art 55 https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-55 accessed 9 February 2026.

15 AP I Commentary of 1987, para 2134.

Next, the question is what is meant by 'natural' environment? This was also an issue debated in the International Law Commission when working on the Protection of the Environment in Relation to Armed Conflict as to whether to qualify it with 'natural' or not.[16] Most multilateral environmental agreements, particularly those that were negotiated and adopted in the 1990s and afterwards, don't use this terminology of 'natural environment' but simply the 'environment'. The final outcome of the work of the Commission excluded the use of 'natural'.[17]

4.2. ENMOD

After the Vietnam War and the use of Agent Orange, the Convention on the Environmental Modification, formally the Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques (ENMOD), was adopted in 1976.[18] Professor Richard Falk, a very well-known international law professor, was one of the first who introduced the term of 'ecocide'.[19] In fact, the original idea for the scope of ENMOD was much broader. It was intended as a response to the use of environmental destructive chemicals such as Agent Orange. As adopted, ENMOD prohibits the weaponizing of climate modification. Article 1 prohibits States from engaging 'in military or any other hostile use of environmental modification techniques having widespread, long-lasting or severe effects as the means of destruction, damage or injury to any other State Party.' [20]

One difference from Protocol I is that under ENMOD the standard is 'widespread, long lasting *or* severe effects…'[21]. Where Additional Protocol I uses the conjunctive 'and' for all three elements, Article 1 of

16 International Law Commission, 'Statement of the Drafting Committee Chair', International Law Commission, Sixty-seventh Session, https://legal.un.org/ilc/documentation/english/statements/2015_dc_chairman_statement_peac.pdf accessed 9 February 2026.

17 UNGA Res 77/10, *Protection of the Environment in Relation to Armed Conflict* UN Doc A/RES/77/10 (2022).

18 *Convention on the Prohibition of Military or any Other Hostile Use of Environmental Modification Techniques* (adopted 18 May 1977) 1108 UNTS 151.

19 Richard A Falk, 'Environmental Warfare and Ecocide — Facts, Appraisal, and Proposals' (1973) 4 *Bulletin of Peace Proposals* 80–96; see also David Zierler, *Invention of Ecocide: Agent Orange, Vietnam, and the Scientists Who Changed the Way We Think About the Environment* (University of Georgia Press 2011).

20 ENMOD (n16).

21 *Ibid.*

ENMOD uses the disjunctive. This means that under ENMOD either one of these thresholds —widespread, long-lasting or severe effects —I would suffice, whereas in the additional protocol all three are required. However, ENMOD has only 78 Parties to date compared to Additional Protocol I.

4.3. Other IHL Instruments

There are also other IHL instruments of indirect application to the environment such as:

- Protocol for the Prohibition of the Use of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare;[22]
- Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction;[23]
- Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects.[24]

There is also the Rome Statue, which applies to individual criminal liability for war crimes. Article 2(b)(iv) establishes environmental destruction as a war crime: 'Intentionally launching an attack in the knowledge that such attack will cause incidental loss of life or injury to civilians or damage to civilian objects or widespread, long-term and severe damage to the natural environment which would be clearly excessive in relation to the concrete and direct overall military advantage anticipated.'[25]

Here, as in article 55 of Additional Protocol I, the standard is in the conjunctive requiring all elements of 'widespread, long term *and* severe damage to the natural environment'.

---

22 *Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare* 94 LNTS 65 (adopted 16 June 1925).

23 *Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destructio*n 1015 UNTS 163 (adopted 10 April 1972).

24 *Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be Deemed to be Excessively Injurious or to have Indiscriminate Effects* 1342 1342 UNTS 137 (adopted 10 October 1980).

25 *Rome Statute of the International Criminal Court* (adopted 17 July 1998) 2187 UNTS 3.

