INTERNATIONAL LAW STUDIES
Published Since 1895

Know Thy Enemy: The Use of Biometrics in Military Operations and International Humanitarian Law

Marten Zwanenburg

97 INT'L L. STUD. 1404 (2021)

Volume 97

2021

Published by the Stockton Center for International Law

ISSN 2375-2831

Know Thy Enemy: The Use of Biometrics in Military Operations and International Humanitarian Law

Marten Zwanenburg[*]

CONTENTS

* Professor of Military Law, Faculty of Military Sciences, Netherlands Defense Academy. The author would like to thank Paul Oling, Ferry Koks, Bart van den Bosch, and Rogier Bartels for comments on a previous draft of this article. Any remaining errors are the responsibility of the author.

The thoughts and opinions expressed are those of the author and not necessarily those of the U.S. government, the U.S. Department of the Navy, or the U.S. Naval War College.

I. INTRODUCTION

In the summer of 2012, an American platoon was patrolling in the village of Sarenzai, Zhari district, Afghanistan. They stopped in the village and set up a security perimeter when they noticed a man they did not recognize. After stopping and questioning him, they used a device called the Secure Electronic Enrollment Kit (SEEK) to capture the man's biometrics. The SEEK compared the digital fingerprints of the man to stored data. It showed that the man was the second most wanted Taliban in southern Afghanistan.[1]

This example shows why armed forces are increasingly adopting biometrics. It is a way in which persons, including enemy personnel, can be identified quickly and authoritatively—a capability considered important by armed forces. On the modern battlefield, parties to armed conflicts often rely on anonymity. This is particularly the case for terrorist groups. Biometrics can be a powerful tool to deny that anonymity.

Therefore, it is no surprise that biometrics has been used in recent conflicts, such as those in Afghanistan and Iraq. Although the United States military is still the principal military user of the technology, it is increasingly being adopted by other States' armed forces.

Important questions in relation to the use of biometrics by armed forces concern the legal framework that governs such use. During armed conflict, that legal framework consists mainly of international humanitarian law (IHL). The main IHL treaties, the four 1949 Geneva Conventions and two 1977 Additional Protocols, were adopted before this new technology began to be used by armed forces. Does this mean that IHL does not regulate the use of biometrics at all? Is there a need for the drafting of new rules that govern biometrics? Or are the existing rules of IHL sufficiently technologically neutral to allow application to this new technology?

This article will investigate the relationship between IHL and biometrics in an attempt to answer these questions. In order to do so, it will first provide a description of biometrics (Part II) and its use during armed conflict (Part III). This is followed by a discussion of the application of the duty to review new methods and means of warfare in Article 36 of Additional Protocol I[2]

1. ANNIE JACOBSEN, FIRST PLATOON: A STORY OF MODERN WAR IN THE AGE OF IDENTITY DOMINANCE 6–8 (2021).

2. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 36, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I].

(AP I) to biometrics (Part IV). The remainder of the article is structured on the basis of different activities carried out during armed conflict in which biometrics can play a role: targeting (Part V), detention (Part VI), identifying the missing and the dead (Part VII), and enforcement of IHL (Part VIII). The article concludes with a number of final remarks.

This article will not address the issue of protection of biometric data under IHL. That issue is part of a larger debate on the legal regime for protecting data, including, but not limited to, biometric data during armed conflict.[3] As such, it is outside the scope of this article. The article will also not examine the application of other legal regimes, such as international human rights law. These other regimes may also be relevant to the use of biometrics by armed forces, including during armed conflict,[4] but are beyond the scope of this article. In the case of concurrent application of these regimes and IHL, the issue of the interrelationship between the different regimes will become an issue.[5]

II. WHAT IS BIOMETRICS?

"Biometrics" or "biometric recognition" is defined as the "automated recognition of individuals based on their biological and behavioural characteristics."[6] It uses the physical, physiological, or behavioral characteristics of individuals to recognize them.[7] Examples of such characteristics are face topography, hand topography, finger topography, iris structure, vein structure of the hand, voice, gait, and DNA.[8] These characteristics are unique, which makes them very suitable for identifying persons.[9]

---

3. Robin Geiß & Henning Lahmann, *Protection of Data in Armed Conflict*, 97 INTERNATIONAL LAW STUDIES 556 (2021).

4. *See, e.g.*, William H. Boothby, *Biometrics, in* NEW TECHNOLOGIES AND THE LAW IN WAR AND PEACE 392, 406–14 (William H. Boothby ed., 2019).

5. On the interrelationship between IHL and international human rights law generally, see Terry Gill, *Some Thoughts on the Relationship between International Humanitarian Law and International Human Rights Law: A Plea for Mutual Respect and a Common-sense Approach*, 16 YEARBOOK OF INTERNATIONAL HUMANITARIAN LAW 251 (2013).

6. *Information Technology – Vocabulary – Part 37: Biometrics*, ISO/IEC DIS 2382-37, ISO, https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-37:dis:ed-3:v1:en (last visited Oct. 5, 2021) [hereinafter, ISO/IEC DIS 2382-37].

7. For an extensive description of biometrics, see, e.g., NANCY Y. LIU, BIO-PRIVACY: PRIVACY REGULATIONS AND THE CHALLENGE OF BIOMETRICS 29–59 (2012).

8. For additional characteristics, see Boothby, *supra* note 4, at 192.

9. "Recognizing" is used here as a term encompassing verification and identification as defined below.

A "biometric system" is defined as a "system for the purpose of the biometric recognition of individuals based on their behavioural and biological characteristics."[10] It is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database.[11]

A biometric system can be used for verification or identification. Verification refers to validating a person's identity by comparing the captured biometric data with their own biometric template(s) stored in the system database.[12] This is a one-to-one process that answers the question of whether the person concerned is who they claim to be. Identification refers to recognizing an individual by searching the templates of all the users in the database for a match.[13] Identification is a one-to-many comparison to establish an individual's identity without the person concerned having to claim an identity.

A biometric system is an automated process that includes the following steps:

i) Biometric data is collected (sometimes this is also referred to as "capture" or "enrollment") from an individual via a biometric identification device, such as an image scanner for fingerprints or palm vein patterns or a camera to collect facial and iris scans. The data can be captured either directly from the individual or from an object.[14] An example of the latter would be a fingerprint left on an object by the individual.

ii) The system extracts the data from the submitted sample.

iii) It compares the scanned data from those captured for reference.

iv) It matches the submitted sample with templates.

v) It determines or verifies whether the identity of the biometric data holder is authentic.[15]

Biometric technologies, therefore, consist of both hardware and software. A biometric identification device is hardware that collects, reads, and compares biometric data. Biometric data is a sample taken from an individual

10. ISO/IEC DIS 2382-37, *supra* note 6.

11. Anil Jain, Arun Ross & Salil Prabhakar, *An Introduction to Biometric Recognition*, 14 IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY 4, 5 (2004).

12. *Id.*

13. *Id.* at 6.

14. For more detail, see WILLIAM BUHROW, BIOMETRICS IN SUPPORT OF MILITARY OPERATIONS: LESSONS FROM THE BATTLEFIELD 11–14 (2017).

15. Rawlson King, *What are Biometrics?*, BIOMETRIC UPDATE.COM, https://www.biometricupdate.com/201601/what-are-biometrics-2 (last visited Oct. 5, 2021).

that is unique to that individual. Software is used to process gathered biometric data.[16] The software typically works with the hardware to operate the biometric data capture process, extract the data, and undertake comparison, including data matching.[17]

Various biometric characteristics exist and are used in biometric systems. Some of them are mentioned above. Each has its own advantages and drawbacks in general and in the context of military applications.[18] For instance, some characteristics are more permanent than others. Facial features, for example, will change over time as a person grows older, while DNA will remain the same. Another relevant difference between modalities is collectability. Some characteristics are more difficult to collect than others. For example, it is easier to take a picture of someone's face than to take fingerprints of each of their ten fingers. Most biometric systems presently employed in the military domain use a single biometric characteristic to establish identity. There are also systems that integrate the evidence presented by multiple sources of information. These are called multimodal biometric systems because they use more than one characteristic or mode.