Protection of the environment in relation to armed conflict is also addressed in the San Remo Manual on International Law Applicable to Armed Conflicts at Sea, which is not a treaty but is deemed to reflect customary international law.[26] The San Remo Manual includes the protection of marine areas in Section IV, paragraph 10. It encourages parties in conflict to agree that no hostile actions will be conducted in marine areas containing rare or fragile ecosystems (*a*) rare or fragile ecosystems; or (*b*) the habitat of depleted, threatened or endangered species or other forms of marine life. This language parallels Article 194 (5) of the United Nations Convention on the Law of the Sea.[27]

4.4. Rights of Indigenous People

It is important to consider the interests of indigenous peoples as well, which is becoming increasingly important, and is also reflected in the work of the International Law Commission on the Protection of the Environment in Relation to Armed Conflict. There is also The UN Declaration on the Rights of Indigenous People that was adopted 2007 was ground-breaking as it recognizes the important relationship indigenous peoples have with the land. Article 30 prohibits the military activities from taking place in the lands or territories of indigenous peoples, unless justified by a relevant public interest or otherwise freely agreed with or requested by the indigenous peoples concerned, and requires States to undertake effective consultations with the indigenous peoples concerned, through appropriate procedures and in particular through their representative institutions, prior to using their lands or territories for military activities.

5. Environmental Instruments

5.1. 1972 Stockholm Declaration and the 1992 Rio Declaration Principles

An important marker for international environmental law was the famous 1972 United Nations summit that took place in Stockholm in

26 *San Remo Manual on International Law Applicable to Armed Conflicts at Sea* (12 June 1994) https://ihl-databases.icrc.org/en/ihl-treaties/san-remo-manual-1994 accessed 9 June 2026.

27 Convention on the Law of the Sea, 1833 UNTS 397, adopted 10 Dec. 1982. Article 194 (5) provides that in relation to the obligation for State Parties to prevent, control and reduce pollution of the marine environment that "the measures taken in accordance with this Part shall include those necessary to protect and preserve rare or fragile ecosystems as well as the habitat of depleted, threatened or endangered species and other forms of marine life.

1972. This gathering was the first time States came together specifically to discuss protection of the environment. One of the outcomes was the Stockholm Declaration that included a set of principles. Among these is Principle 26 entitled 'Ban on nuclear weapons' that declaring that 'Man and his environment must be spared the effects of nuclear weapons and all other means of mass destruction.'[28]

In 1992 again, 20 years later, another very significant governmental summit took place in Rio de Janeiro and adopted the Rio Declaration and a new set of principles.[29] Relevant principles for armed conflict are:

- Principle 23: The environment and natural resources of people under oppression, domination and occupation shall be protected.
- Principle 24: Warfare is inherently destructive of sustainable development. States shall therefore respect international law providing protection for the environment in times of armed conflict and cooperate in its further development, as necessary.
- Principle 25: Peace, development and environmental protection are interdependent and indivisible.[30]

Principle 23, specifically focusses on occupation, which is also a part of armed conflict. The environment and natural resources of people under oppression, domination and occupation shall be protected. The obligations of the occupying power is also reflected in the work of the International Law Commission on the Protection of the Environment in Relation to Armed Conflict.

Principle 24 of the Rio Declaration recognizes the inherently destructive nature of war for sustainable development. The notion of sustainable development–defined as "development that meets the needs of the present without compromising the ability of future generations to meet their own needs'– emerged in 1987 with the historic Brundtland report 'Our Common Future' and has been further advanced by the United Nations Sustainable Development Goals.

28 *Stockholm Declaration on the Human Environment*, UN Doc A/CONF. 48/14 (1972).

29 *Rio Declaration on Environment and Development*, UN Doc A/CONF.151/26 (Vol. 1) (1992).

30 *Rio Declaration on Environment and Development*, UN Doc A/CONF.151/26 (Vol. 1) (1992).

5.2. UNEP

In 2009, the United Nations Environment Program (UNEP) together with the Environmental Law Institute published a report on armed conflict and the environment.[31] The report included UN Secretary General, Ban-ki Moon's message delivered on 6 November 2009 for International Day for Preventing the Exploitation of the Environment in War and Armed Conflict stated that 'There can be no durable peace if the natural resources that sustain livelihoods are damaged or destroyed'.[32] Moreover, the report highlighted that 'Despite the protection afforded by several important legal instruments, the environment continues to be the silent victim of armed conflicts worldwide'.[33] 'The report identified gaps in the international legal framework and pointed to the need to update the very anachronistic international legal framework for protection of the environment in relation to armed conflict. Among its findings the report observed that:

> 1. 'Articles 35 and 55 of Additional Protocol I to the 1949 Geneva Conventions do not effectively protect the environment during armed conflict due to the stringent and imprecise threshold required to demonstrate damage: While these two articles prohibit 'widespread, long-term and severe' damage to the environment, all three conditions must be proven for a violation to occur. In practice, this triple cumulative standard is nearly impossible to achieve, particularly given the imprecise definitions for the terms 'widespread,' 'long-term' and 'severe'.[34]
>
> 2. Provisions in humanitarian law that regulate the means and methods of warfare or protect civilian property and objects provide indirect protection of the environment: Restrictions on the means of warfare (in particular weapons) and the methods of warfare (such as military tactics) provide indirect protection to the environment, although new technologies, such as the use of depleted uranium, are not yet addressed—except by the general principles of the law of war.
>
> Provisions that protect civilian property and objects, including industrial installations and cultural/ natural sites, also provide indirect protection to the environment. However, these protections have rarely been effectively implemented or enforced.[35]

31 David Jensen and Carl Bruch, *Protecting the Environment During Armed Conflict: An Inventory and Analysis of International Law* (UNEP 2009).

32 *Ibid.*

33 *Ibid* at p. 4 (Executive Summary).

34 *Ibid.*

35 *Ibid.*

> 3. The majority of international legal provisions protecting the environment during armed conflict were designed for international armed conflicts and do not necessarily apply to internal conflicts: Given that most armed conflicts today are non-international or civil wars, much of the existing legal framework does not necessarily apply. This legal vacuum is a major obstacle for preventing the often serious environmental damage inflicted during internal conflicts. There are also no institutionalized mechanisms to prevent the looting of natural resources during armed conflict or to restrict the granting of concessions by combatants that may lack legitimacy or legal authority.[36]
>
> 4. In addition, there are no systematic mechanisms to prevent in causing environmental damage or looting natural resources. States or corporations from aiding and abetting civil war parties. There is no permanent international mechanism to monitor legal infringements and address compensation claims for environmental damage sustained during international armed conflicts.
>
> 5. The general humanitarian principles of distinction, necessity, and proportionality may not be sufficient to limit damage to the environment.[37]
>
> 6. Unless otherwise stated, international environmental law continues to apply during armed conflicts and could be used as a basis for protection: The provisions of multilateral environment agreements (MEAs) should be regarded as continuing to apply during both international and non-international armed conflict, unless they specifically stipulate otherwise. The notion that international humanitarian law replaces international environmental law as the operational body of law during armed conflict is no longer the prevailing opinion of legal experts, including the International Law Commission. In addition, international environmental law could be used in the interpretation of incomplete or insufficiently clear norms of international humanitarian law.[38]

The UNEP Report made recommendations that included that International Law Commission should examine the existing international law for protecting the environment during armed conflict and recommend how it can be clarified, codified and expanded.[39]

36 *Ibid.*

37 *Ibid.* at p. 6.

38 *Ibid.*

39 *Ibid*, 6 and 53.

6. The International Law Commission

6.1. Background on the International Law Commission

The International Law Commission was established in 1947, held its first meeting 1948. It is a subsidiary body of the General Assembly of the UN. Its mandate is for the progressive development of international law and its codification. Over the years, it has engaged in the development towards the codification of treaties, such as the Vienna Convention on the Law of Treaties, the Vienna Convention on Consular Relations and many more. As a legal expert body under the General Assembly it has direct relations with the Sixth Committee, that is the Legal Committee of the General Assembly. As a result, all the work of the Commission goes directly to the Sixth Committee, which in turn makes comments that the Commission takes into account in its work. The Commission is not an academic party, and this is one big difference from other highly esteemed academic associations such as the Institut de Droit International or the International Law Association. These are private entitled and more academically oriented. Whereas the Commission is focused on States.