Biometric systems vary in how close a person must be for it to be possible to enroll that person biometrically. Traditionally, systems need to be close to the person or even in physical contact with the person so that enrollment is difficult without that person's knowledge. However, technologies that can enroll biometric data remotely are being developed or have already been developed. According to William Buhrow, from the perspective of combat operations, there will be a move towards biometric systems that provide better standoff distance between sensor and target.[19] It was reported in May 2021 that the United States Intelligence Advanced Research Projects Activity, an organization that falls under the Office of the Director of National Intelligence, has a program called Biometric Recognition and Identification at Altitude and Range.[20] This program aims to cultivate new algorithm-based

16. *Id.*

17. *Id.*

18. For a discussion of some relevant differences, see BUHROW, *supra* note 14, at 127–29.

19. *Id.* at 75.

20. Jon Harper, *Shadow Warriors Pursuing Next-gen Surveillance Tech*, NATIONAL DEFENSE (May 7, 2021), https://www.nationaldefensemagazine.org/articles/2021/5/7/shadow-warriors-pursuing-next-gen-surveillance-tech; Zak Doffman, *New Pentagon Laser Identifies Individuals by Their Heartbeat*, FORBES (June 27, 2019), https://www.forbes.com/sites/zakdoffman/2019/06/27/u-s-military-laser-can-identify-people-by-their-heartbeats-mit-reports/?sh=1a8b01bb2dc6.

software systems capable of performing "whole body biometric identification from drones and other platforms."[21] It has also been reported that the Turkish armed forces have unmanned aerial vehicles capable of facial recognition.[22] The drones use facial recognition to detect human targets and can autonomously launch fire-and-forget missiles through the entry of target coordinates, it is reported.[23]

The use of biometrics offers advantages in comparison to recognition systems used previously. In particular, they promise greater accuracy. Biological and behavioral characteristics used in biometric systems are unique to an individual. This means that they allow the recognition of that individual with scientific accuracy.[24] Another advantage has to do with the fact that a biometric system is an automated system. As a result, the process of recognizing an individual can be carried out much faster than if it had to be done manually.

The fact that biometrics promises recognition with scientific accuracy does not mean that such systems are infallible. No biometric technique is completely accurate. As Anil Jain, Arun Ross, and Salil Prabhakar explain:

> Two samples of the same biometric characteristic from the same person (e.g., two impressions of a user's right index finger) are not exactly the same due to imperfect imaging conditions (e.g., sensor noise and dry fingers), changes in the user's physiological or behavioral characteristics (e.g., cuts and bruises on the finger), ambient conditions (e.g., temperature and humidity), and user's interaction with the sensor (e.g., finger placement).[25]

Because no biometric system is perfectly accurate, the response of a biometric matching system typically takes the form of a matching score that quantifies the similarity between the input and the template it is compared with.[26]

An error by a biometric system can take the form of either a false positive or a false negative. A false negative refers to an error when the technology

---

21. Harper, *supra* note 20.

22. Luana Pascu, *Turkey Adds Autonomous Facial Recognition Kamikaze Drones to Military Portfolio*, BIOMETRIC UPDATE.COM (Nov. 11, 2019), https://www.biometricupdate.com/201911/turkey-adds-autonomous-facial-recognition-kamikaze-drones-to-military-portfolio.

23. *Id.*

24. Alison Mitchell, *Distinguishing Friend from Foe: Law and Policy in the Age of Battlefield Biometrics*, 50 CANADIAN YEARBOOK OF INTERNATIONAL LAW 289, 297 (2012).

25. Jain, Ross & Prabhakar, *supra* note 11, at 6.

26. *Id.*

fails to identify a person already enrolled. A false positive transpires when an erroneous match is made, thus misidentifying a person. Some of the limitations of biometric systems using a single mode can be addressed by deploying biometric systems that integrate the evidence presented by multiple sources of information.[27] The use of multimodal systems can mitigate the risk of false positives but cannot exclude them.

Finally, the accuracy of a biometric system also depends on the individual who operates and maintains it.[28] Involuntary or intentional misuse of the system may lead to errors. The system's effectiveness is largely dependent on the quality of enrollment carried out by operators in the field. Poor quality input will decrease the chances of matching data.[29] Despite the fact that a biometric system is an automated system, humans play an important role in the process of comparing biometric data.

III. THE USE OF BIOMETRICS DURING ARMED CONFLICT

Biometrics was initially developed for civilian applications. Use of the technology by armed forces is of more recent date.[30] The U.S. armed forces have been and remain at the forefront of adopting biometrics in military operations. Other armed forces are following suit, and its use will likely become pervasive in the future.[31]

This development is illustrated by the way the North Atlantic Treaty Organization (NATO) has approached biometrics. In recent years, NATO has identified the need to recognize threat actors and reduce their ability to remain anonymous. To this end, biometrics is considered one of the

27. Arun Ross & Anil Jain, *Multimodal Biometrics: An Overview*, PROCEEDINGS OF 12TH EUROPEAN SIGNAL PROCESSING CONFERENCE (EUSIPCO) 1221, 1221 (2004).

28. Robin Feldman, *Considerations on the Emerging Implementation of Biometric Technology*, 25 HASTINGS COMMUNICATIONS AND ENTERTAINMENT LAW JOURNAL 653, 664 (2003).

29. Air Land and Sea Application Center, ATP 2-22.85, MCRP 3-33.1.J, NTTP 3-07.16, AFTTP 3.2.85, CGTTP 3-93.6, Biometrics: Multi-Service Tactics, Techniques, and Procedures for Tactical Employment of Biometrics in Support of Operations25–29 (2014), https://www.marines.mil/Portals/1/MCRP%203-33.1J%20BIOMETRICS%201.pdf.

30. Mitchell, *supra* note 24, at 292.

31. In 2012 Mitchell wrote, "[i]n the space of just over ten years, the use of this tool has gone from being virtually unknown to being an everyday occurrence." *Id.* at 290. This may be overstating the case, at least with respect to the armed forces of less developed States.

organization's top strategic and operational capabilities.[32] Particularly in the last decade, NATO and NATO member States have developed both doctrine and capabilities in relation to biometrics.[33] In 2012, the organization adopted a Concept for Biometrics in Support of Operations, which was followed by other doctrinal publications elaborating on that concept.[34] In 2020, NATO announced its own Automated Biometrics Identification System developed by the NATO Communications and Information Agency.[35]

There are a great number of potential applications of biometrics in the military domain.[36] It can be used throughout the full range of operations, including combat operations, security operations, peace support operations, and peacetime military engagement. Many of the potential applications are relevant to situations of armed conflict in which IHL applies. In general, biometrics allows verification of the identity of personnel and identification of enemy threats with a high degree of confidence.[37] More specifically, possible applications during situations of armed conflict include, but are not limited to:

(i) Verification of the identity of persons who wish to gain access to military facilities: Biometrics can be used to check that persons entering military facilities have the proper authorization to do so.[38] This application has been used by U.S. forces in Iraq, for example.[39]

(ii) Identification of persons applying for posts requiring security clearances: Biometrics can assist in identifying persons that will, for example, be working closely with friendly forces. One instance of this application was its

32. Mark Lunan, *New Doctrinal Concepts: Biometrics*, 33 THE THREE SWORDS MAGAZINE 37, 38 (2018), https://www.jwc.nato.int/images/stories/threeswords/Biometrics_2018.pdf.