However, the work of the Commission has shifted towards soft law, such as draft principles, draft conclusions and draft guidelines. Nonetheless, the work of the Commission is considered to be authoritative and while not directly a source of international law, such as the Articles of State Responsibility for Internationally Wrongful Acts, which has never been codified by States and remains in the form adopted by the Commission.

Under the Statute for the Commission, an international organization of the UN, or a member State can make a request to the Commission to take up a topic.[40] UNEP, while it was not a formal, did request to the Commission to address the need for updated rules on protection of the environment in relation to armed conflict.

40 *Statute of the International Law Commission*, GA Res 174 (II) (21 November 1947), as amended by GA Res 174 (II) (21 November 1947), as amended by GA Res 485 (V) (12 December 1950), 984 (X) (3 December 1955), 985 (X) (3 December 1955) and 36/39 (18 November 1981), art 17(1).

6.2. The Draft Principles on the Protection of the Environment in Relation to Armed Conflict in the Commission

The International Law Commission decides what topics to put on its long-term work program, and then from the long-term work program to place on its current working program.[41] In 2013 the topic of protection of the environment in relation to armed conflict was placed on the current work program. Marie Jacobson, Ambassador from Sweden, was appointed as Special Rapporteur.[42] The special rapporteur takes a leading role in guiding the Commission in its work on a topic.[43] The special rapporteur prepares reports and proposes draft outcomes for the work of the Commission. These drafts are debated on within the Commission and then, upon the recommendation of the plenary session, moved to the drafting committee. However, it is the at the plenary session of the Commission where the draft outcomes from the drafting committees are adopted.

When Ambassador Marie Jacobson left the Commission, she was replaced by Marja Lehto from Finland, who was also an ambassador. She was appointed as Special Rapporteur in 2018.[44] The final draft principles were adopted in 2022 by the Commission with commentaries. The commentaries to the work of the Commission are very important because they explain why the Commission adopted what they did and provide support, in particular State practice or decisions by courts and tribunals. The final outcome of the work of the Commission, including the commentaries are considered a collective work. While the Special Rapporteurs prepare the initial drafts of the commentaries, the members of the Commission also contribute and the commentaries are adopted by consensus.

Rather than taking the traditional approach of protection of the environment from the lens of warfare in its work on the draft principles

41 See International Law Commission, 'Programme of Work' <https://legal.un.org/ilc/programme.shtml> accessed 9 February 2026.

42 ILC, *Report of the International Law Commission*, UN Doc A/68/10 (2013) ch IX, paras 130–144, para 131.

43 International Law Commission, 'Structure and Membership' https://legal.un.org/ilc/structure.shtml accessed 9 February 2026.

44 ILC, *Report of the International Law Commission*, UN Doc A/72/10 (2017) ch X, paras 253–262, para 262.

on protection of the environment in relation to armed conflict, the Commission opted for a more modern and up-to-dated approach which adopted a broader environmental perspective. As stated earlier, protection of the environment in armed conflict in IHL treaties is only addressed by Article 35 and Article 55 of Additional Protocol I and the ENMOD convention, as well as the San Remo manual which is deemed to reflect customary international law. However, in light of modern warfare and the development of environmental law since these instruments were developed, a need emerged for a framework for protection of the environment and armed conflict that encompassed all these important developments.

6.3. Overview of the Work of the Commission on the Draft Principles of Protection of the Environment in Relation to Armed Conflict

In developing the topic, the Commission adopted the outcome format of draft principles. Next, the Commission, under the leadership of the Special Rapporteur, structured the work along temporal lines, by distinguishing three stages of armed conflict: before armed conflict, during armed conflict, and after armed conflict, including times of occupation. The final draft principles, as adopted, also includes a preamble.[45]

The scope of the draft principles is defined in Principle 1 as applying to the protection of the environment before, during or after an armed conflict, including in situations of occupation. Principle 3 requires States pursuant to their obligations under international law to take the effective legislative, administrative, judicial and other measures to enhance the protection of the environment in relation to armed conflicts. However, the Principle 3 goes beyond simply application of existing obligations under international law but also exhorts for States to 'take further measures, as appropriate, to enhance the protection of the environment in relation to armed conflicts.'

The draft principles, as adopted, have included modern aspects of international environmental law. For example, under Principle 4 States

45 ILC, *Draft Principles on Protection of the Environment in Relation to Armed Conflicts,* in Report of the International Law Commission, UN Doc A/77/10 (2022); see also *Yearbook of the International Law Commission*, vol II, Part Two (2022).

should designate protected areas. The interests of indigenous peoples are also addressed in Principle 5. The draft principles also include peace operations in Principle 6. The obligation to prevent, mitigate and remediate harm to the environment in areas where persons displaced by armed conflict is found in Principle 8. Importantly, Principle 9 recognizes the responsibility of States for an internationally wrongful in relation to an armed conflict that causes damage to the environment including an obligation to make full reparation for such damage, including damage to the environment in and of itself. As explained in the commentaries, in addition to be consistent with prior work of the Commission, it also reflects the judgment of the International Court of Justice in the *Certain Activities (Costa Rica v. Nicaragua)* case, in which the Court found that 'it is consistent with the principles of international law governing the consequences of internationally wrongful acts, including the principle of full reparation, to hold that compensation is due for damage caused to the environment, in and of itself'.[46]

Other innovative and important draft principles developed include addressing the duty of private enterprises. Principle 10 exhorts States to take appropriate measures aimed at ensuring that business enterprises operating in or from their territories, or territories under their jurisdiction, exercise due diligence with respect to the protection of the environment, including in relation to human health, when acting in an area affected by an armed conflict. Such measures include those aimed at ensuring that natural resources are purchased or otherwise obtained in an environmentally sustainable manner. Moreover, principle 11 actually requires that States should take appropriate measures aimed at ensuring that business enterprises operating in or from their territories, or territories under their jurisdiction, can be held liable for harm caused by them to the environment, including in relation to human health, in an area affected by an armed conflict.

Business enterprises, such as corporations, can have a major impact on what happens in some of these conflict ridden areas as they exploit natural

46 ILC, *Draft Principles on Protection of the Environment in Relation to Armed Conflicts, with Commentaries, in Report of the International Law Commission*, UN Doc A/77/10 (2022) para 7; *Yearbook of the International Law Commission*, vol II, Part Two (2022), citing *Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v Nicaragua) (Compensation Judgment)* [2018] ICJ Rep 15, 28, para 41; see also *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda) (Reparations)* [2022] ICJ Rep para 348.

resources, including violations of human rights. The draft principles provide business enterprises have a due diligence obligation to make sure that they are not engaging in operations directly or operations under their control that is going to have an adverse impact on protecting the environment and also human health. This runs across the entire supply chain of natural resources being exploited in conflict zones. A notable example is the history of blood diamonds from conflict-ridden areas of Africa. There must be a process in place to be sure that the natural resources are obtained in environmentally sustainable manner. The commentary explains that 'to the extent that a business enterprise is engaged in illegal exploitation of natural resources that amounts to pillage, the law of armed conflict provides a basis for preventing and punishing such acts'.[47]

Another important innovative contribution was Principle 12 that includes a Martens Clause, (found in the Hague Convention (II) with Respect to the Laws and Customs of War on Land, in the Geneva Conventions, and in Additional Protocol I to the Geneva Conventions) for the environment. This was debated quite a bit in the Commission as to whether it would be appropriate or not.[48] In IHL law, the Martens Clause provides that if there's a gap in the existing legal framework, this should mean that the laws of international humanitarian law are not applicable. It is based on the notion of the 'principles of humanity' law of course, the public conscience. Consensus was reached and a Marten Clause was included to apply for protection of the environment during armed conflict. As stated in the statement of the Chair of the Drafting Committee, 'The Drafting Committee concluded that retaining the expression "the principles of humanity" was appropriate to preserve the integrity of the text of the original Martens Clause and to demonstrate the intrinsic link between the survival of people and the state of the environment in which they live'.[49]