33. *Id.*

34. *Id.*

35. Chris Burt, *NATO Announces In-house Biometrics System for Secure Data-sharing,* BIOMETRIC UPDATE.COM (Nov. 18, 2020), https://www.biometricupdate.com/202011/nato-launches-in-house-biometrics-system-for-secure-data-sharing.

36. *See, e.g.*, BUHROW, *supra* note 14, at 41–68.

37. Mitchell, *supra* note 24, at 295–96.

38. Boothby, *supra* note 4, at 396.

39. Noah Shachtman, *Iraq's Biometric Database Could Become "Hit List": Army*, WIRED (Aug. 15, 2007), https://www.wired.com/2007/08/also-two-thirds/; Joshua Steinhauer, *US Biometric and Identity Intelligence Programme, Part 1: How the American Department of Defense Overcame Anonymity on the Battlefield*, KEESINGS (June 1, 2014) https://platform.keesingtechnologies.com/us-biometric-and-identity-intelligence-programme-4/.

use by U.S. armed forces in Afghanistan.[40] Another example is the use of biometrics by U.S. armed forces to vet local drivers who carry out the sustainment of U.S. forces in Syria.[41]

(iii) Identifying persons responsible for the manufacture, transport, and placing of improvised explosive devices (IEDs) and other material used by the enemy: Biometrics played an important role in countering IEDs by U.S. and other forces in Afghanistan and Iraq.[42] Whether detonated or not, when an IED is discovered, it can be examined for fingerprints or DNA (latent biometric traces). If a fingerprint or DNA is found, it can be scanned, stored, and compared with fingerprints or DNA in a database, which may lead to identifying a person involved in manufacturing, transporting, or placing the IED, and possibly the network of which they form part.[43] The recent development of so-called "rapid DNA" promises to further stimulate this military application of biometrics. Rapid DNA technology is described as making it possible "to extract the identifying component within human DNA from all kinds of materials in less than two hours, for example from saliva or blood, but also from cigarette ends, hairs, skin epithelium and other trace materials left behind on [objects]."[44]

(iv) Identifying an individual in the context of targeting: Biometrics can contribute to identifying persons for the purpose of targeting during various phases of the targeting process. It is a particularly reliable way to identify a target.

(v) Identifying persons upon capture and during the detention process: Biometrics can help identify who has been captured and ensure the right

40. Department of Defense Biometrics Task Force, *Biometrics on the Ground and in the DOD*, U.S. ARMY (June 1, 2009), https://www.army.mil/article/21940/biometrics_on_the_ground_and_in_the_dod.

41. Elizabeth Rogers, *Soldiers Use Biometrics to Vet Drivers Sustaining Syrian Logistics Ops*, U.S. ARMY (Feb. 18, 2021), https://www.army.mil/article/243454/soldiers_use_biometrics_to_vet_drivers_sustaining_syrian_logistics_ops.

42. *See, e.g.*, David F. Eisler, *Counter-IED Strategy in Modern War*, MILITARY REVIEW, Jan.-Feb. 2012, at 9, https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/militaryreview_20120229_art006.pdf.

43. *See, e.g.*, NATO, AJP-3.15 (A), Allied Joint Doctrine for Countering – Improvised Explosive Devices (2011), https://www.dtra.mil/Portals/61/Documents/Missions/NATO%20AJP-3.15(A)%20ALLIED%20C-IED%20MAR%2011.pdf?Ver=2017-03-10-134619-480.

44. Paul Oling, Martijn van Latum & Jasmijn Motshagen, *Rapid-DNA Denies Anonymity: It Takes a Network to Take Down a Network*, http://oling.org/APA_Rapid-DNA_ENG.pdf (last visited Oct. 5, 2021).

person is detained with a high degree of certainty.[45] It can help ensure an up-to-date and complete account of detainees being held. This is why it is increasingly being used for this purpose by armed forces. Doctrine for U.S. armed forces on detainee operations states that "biometric samples and associated data will be collected and recorded on each detainee captured and detained by the Armed Forces of the United States."[46]

(vi) Identifying dead persons who fall into the hands of a party to an armed conflict: When a person dies, there is a limited time during which their biometric data can be enrolled. For example, it has been reported that iris and fingerprint biometric data can be obtained for up to four days postmortem in warmer seasons and fifty or more days in the winter.[47] This means that the individual's biometric characteristics can be used to identify them during that period. Being able to identify dead persons is of importance to parties to an armed conflict, *inter alia*, because of obligations under IHL or because of operational requirements.[48] An example of the latter is the use of DNA analysis and biometrics by the U.S. special forces that killed Osama bin Laden to verify his identity.[49] Similarly, after Abu Bakr al-Baghdadi was killed in October 2019, a DNA sample was taken from his remains. Rapid analysis resulted in a match with a sample taken from al-Baghdadi at a detention center in 2004.[50]

IV. THE DUTY TO REVIEW NEW WEAPONS

Under IHL, States have an obligation to review new weapons before they are employed. Article 36 AP I provides,

---

45. BUHROW, *supra* note 14, at 58–61.

46. Chairman, Joint Chiefs of Staff, JP 3-63, Detainee Operations III-5 (2014), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_63.pdf [hereinafter JP 3-63].

47. Kelly Sauerwein, Tiffany Saul, Dawnie Steadman & Chris Boehnen, *The Effect of Decomposition on the Efficacy of Biometrics for Positive Identification*, 62 JOURNAL OF FORENSIC SCIENCES 1599 (2016).

48. For discussion of legal obligations in this regard, see *infra* Part VII.

49. Madison Park & Sabriya Rice, *How Did the U.S. Confirm the Body Was bin Laden's?* CNN (May 3, 2011), http://edition.cnn.com/2011/HEALTH/05/02/bin.laden.body.id/index.html.

50. Jim Garamone, *Central Command Chief Gives Details on Baghdadi Raid*, U.S. DEPARTMENT OF DEFENSE (Oct. 30, 2019), https://www.defense.gov/Explore/News/Article/Article/2003960/central-command-chief-gives-details-on-baghdadi-raid/.

> 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.[51]

It is controversial whether this obligation or a similar obligation also applies as a rule of customary international law. It is notable that the International Committee of the Red Cross's (ICRC) customary law study[52] does not contain a rule on weapons reviews. But the guide that the ICRC has drawn up for the implementation of Article 36 states that "[t]he requirement that the legality of all new weapons, means and methods of warfare be systematically assessed is arguably one that applies to all States, regardless of whether or not they are party to Additional Protocol I."[53] According to the guide, this flows logically from the truism that States are prohibited from using illegal weapons and means and methods of warfare or from using weapons and means and methods of warfare in an illegal manner.[54] The view that the obligation is part of customary IHL also finds support among some commentators.[55] Others are more uncertain or conclude that there is no such obligation under customary IHL.[56]

---

51. Additional Protocol I, *supra* note 2, art. 36.

52. 1 CUSTOMARY INTERNATIONAL HUMANITARIAN LAW (Jean-Marie Henckaerts & Louise Doswald-Beck eds., 2005) [hereinafter ICRC CUSTOMARY LAW STUDY].

53. International Committee of the Red Cross, *A Guide to the Legal Review of New Weapons, Methods and Means of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977*, 88 INTERNATIONAL REVIEW OF THE RED CROSS 931, 933 (2006).

54. *Id.*

55. *See, e.g.*, Chairperson of the Informal Meeting of Experts, Report of the 2016 Informal Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS): Advanced Version ¶ 50, https://docs-library.unoda.org/Convention_on_Certain_Conventional_ Weapons_-_Informal_Meeting_of_Experts_(2016)/ReportLAWS_2016_AdvancedVersion.pdf (last visited Oct. 5, 2021) (noting that several delegations found that weapons reviews are an obligation under customary law); *see also* Michael N. Schmitt, *Foreword* to CYBERWAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS, at v–vi (Jens David Ohlin, Kevin Govern & Claire Finkelstein eds., 2015) ("This provision [Article 36] generally reflects customary law, and thus binds all states irrespective of party status."); Jean-Marie Henckaerts, *The Development of International Humanitarian Law*, *in* THE LEGITIMATE USE OF MILITARY FORCE 117, 128 (Howard M. Hensel ed., 2008).

56. *See, e.g.*, Natalia Jevglevskaja, *Weapons Review Obligation under Customary International Law*, 94 INTERNATIONAL LAW STUDIES 186, 220 (2018) ("the weapons review obligation under Article 36 has not crystallized into customary law").

The duty to review in Article 36 AP I, and a similar obligation under customary law to the extent that it exists, raises the question of whether biometric technology qualifies as a "weapon, means or method." If the answer to that question is in the affirmative, then the question of whether it is new must be answered, in which case it is subject to the obligation to review.

IHL instruments do not contain a definition of "weapon" or "means or method of warfare." Weapon has been defined elsewhere as "a means of warfare used in combat operations, including a gun, missile, bomb or other munitions, that is capable of causing either (i) injury to, or death, of persons; or (ii) damage to, or destruction of, objects."[57]

Means of warfare have been described as comprising weapons, weapon systems, or platforms employed for the purposes of attack, and methods of warfare as activities designed adversely to affect the enemy's military operations or military capacity.[58] Method of warfare has also been described as referring to tactics, techniques, and procedures by which hostilities are conducted,[59] or as referring to any particular manner of using weapons or of otherwise conducting hostilities, irrespective of permissibility or appropriateness, and ranging from the use of emblems, flags, uniforms, and weapons or other equipment to the choice of targets for attack.[60]

Taking these definitions as a starting point, it appears that biometrics is not a weapon or other means of warfare. Biometrics in itself is not capable of causing injury, death, damage, or destruction. Biometrics is also not a weapons system or platform and is not employed for the purposes of attack as a means in itself but only in support of attacks by other means. Arguably, biometrics also does not constitute a method of warfare. It is not a manner of using a weapon or otherwise conducting hostilities, although its use can, if applied in particular ways, support the use of weapons. This conclusion is supported by the fact that, as far as the author is aware, no State has conducted legal reviews of biometrics based on Article 36 of AP I. However,

57. PROGRAM ON HUMANITARIAN POLICY AND CONFLICT RESEARCH AT HARVARD UNIVERSITY, MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE ¶ 1(ff) (2009).

58. Bill Boothby, *How Will Weapons Reviews Address the Challenges Posed by New Technologies*, 52 MILITARY LAW AND THE LAW OF WAR REVIEW 37, 40 (2013).

59. Michael. N. Schmitt, *Autonomous Weapon Systems and International Humanitarian Law: A Reply to the Critics*, 4 HARVARD NATIONAL SECURITY JOURNAL 1, 27 (2013).

60. Gloria Gaggioli & Nils Melzer, *Methods of Warfare, in* OXFORD GUIDE TO INTERNATIONAL HUMANITARIAN LAW 235, 237 (Ben Saul & Dapo Akande eds., 2020).

new weapons or methods of warfare that are enhanced by biometrics would require a legal review.[61]

V. TARGETING

As became clear in Part III, biometrics can be used to support targeting decisions.[62] Targeting involving the use of biometrics must conform to the rules applicable to the conduct of hostilities. Those rules notably include the principles of distinction and precautions.[63]

The principle of distinction requires that a distinction be made between civilians on the one hand and combatants on the other hand. Civilians may not be the object of an attack, except civilians who directly participate in hostilities. In case of doubt as to whether a person is a civilian, that person must be considered a civilian.[64] Not every level of doubt concerning the status of a person precludes attack. The degree of doubt must be at a level that would cause a reasonable attacker in the same or similar circumstances to question the status of the person concerned.[65]

The use of biometrics may facilitate observance of the principle of distinction.[66] The technology cannot identify the status of persons under IHL as such, but it does contribute to confirming the identity of persons. Indirectly, this may contribute to establishing the status of that person under IHL. For instance, this would be the case if a person's identity is established through the use of remote biometrics and there is information that that particular person is a commander of an organized armed group. An example would be the use of voice recognition to identify a person remotely, where the person identified is known to be an enemy commander.[67]

---

61. Boothby, *supra* note 4, at 400.

62. *Id.* at 396.

63. Biometrics appears less directly relevant to the application of the principle of proportionality, which is why that principle is not discussed here.

64. Additional Protocol I, *supra* note 2, art. 50(1).

65. Michael N. Schmitt & Eric Widmar, *The Law of Targeting, in* TARGETING: THE CHALLENGES OF MODERN WARFARE 121, 129 (Paul Ducheine, Michael N. Schmitt & Frans Osinga eds., 2016).

66. Mitchell, *supra* note 24, at 305.

67. Voice recognition has been reportedly used in this way. *See* Matthew Weaver, *Search for UK Jihadi in ISIS Video to Use Voice and Vein Recognition Software*, THE GUARDIAN (Jan. 4, 2016), https://www.theguardian.com/world/2016/jan/04/isis-video-uk-jihadi-voice-vein-recognition-software.

In practice, biometrics is only useful in cases in which persons who are likely to be targeted have previously been enrolled. In such cases, there is a realistic possibility of a match, and thus of identifying the individual through the use of biometrics. At the moment, this means that this will be an option only in limited cases and for a limited number of armed forces.

When using biometrics to support targeting, it is important to remember that the technology is not infallible. In addition, characteristics that could typically be used for remote use, such as facial recognition and gait, are reported to be relatively indistinctive.[68] Therefore, reliance on this technology alone to ensure respect for the principle of distinction may not be sufficient. The less reliable the use of technology under the circumstances concerned and the less certain that the identification is accurate means it is less likely that the threshold of doubt in Article 50 of AP I will be overcome.

The principle of precautions requires that constant care shall be taken to spare the civilian population, civilians, and civilian objects.[69] Article 57 of AP I contains a number of specific measures that must be taken to this end. The first is the obligation for those who plan or decide upon an attack to do everything feasible to verify that the objective to be attacked is not a civilian or civilian object. This obligation is closely linked to the principle of distinction.

The word "feasible" is not defined in AP I but is generally understood to mean that which is practicable or practically possible, taking into account all circumstances prevailing at the time, including humanitarian and military considerations.[70] What is practicable or practically possible will have to be determined on a case-by-case basis. Many different circumstances may be relevant, including the means available to the attacker, whether those means are required elsewhere, the importance of the target, the urgency of the situation, and the characteristics of the target. The factors that are relevant will differ from attack to attack. In the case of biometrics, factors that might be relevant include whether the armed forces doing the targeting have a standoff biometrics capability available in theater, whether the capability is more urgently needed elsewhere, how quickly the system can be used in relation to how fleeting the targeting opportunity is, and how accurate the system is under the conditions at the time, such as dust, fog, heat, etc.

A commander, in deciding whether to attack a particular objective, will have to take into account the information available to them at the time.