Principle 16 addresses the prohibition of pillage. The prohibition of pillage is prohibited under IHL as covered by Article 47 of the Hague

47 ILC, *Draft Principles on Protection of the Environment in Relation to Armed Conflicts*, with Commentaries, Principle 10, para 9, in Report of the International Law Commission, UN Doc A/77/10 (2022); *Yearbook of the International Law Commission*, vol II, Part Two (2022).

48 International Law Commission, 'Statement of the Drafting Committee Chair', Seventy-first Session (2019) 12–14.

49 *Id.* at 13.

Regulations of 1907 and Article 33 of the Fourth Geneva Convention of 1949 as well as other sources. In the case of the *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)*, the Court specifically found there to be sufficient evidence that Uganda had violated its duty of vigilance by not taking adequate measures to ensure that its military forces did not engage in the looting, plundering, pillage and exploitation of the DRC's natural resources.[50]

Principle 17 on the protection of the environment in relation to armed conflict provides for a prohibition against engaging in military or any other hostile use of environmental modification techniques having widespread, long-lasting or severe effects as the means of destruction, damage or injury to any other State, echoing the ENMOD convention.

Principle 18 specifically provides for the protection of areas against attack that are of environmental importance, as well as areas of cultural importance to be protected against any attack, unless a military objective exists. Such protected zones are required to benefit from any additional agreed protections. This represents principle is innovative and is an advancement where IHL and environmental law are combined. An area of environmental importance reflects international environment under the Convention for Biological Diversity,[51] a convention with near universal membership of States, and also the UNESCO World Heritage Convention.[52] The on exception include to Principle 18 is if there is a military objective.

Lastly, in Part 4 of the Principles on protection of the environment in relation at armed conflict, the Commission adopted another set of important and progressive principles applicable during times of occupation. Accordingly, the occupying power has duties and obligations specifically to respect and protect the environment of the occupied territory in accordance with the applicable international law, to prevent significant harm to the environment of the occupied territory (Principle 19) and also to engage in sustainable use of the resources of the occupied territory (Principle 20). These principles are an interesting combination

50 *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda)* (Judgment) [2005] ICJ Rep 168, para 244.

51 *Convention on Biological Diversity* (adopted 5 June 1992) 1760 UNTS 79.

52 *Convention concerning the Protection of the World Cultural and Natural Heritage* (adopted 16 November 1972) 1037 UNTS 151.

of IHL with modern environmental law obligations including the important principle of the sustainable use of natural resources.

Part Five includes those principles applicable after armed conflict. Notably, Principle 22 specifically applies to the peace process requiring that Parties to an armed conflict should, as part of the peace process, including where appropriate in peace agreements, address matters relating to the restoration and protection of the environment damaged as a result of the conflict. Once again, incorporating modern international environmental law, Principle 23 on the sharing and granting access to information pertaining to the environment, Principle 24 providing that States and international organizations should cooperate with respect to post-armed conflict environmental assessments and remedial measures. Principle 25 addresses the situation of when the source of environmental damage is unidentified, or reparation is unavailable, States and relevant international organizations should take appropriate measures so that the damage does not remain unrepaired or uncompensated, and may consider establishing special compensation funds or providing other forms of relief or assistance; and lastly Principles 26 and 27 apply to remnants of war and remnants of war at sea respectively.

In 2020, the ICRC also adopted the Guidelines on the Protection of Natural Environment and Armed Conflict.[53] The work of the ILC and that of the ICRC are both, and are complementary to each other in the effort to modernize the existing IHL framework on the protection of the environment much needed.