68. Jain, Ross & Prabhakar, *supra* note 11, at 9.

69. Additional Protocol I, *supra* note 2, art. 57(1).

70. IAN HENDERSON, THE CONTEMPORARY LAW OF TARGETING 161 (2009).

However, doing everything reasonably feasible must be understood to also require making a reasonable effort to discover pertinent information.[71] This has been understood to mean that a commander is required to take all practicable steps to obtain the information necessary to make a good-faith assessment.[72]

According to William Boothby, doing everything feasible would definitely include obtaining all the reasonably available biometric data in order to verify that the intended human objective is, in fact, a lawful target.[73] This, of course, presupposes that the armed forces doing the targeting have already undertaken biometric enrollment of persons in the area of operations. Without enrollment, obtaining biometric data of the intended target would be of no use because it could not be compared to other data. It also presupposes that the armed forces concerned are able to capture biometric data from a distance. It appears that such technology is already being put into service. Nevertheless, it is likely that at present there are few States, let alone organized armed groups, that possess such a capability. If they do, however, depending on the circumstances, the principle of precaution may require them to use this capability.

Boothby also states that doing everything feasible would likely include taking reasonably available steps to seek to verify that the sources of biometric identification are reliable, that any associated equipment is working properly, and, if it can be done reasonably easily, checking that the biometric test results that are being used to inform targeting decisions have not been corrupted by, for instance, malfunction, interference, or spoofing.[74]

VI. CAPTURE, DETENTION, AND PROSECUTION

When a party to an armed conflict captures a person, that party will want to know who it has captured. If that party goes on to detain the person after capture, it will be all the more important for it to know who it is holding. Apart from practical considerations, the Geneva Conventions contain requirements concerning the registration of persons who have been taken prisoner of war (POW) or interned as a civilian. Article 122 of the Geneva Convention Relative to the Treatment of Prisoners of War (GC III) requires a party to an international armed conflict (IAC) to establish an Information

71. *Id.* at 163.
72. *Id.* at 165.
73. Boothby, *supra* note 4, at 400.
74. *Id.*

Bureau for Prisoners of War.[75] It must provide this bureau with certain information concerning the POW, as set out in paragraphs 4–6 of the Article. Article 136 of the Geneva Convention Relative to the Protection of Civilian Persons in Time of War (GC IV) also contains an obligation to establish an information bureau, which is responsible for receiving and transmitting information in respect of protected persons in the power of that party.[76] Article 138 provides that the information received by the national bureau shall be of such a character as to make it possible to identify the protected person exactly.[77] It provides a non-exhaustive list of types of information that must be provided, including surname, first names, place and date of birth, nationality, last residence, and distinguishing characteristics. The rationale behind these specific requirements is to ensure that no one goes missing or is forcibly disappeared.

With regard to non-international armed conflicts (NIACs), the ICRC's customary law study states that it is a rule of customary IHL in both IACs and NIACs that the personal details of persons deprived of their liberty must be recorded.[78]

Although it is obvious that collecting biometric data may contribute to the purpose underlying these rules, these rules do not require such collection. The updated ICRC *Commentar*y to GC III states that "Article 122 does not provide a basis to collect biological samples and the resulting DNA profiles from all prisoners of war; there must be a specific purpose for doing so."[79] At the same time, the rules discussed above do not expressly prohibit the collection of biometric data from persons who have been captured.

This raises the question of whether there are IHL provisions that do prohibit such collection.[80] Two articles from the Geneva Conventions, in particular, merit further discussion in this regard.

Article 17 of GC III provides that every POW, when questioned on the subject, is bound to give only his surname, first names, rank, date of birth, and army, regimental, personal, or serial number, or equivalent

---

75. Convention (III) Relative to the Treatment of Prisoners of War art. 122, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter Geneva Convention III].

76. Convention (IV) Relative to the Protection of Civilian Persons in Time of War art. 136, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287 [hereinafter Geneva Convention IV].

77. *Id.* art. 138.

78. ICRC CUSTOMARY LAW STUDY, *supra* note 52, at 439.

79. INTERNATIONAL COMMITTEE OF THE RED CROSS, COMMENTARY ON THE THIRD GENEVA CONVENTION: CONVENTION (III) RELATIVE TO THE TREATMENT OF PRISONERS OF WAR ¶ 4795 (2020) [hereinafter GC III 2020 COMMENTARY].

80. *See also* Mitchell, *supra* note 24, at 305–10.

information.[81] The Article continues by stating that if a POW "willfully infringes this rule," the only possible sanction is a restriction of the privileges accorded to his rank or status.[82] This means that other sanctions are not allowed. One possible view would be that compelling the POW to give information in the form of his biometric characteristics would be a sanction that is not allowed under Article 17. The updated *Commentary* to GC III can be read as supporting this view. The commentary to Article 17 only mentions the possibility of using biometrics in connection with the fifth paragraph of the Article.[83] That paragraph provides that the identity of POWs who, "owing to their physical or mental condition, are unable to state their identity . . . shall be established by all possible means."[84] This suggests biometrics may be used in the case of that particular category of POWs, but not when POWs are able to provide information concerning their identity but decline to do so. Such a view also seems to find support in the updated ICRC commentary to Article 16 of the Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in the Armed Forces in the Field (GC I), which will be discussed in more detail in Part VII below. For present purposes, it suffices to note that it deals with recording and forwarding of information on each wounded, sick, or dead person of the adversary falling into the hands of an opposing belligerent. The Article does not contain an exhaustive list of information that may be recorded, and, in principle, biometric data is therefore not excluded. The updated *Commentary* to GC I, however, states in respect specifically of DNA samples that these "may not be taken without the person's consent, unless there is a legal justification, such as in the case of a criminal investigation, or to identify remains."[85] The *Commentary* does not explain why this is the case, but it may be that the drafters considered that there was a link with Article 17 of GC III. After all, wounded or sick members of the armed forces who fall into the hands of the enemy are, in principle, POWs. It must be remembered, however, that the taking of a DNA sample requires taking body material, whether directly from the individual concerned or something that the person left behind. Other

81. Geneva Convention III, *supra* note 75, art. 17.

82. *Id.*

83. GC III 2020 COMMENTARY, *supra* note 79, ¶ 1833.

84. Geneva Convention III, *supra* note 75, art. 17.

85. INTERNATIONAL COMMITTEE OF THE RED CROSS, COMMENTARY ON THE FIRST GENEVA CONVENTION: CONVENTION (I) FOR THE AMELIORATION OF THE CONDITION OF THE WOUNDED AND SICK IN THE ARMED FORCES IN THE FIELD ¶ 1584 (2016) [hereinafter 2016 GC I COMMENTARY].

biometric modalities, such as scanning the iris or voice recognition, do not require taking actual material. As a result, it can be argued that capturing such biometrics is less invasive than taking DNA. Such a view seems to be supported by the commentary to Article 16 of GC I, which states that "an individual may be fingerprinted or photographed" without making any reference to the consent of the individual concerned.[86]

Another view on the meaning of Article 17 of GC III is also possible. It can be argued that taking biometric data from a POW does not constitute a sanction. Under this view, the purpose of taking biometric data is not to punish a POW, but to make it possible to identify them through alternative means rather than having the POW provide the information. In this sense, the involuntary taking of biometric data would not constitute exposure to "unpleasant or disadvantageous treatment" in the sense of Article 17's fourth paragraph.[87] This would, in any case, apply to the capturing of biometric data in so far as it is done without physically restraining the POW or forcing him to adopt a certain position. As was discussed in Part II, there are possibilities for doing so. Even with respect to the capturing of biometric data while physically restraining the POW or forcing them to adopt a certain position, it can be argued that identification of the POW using such alternative means contributes to the objective underlying the obligation to register a POW: to ensure that no one goes missing or is forcibly disappeared. Thus, Article 17 should not be read as prohibiting this.

Article 31 of GC IV states that "No physical or moral coercion shall be exercised against protected persons, in particular to obtain information from them or from third parties."[88] One interpretation of this rule would be that it prohibits compelling civilians to be biometrically enrolled. Under this view, taking their biometric data against their will would constitute coercion, and any biometric data obtained would constitute "information from them" in the sense of Article 31.[89] In this case, however, another interpretation is possible. As the ICRC *Commentary* to Article 31 explains, the Article needs to be considered in light of other provisions of the Convention:

> It will then be seen that there is no question of absolute prohibition, as might be thought at first sight. The prohibition only applies in so far as the other provisions of the Convention do not implicitly or explicitly authorize

86. *Id.*
87. Geneva Convention III, *supra* note 75, art. 17.
88. Geneva Convention IV, *supra* note 76, art. 31.
89. *Id.*

> a resort to coercion. Thus, Article 31 is subject to the unspoken reservation that force is permitted whenever it is necessary to use it in the application of measures taken under the Convention.[90]

The *Commentary* states that one of the exceptions to the general rule in Article 31 is "in regard to everything connected with internment."[91] On this basis, it could be argued that identifying an internee falls within the scope of "everything connected with internment" and that compelling a civilian internee to provide biometric data is allowed.

Another relevant aspect in this regard is that the taking of biometric data can, in principle, be done without any coercion, even if it is involuntary. As was explained in Part II, biometric enrollment does not necessarily require physically restraining the person concerned. If moral coercion is understood to mean psychological pressure to compel the person concerned to cooperate, this is also not necessarily required for biometric enrollment. In principle, this can be done without the cooperation of the person concerned, although this will be more difficult.

Article 27 of GC IV provides that "protected persons are entitled, in all circumstances, to respect for their persons."[92] According to the ICRC *Commentary*, this covers "in particular the right to physical, moral and intellectual integrity."[93] If this right includes a right to privacy, the Article would limit the possibilities for biometric enrollment. However, this does not seem to be how it is interpreted.[94] Separately, Article 27 states that the parties to the conflict "may take such measures of control and security in regard to protected persons as may be necessary as a result of the war." One could argue that such measures may include biometric enrollment. However, this does not affect the obligation to respect the fundamental rights of protected persons, which must be respected "in all circumstances,"[95] as set out in the aforementioned Article.

---

90. OSCAR M. UHLER ET AL., COMMENTARY TO GENEVA CONVENTION IV RELATIVE TO THE PROTECTION OF CIVILIAN PERSONS IN TIME OF WAR 220 (1958) [hereinafter GC IV COMMENTARY].

91. *Id.*

92. Geneva Convention IV, *supra* note 76, art. 27.

93. GC IV COMMENTARY, *supra* note 90, at 201.

94. *See, e.g.*, Asaf Lubin, *The Rights to Privacy and Data Protection under International Humanitarian Law and Human Rights Law*, *in* RESEARCH HANDBOOK ON HUMAN RIGHTS AND HUMANITARIAN LAW: FURTHER REFLECTIONS AND PERSPECTIVES (Robert Kolb, Gloria Gaggioli & Pavle Kilibarda eds., forthcoming 2021).

95. Geneva Convention IV, *supra* note 76, art. 27.

There is some evidence in State practice to support the view that Articles 17, 31, and 27 do not prohibit the involuntary taking of biometric data. For example, official United States doctrine on detention states, without making distinctions between categories of detained persons,

> Once the capture of individuals has occurred, the proper identification and classification of those personnel is critical to the overall intelligence and detainee operations effort. Rapid collection of biometrics information from detainees is critical to ensuring their prompt identification, and is a crucial step that must be conducted as soon as possible after detention.[96]

Similarly, the Norwegian *Manual of the Law of Armed Conflict* provides that "Prisoners of war must be identified and registered as soon as possible. In order to determine the identity of prisoners, biometric data may be collected, including fingerprints, DNA, voice samples, iris scans, etc."[97]

It must be stressed that this article only discusses IHL and no other bodies of law. It cannot be excluded that other bodies of law, such as human rights law and data protection law, will continue to apply during an armed conflict and will impose additional restrictions to those imposed by IHL.

VII. THE MISSING AND THE DEAD

The Geneva Conventions contain a number of provisions on the identification of missing and dead persons. Article 16 of GC I and Article 19 of GC II provide that parties to a conflict must record any information which may assist in the identification of each dead person of the adverse Party falling into their hands.[98] GCs III and IV also contain obligations to identify POWs and civilian internees who die.

Article 33 of AP I requires that as soon as circumstances permit, and at the latest the end of active hostilities, each party to the conflict shall search for the persons who have been reported missing by an adverse party.[99] Such

96. JP 3-63, *supra* note 46, at IV-1.

97. CHIEF OF DEFENCE (Norway), MANUAL OF THE LAW OF ARMED CONFLICT 129 (2013), https://usnwc.libguides.com/ld.php?content_id=47416967.

98. Convention (I) for the Amelioration of the Condition of the Wounded and Sick in the Armed Forces in the Field art. 16, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31 [hereinafter Geneva Convention I]; Convention (II) for the Amelioration of the Condition of the Wounded, Sick, and Shipwrecked Members of Armed Forces at Sea art. 19, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85 [hereinafter Geneva Convention II].

99. Additional Protocol I, *supra* note 2, art. 33.

adverse party shall transmit all relevant information concerning such persons in order to facilitate such searches. Article 33(2)(b) requires parties to an armed conflict to facilitate and, if need be, carry out the search for and the recording of information concerning persons referred to in Article 33(1) if they have died as a result of hostilities or occupation outside of a situation of detention.

According to the ICRC's customary law study, it is a rule of customary IHL applicable in both IACs and NIACs that with a view to identification of the dead, each party to the conflict must record all available information prior to disposal of the body.[100]

Biometrics may contribute to the aim of these IHL rules, namely the identification of the person concerned. Some of the articles mentioned above contain lists of information to be recorded. This is the case for Article 16 of GC I, for example, which in its second paragraph includes a list of information that should be recorded if possible. This list does not contain biometric data, which is not surprising considering that this technology was not in use in 1949. This does not mean that biometric data is outside the scope of the Article. The updated ICRC *Commentary* states in this regard that:

> The guiding principle in this area is that as much information as possible that may assist in the identification of the . . . dead person is to be recorded. Accordingly, items or particulars that are not mentioned in the article, such as photographs, fingerprints, body measurements, names and addresses of next of kin, and distinguishing features or markings such as scars or tattoos, may be included in the record.[101]

Biometric data would certainly be of a nature to assist in the identification and must therefore be understood to be included. The *Commentary* suggests that in the case of DNA samples, these may only be taken with the person's consent.[102] However, it then goes on to state that such consent is not required if there is a legal justification "such as in the case of a criminal investigation, or to identify remains."[103] Consequently, the taking of DNA samples to identify remains must be presumed to be permitted. This applies *a fortiori* to those biometric data that can be taken without taking physical

100. ICRC CUSTOMARY LAW STUDY, *supra* note 52, at 417.
101. 2016 GC I COMMENTARY, *supra* note 85, ¶ 1559.
102. *Id.* ¶ 1584.
103. *Id.*

material from the body or even touching it. This is also supported by State practice.

It must be underlined that if biometric data is taken from the dead, this must be done while taking into account IHL provisions on respect for the dead. Common Article 3 of the Geneva Conventions prohibits outrages upon personal dignity, in particular, humiliating and degrading treatment.[104] This prohibition also applies to the dead,[105] an interpretation that has been confirmed in several recent judgments of domestic courts in, *inter alia*, Germany, Finland, and the Netherlands.[106] According to the ICRC's customary law study, the prohibition of mutilating dead bodies is a norm of customary IHL in both IACs and NIACs.[107]

Arguably an example of a violation of this prohibition in the context of the collection of biometric data is provided by an incident involving Australian special forces in Afghanistan in 2013.[108] During the fighting in the southern province of Zabul, four insurgents were killed by these forces. A corporal in the Australian forces then severed a hand of one of the dead fighters with a scalpel. He repeated the process with two other fighters, cutting off their right hands. When questioned, the corporal stated that he had done this as there was time pressure to retrieve the biometric material and return to the helicopters for extraction.[109]

---

104. *See, e.g.*, Geneva Convention I, *supra* note 98, art. 3.