7. Conclusion

In conclusion, protection of the environment as part of IHL was a relatively neglected area as evidenced by the scant reference in existing traditional IHL instruments. Over time, the need for a modern framework of IHL rules for the protection of the environment in relation to armed conflict gained prominence in 1990s after the Kuwait invasion of Iraq resulting in UN General Assembly resolutions. Afterward a study undertaken by UNEP recommended that the International Law Commission should

53 International Committee of the Red Cross, *Guidelines on the Protection of the Natural Environment in Armed Conflict: Rules and Recommendations Relating to the Protection of the Natural Environment Under International Humanitarian Law, with Commentary* (ICRC 2020).

examine the existing international law for protecting the environment during armed conflict and recommend how it can be clarified, codified and expanded to develop. The Commission undertook this work in 2013 and completed its work in after which the General Assembly adopted 27 Principles on the Protection of the Environment in Relation to Armed Conflict covering the periods of armed conflict before, during and after, including occupation. The principles combine traditional IHL rules with modern international environmental law. Likewise, in 2020, the ICRC also developed a set of guidelines for the protection of the natural environment in armed conflict.

It is regrettable that the need for an updated IHL framework for protection of the environment continues in light of recent armed conflict between Russia and Ukraine and more recently the Israeli attack on Gaza. The devastation on human life from armed conflict is of foremost concern, but the harmful impact on the environment is also important. The work of the ILC and that of the ICRC constitute important steps to strengthening the protection of the environment before, during, and after, including in situations of occupation.

Bibliography

Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda) (Judgment) [2005] ICJ Rep 168.

Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v Nicaragua) (Compensation) [2018] ICJ Rep 15.

Convention concerning the Protection of the World Cultural and Natural Heritage (adopted 16 November 1972) 1037 UNTS 151.

Convention on Biological Diversity (adopted 5 June 1992) 1760 UNTS 79.

Convention on the Law of the Sea (adopted 10 December 1982) 1833 UNTS 397.

Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be Deemed to be Excessively Injurious or to have Indiscriminate Effects (adopted 10 October 1980) 1342 UNTS 137.

Convention on the Prohibition of Military or any Other Hostile Use of Environmental Modification Techniques (adopted 18 May 1977) 1108 UNTS 151.

Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction (adopted 10 April 1972) 1015 UNTS 163.

Falk RA, 'Environmental Warfare and Ecocide — Facts, Appraisal, and Proposals' (1973) 4 *Bulletin of Peace Proposals* 80.

Heiderscheidt D, 'The Impact of World War One on the Forests and Soils of Europe' (2018) 7 *Ursidae: The Undergraduate Research Journal at the University of Northern Colorado* https://digscholarship.unco.edu/cgi/viewcontent.cgi?article=1175&context=urj accessed 9 February 2026.

International Committee of the Red Cross, *Guidelines on the Protection of the Natural Environment in Armed Conflict: Rules and Recommendations Relating to the Protection of the Natural Environment under International Humanitarian Law, with Commentary* (ICRC 2020).

International Law Commission, *Draft Principles on the Protection of the Environment in Relation to Armed Conflicts, in Report of the International Law Commission,* UN Doc A/77/10 (2022).

International Law Commission, *Draft Principles on the Protection of the Environment in Relation to Armed Conflicts, with Commentaries*, in Report of the International Law Commission, UN Doc A/77/10 (2022).

International Law Commission, 'Programme of Work' <https://legal.un.org/ilc/programme.shtml> accessed 9 February 2026.

International Law Commission, *Report of the International Law Commission*, UN Doc A/68/10 (2013).

International Law Commission, *Report of the International Law Commission*, UN Doc A/72/10 (2017).

International Law Commission, 'Statement of the Drafting Committee Chair', Seventy-first Session (2019).

Jensen D and Bruch C, *Protecting the Environment During Armed Conflict: An Inventory and Analysis of International Law* (UNEP 2009).

Leaning J, 'Environment and Health: Impact of War' (2000) 163 *Canadian Medical Association Journal* 1157.

Linden O, Jerneloev A and Egerup J, T*he Environmental Impacts of the Gulf War 1991* (IIASA, Laxenburg 2004) https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8600662/ accessed 9 February 2026.