105. Anna Petrig, *The War Dead and Their Gravesites*, 91 INTERNATIONAL REVIEW OF THE RED CROSS 341, 350 (2009) ("Relatives of the deceased falling within the personal scope of application of Common Article 3 could also invoke its guarantees, for instance by claiming that non-respect for their relative's mortal remains constitutes inhuman treatment or, more specifically, an outrage upon their dignity."); *see also* International Criminal Court, Elements of Crimes art. 8(2)(b)(xxi)(1), n.49, Doc. No. ICC-PIDS-LT-03-002/11_Eng (2011), https://www.icc-cpi.int/iccdocs/PIDS/publications/ElementsOfCrimesEng.pdf.

106. Bundesgerichtshof [BGHST] [Federal Court of Justice] July, 27, 2017, Judgment No. 3 Str 57/17 (Ger.); Prosecutor v. Ammar Jebbar-Salman, District Court of Pirkanmaa, Case R 16/1340, Mar. 18, 2016 (Fin.); Rechtbank Den Haag [The Hague District Court], Case No. 09/748003-18V, July 23, 2019, https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2019:10647 (Neth.).

107. ICRC CUSTOMARY LAW STUDY, *supra* note 52, at 409 (Rule 113).

108. *Australian Soldier Allegedly Cut Off Hands of Dead Taliban Fighters*, THE GUARDIAN (Oct. 29, 2014), https://www.theguardian.com/world/2014/oct/29/australian-soldier-allegedly-cut-off-hands-of-dead-taliban-fighters.

109. Dan Oakes & Sam Clark, '*What the F*** are you Doing?': Chaos over Severed Hands*, ABC NEWS (July 10, 2017), https://www.abc.net.au/news/2017-07-11/afghan-files-shed-light-on-notorious-severed-hands-case/8496654?Nw=0.

VIII. ENSURING COMPLIANCE WITH IHL

The Geneva Conventions and Additional Protocols provide for a number of compliance mechanisms.[110] Mechanisms that are not part of IHL treaty law also contribute to ensuring compliance. Biometrics potentially has an important role to play in various of these mechanisms.

One important element in ensuring compliance is fact-finding.[111] To ensure compliance with a body of law, fact-finding may require an investigation of the facts. Such an investigation aims to bring to light what actually happened, which in turn makes it possible to determine whether what happened conformed with the law. This is of particular importance in the case of IHL because much of what happens during an armed conflict may initially be obscured by the fog of war.

The Geneva Conventions provide for the establishment of ad hoc fact-finding commissions on the request of a party to the conflict. The relevant provisions allow for parties to have a neutral third State, most likely the Protecting Power, make an inquiry into alleged violations of the Conventions.[112] Additional Protocol I established a standing International Humanitarian Fact-finding Commission (IHFFC).[113] In practice, neither the inquiry procedure provided for in the Geneva Conventions nor the IHFFC has been used by parties to an armed conflict as envisaged. This does not mean that fact-finding into alleged violations of IHL is not undertaken. In recent years, a number of ad hoc commissions of inquiry have been established to investigate compliance with, *inter alia*, IHL. Many of these commissions were created by the U.N. Human Rights Council.[114] Biometric techniques could

---

110. *See, e.g.*, Silja Vöneky*, Implementation and Enforcement of International Humanitarian Law, in* HANDBOOK OF INTERNATIONAL HUMANITARIAN LAW 690 (Dieter Fleck ed., 4th ed. 2021).

111. *See, e.g.*, Michael Bothe, *Fact-finding as a Means of Ensuring Respect for International Humanitarian Law, in* INTERNATIONAL HUMANITARIAN LAW FACING NEW CHALLENGES 249 (Wolff Heintschel von Heinegg & Volker Epping eds., 2007).

112. Geneva Convention I, *supra* note 98, art. 52; Geneva Convention II, *supra* note 98, art. 53; Geneva Convention III, *supra* note 75, art. 132; Geneva Convention IV, *supra* note 76, art. 149.

113. Additional Protocol I, *supra* note 2, art. 90. On the IHFFC, see, *inter alia*, Elzbieta Mikos-Skuza*, The International Humanitarian Fact-Finding Commission: An Awakening Beauty?*, *in* FRIEDEN IN FREIHEIT - PEACE IN LIBERTY - PAIX EN LIBERTÉ: FESTSCHRIFT FÜR MICHAEL BOTHE ZUM 70. GEBURTSTAG 493 (Andres Fischer-Lescano, Hans-Peter Gasser, Thilo Marauhn & Natalino Ronzitti eds., 2008).

114. An example is the Independent Investigative Mechanism for Myanmar, established by the U.N. Human Rights Council in 2017. The mechanism was established on the basis

contribute to fact-finding in armed conflicts, in particular by identifying victims of alleged IHL violations.[115]

Individual criminal responsibility has taken on an increasingly important role in ensuring compliance with IHL. National courts play an essential role in enforcing IHL,[116] both with regard to the conduct of a State's own nationals and in conflicts for which the international community has not created an international court or tribunal or failed to provide the International Criminal Court jurisdiction.[117] The Geneva Conventions and Additional Protocol I require States Parties to criminalize so-called "grave breaches" of the Conventions and the Protocol and to prosecute or extradite persons alleged to have committed such crimes.[118] They must also take measures necessary for the suppression of all acts contrary to the Conventions other than grave breaches. This is understood to mean that States Parties are under an obligation to address such acts, and it is implied that they may take a wide range of measures to do so.[119] One possible measure is to take judicial action.[120] Although treaty law on NIACs contains no provisions on criminal prosecution for war crimes, it is now generally accepted that war crimes can also be committed in NIACs.[121] According to the ICRC's customary law study, it is a rule of customary IHL in both IACs and NIACs that States must investigate war crimes allegedly committed by their nationals or armed forces or on their territory, and, if appropriate, prosecute the suspects.[122] They must also

---

of a resolution of the Council. Human Rights Council Res. 39/2, Situation of Human Rights of Rohingya Muslims and Other Minorities in Myanmar, U.N. Doc. A/HRC/RES/39/2 (Oct. 3, 2018).

115. *See supra* Part VII.

116. Gentian Zyberi, *Enforcement of International Humanitarian Law, in* INTERNATIONAL HUMAN RIGHTS INSTITUTIONS, TRIBUNALS AND COURTS 377 (Gerd Oberleitner ed., 2018).

117. *See, e.g.*, *National Courts Lead the Way in Prosecuting Syrian War Crimes*, AL JAZEERA (Mar. 15, 2021), https://www.aljazeera.com/news/2021/3/15/national-courts-lead-the-way-in-prosecuting-syrian-war-crimes (discussing cases initiated in several European countries against Syrian officials and military members for alleged war crimes).

118. Geneva Convention I, *supra* note 98, art. 49; Geneva Convention II, *supra* note 98, art. 50; Geneva Convention III, *supra* note 75, art. 129; Geneva Convention IV, *supra* note 76, art. 146; Additional Protocol I, *supra* note 2, art. 85.

119. COMMENTARY TO GENEVA CONVENTION I, *supra* note 85, at 1033.

120. *Id.*

121. YORAM DINSTEIN, NON-INTERNATIONAL ARMED CONFLICTS IN INTERNATIONAL LAW 173–204 (2014).

122. ICRC CUSTOMARY LAW STUDY, *supra* note 52, at 607.

investigate other war crimes over which they have jurisdiction and, if appropriate, prosecute the suspects.[123]

In the last decades, a number of international courts and tribunals have been established for the purpose of trying persons accused of international crimes, including war crimes.[124] These include the ad hoc tribunals for the former Yugoslavia and Rwanda, as well as the International Criminal Court.

The initial development of biometrics was closely connected to the criminal justice process. Therefore, it could be expected that the technology also plays a role in the investigation and prosecution of war crimes at the national and international levels. War crimes can be very difficult to prosecute. Biometric data can be an invaluable asset during investigation and trial. It can enable identifying victims, possibly establishing that war crimes were committed. Biometric information can also assist in identifying war crimes suspects and, in some cases, linking them to a particular crime or crime scene. This is not without challenges, however, because in many cases no information is collected at the crime scene. In other cases, the persons being prosecuted were not present at the actual scene of the crime (particularly in leadership cases). It appears that in practice, limited use has so far been made of biometrics in war crimes investigations and prosecutions. Although biometrics are used in an increasing number of domestic criminal systems, there is very little evidence of its use in war crimes cases.[125] There is also little information on the use of biometrics by international courts and tribunals.

There are some notable domestic cases of the use of biometrics, however. Biometrics has played a prominent role in the conviction of Taliban fighters before Afghan courts. Evidence based on biometrics was collected by international forces in Afghanistan and handed over to Afghan authorities for use in criminal prosecution as part of evidence packages.[126] This was particularly the case in the National Security Court at the Justice Center in Parwan (JCIP), an Afghan court supported by foreign advisors.[127] In January

123. *Id.*

124. Zyberi, *supra* note 116, at 393.

125. In contrast to the use of forensic evidence in other circumstances, in particular for the identification of victims. *See, e.g.*, Catherine Fournet, *Forensic Evidence in Atrocity Trials*, 69 JOURNAL OF FORENSIC AND LEGAL MEDICINE 1 (2020).

126. Joop Voetelink, *EvBO: Evidence-Based Operations How to Remove the Bad Guys from the Battlefield*, 26 JOURNAL OF INTERNATIONAL LAW OF PEACE AND ARMED CONFLICT 194, 199 (2013).

127. *See, e.g.*, Arizona Mosley, *Afghan Judiciary Now Using Biometric Forensics*, BIOMETRIC UPDATE.COM (Aug. 20, 2012), https://www.biometricupdate.com/201208/afghan-judiciary-now-using-biometric-forensics.

2014, it was reported that "the use of biometrics in prosecutions at JCIP now plays a prominent role in the convictions of those individuals who have been so matched to criminal offenses."[128] This does not seem to have been the case for courts in Afghanistan more generally, however.[129]

A war crimes case in which biometrics played an important role was that of U.S. Army Lieutenant Clint Lorance. Lorance was tried by court-martial for allegedly ordering his platoon to fire on unarmed villagers in Afghanistan in July 2012, killing two men.[130] Following these deaths, Lorance claimed that he was not able to complete a proper battle damage assessment on the men because other villagers had already taken away their bodies. A member of Lorance's platoon subsequently reported him to military authorities. Lorance was convicted at a general court-martial of second-degree murder and sentenced to nineteen years of confinement. Lorance was pardoned by President Trump in 2019.[131] Biometrics played an important role in obtaining this pardon.[132] Lorance's defense team argued that biometric data established that the Afghan men killed were Taliban bomb makers, not civilians. However, it has been claimed that the data was wrong and did not actually prove this.[133]

The latter example demonstrates that the use of biometrics in the context of criminal investigations and prosecutions, including in war crimes cases, is not a panacea. As discussed in Part II, biometrics as a technology is not infallible. Perhaps more importantly, biometrics is a technology that is used by humans. How accurate findings based on the technology are, is, therefore,

128. David Pendall & Cal Sieg, *Biometric-Enabled Intelligence in Regional Command-East*, 72 JOINT FORCE QUARTERLY, 1st Quarter 2014, at 69, https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-72/Article/577484/biometric-enabled-intelligence-in-regional-command-east/.

129. *Id.*

130. United States v. Lorance, No. 20130679, 2017 WL 2819756, at *1–2 (A. Ct. Crim. App. June 27, 2017), *rev. denied*, 77 M.J. 136 (C.A.A.F. 2017).

131. Jean Galbraith, *Issuing Several Pardons, President Trump Intervenes in Proceedings of U.S. Troops Charged or Convicted of Acts Amounting to War Crimes*, 114 AMERICAN JOURNAL OF INTERNATIONAL LAW 307 (2019).

132. Jim Nash, *Misuse of Biometric System Won Accused U.S. War Criminal a Presidential Pardon—Report*, BIOMETRIC UPDATE.COM (Jan. 18, 2021), https://www.biometricupdate.com/202101/misuse-of-biometric-system-won-accused-u-s-war-criminal-a-presidential-pardon-report.

133. JACOBSEN, *supra* note 1, at 290.

dependent on the use or misuse of the technology by humans. Those humans may make mistakes or may even act in bad faith.[134]

IX. CONCLUSION

Biometrics is being used by armed forces during armed conflict and, given its advantages, is likely to be adopted on an even larger scale in the future. As was discussed in Part III, biometric techniques are relevant to a wide variety of military activities, including activities that are part of armed conflict.[135] These activities range from access control to military facilities to identifying the deceased. IHL contains no rules that expressly regulate the use of biometrics. This is unsurprising since biometrics, as defined in this article, did not exist when the Geneva Conventions and Additional Protocol I were drafted. This article has demonstrated that there are, nevertheless, IHL rules regulating certain activities that are relevant to the use of biometrics. Indeed, it is generally recognized that IHL applies in principle to new technologies developed after the adoption of the IHL rules concerned. In the case of biometrics, this article has shown that IHL rules may require the use of biometrics under certain circumstances and that, in other circumstances, IHL rules may limit the use of biometrics. The article also made clear that the application of certain rules of IHL to biometrics raises questions of interpretation. A case in point is Article 17 of GC III and Article 31 of GC IV, discussed in Part VI. Different interpretations of these articles appear defendable, with important differences in outcome for the permissibility of biometrics.

Such cases raise the question of whether new law is needed to regulate the use of biometrics during armed conflict. It is submitted that it is too early to answer this question in the affirmative. This is because there appears to have been very little discussion among States so far on the application of IHL to biometrics. Such discussion is arguably a necessary step before determining whether new rules are required or whether clarification of the law will suffice. If the outcome of such a discussion is that new rules are required, it can also inform the content of new rules to be proposed. In any event, the statement made in 2012 that States are likely unwilling, at this stage, to create

134. On the human factor in the use of biometrics, see, e.g., Kasey Wertheim, *Human Factors in Large-Scale Biometric Systems: A Study of the Human Factors Related to Errors in Semiautomatic Fingerprint Biometrics*, 4 IEEE SYSTEMS JOURNAL 138 (2010).

135. Boothby, *supra* note 4, at 399.

an international treaty on the collection of battlefield biometrics, let alone biometrics writ large, seems to still apply.[136]

What seems most urgently required at this point in time is for an international debate on a legal framework for the use of biometrics during armed conflict to be initiated. Such a debate would not only focus on IHL but also take into account other relevant fields of international law, notably international human rights law. It appears that in recent years some discussion on the legal framework for the use of biometrics during military operations has already taken place, but this has been only between certain States and limited in scope. The initiative for such a broader discussion could be taken by one or more States or even by the ICRC.

Such discussion could also be part of an exercise to develop best practices for the use of biometrics during armed conflict. The drafting of a document with non-binding "best practices" or guidelines on the use of biometrics has been suggested in the past. Such an effort could be a first step towards creating new international legal norms.[137]

136. Mitchell, *supra* note 24, at 324.
137. *Id.* at 325.