National Geographic, 'Red Zone' https://education.nationalgeographic.org/resource/red-zone/ accessed 9 February 2026.

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

Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare (adopted 16 June 1925) 94 LNTS 65.

Rio Declaration on Environment and Development, UN Doc A/CONF.151/26 (Vol I) (1992).

Rome Statute of the International Criminal Court (adopted 17 July 1998) 2187 UNTS 3.

San Remo Manual on International Law Applicable to Armed Conflicts at Sea (12 June 1994) https://ihl-databases.icrc.org/en/ihl-treaties/san-remo-manual-1994 accessed 9 February 2026.

Statute of the International Law Commission, GA Res 174 (II) (21 November 1947), as amended by GA Res 485 (V) (12 December 1950), 984 (X) (3 December 1955), 985 (X) (3 December 1955) and 36/39 (18 November 1981).

Stockholm Declaration on the Human Environment, UN Doc A/CONF.48/14 (1972).

Truong KN and Din KV, 'Agent Orange: Half-Century Effects on the Vietnamese Wildlife Have Been Ignored' (2021) 55(22) *Environmental Science & Technology* 15007.

UN General Assembly Decision 46/417, UN Doc A/46/417 (9 December 1991).

UN General Assembly Resolution 77/10, Protection of the Environment in Relation to Armed Conflict, UN Doc A/RES/77/10 (2022).

Yearbook of the International Law Commission, vol II, pt 2 (2022).

Zierler D, *Invention of Ecocide: Agent Orange, Vietnam, and the Scientists Who Changed the Way We Think About the Environment* (University of Georgia Press 2011).

The Editors would like to express their sincere appreciation to all the authors for their invaluable contributions to the second volume of the Kırımlı Dr. Aziz Bey Collected Courses on International Humanitarian Law. Following the publication of the first volume, it is our great pleasure to present this new collection, which continues the initiative of the Istanbul Center for International Law (ICIL) and Türk Kızılay within the framework of the Kırımlı Dr. Aziz Bey Advanced Summer School and International Humanitarian Law Competition project.

As editors, we remain mindful of the limited availability of comprehensive resources on international humanitarian law (IHL) in Türkiye. It is our hope that this second volume, together with its forthcoming Turkish translation, will further contribute to the growing body of IHL scholarship available in Turkish and English, serving as a valuable resource for students, practitioners, and scholars alike. Building upon the foundations laid by the first volume, this collection continues to address core areas of IHL while reflecting the ongoing commitment of the project to advancing education and scholarship in the field.

We are deeply grateful to **Nilüfer Oral, Daniele Amoroso, Eitan Diamond,** and **Onur Dur** for enriching this volume with their scholarly contributions. We also wish to acknowledge **Jure Vidmar, Riccardo Pavoni, Gökhan Güneysu, F. Şeyda Kahraman, Saba Pipia, Kaan Saner, Mustafa Can Sati, Raphaël Gonçalves Alves, Beyza Arslan** and **Khalil Dewan** for their generous participation as lecturers and/or jury members during the Summer School and Competition.

Our sincere thanks also go to our colleagues at Türk Kızılay- **Alpaslan Durmuş, Selman Salim Kesgin, Hafize Zehra Kavak, Fatma Sena Yasan**, and the many other members of the Türk Kızılay team—whose dedication, commitment, and countless hours of work were instrumental in bringing this project to fruition.

We are equally indebted to **Ceyda Toparlak, Ebru Korkmaz** and **Sara La Vecchia** for their exceptional dedication and outstanding mentorship throughout the competition. Finally, we wish to express our heartfelt gratitude to the President of the Istanbul Center for International Law, **Cihat Gökdemir**, for his unwavering support and encouragement, which have been instrumental in the continued success of this initiative.

We hope that this second volume will further strengthen the Kırımlı Dr. Aziz Bey Collected Courses on International Humanitarian Law as a lasting contribution to international humanitarian law scholarship and education, and that it will continue to serve as a useful resource for future generations of students, practitioners, and researchers.

